Quantum Information & Computation
ISSN 1533-7146 Volume 25 (2025) pp.488–508

Cerebration Science Publishing

Article

Twin-Field Quantum Network Coding for Multi-Party Key Distribution

Yuchen Liu, Tao Shang * and Keyu Xiong

School of Cyber Science and Technology, Beihang University, Xueyuan Road, Beijing 100191, China; lyuchen@buaa.edu.cn (Y.L.); xky@buaa.edu.cn (K.X.)
* Corresponding author: shangtao@buaa.edu.cn

Received date: 4 July 2025; Accepted date: 29 September 2025; Published online: 11 October 2025

Abstract: Quantum network coding enables multi-party quantum interactions over bottleneck channels. The communication distance is usually constrained by the instability of quantum states. Twin-field quantum key distribution is designed to improve the communication distance, but it can only be applied in point-to-point scenarios. In this paper, we propose a feasible twin-field quantum network coding scheme, which enables multi-party key distribution over long distance in networks with bottleneck channels. Firstly, a butterfly network model is designed for long-distance communication. Then, the coding method at each intermediate node is designed to overcome the limitations of bottleneck channels. Finally, the key rate and decoy-state transmission features are derived to demonstrate the security and efficiency advantages. Compared with the original point-to-point twin-field quantum key distribution protocol, the proposed scheme can distribute a group key among the four end nodes of the butterfly network with only one transmission round. The key rate R and the channel transmittance η still satisfy $R \propto \eta^{1/2}$. Such results will extend the communication distance and provide a foundation for the construction of large-scale quantum networks.

Keywords: quantum network coding; quantum key distribution; twin-field; coherent measurement

1. Introduction

Based on the fundamental principles of quantum physics, quantum communication has achieved a revolutionary breakthrough compared to classical communication. Currently, quantum communication has developed from point-to-point transmission to network architecture. In both quantum and classical networks, bottleneck channels often severely restrict communication efficiency. In 2000, Ahlswede and Cai [1] introduced the concept of classical network coding. It allows data encoding at intermediate nodes to maximize the network throughput through bottlenecks. To solve analogous problems in quantum networks, Hayashi [2] introduced the first quantum network coding (QNC) scheme, XQQ, in 2007. It utilized universal cloning and local unitary operations to simulate the replication and encoding operations of classical network coding. Later, the scheme was further enhanced by incorporating pre-shared entanglement (PE) [3], enabling perfect cross-transmission of two quantum states through a bottleneck channel. Subsequent researches were inspired and started to focus on perfect multi-unicasts. In 2014, Shang et al. [4] proposed a QNC scheme based on controlled teleportation, introducing a controller to manage the decoding process. In 2016, Li et al. [5] utilized 2D and 3D cluster states to achieve quantum multi-unicast over directed acyclic networks. In 2023, Shang et al. [6] proposed a QNC scheme based on quantum steering, relaxing the constraints on quantum entanglement and the security assumptions for intermediate nodes. Same as the classical network coding, QNC is also expected to achieve multicast. The no-cloning theorem prohibits the perfect replication of unknown quantum states, making it impossible to achieve perfect multicast in quantum networks. The first QNC to realize strict multicast was proposed by Shi et al. [7] in 2006. It sends existing clones of a state without cloning it during the transmission. In 2022, Hirota et al. [8] reformulated quantum multicast as an approximation cloning problem and designed a QNC scheme to multicast asymmetric optimal clones of an unknown quantum state. In 2023, Pandey et al. [9] proposed a QNC scheme based on measurement-based quantum computing (MBQC) and addressed the challenges of both multi-unicast and strict multicast across different computational bases. In 2024, Yang et al. [10] introduced quantum multiplexing into QNC, making it possible for several source nodes to send states with different qubit numbers at the same time.

DOI: 10.2478/qic-2025-0027

Current QNC schemes are still confronted with some challenges. Quantum states are highly susceptible to environmental factors. It has emerged as a critical issue to extend the communication distance. Quantum repeaters are commonly used in QNC to overcome the limit of distance. In 2015, Shang et al. [11] designed a QNC scheme based on quantum repeaters, employing local operations and classical communication (LOCC) algorithms for arbitrary entangled states to generate long-distance quantum channels. In 2020, Liu et al. [12] proposed a QNC scheme with the entanglement distribution of separable states and remote state preparation, enabling long-distance cross-transmission of quantum states on a butterfly network with reduced resources. In 2021, Shang et al. [13] transmitted quantum correlations rather than states over a butterfly network. This approach minimized decoherence effects on state selection and improved the communication distance of QNC. In quantum key distribution (QKD), twin-field (TF) structure [14] was designed for long-distance communication. The key rate of TF-QKD scales with the square root of the channel transmittance. If QNC can be combined with TF-QKD, it is possible to realize long-distance multi-party key distribution.

As the most developed quantum technology to date, QKD has been widely implemented. QKD protocols allow legitimate parties to obtain quantum keys with unconditional security in the presence of illegal eavesdroppers. Since the first QKD protocol BB84 was introduced by Bennett and Brassard [15]. In 1984, QKD has undergone various developments and become one of the most widely adopted quantum communication technologies with unparalleled technological maturity. In 1991, Ekert [16] proposed the E91 protocol based on entanglement distribution, which ensures the security of QKD by verifying the violation of Bell's inequality. As QKD protocols have been increasingly deployed, studies have started to focus more on security. In practical QKD systems, it is impossible to maintain ideal environment and device conditions. For instance, non-ideal light sources make the system vulnerable to photon number splitting (PNS) attacks, where eavesdroppers exploit multi-photon emissions to gain information about the key. Non-ideal detectors at the receiver end may also lead to side-channel attacks such as time-shift, Trojan-horse, fake-state, and avalanche-transition attacks [17–19]. Hwang [20] first proposed the concept of decoy states as a countermeasure against PNS attacks. Decoy-state (DS) techniques have since evolved rapidly and have been integrated into a wide range of QKD systems [21,22]. In 2010, Gisin et al. [23] proposed the device-independent (DI) QKD, which enables secure communication over an untrusted network with untrusted devices. Then, Laing et al. [24] introduced the reference-frame-independent (RFI) QKD, mitigating the problem of reference frame misalignment. In 2012, Lo et al. [25] further proposed the measurement device-independent (MDI) QKD. It involves two senders and one untrusted receiver, providing robust resistance against side-channel attacks targeting measurement devices. In systems with detector losses and other experimental imperfections, none of the aforementioned QKD protocols can surpass the secret-key capacity (SKC) bound, the theoretical maximum amount of secret information that can be transmitted through QKD. To overcome this limitation, Lucamarini et al. [14] introduced TF-QKD based on MDI-QKD in 2018. In TF-QKD, two distant nodes independently generate phase-randomized states and subsequently transmit them to an intermediate node for interference. Moreover, TF-QKD can be directly implemented on the existing hardware of MDI-QKD, so it inherently retains the measurement-device-independent security. There are numerous variants of TF-QKD designed for different scenarios. Notable examples include the sending-or-not-sending (SNS) and the phase-matching (PM) protocol [26,27], advancing the practicality and scalability of TF-QKD. The twin-field structure and the coherent measurement at the intermediate node are applied in TF-QKD to improve communication distance, which also reveals a viable pathway to overcome the distance limitation in QNC. QNC typically requires end-to-end transmission of quantum states, making it impossible to surpass the SKC bound even with the assistance of repeaters. If the twin-field structure and coherent measurements were introduced, QNC will be able to support long-distance multi-party interactions in the networks with bottlenecks.

In this paper, we propose a twin-field quantum network coding scheme. The transmission directions in the butterfly network model are changed and coherent measurements are introduced to intermediate nodes, enabling simultaneous quantum key distributions for multiple node pairs with only one transmission round through the bottleneck. Considering the security threats from malicious intermediate nodes, we also derive various decoy-state transmission features for this scheme so that all parties are able to determine whether eavesdroppers or malicious nodes exist. The main contributions of this paper are summarized as follows:

(i) A butterfly network model with centripetal transmission directions on both sides of the bottleneck is designed to support long-distance communication. All four end nodes are designated as senders, transmitting states to the intermediate nodes. Quantum transmission does not need to traverse the entire end-to-end channel, so the communication distance can be increased with a proper coding scheme.

(ii) A twin-field quantum network coding (TF-QNC) scheme for multi-party key distribution is proposed. Beam splitters and coherent measurement operations are implemented at the two intermediate nodes, allowing all communication parties to derive key bits based on the measurement results. The intermediate nodes have only access to the phase difference instead of the absolute phase, so they are incapable of deducing the key bits if they are malicious.

(iii) The key rate and decoy-state transmission features in TF-QNC are derived to demonstrate the performance and security of the scheme. The decoy-state method suggests that eavesdroppers can be detected with a comparison between the actual features and their theoretical values. In the proposed scheme, quantum transmission involves more than one node, and untrusted intermediate nodes act as both signal receivers and measurement units, so the implementation of the decoy-state method is non-trivial.

2. Related Works

2.1. Twin-Field Quantum Key Distribution

TF-QKD [14] was designed based on MDI-QKD to overcome the communication distance limitations of traditional QKD. The phase difference of two signals is obtained at the intermediate node through coherent measurement, so that two remote nodes can deduce key bits without end-to-end transmission of quantum states.

The basic structure of TF-QKD is depicted in Figure 1. Alice and Bob are the legitimate, end nodes, and Charlie is an untrusted intermediate node. Prior to the transmission, Alice and Bob first agree to divide the phase interval $[0, 2\pi)$ into m equally spaced slices. Then, they each select a random phase, respectively, and note down which slice $(\Delta_a, \Delta_{a+1}]$ or $(\Delta_b, \Delta_{b+1}]$ the phase is in, where $a, b \in \mathbb{Z} \cap [0, m)$ and $\Delta_m = \Delta_0$. To deliver information and confuse eavesdroppers, they also have to choose random bit phases α_{Alice}, α_{Bob} and basis phases β_{Alice}, β_{Bob}. Finally, Alice prepares a state with phase $\phi_{Alice} = (\rho_{Alice} + \alpha_{Alice} + \beta_{Alice}) \bmod 2\pi$ and selected intensity μ_{Alice}, while Bob prepares a state with phase $\phi_{Bob} = (\rho_{Bob} + \alpha_{Bob} + \beta_{Bob}) \bmod 2\pi$ and selected intensity μ_{Bob} and sends them both to Charlie. Charlie uses two detectors D_0 and D_1 to measure the phase difference χ between ϕ_{Alice} and ϕ_{Bob} and publish it. The difference is 0 or π. Alice now reveals the intensity μ_{Alice}, basis phase β_{Alice} and slice $(\Delta_a, \Delta_{a+1}]$. According to these data, Bob can determine whether the states match or not. After all rounds are completed, Bob announces the matching rounds and discards the non-matching ones. For the matching rounds, they disclose the bits corresponding to non-signal states, which are then used to detect eavesdropping. To generate key bits, Bob deduces Alice's bit phase of every signal state as $\alpha_{Alice} = |\chi - \alpha_{Bob}|$. The bit corresponding to α_{Alice} will serve as the shared key bit.

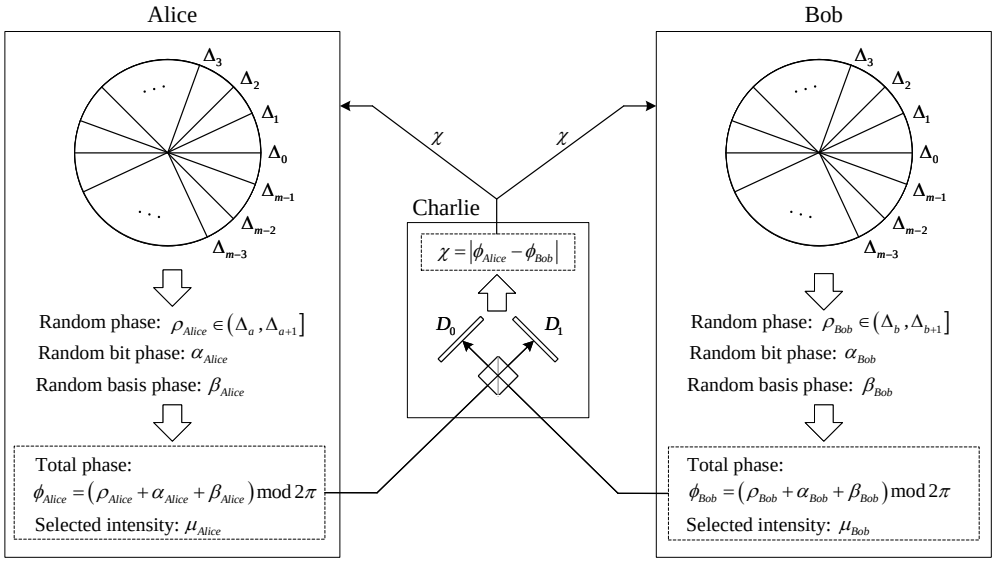

Figure 1. The basic structure of TF-QKD.

According to the analysis of TF-QKD, the key rate can be expressed as

$$R(\mu, L) = \frac{d}{M}\left\{Q_1|_{\mu,\frac{L}{2}}\left[1 - h\left(e_1|_{\mu,\frac{L}{2}}\right)\right] - fQ_{\mu,\frac{L}{2}}h\left(E_{\mu,\frac{L}{2}}\right)\right\}, \tag{1}$$

where μ is the signal intensity and L is the distance between the two end nodes. Q_1 is the single-photon gain. Function $h(\cdot)$ is the binary entropy and e_1 is the single-photon error rate. Q and E are the overall gain and error rate in the transmission, respectively.

2.2. Decoy-State Method

In practical implementations, weak coherent state sources are often employed instead of ideal single-photon sources, which means it is possible to have more than one photon in one pulse. This vulnerability can be exploited by an eavesdropper through a PNS attack. They extract information on key bits by intercepting photons from multi-photon pulses. In the decoy-state method, eavesdropping is detected by the estimation and verification of the decoy-state transmission features. The features must be sensitive to photon numbers, such as the transmission gain Q and error rate E.

We assume that the sender emits a weak coherent state $\left|\sqrt{\mu}e^{i\theta}\right\rangle$ where the photon number follows a Poisson distribution with parameter μ. In other words, the probability that the signal contains n photons is $p_n = e^{-\mu}\mu^n/n!$. The gain Q_μ represents the overall probability that the receiver's detector will respond to the signal after transmission, expressed as

$$Q_\mu = \sum_n p_n Y_n = \sum_n \frac{\mu^n}{e^\mu n!} Y_n, \tag{2}$$

where Y_n denotes the n-photon yield. The error rate E_μ represents the overall probability to have a wrong result in the receiver's detector, expressed as

$$E_\mu = \sum p_n Y_n e_n = \sum_n \frac{\mu^n}{e^\mu n!} Y_n e_n, \tag{3}$$

where e_n denotes the ratio of wrong bits received by the receiver's detector for a signal with n photons.

After transmission, the actual values of Q_μ and E_μ are observed. If they obviously deviate from the theoretical predictions, the transmission is highly likely to be eavesdropped.

3. Twin-Field Quantum Network Coding Scheme

Inspired by the coherent measurement introduced to the intermediate node in TF-QKD to improve communication distance, we design a twin-field quantum network coding scheme to distribute keys for multiple parties through a bottleneck channel. Based on a new butterfly network model with reconfigured transmission directions, we enable intermediate nodes to perform coherent measurement, beam splitting, and coding operations, thereby allowing a single quantum transmission in the bottleneck channel to carry more information.

Firstly, we describe a novel butterfly network model for twin-field transmission scenario. To provide a clear and structured explanation, we divide the proposed scheme into two stages. Then, we introduce the quantum transmission process and the coherent measurement operations performed by the intermediate nodes. Finally, we introduce the coding and classical transmission process after the measurement results are obtained at the intermediate nodes.

3.1. Butterfly Network Model for Twin-Field Transmission

The proposed scheme is based on a butterfly network model depicted in Figure 2. Solid lines denote quantum channels. The bottleneck channel is capable of transmitting one quantum state at a time, and the others are capable of transmitting either one quantum state or one classical bit. Dashed lines denote classical channels. The nodes s_1 to s_4 are the communication parties and are mutually trusted. The nodes n_1 and n_2 are untrusted intermediate nodes. The four communication nodes are distributed over long distance. The distance between node group A and B is even longer than the distance inside each group. To alleviate the pressure of long-distance communication and optimize the use of channel resources, we assume that the classical channels s_1s_3 and s_2s_4 between the two node groups can only be used once, while free classical transmission is allowed within each group.

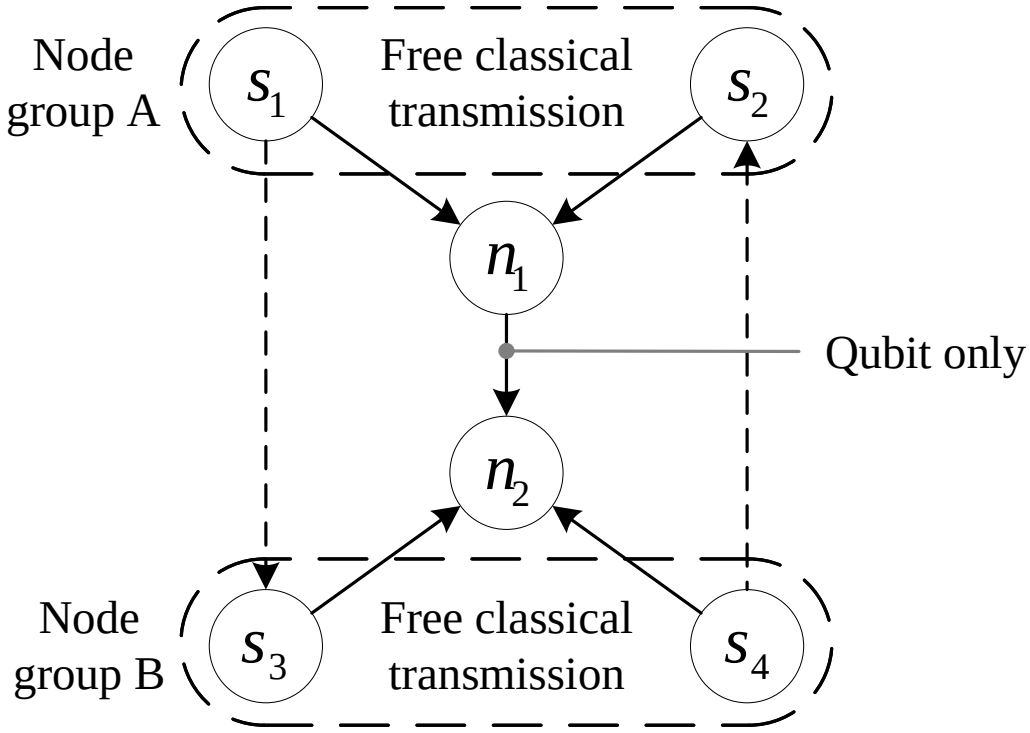

Figure 2. Butterfly network model for twin-field transmission.

We assume that the end nodes s_1 to s_4 expect to securely distribute keys among themselves. The keys between one pair of nodes can be identical or distinct to each other. Considering the distances between the nodes, the distribution of secure keys necessitates the use of TF-QKD. To extend TF-QKD to support long-distance multi-party communication in the new network model, the transmission directions of the traditional butterfly network model are changed, as illustrated by the arrows in Figure 2. The end nodes s_1 to s_4 all serve as the senders of quantum states, and the intermediate nodes n_1 and n_2 serve as the receivers. The current circumstances on both sides of the bottleneck channel are completely symmetric, so we reasonably assume that the quantum transmission in the bottleneck channel is directed from n_1 to n_2. In TF-QKD, classical transmission between source nodes is needed to determine the rounds that match, so at least two interactions, one in each direction, are necessary between the two node groups. For simplicity, we further assume that the classical transmission is directed from s_1 to s_3 and from s_4 to s_2.

Compared to butterfly network models in other schemes, the transmission directions in the proposed model are changed to support longer communication distances. Quantum states are transmitted from the end nodes to the intermediate nodes. Additionally, the bottleneck in the model is a quantum channel, which is more common in current quantum systems. The side channels are only used to transmit auxiliary classical information in round selection.

The TF-QKD protocol is designed to achieve point-to-point key distribution. If we aim to enable communication between any two of the four nodes, we need to distribute $C(4,2) = 6$ pair of keys, where $C(n,k)$ denotes the binomial coefficient. Four pairs of keys must be transmitted through the bottleneck quantum channel, which is impossible for a single round of quantum transmission without coding. Therefore, we will introduce the transmission and coding procedures of the TF-QNC scheme.

Our TF-QNC scheme contains two stages in sequence. In the quantum transmission stage, the end nodes in the network transmit phase-randomized quantum states to the intermediate nodes. The intermediate nodes then perform coherent measurements on the states. In the classical transmission stage, the intermediate nodes calculate the phase differences between the states and send them to the end nodes in the form of classical bits. Based on the locally prepared states and the phase differences, the end nodes can derive the group key.

3.2. Quantum Transmission Stage

In systems with insecure channels, single-photon signals can perfectly prevent eavesdropping. Due to the imperfections of light sources, attenuated weak coherent states are commonly used in practical implementations as a substitute for ideal single-photon signals. This makes PNS attacks possible, since a certain proportion of the signals contain more than one photon. Current decoy-state methods can effectively prevent PNS attacks in systems with

imperfect light sources. Thus, it will not undermine the security of the transmission to deliver information with the redundant photons in the unavoidable multi-photon signals.

Replication and coding are the two fundamental operations in classical network coding, which are usually simulated in QNC using approximate cloning and unitary transformations. In the proposed scheme, we simulate replication by employing beam splitters to split multi-photon signals and simulate linear coding by employing coherent measurements to obtain phase differences at each intermediate node. The quantum transmission stage based on the proposed network model is illustrated in Figure 3. In this stage, quantum transmission is achieved via the quantum channels in the model. Each channel is used only once, carrying one single quantum state per transmission.

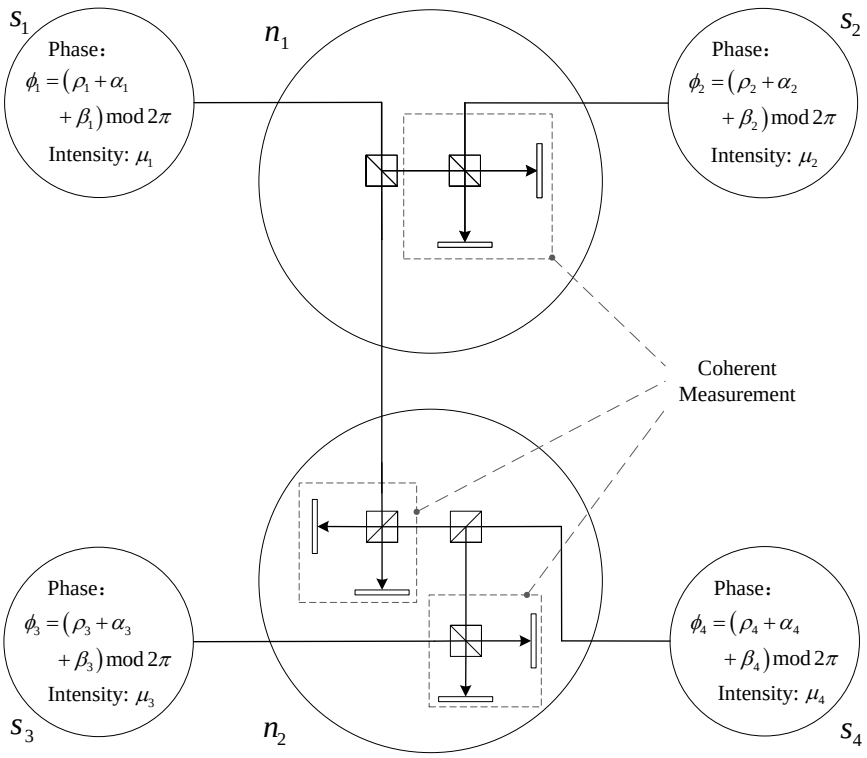

Figure 3. Quantum operations at each node in the butterfly network.

The detailed process of the quantum transmission stage is described as follows. In this process, Steps 1 and 2 are performed only once before the first round of transmission begins, while all other steps are repeated in every round thereafter.

Step 1: System initialization. Similar to the initialization in TF-QKD, the four end nodes s_1 to s_4 agree to divide the phase interval $[0, 2\pi)$ into m equally spaced slices $(\Delta_k, \Delta_{k+1}]$ before all transmission rounds begin, where $k \in \mathbb{Z} \cap [0, m)$ and $\Delta_m = \Delta_0$. Furthermore, for each quantum channel in the butterfly network model, the sender of the signal needs to transmit an unmodulated high-intensity pulse to the receiver to enable precise channel calibration.

Step 2: Intensity selection. According to the decoy-state method, each end node can send three types of states: signal, decoy, and vacuum. Although the decoy-state method theoretically requires an infinite number of decoy states with different intensities to guarantee the detection of eavesdropping, it has been proven that only a limited number of decoy states are enough to achieve approximate performance [28]. In real-world implementations, two decoy states are able to meet the security requirements for most scenarios. Assuming that the current transmission plans to use two decoy states, the end node s_i, $i \in \mathbb{Z} \cap [1, 4]$ needs to select the intensity $\mu_i \in \{\mu, v, w, 0\}$ based on the type of state to be sent, where μ corresponds to signal states, v and w correspond to different decoy states, respectively.

Step 3: Phase selection. Each end node s_i needs to determine the phase of the state to be sent. The phase of each state consists of three components. Firstly, s_i randomly selects a bit phase $\alpha_i \in \{0, \pi\}$, where 0 and π correspond to the key bits 0 and 1. Secondly, it randomly selects a basis phase $\beta_i \in \{0, \pi/2\}$, where 0 and $\pi/2$ correspond to the measurement bases X and Y, respectively. Finally, to realize phase randomization, it randomly selects another phase $\rho_i \in [0, 2\pi)$ and notes down which phase slice $(\Delta_{k_i}, \Delta_{k_i+1}]$ the phase ρ_i is in, where $k_i \in \mathbb{Z} \cap [0, m)$.

Step 4: State preparation. Each end node s_i prepares a signal S_i with phase $\phi_i = (\alpha_i + \beta_i + \rho_i) \mod 2\pi$ and intensity μ_i.

Step 5: Non-bottleneck transmission. The nodes s_1 and s_2 send signals S_1 and S_2 to n_1. The nodes s_3 and s_4 send signals S_3 and S_4 to n_2.

Step 6: Measurement at the node n_1. At n_1, beam splitting on one of the received signals should be performed first. Given that the signals are attenuated and have an average photon number of 1, only a minor portion of them contain more than one photon. To improve the success rate of the measurement and forwarding operation, we do not predetermine the signal to be split. The process proceeds as long as at least one of the signals contains more than one photon. Initially, a photon number resolving detector (PNRD) [29] is used to ascertain the photon numbers of signals S_1 and S_2. If S_1 contains more than one photon, the beam splitting is performed on S_1. If S_1 contains only one photon and S_2 contains more than one photon, the beam splitting is performed on S_2. Otherwise, the current round is discarded. Without loss of generality, we assume that S_1 is the signal to be split. The intermediate node n_1 performs the beam splitting on S_1 and gets S_{11} and S_{12}. Then, it forwards S_{11} to n_2 and performs a coherent measurement on S_{12} and S_2. The coherent measurement here is identical to the measurement performed in the original TF-QKD [14]. It is implemented by interfering the two incoming optical pulses on a 50:50 beam splitter and monitoring the outputs with a pair of single-photon detectors. A detection event in exactly one detector heralds a successful measurement and reveals the phase difference between the two input pulses. If both detectors click or neither clicks, the current round is discarded. If only one detector clicks, the phase difference $\chi_{12} = |\phi_1 - \phi_2|$ is obtained.

Step 7: Measurement at the node n_2. Similar to the process at n_1, at n_2, beam splitting should be performed first on one of the signals received from the source nodes s_3 and s_4. We assume that the signal S_4 from s_4 contains more than one photon. The node n_2 performs beam splitting on S_4 and gets S_{41} and S_{42}. Then, it performs two coherent measurements, one on S_{11} (received from n_1) and S_{41}, the other on S_{42} and S_3. In any of the two measurements, if both detectors click or neither clicks, the current round is discarded. If only one detector clicks in both measurements, the phase difference $\chi_{14} = |\phi_1 - \phi_4|$ between S_{11} and S_{41} is obtained as well as the phase difference $\chi_{34} = |\phi_3 - \phi_4|$ between S_{42} and S_3.

In the quantum transmission stage, information is transmitted from source nodes to intermediate nodes. All the following transmissions will be accomplished via classical communication. The maximum distance for quantum transmission is two hops, which is shorter than the end-to-end distance, thereby extending the communication range of the quantum network. Meanwhile, since only one quantum state transmission is required in the bottleneck channel, the overall efficiency of the network is improved.

3.3. Classical Transmission Stage

After the coherent measurement, the intermediate nodes n_1 and n_2 need to transmit the results via classical communication to the end nodes for key bit deduction. We consider two scenarios:

1. All four end nodes s_1 to s_4 expect to distribute a group key through the butterfly network with bottleneck.
2. Two pairs of end nodes expect to distribute distinct keys simultaneously. For example, s_2 and s_3 want to share a key different from the key shared by s_1 and s_4.

In the first scenario, if only the point-to-point TF-QKD protocol is used to cover the distance, the keys distributed between every pair of nodes are different due to the randomness of information encoded in each quantum state. To enable communication among the nodes s_1 to s_4, a key must be distributed between each two nodes, which requires the protocol to be executed $C(4,2) = 6$ times. Consequently, the bottleneck channel must be used at least 4 times, and each of the other quantum channels must be used at least twice.

In the second scenario, if only the point-to-point TF-QKD protocol is used to cover the distance, the interaction between s_2 and s_3 requires transmission in the bottleneck channel as well as the interaction between s_1 and s_4. Two different quantum states need to traverse the same channel, so the channel must be used at least twice.

Without any coding scheme, both scenarios require more than one round of quantum transmission. Channel resources are not fully utilized, thereby constraining the efficiency of the network. The goal is to achieve key distribution with only one round of quantum transmission by coding the coherent measurement results. The quantum transmissions for both scenarios are identical. The classical transmission process is shown in Figure 4. In the quantum stage, the choice of the forwarded signal has no impact on the state transmission or measurement process. However, in the classical stage, if the forwarded signal is not specified, the end nodes will have trouble generating identical key bits. To optimize channel resource utilization, instead of using an additional round to identify the forwarded signal, we calculate the phase differences between the forwarded signal and the signal sent from each node. Consequently, all four end nodes can deduce the bit encoded in the forwarded signal as the shared key bit. For each round, the classical process for the first scenario is described as follows.

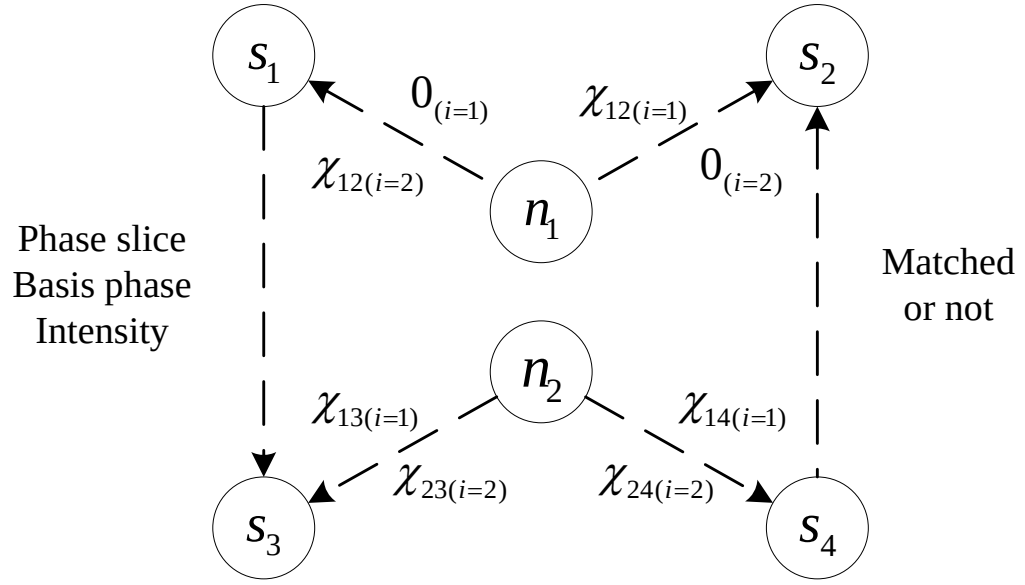

Figure 4. Classical transmission after the coherent measurements.

Step 1: Phase difference coding at the node n_1. Let S_i, $i \in \{1,2\}$ denote the signal successfully split and forwarded at n_1. The node n_1 computes the phase differences χ_{1i} and χ_{2i}. When $i = 1$, i.e., S_1 is the forwarded signal, χ_{1i} and χ_{2i} can be expressed as

$$\chi_{1i} = |\phi_1 - \phi_i| = |\phi_1 - \phi_1| = 0, \tag{4}$$

and

$$\chi_{2i} = |\phi_2 - \phi_i| = |\phi_2 - \phi_1| = \chi_{12}, \tag{5}$$

where χ_{12} is the measurement result obtained in the quantum stage. When $i = 2$, i.e., S_2 is the forwarded signal, χ_{1i} and χ_{2i} can be expressed as

$$\chi_{1i} = |\phi_1 - \phi_i| = |\phi_1 - \phi_2| = \chi_{12}, \tag{6}$$

and

$$\chi_{2i} = |\phi_2 - \phi_i| = |\phi_2 - \phi_2| = 0. \tag{7}$$

Step 2: Phase difference coding at the node n_2. Similarly and simultaneously, let S_j, $j \in \{3,4\}$ denote the signal successfully split and forwarded at n_2. The node n_2 computes the phase differences $\chi_{3i} = |\phi_3 - \phi_i|$ and $\chi_{4i} = |\phi_4 - \phi_i|$. Different from n_1, n_2 performs two coherent measurements after beam splitting to obtain phase differences χ_{34} and χ_{ij}. The coherent measurement only detects two possible phase differences, 0 or π. Due to the binary nature of the phase difference measurement and the modulo 2π arithmetic, when $j = 3$, i.e., S_3 is the forwarded signal, χ_{3i} and χ_{4i} can be expressed as

$$\chi_{3i} = |\phi_3 - \phi_i| = |\phi_3 - \phi_j| + |\phi_i - \phi_j| = \chi_{ij} \pmod{2\pi}, \tag{8}$$

and

$$\chi_{4i} = |\phi_4 - \phi_i| = |\phi_4 - \phi_j| + |\phi_i - \phi_j| = \chi_{34} + \chi_{ij} \pmod{2\pi}, \tag{9}$$

where, χ_{34} and χ_{ij} are both known from the coherent measurements. When $j = 4$, i.e., S_2 is the forwarded signal, χ_{3i} and χ_{4i} can be expressed as

$$\chi_{3i} = |\phi_3 - \phi_i| = |\phi_3 - \phi_j| + |\phi_i - \phi_j| = \chi_{34} + \chi_{ij} \pmod{2\pi}, \tag{10}$$

and

$$\chi_{4i} = |\phi_4 - \phi_i| = |\phi_4 - \phi_j| + |\phi_i - \phi_j| = \chi_{ij} \pmod{2\pi}. \tag{11}$$

Step 3: Phase difference transmission. The node n_1 sends one classical bit to each of s_1 and s_2, encoding χ_{1i} and χ_{2i}, respectively. The node n_2 sends one classical bit to each of s_3 and s_4, encoding χ_{3i} and χ_{4i}, respectively. The

binary values $\{0,1\}$ of each classical bit map to the phase differences $\{0,\pi\}$, following the correspondence $0 \to 0$ and $1 \to \pi$.

Step 4: Round matching. In the proposed butterfly network model, classical information exchange is assumed to be unlimited between s_1 and s_2 as well as between s_3 and s_4. Any end node may initiate the round matching. Let s_3 first disclose the modulation settings of its signal. For signal states, the settings include the phase slice, basis phase, and intensity. For decoy states, bit phase is also included for eavesdropping detection. The matching process can be further decomposed into four substeps:

Substep 1: The node s_3 discloses its modulation settings to s_4.

Substep 2: The node s_4 verifies the consistency between the received settings and its own. If matched, s_4 forwards the information to s_2 via the long-distance channel. Otherwise, it notifies s_2 and s_3 to discard the round, and s_2 then informs s_1.

Substep 3: The node s_2 verifies the consistency between the received settings and its own. If matched, s_2 forwards the information to s_1. Otherwise, it notifies s_1 to discard the round. Then s_1 informs s_3 and s_3 informs s_4.

Substep 4: The node s_1 will obtain the final matching result after its verification. It forwards the result to s_3 via the long-distance channel and to s_2. Then, s_3 informs s_4.

All end nodes ultimately determine the valid rounds for key generation. The two long-distance channels are used only once. This matching process and subsequent key generation steps can also be performed after all rounds have been completed, which introduces additional decoding latency and reduces the pressure on classical transmissions at the same time.

Step 5: Key generation. For the matched rounds, the end nodes need to decode the key bits based on local information. Before key generation, each node s_n, $n \in \mathbb{Z} \cap [1,4]$ has access to its own bit phase α_n and the phase difference χ_{ni} relative to signal S_i. According to the mapping rules in Step 3, if the classical bit corresponding to α_n and χ_{ni} is denoted as b_n and b_{ni}, s_n can deduce the classical bit b_i corresponding to the bit phase if signal S_i by

$$b_i = b_n \oplus b_{ni}. \tag{12}$$

After the classical transmission stage, all end nodes obtain the same b_i, which then serves as the key bit generated in the current round. After all rounds are completed, the final secret key is obtained by concatenating the bits generated in each round.

As for the second scenario, the coding and transmission of the phase differences remain the same. Before round matching, the two pairs of end nodes first negotiate to use states with different basis phases during key distribution. For example, s_2 and s_3 use the states with basis phase of 0, while s_1 and s_4 use the states with basis phase of $\pi/2$. During key generation, each node only decodes the states that match its own basis phase, which enables the two pairs of nodes to generate different keys. An external eavesdropper cannot infer one key from the other. If the two pairs are mutually untrusted, the latter node in a pair may choose to encrypt the matching result with the former node's public key during round matching.

It should be noted that in early QKD protocols such as BB84 [15], basis phases are used to distinguish signal states from decoy states rather than carrying key-related information. In advanced protocols such as the original TF-QKD [14], signal and decoy states can be differentiated by light intensity so that basis phases can carry other information.

4. Properties of the Proposed Scheme

TF-QNC is designed to distribute long-distance multi-party quantum keys and improve network efficiency. Since QNC and TF-QKD are combined in the proposed scheme, two properties can be obtained as follows:

(i) TF-QNC extends the point-to-point QKD process to multi-party scenarios by introducing additional coding operations at intermediate nodes.

(ii) TF-QNC exhibits advantages in communication distance compared to schemes requiring end-to-end quantum transmissions.

4.1. Group Key Distribution

TF-QNC is more efficient in the distribution of a group key than point-to-point TF-QKD protocols in multi-party scenarios. We first analyze the scenario where the four distant end nodes in the butterfly network expect to distribute quantum keys to enable communication between any two of them. TF-QNC takes only one quantum transmission round to distribute a group key among the end nodes, as demonstrated in Proposition 1.

Proposition 1. *If the nodes s_i, $i \in \mathbb{Z} \cap [1,4]$ in the butterfly network expect to enable communication between any two of them, TF-QNC reduces the number of required transmission rounds to* 20% *of the original.*

Proof. When the original point-to-point protocol is used to distribute keys among end nodes, pairwise keys must be distributed, so the protocol must be executed $C(4,2) = 6$ times. Since states are randomized in the protocol, one node cannot distribute keys to multiple nodes in one transmission. To minimize the total number of rounds, we take simultaneous transmissions across different quantum channels into account. The detailed process is described as follows.

Step 1. The nodes s_1 and s_2 send their states to the intermediate node n_1. Then n_1 measures the phase difference between the two states and sends the results to s_1 and s_2. Meanwhile, the nodes s_3 and s_4 send their states to the intermediate node n_2. Then n_2 measures the phase difference between the two states and sends the results to s_3 and s_4. The two protocols can be executed simultaneously.

Step 2. The node s_1 sends a state to n_1. The node s_3 sends a state to n_2 and n_2 forwards it to n_1. Then n_1 measures the phase difference between the two states and sends the results to s_1 and s_3.

Step 3. The node s_1 sends a state to n_1. The node s_4 sends a state to n_2 and n_2 forwards it to n_1. Then n_1 measures the phase difference between the two states and sends the results to s_1 and s_4.

Step 4. The node s_2 sends a state to n_1. The node s_3 sends a state to n_2 and n_2 forwards it to n_1. Then n_1 measures the phase difference between the two states and sends the results to s_2 and s_3.

Step 5. The node s_2 sends a state to n_1. The node s_4 sends a state to n_2 and n_2 forwards it to n_1. Then n_1 measures the phase difference between the two states and sends the results to s_2 and s_4.

In each step, one classical round and one quantum round are needed. Round matching can be completed in a single round during post-processing. Apart from the transmissions for round matching, the process requires five classical rounds and five quantum rounds in total.

In TF-QNC, a shared key bit is distributed among the end nodes with only one classical round and one quantum round.

During the quantum round, all four end nodes simultaneously prepare and transmit their quantum states to the intermediate nodes n_1 and n_2. The bottleneck channel is used only once to transmit a split signal from n_1 to n_2 or vice versa.

During the classical round, the intermediate nodes calculate the phase differences for each end node and then send them back through classical channels. Each end node will deduce the common key bit based on the classical information and the state they sent during the previous quantum round.

According to the descriptions above, our scheme requires only one execution to distribute the group key, which contains one quantum round and one subsequent classical round. In contrast, key distribution among the four nodes using point-to-point TF-QKD needs to be serialized owing to the existence of the bottleneck channel. Therefore, it takes 20% of the original transmission rounds for TF-QNC to generate keys when the end nodes in the butterfly network expect to enable communication between any two of them. □

Now we analyze the scenario where two pairs of nodes expect to distribute different keys through the bottleneck channel. TF-QNC can achieve the goal with half the transmission rounds at minimum, as demonstrated in Proposition 2.

Proposition 2. *If the nodes s_2 and s_3 expect to distribute one key while s_1 and s_4 expect to distribute another, TF-QNC takes* 50% *transmission rounds of the original at minimum.*

Proof. When the original point-to-point protocol is used to distribute keys, two keys need to be generated independently. The node s_2 first sends a state to n_1. Simultaneously, s_3 sends a state to n_2 and n_2 forwards it to n_1. Then, s_1 sends a state to n_1. Simultaneously, s_4 sends a state to n_2 and n_2 forwards it to n_1. Apart from the transmissions for round matching, the process requires two classical rounds and two quantum rounds in total.

In TF-QNC, only one classical round and one quantum round are needed to generate one key bit. If the two pairs of nodes eventually distribute keys with identical bits, the scenario becomes completely equivalent to the first one. Thus, only 50% of the rounds are needed at minimum. The more overlapping bits between the two keys, the less rounds required when using TF-QNC. □

In both scenarios with multi-party interactions, TF-QNC effectively reduces the number of transmission rounds, thereby improving the efficiency of the network.

4.2. Distance Advantage

TF-QNC is designed to achieve multi-party key distribution over long distances. Additional beam splittings at intermediate nodes may reduce the proportion of photons available for coherent measurement, which degrades the key rate of the scheme. We expect to show that the proposed scheme still maintains a communication distance advantage over schemes requiring end-to-end quantum transmissions such as conventional QKDs, as demonstrated in Proposition 3.

Proposition 3. *Among the three paths in TF-QNC where twin-field coherent measurements are used to obtain phase differences, the theoretical key rate on the most distance-constrained path scales linearly with $\eta^{1/2}$, where η denotes the channel transmittance.*

Proof. According to the analysis of the original TF-QKD protocol [14], the key rate satisfies $R_{TF-QKD} \propto \eta^{1/2}$ and the key rate of any other conventional QKD protocol satisfies $R_{QKD} \propto \eta$. The channel transmittance η can be expressed as the geometric mean of the transmittances of all sub-channels. Therefore, TF-QKD improved the key rate over long distance compared to conventional QKD. In the proposed scheme, a twin-field signal transmission mode is applied three times on distinct paths, each on distinct directions and channels. In the proposed model, the distance between nodes in the direction parallel to the bottleneck channel is much longer, so the path traversing the bottleneck channel becomes the most distance-constrained. Now we analyze the key rate on this path in detail.

We assume that the signals used for coherent measurement in the most distance-constrained path are S_1 and S_3. The analysis for other cases is similar. Let η_1 denote the channel transmittance between s_1 and n_1, η_2 denote the channel transmittance between n_1 and n_2, η_3 denote the channel transmittance between s_3 and n_2. The average transmittance $\overline{\eta}$ of the three channels can be expressed as $\overline{\eta} = (\eta_1\eta_2\eta_3)^{1/2}$, which means the original TF-QKD protocol achieves a key rate of

$$R_{TF-QKD} = \lambda_1\overline{\eta}^{\frac{1}{2}} = \lambda_1(\eta_1\eta_2\eta_3)^{\frac{1}{4}}, \tag{13}$$

where λ is a constant proportionality coefficient.

In the proposed scheme, beam splitters are introduced to intermediate nodes. Let t_1 denote the transmittance of the beam splitter at n_1 and t_2 denote the transmittance of the beam splitter at n_2, so the channel transmittance between s_1 and n_1 becomes $t_1\eta_1$, the channel transmittance between s_3 and n_2 becomes $t_2\eta_3$. The key rate in the most distance-constrained path can be expressed as

$$R_{TF-QNC} = \lambda_1(t_1\eta_1\eta_2t_2\eta_3)^{\frac{1}{4}} = \lambda_2\overline{\eta}^{\frac{1}{2}}, \tag{14}$$

where $\lambda_2 = (t_1t_2)^{\frac{1}{4}}\lambda_1$. Therefore, the key rate in the most distance-constrained path still satisfies $R_{TF-QNC} \propto \eta^{1/2}$, which is improved over conventional QKD protocols. □

According to the proof of Proposition 3, we also know that $R_{TF-QNC} = (t_1t_2)^{1/4}R_{TF-QKD}$. Although $R_{TF-QNC} < R_{TF-QKD}$ as $(t_1t_2)^{\frac{1}{4}} < 1$, the scaling relation $R_{TF-QNC} \propto \eta^{1/2}$ still holds. This result is important for two reasons. First, it demonstrates that the performance influence incurred by the beam splitters, which is essential for enabling multi-party key distribution, is merely a constant factor reduction, not a degradation of the scaling law itself. Second, it guarantees that our scheme inherits the primary advantage of TF-QKD over conventional QKDs. This preservation of the square-root scaling is what enables our scheme to outperform sequential point-to-point TF-QKD and other QNC schemes in long-distance multi-party scenarios.

QKD protocols typically attenuate optical signals to maximize the proportion of single-photon states in transmission, which serves as a countermeasure against PNS attacks. In decoy-state method, specific channel parameters will be analyzed to resist PNS attacks targeting multi-photon states. For QKD protocols with decoy-state method, an additional proportion of multi-photon states brings no substantial security risks. If the intensity of the signal can be increased, we can achieve the same key rate as in TF-QKD, which is demonstrated in Proposition 4.

Proposition 4. *Under the same channel parameters, if the original TF-QKD scheme achieves a key rate of R with intensity μ, TF-QNC achieves a key rate of R with intensity*

$$\mu' = -n \cdot W\left(-\frac{\mu}{(t_1t_2)^{\frac{1}{n}}e^{\frac{\mu}{n}}}\right), \tag{15}$$

where n denotes the average photon number of the states when the key rate is R, $W(\cdot)$ denotes the Lambert W function.

Proof. In the most distance-constrained path, the signals undergo beam splittings with transmittances t_1 and t_2 at n_1 and n_2. The probability P_{TF-QNC} of achieving the photon number n satisfies

$$P_{TF-QNC}(\mu) = t_1 t_2 P_{TF-QKD}(\mu), \tag{16}$$

where P_{TF-QKD} denotes the probability of TF-QKD to achieve the same photon number without additional beam splitting. The photon number of each signal is assumed to follow a Poisson distribution. The adjusted intensity μ' satisfies

$$\frac{\mu'^n}{n!e^{\mu'}} = \frac{1}{t_1 t_2} \cdot \frac{\mu^n}{n!e^{\mu}}. \tag{17}$$

Express μ' with μ and we obtain

$$\mu' = -n \cdot W\left(-\frac{\mu}{(t_1 t_2)^{\frac{1}{n}} e^{\frac{\mu}{n}}}\right), \tag{18}$$

where $W(\cdot)$ is the Lambert W function. □

Therefore, TF-QNC achieves the same key rate as TF-QKD in the most distance-constrained path if μ is raised to μ'. This result confirms that the performance reduction introduced with additional operations such as beam splitters is not a permanent deficit. It can be dynamically compensated for by adjusting the source intensity. This makes our scheme highly adaptable. Equation (15) provides a direct method to determine the intensity μ' required to achieve a desired key rate R over long distances.

5. Scheme Analysis

In this section, we analyze the scheme from the aspects of performance, security, and resource consumption.

5.1. Performance

To demonstrate the overall performance of TF-QNC, we analyze the key rate in a complete transmission round, as formalized in Proposition 5.

Proposition 5. *Assuming that all non-bottleneck quantum channels have identical transmission parameters, the overall key rate in TF-QNC can be expressed as*

$$R' = [t_1 t_2 (1-t_1)(1-t_2)]^{\frac{1}{4}} R\big(\mu_s, L_b + 2L_p\big) R^2\big(\mu_s, 2L_p\big), \tag{19}$$

where t_x denotes the ratio of beam splitting at n_x, $x \in \{1,2\}$ and μ_s denotes the intensity of a signal state. L_b and L_p denote the length of the bottleneck channel and the others, respectively. $R(\cdot)$ denotes the key rate of TF-QKD in Equation 1.

Proof. Provided that all non-bottleneck quantum channels have identical transmission parameters, the actual states to be split at n_1 and n_2 do not affect the key rate derivation, so we assume S_1 and S_3 to be the signal to be split. We derive the key rate of TF-QNC from the key rate of TF-QKD. According to the proof of Proposition 3, the key rate of TF-QNC in the most distance-constrained path between S_1 and S_3 satisfies

$$R_{13} = (t_1 t_2)^{\frac{1}{4}} R\big(\mu_s, L_b + 2L_p\big), \tag{20}$$

where t_1 and t_2 are the transmittance of beam splitting at n_1 and n_2 toward the current path, respectively.

Similarly, we can derive the key rates on the other two paths in TF-QNC. For the path between S_1 and S_2, the key rate satisfies

$$R_{12} = (1-t_1)^{\frac{1}{4}} R\big(\mu_s, 2L_p\big), \tag{21}$$

and for the path between S_3 and S_4, the key rate satisfies

$$R_{34} = (1-t_2)^{\frac{1}{4}} R\big(\mu_s, 2L_p\big). \tag{22}$$

In TF-QNC, all the end nodes need to generate the group key simultaneously based on the phase difference information in each path, so the overall key rate of TF-QNC is

$$R' = R_{13}R_{12}R_{34}. \tag{23}$$

Then we obtain the expression of overall key rate in Proposition 5. □

To illustrate the impact of beam splitting, we provide a numerical example based on Proposition 5. Assuming symmetric 50:50 beam splitters are used at both intermediate nodes and all non-bottleneck channels have identical parameters, we have $t_1 = t_2 = 0.5$, so Equation 19 can be simplified to

$$\begin{aligned} R' &= [t_1 t_2 (1-t_1)(1-t_2)]^{\frac{1}{4}} R\left(\mu_s, L_b + 2L_p\right) R^2\left(\mu_s, 2L_p\right) \\ &= \frac{1}{2} R\left(\mu_s, L_b + 2L_p\right) R^2\left(\mu_s, 2L_p\right), \end{aligned} \tag{24}$$

This result indicates that the overall key rate R' of the TF-QNC scheme is reduced by half compared to the case without multicast. The reduction is a fundamental performance trade-off for enabling the multi-cast functionality. It can be seen that the reduction is a constant factor that is independent of the transmission distance, so it does not compromise the fundamental distance advantage of the twin-field structure. Comparing the performance of a multi-party scheme to that of a point-to-point scheme is a comparison of two distinct design choices with different objectives. In multi-party scenarios, the proposed scheme retains superiority over pairwise TF-QKD implementations.

To validate the theoretical derivations and intuitively demonstrate the performance advantages of the proposed scheme, we now present the results of numerical simulation. The simulation parameters were primarily chosen in accordance with the pioneering work on TF-QKD [14] and the specifications of typical contemporary QKD systems to ensure the comparability and practical relevance of our results.

In our simulation, we assume that each node sends one signal state, one decoy state, and one vacuum state in one transmission. The intensities are set to $\mu = 0.5$ for the signal state, $\nu = 0.1$ for the decoy state, and $\omega = 0$ for the vacuum state, respectively. The channel model is similar to the one used in [14] with detector efficiency $\eta_d = 60\%$ and dark count rate $Y_0 = 10^{-7}$. The error rate e_0 caused by the dark count rate is set to 0.5. The inherent system error rate caused by optical misalignment can be calculated from visibility V as $e_d = (1-V)/2$, where V is set to a reasonable value as 99.65%. Based on the parameters in a standard optical fiber channel, the attenuation coefficient is set to $\alpha = 0.2$ dB/km, and the error correction efficiency factor is set to $f = 1.16$.

The simulation results are displayed in Figure 5 and Figure 6. Figure 5 shows the key rate comparison in a point-to-point scenario. Since beam splitters are introduced to support strict multicast, the key rate of TF-QNC has been slightly affected compared to the original TF-QKD when considering only point-to-point transmission. However, as shown in Figure 5, the attenuation rate of the TF-QNC key rate still satisfies the relationship $R_{TF-QNC} \propto \eta^{1/2}$, which remains significantly superior to that of traditional QKD. Such evidence indicates that on a point-to-point path, TF-QNC inherits all the distance advantages of TF-QKD, introducing only a minor constant-factor reduction due to the additional beam-splitting operations. Meanwhile, TF-QNC shows a much better performance than TF-QKD in multi-party scenarios.

Figure 6 shows the key rate comparison in a multi-party group key distribution scenario. TF-QKD undertakes a severe key rate reduction in this context, as it requires the sequential execution of the protocol multiple times for different user pairs. Our scheme accomplishes the distribution of a group key in a single execution, resulting in a much higher key rate. Furthermore, when we adjust the signal intensity of TF-QNC to $\mu_s = 1.5$ to ensure a fair comparison under the same output power, its performance advantage becomes even more profound, particularly in the long-distance regime. Such evidence proves that TF-QNC is superior to the traditional method not only in terms of protocol efficiency but also in resource utilization efficiency.

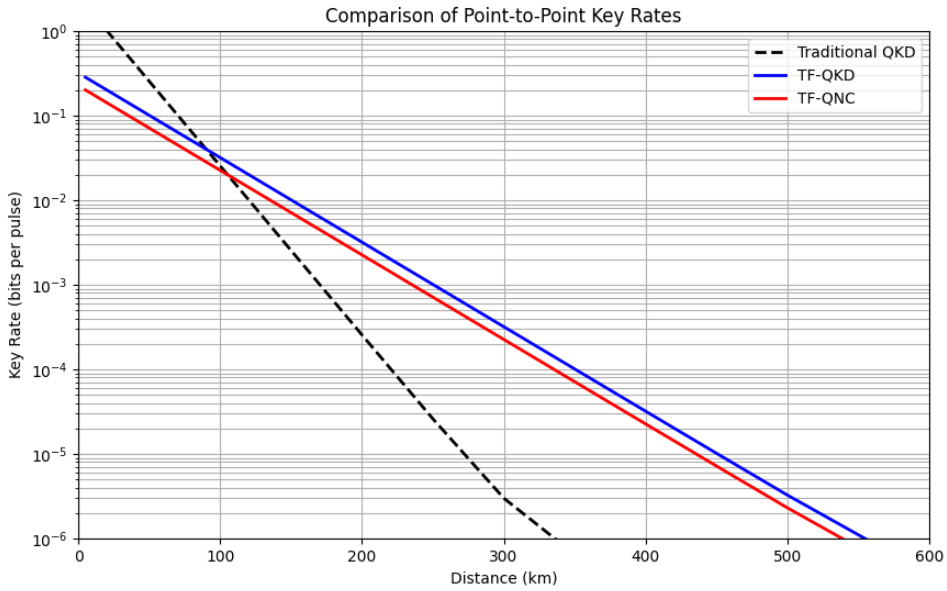

Figure 5. Comparison of point-to-point key rates.

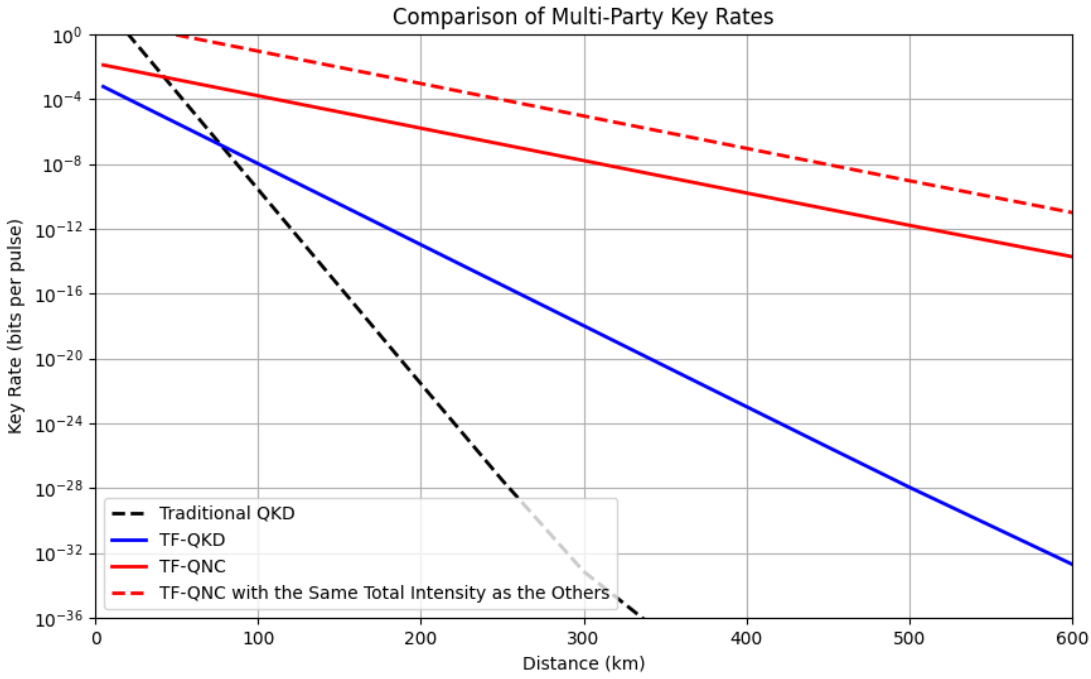

Figure 6. Comparison of multi-party key rates.

The numerical simulation results provide strong support for our theoretical analysis. The TF-QNC protocol successfully extends the square root attenuation rate advantage of TF-QKD from the point-to-point scenario to the multi-party scenario. It effectively addresses the critical issue of bottleneck channels constraining multi-party efficiency in quantum networks without compromising security, offering a viable solution for constructing large-scale, long-distance quantum networks.

5.2. Security

In the original TF-QKD, the intermediate node can only acquire the phase difference between the states instead of the absolute phase, so even if the intermediate node is malicious, it cannot deduce the secret key bits distributed by

the protocol. The TF-QNC scheme is expected to retain the same security property under the condition of untrusted intermediate nodes, as demonstrated in Proposition 6.

Proposition 6. *In TF-QNC, malicious intermediate nodes n_1 and n_2 cannot deduce the phase of any states sent from the end nodes s_1 to s_4.*

Proof. The functionality of n_1 is divided into two parts: beam splitting and coherent measurement. A malicious n_1 can be modeled as a combination of an eavesdropper capable of tuning the beam-splitting ratio and a malicious intermediate node in TF-QKD. Both threats also emerge in the original TF-QKD scenario and are already defended by the decoy-state method and the inherent twin-field structure.

Concretely, if n_1 intercepts some photons originally designated for coherent measurement during beam splitting, the probability of successful phase difference acquisition at n_1 will decrease. Similarly, if n_1 intercepts some photons originally designated to be forwarded, the probability of successful phase difference acquisition at n_2 will decrease. The total gain and the quantum bit error rate (QBER) will be affected in both cases. In the decoy-state method, these values will be compared with theoretical predictions and such malicious behaviors will be detected. From the perspective of an attacker, if n_1 extracts no additional information during beam splitting, it will reduce to an intermediate node in the original TF-QKD, remaining incapable of deducing the absolute phase held by any end nodes.

The functionality of n_2 is divided into three parts: one beam splitting and two coherent measurements. The situation of n_2 intercepting photons by adjusting the beam-splitting ratio is the same as n_1. Any malicious behavior will be detected by the decoy-state method. An advancement over n_1 is that n_2 can obtain the phase differences between any pair of the three states from the two coherent measurements. However, if no photon is intercepted, it is still impossible for n_2 to deduce the absolute phase of any node. □

If s_1 to s_4 expect to distribute a group key, the primary security threats come from eavesdroppers and untrusted intermediate nodes. If two pairs of nodes expect to distribute different keys, each pair must further guarantee that the other pair cannot deduce their key, as demonstrated in Proposition 7.

Proposition 7. *If s_1 and s_4 expect to distribute a key k_a using the rounds in set $\mathcal{R}_a$ while s_2 and s_3 expect to distribute a different key k_b using the rounds in $\mathcal{R}_b$, s_2 and s_3 cannot deduce k_a based on their knowledge of k_b and the classical information exchanged during the interactions when $\mathcal{R}_a \not\subseteq \mathcal{R}_b$.*

Proof. There are two main mechanisms in our scheme to prevent inter-group information leakage:

(i) Basis mismatch.

The two node pairs negotiate to use different bases for state preparation. During key generation, each node only processes the phase difference information that matches their own pre-negotiated basis. Consequently, the key k_a derived by s_1 and s_4 appears random to s_2 and s_3 due to the basis mismatch, which effectively prevents s_2 and s_3 from deducing k_a based on the key k_b they derived themselves.

(ii) Blinded round matching.

The critical mechanism against leakage lies in the classical round matching process. In our scheme, all the end nodes need to participate in each round of quantum transmission. If s_2 and s_3 are both attackers, they may deduce information toward k_a based on the classical feedback from the intermediate nodes at the end of each round. Therefore, we use the blinded round matching mechanism to hide the round matching results from different node pairs.

Since $\mathcal{R}_a \not\subseteq \mathcal{R}_b$, there exists at least one round r where $r \in \mathcal{R}_a$ and $r \notin \mathcal{R}_b$. In round r, s_2 and s_3 may use the wrong basis or intensity settings for the states intended for k_a. During the round matching process, the matching results need to traverse all nodes. Assuming s_4 is the latter node in the pair, it will encrypt the matching result with the public key of s_1 before forwarding it to the next node whether the current round matches or not.

When s_2 or s_3 receives the encrypted message, it cannot decrypt it without the private key of s_1. Therefore, they cannot determine whether their settings for round r is correct for generating k_a or not and are forced to discard round r as invalid. After all rounds are completed, s_2 and s_3 lack the information for all the rounds like r. The final key k_a is the concatenation of bits from all rounds in $\mathcal{R}_a$. Missing even a single bit makes deducing the complete key k_a information-theoretically impossible.

Therefore, the two pairs can securely generate their respective keys without leaking information to each other. The security can be further enhanced by minimizing the intersection $\mathcal{R}_a \cap \mathcal{R}_b$. □

According to Proposition 7, the smaller the intersection between sets $\mathcal{R}_a$ and $\mathcal{R}_b$, the less information s_2 and s_3 can get toward the key shared between s_1 and s_4. It implies that if the two node pairs are mutually untrusted, minimizing the number of common rounds enhances the security of the scheme.

In current decoy-state methods, photon-number-sensitive channel parameters such as the transmission gain and QBER are usually statistically analyzed and compared with theoretical predictions to determine whether PNS attacks exist. To further specify the implementation of the decoy-state method in the proposed scheme, we derive the theoretical transmission gain and QBER. In the decoy-state method, the gain for a coherent state with intensity is defined as the probability that a signal pulse leads to a detection event at the receiver after transmission through a quantum channel. This probability contains all possible causes of detection, including the desired single-photon and multi-photon events as well as the noise from dark counts. We first examine the transmission gain in TF-QNC, as formalized in Proposition 8.

Proposition 8. *Assuming that all non-bottleneck quantum channels have identical transmission parameters and both intermediate nodes use* 50:50 *beam splitters, the overall gain of decoy-state transmission in TF-QNC can be expressed as*

$$Q = Q_d(L_p, \frac{1}{2})^3[Q_d(L_p, 1) + Q_d(L_p, \frac{1}{2})]^2 Q_d(L_p + L_b, \frac{1}{2}). \tag{25}$$

The function $Q_d(L,t)$ is the point-to-point gain. In a channel of length L with attenuation coefficient α, detector efficiency η_d and dark count Y_0, $Q_d(L,t)$ can be expressed as

$$Q_d(L,t) \approx tY_0 + t\mu_d\eta(L), \tag{26}$$

where μ_d denotes the intensity corresponding to decoy states and the transmittance is expressed as $\eta(L) = \eta_d \times 10^{-\alpha L/10}$.

Proof. A single transmission round in which all end nodes send states with intensity μ_d is considered. According to the decoy-state method, if the photon number follows a Poisson distribution and there is a beam splitter with transmittance t on the path, the gain $Q_d(L,t)$ can be expressed as

$$Q_d(L,t) = t\sum_n p_n(\mu_d)Y_n|_L = t\sum_n \frac{\mu_d^n}{e^{\mu_d} n!} Y_n|_L, \tag{27}$$

Where $Y_n|_L$ is the yield of an n-photon pulse. It is the conditional probability of a detection event at the receiver's side given that the source emitted a pulse containing exactly n photons. It is assumed to follow a Poisson distribution, and the overall value is taken over this distribution in the calculation of the gain. Under the assumptions of the standard decoy-state method, the multi-photon contributions are negligible for a low-intensity pulse, i.e., $\mu_d << 1$. Furthermore, the vacuum yield is dominated by the dark count rate, so we have $Y_0|_L \approx Y_0$. The single-photon yield approximates the channel transmittance, so we have $Y_1|_L \approx \eta(L)$. Therefore, the expression simplifies to

$$Q_d(L,t) \approx t[e^{-\mu_d}Y_0 + \mu_d e^{-\mu_d}\eta(L)], \tag{28}$$

Given that $\mu_d << 1$, we can approximate $e^{-\mu_d} \approx 1$, leading to the form of

$$Q_d(L,t) \approx tY_0 + t\mu_d\eta(L), \tag{29}$$

To obtain valid results in the coherent measurement at n_1, one of the signals S_1 and S_2 must be split successfully. If S_1 fail to be split, the beam splitting is performed on S_2. Therefore, the gain at n_1 can be expressed as

$$Q_{n_1} = Q_d(L_p, 1-t_1)\big[Q_d(L_p,1) + Q_d(L_p,t_1)\big]. \tag{30}$$

There is a similar process at n_2, so the gain of it can be expressed as

$$Q_{n_{21}} = Q_d(L_p, 1-t_2)\big[Q_d(L_p,1) + Q_d(L_p,t_2)\big]. \tag{31}$$

Additionally, n_2 also have to perform a coherent measurement on the other half of the split signal and the signal sent from n_1. The gain can be expressed as

$$Q_{n_{22}} = Q_d(L_p + L_b, t_1)Q_d(L_p, t_2). \tag{32}$$

The overall decoy-state gain in TF-QNC is

$$Q = Q_{n_1} Q_{n_{21}} Q_{n_{22}}. \tag{33}$$

When the ratio of each beam splitter is 50:50, t_1 and t_2 satisfy $t_1 = t_2 = 1/2$. After substitution, we obtain Equation (25) in Proposition 8. □

The QBER in a channel is also a photon-number-sensitive parameter, so it is also used to detect eavesdropping in the decoy-state method. According to the decoy-state method, if the photon number follows a Poisson distribution and there is a beam splitter with transmittance t on the path, the QBER $E_d(L, t)$ can be expressed as

$$E_d(L, t) = t \sum_n p_n(\mu_d) Y_n|_L e_n|_L = t \sum_n \frac{\mu_d^n}{e^{\mu_d} n!} Y_n|_L e_n|_L, \tag{34}$$

where $e_n|_L$ denotes the n-photon error rate in a channel with length L. Similar to the transmission gain, the overall QBER of TF-QNC can be expressed as

$$E = E_d(L_p, \frac{1}{2})^3 [E_d(L_p, 1) + E_d(L_p, \frac{1}{2})]^2 E_d(L_p + L_b, \frac{1}{2}), \tag{35}$$

where the ratio of each beam splitter is 50:50 and all non-bottleneck quantum channels are assumed to have identical transmission parameters.

Within the theoretical framework of the decoy-state method, which assumes predictable devices and a known channel model, an obvious statistical deviation between the observed values and the theoretical predictions of gain and QBER is one of the important indicators when detecting the potential presence of eavesdropping.

5.3. Resource Consumption

In this section, the channel consumption and quantum resource consumption of the TF-QNC scheme are discussed. If the additional beam splitting operations are not considered, the proposed scheme distributes multi-party keys with 20% of the transmission rounds at minimum, which shows an advantage in resource consumption. Additional beam splitting may reduce the key rate over point-to-point paths, necessitating more transmissions to generate one key bit successfully. We expect to show that, even when the key rate on each point-to-point path is reduced due to additional beam splitting, the proposed scheme still requires less resource to distribute keys among the four end nodes compared to point-to-point TF-QKD protocols.

In both TF-QNC and TF-QKD, round matching can be performed after all quantum states and phase differences have been transmitted. If the round matching process is not considered, the proposed scheme requires the same number of channels and particles as the original TF-QKD for a single transmission along a point-to-point path. Specifically, two channels between the end nodes and the intermediate node are each used twice to transmit one qubit and one classical bit, respectively. For the most distance-constrained path mentioned in Proposition 3, the proposed scheme requires one classical transmission less than TF-QKD since no classical transmission is required in the bottleneck channel.

For the process of distributing keys among the four end nodes, in the proposed scheme, four non-bottleneck channels are each used twice to transmit one qubit and one classical bit, respectively. Additionally, the bottleneck channel is used once to transmit one qubit. In TF-QKD, keys must be distributed between any two nodes. Each node must send states and receive phase differences in three paths, so four non-bottleneck channels are each used six times, three for qubits and three for classical bits. Additionally, each node must distribute keys with the two nodes on the other side of the bottleneck, so the bottleneck channel needs to be used four times.

If the impact of additional beam splitting operations is taken into consideration, we have already derived the overall key rate of TF-QNC in Equation (19). The overall key rate of using point-to-point TF-QKD protocols to enable multi-party communication can be expressed as

$$R_0 = R^4(\mu_s, L_b + 2L_p)R^2(\mu_s, 2L_p). \tag{36}$$

In the proposed butterfly network model, we assumed the bottleneck channel to be even longer than the others. To simplify the calculation, we assume $L_b = 2L_p$ and the ratio of beam splitting is 50%. According to the inherent properties of TF-QKD, the key rate $R_{TF-QKD} = \beta\eta^{1/2}$, where β is a constant coefficient. The transmittance $\eta = \eta_0 e^{-\alpha L}$, where η_0 is the initial transmittance, α is the attenuation coefficient, so there is

$$R(\mu_s, L_b + 2L_p) = R(\mu_s, 4L_p) = \frac{R^2(\mu_s, 2L_p)}{\beta\eta_0^{\frac{1}{2}}}. \tag{37}$$

Then, the overall key rate of TF-QNC can be expressed as

$$R' = \frac{R^4(\mu_s, 2L_p)}{2\beta\eta_0^{\frac{1}{2}}} = \frac{1}{2}\beta^{\frac{3}{5}}\eta_0^{\frac{3}{10}}\left[\frac{R^{10}(\mu_s, 2L_p)}{\beta^4\eta_0^2}\right]^{\frac{2}{5}} = \frac{1}{2}\beta^{\frac{3}{5}}\eta_0^{\frac{3}{10}}R_0^{\frac{2}{5}}. \tag{38}$$

Therefore, $R' \propto R_0^{2/5}$, which means that R' decays slower than R_0. When $\eta_0 = 1$, $R' = \frac{1}{2}\beta^{3/5}R_0^{2/5}$. If TF-QKD needs to be executed n_1 and n_2 times in point-to-point and multi-party scenarios, TF-QNC needs to be executed $\sqrt{2}n_1$ (according to Proposition 3) and $2\beta^{-3/5}R_0^{3/5}n_2$ times, respectively. Let $\gamma = 2\beta^{-3/5}R_0^{3/5}$. The channel usage of TF-QKD and TF-QNC in both point-to-point and multi-party scenarios is compared in Table 1. For a fair comparison, in the point-to-point scenario, the transmission of TF-QNC on the most distance-constrained path is compared with the original TF-QKD. In the multi-party scenario, TF-QKD executed between any two nodes is compared with the completed TF-QNC. The consumption of quantum states is compared in Table 2.

Table 1. Comparison of channel usage between TF-QNC and TF-QKD.

Scheme	Non-bottleneck channels	Bottleneck channel	Average total times
Point-to-Point TF-QKD	2 channels $\times 2$	2	$6n_1$
Point-to-Point TF-QNC[1]	2 channels $\times 2$	1	$5\sqrt{2}n_1$
Multi-Party TF-QKD[2]	4 channels $\times 6$	4	$28n_2$
Multi-Party TF-QNC	4 channels $\times 2$	1	$9\gamma n_2$

[1]Point-to-Point TF-QNC stands for TF-QNC executed on the most distance-constrained path;
[2]Multi-party TF-QKD stands for TF-QKD executed between any two nodes in multi-party scenarios.

Table 2. Comparison of quantum states usage between TF-QNC and TF-QKD.

Scheme	Quantum states in one execution	Average total number
Point-to-Point TF-QKD	2 nodes $\times 1$	$2n_1$
Point-to-Point TF-QNC	2 nodes $\times 1$	$2\sqrt{2}n_1$
Multi-Party TF-QKD	4 nodes $\times 3$	$12n_2$
Multi-Party TF-QNC	4 nodes $\times 1$	$4\gamma n_2$

Based on the comparison in Table 1 and Table 2, the proposed scheme exhibits lower resource consumption compared to the direct application of TF-QKD in multi-party communication.

Beyond channel and state consumption, the resources needed by the coherent measurements at the intermediate nodes should also be considered. Each coherent measurement unit requires one 50:50 beam splitter and two single-photon detectors. To achieve multi-party key distribution, three executions of the coherent measurement need to be done at the two intermediate nodes. This part of resource consumption is lower than that of the original TF-QKD since it needs to be executed at least $C(4,2) = 6$ times to complete the same task.

To better demonstrate the advantages of our work within the broader field of quantum network coding, we also provide a comparison between the proposed TF-QNC scheme and several representative QNC schemes. Since our scheme has fundamental differences from other QNC schemes in terms of goals and assumptions, we compare the required resources, the possibility to be used in QKD, and the achievable distance to demonstrate the unique advantages of our scheme. Since existing QNC schemes are not considered in the context of quantum key distribution, we consider a scheme possible to be used in quantum key distribution scenarios if it can deliver states with fidelity 1 during the transmission. The key characteristics of each QNC scheme are summarized in Table 3.

As listed in Table 3, our scheme achieves $R \propto \eta^{1/2}$ without relying on demanding quantum resources such as pre-shared entanglements or repeaters. The weak coherent states used in our scheme are a highly practical and widely deployed light source, which makes it a practical solution for long-distance multi-party quantum networks.

Table 3. Comparison with other QNC schemes.

QNC scheme	Quantum resources	Possibility to be used in QKD	Relationship between key rate and transmittance
XQQ [2]	Non-orthogonal quantum states	No	-
QNC based on PE scheme [3,6,12]	Pre-shared entanglements	Possible	$R \propto \eta$
QNC with repeaters [11]	Quantum repeaters	Possible	$R \propto \eta^{1/n}$
QNC based on MBQC [5,9]	Cluster states	No	-
Our scheme	Weak coherent states	Yes	$R \propto \eta^{1/2}$

6. Conclusion

In this paper, we proposed a twin-field quantum network coding scheme for the purpose of distributing group keys in long-distance multi-party scenarios. In particular, we designed a butterfly network model for long-distance multi-party communication, and then designed the quantum and classical coding process to overcome the bottleneck problem. Through scheme analysis, we demonstrated the security and the advantages in terms of efficiency and resource consumption of the proposed scheme. Compared to directly applying the original point-to-point TF-QKD, the TF-QNC scheme can achieve multi-party key distribution with half of the transmission rounds, with the key rate R_{TF-QNC} on each path and the channel transmittance η still satisfying $R_{TF-QNC} \propto \eta^{1/2}$. TF-QNC provides a foundation for future research on transmission schemes in quantum networks with more nodes and longer communication distances, thereby improving the efficiency of large-scale quantum networks constrained by bottleneck channels.

Author Contributions
Y.L. and T.S. proposed the idea and conducted the analyses. All authors reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding
This project was supported by the National Natural Science Foundation of China (No. 62471020) and the Chinese Universities Industry-Education-Research Innovation Foundation of BII Education Grant Program (No. 2021BCA0200) for valuable help.

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

Data Availability Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. R. Ahlswede and N. Cai (2000). "Network information flow." *IEEE Transactions on Information Theory*, 46: 4, 1204–1216.
2. M. Hayashi, K. Iwama, H. Nishimura, R. R. H. Putra and S. Yamashita (2007). "Quantum network coding." In *Proceedings of STACS 2007*, Heidelberg, pp. 610–621.
3. M. Hayashi (2007). "Prior entanglement between senders enables perfect quantum network coding with modification." *Physical Review A*, 76: 4, 1–4.

4. T. Shang, X. J. Zhao and J. W. Liu (2014). “Quantum network coding based on controlled teleportation.” *IEEE Communications Letters*, 18: 5, 865–868.
5. J. Li, X. Chen, X. Sun, Z. Li and Y. Yang (2016). “Quantum network coding for multi-unicast problem based on 2D and 3D cluster states.” Science China Information Sciences, 4, 1–15.
6. T. Shang, J. Liu, Y. Liu, Y. Zhang, Y. Jiang and R. Du (2023). “Quantum network coding based on quantum steering.” In *Proceedings of 2023 International Conference on Wireless Communications and Signal Processing (WCSP)*, Hangzhou, pp. 171–176.
7. 7. Y. Shi and E. Soljanin (2006). “On multicast in quantum networks.” In *Proceedings of 2006 40th Annual Conference on Information Sciences and Systems*, Princeton, pp. 871–876.
8. Y. Hirota and M. Owari (2022). “Asymmetric quantum multicast network coding: asymmetric optimal cloning over quantum networks.” *Applied Sciences*, 12, 61–63.
9. C. Pandey, S. Gupta, R. R. Das and A. Raina (2023). “Quantum network coding and distribution of maximally entangled states in measurement-based quantum computing.” In *Proceedings of 2023 National Conference on Communications (NCC)*, Guwahati, pp. 1–6.
10. Y. G. Yang, B. X. Liu, G. B. Xu, D. H. Jiang, Y. H. Zhou, W. M. Shi and T. Shang (2024). “Flexible quantum network coding by using quantum multiplexing.” Advanced Quantum Technologies, 9, 7.
11. T. Shang, J. Li, Z. Pei and J. W. Liu (2015). “Quantum network coding for general repeater network.” *Quantum Information Processing*, 14: 9, 3533–3552.
12. R. Liu, T. Shang and J. W. Liu (2020). “Quantum network coding utilizing quantum discord resource fully.” *Quantum Information Processing*, 19: 2, 1–19.
13. T. Shang, Y. Zhang, R. Liu and J. Liu (2021). “Quantum network coding reducing decoherence effect.” *Quantum Information Processing*, 20: 8, 1–21.
14. M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. Shields (2018). “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters.” *Nature*, 557: 6, 400–403.
15. C. H. Bennett and G. Brassard (1984). “Quantum cryptography: Public key distribution and coin tossing.” *Theoretical Computer Science*, 560, 7–11.
16. A. K. Ekert (1991). “Quantum cryptography based on Bell’s theorem.” *Physical Review Letters*, 67: 6, 331.
17. S. Zhang, J. Wang and C. J. Tang (2012). “Improved fake-state attack to the quantum key distribution systems.” *International Journal of Theoretical Physics*, 51: 9, 2719–2726.
18. Y. J. Qian, D. Y. He, S. Wang, W. Chen, Z. Q. Yin, G. C. Guo and Z. F. Han (2019). “Hacking the quantum key distribution system by exploiting the avalanche transition region of single photon detectors.” Physical Review Applied, 13: 3, 1–8.
19. V. Gampala, B. Maram and A. Suja Alphonse (2023). “Secured quantum key distribution encircling profuse attacks and countermeasures.” In *Proceedings of Emerging Technologies in Data Mining and Information Security*, Singapore, pp. 233–241.
20. W. Y. Hwang (2003). “Quantum key distribution with high loss: toward global secure communication.” *Physical Review Letters*, 91: 5, 1–4.
21. K. Reaz, M. M. Hassan, A. Green, N. Crum and G. Siopsis (2024). “Experimental decoy-state asymmetric measurement-device-independent quantum key distribution over a turbulent high-loss channel.” *Physical Review A*, 4, 109.
22. C. Jiang, Z. W. Yu, X. L. Hu and X. B. Wang (2023). “Robust twin-field quantum key distribution through sending or not sending.” *National Science Review*, 4, 76–85.
23. N. Gisin, S. Pironio and N. Sangouard (2010). “Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier.” *Physical Review Letters*, 105: 7, 1–11.
24. A. Laing, V. Scarani, J. Rarity and J. O’Brien (2010). “Reference-frame-independent quantum key distribution.” *Physical Review A*, 82: 1, 7261–7265.
25. H. K. Lo, M. Curty and B. Qi (2012). “Measurement-device-independent quantum key distribution.” *Physical Review Letters*, 108: 13, 1–7.
26. X. B. Wang, Z. W. Yu and X. L. Hu (2018). “Sending or not sending: twin-field quantum key distribution with large misalignment error.” *Physical Review A*, 98, 1–13.
27. W. Cui, Z. Song, G. Huang and R. Jiao (2022). “Satellite-based phase-matching quantum key distribution.” *Quantum Information Processing*, 21: 9, 1–10.

28. B. Qi, H. K. Lo, X. Ma and Y. Zhao (2005). “Practical decoy state for quantum key distribution.” *Physical Review A*, 72, 1–15.
29. P. Ercolano, D. Salvoni, C. Bruscino, M. D. Giancamillo, C. Zhang, M. Ejrnaes, J. Huang, H. Li, L. You and L. Parlato (2023). “Optimal configuration of a superconducting photon number resolving detector.” In *Proceedings of SPIE*, Prague, p. 6.