Measurement-device-independent quantum key distribution based on the multi-scale entanglement renormalization ansatz*

LAI Hong*, #, WANG Shanshan, #, HUANG Zhongrui

College of Computer and Information Science, Southwest University, Chongqing 400715, China

Abstract Measurement-device-independent quantum key distribution (MDI-QKD) has attracted widespread attention due to its effective defense against attacks on the detection side. However, its key generation rate is limited by the success probability of two-photon interference, which drops sharply under high channel loss and thereby limits high-throughput long-distance communication. moreover, each successful interference event yields only 1 bit of key information. To overcome these limitations, we propose the introduction of the multi-scale entanglement renormalization ansatz (MERA) into the MDI-QKD protocol. This constructs a hierarchical entanglement structure capable of efficiently encoding multi-bit information, aiming to significantly enhance the key rate, extend communication distance, and maintain theoretical security.

We design three MERA-based MDI-QKD implementation schemes: 1) A single-photon scheme based on the compressed single-photon state at the L-th layer of MERA, which compresses multi-layer information into a single-photon state, enabling the extraction of multiple key bits from a single successful interference event, making it suitable for short-to-medium distance scenarios requiring high key rates; 2) an entanglement-based scheme based on the compressed entangled state at the $(L-1)$-th layer of MERA, which leverages the strong correlations of entangled states to enhance noise resistance, making it suitable for long-distance and high-loss channels; 3) a hybrid adaptive scheme that dynamically switches between the above two modes based on real-time channel quality, achieving optimal performance adaptation across all distances.

All schemes employ the hierarchical compression mechanism of MERA, utilizing the disentangling operator U and the isometric mapping operator W to compress the quantum state layer by layer, and reconstructing the state via inverse operations for

---

* The paper is an English translated version of the original Chinese paper published in Acta Physica Sinica. Please cite the paper as: **LAI Hong, WANG Shanshan, HUANG Zhongrui, Measurement-device-independent quantum key distribution based on the multi-scale entanglement renormalization ansatz .** *Acta Phys. Sin.*, 2026, 75(7): 070601. DOI: 10.7498/aps.75.20251450

multi-level key extraction. The protocol incorporates the decoy-state method for eavesdropping detection, and uses basis sifting and multi-layer fidelity verification to ensure information integrity and security. Additionally, by designing four predefined MERA topological structures, efficient structural matching and information synchronization are achieved.

Numerical simulations show that, Within the 0—200 km range, the single-photon scheme SI-MERA-MDI-QKD improves the key generation rate by approximately 22931% compared to classical MDI-QKD. The entanglement-based scheme ES-MERA-MDI-QKD and the hybrid scheme HY-MERA-MDI-QKD still maintain an effective key rate of 10^{-11} bit/pulse at 350 km, extending the effective communication distance of classical MDI-QKD by approximately 150 km. Under varying detector efficiencies and channel loss conditions, the proposed schemes all demonstrate significant performance advantages. Coding capacity analysis shows that, under zero-error conditions, the encoding capability of MERA-MDI-QKD can exceed that of classical MDI-QKD by more than 221 times.

Security analysis shows that the proposed schemes exhibit strong robustness against collective attacks, intercept-resend attacks, and Trojan-horse attacks. Under collective attacks, any eavesdropping behavior leads to the non-orthogonality of ancillary states, resulting in detectable errors. Under intercept-resend attacks, attackers struggle to reconstruct the original entanglement structure. Under Trojan-horse attacks, the protocol still maintains a high secure key rate through multi-layer encoding.

Keywords measurement-device-independent; multi-scale entanglement renormalization ansatz; long-distance communication; key generation rate

doi: 10.7498/aps.75.20251450
cstr: 32037.14.aps.75.20251450

1 Introduction

Quantum key distribution (QKD) provides a communication method that theoretically enables unconditionally secure key sharing between two parties. Since Bennett and Brassard[1] proposed the BB84 protocol in 1984, QKD has been extensively studied both theoretically[2-5] and experimentally[6-9]. The BB84 protocol relies on quantum mechanical principles to ensure that any eavesdropping leaves detectable traces during communication, thereby guaranteeing the security of key distribution. However, imperfections in practical systems allow eavesdroppers to launch attacks from the source or measurement ends. Examples include Trojan horse attacks[10], photon number splitting attacks[11], and blinding attacks[12].

To counter these attacks, Ac ń et al.[13] proposed the device-independent (DI)-QKD protocol to address vulnerabilities in quantum devices. DI-QKD makes no trusted assumptions about the devices in the system, deriving its security from loophole-free Bell tests[14]. Although DI-QKD offers high security, it requires a system detection efficiency exceeding 82.6%[15]. Achieving this remains challenging under current technological conditions, significantly limiting its applicability. In 2012, Lo et al.[16] proposed the measurement-device-independent (MDI) QKD protocol. By employing the concept of time-reversed entanglement distribution[17], this protocol inherently immunizes against measurement-end attacks. It also simplifies measurement device requirements and reduces system complexity, achieving a favorable balance between security and practicality. Furthermore, it naturally adapts to the multi-scale entanglement renormalization ansatz (MERA)[18] quantum control framework. In 2018, Lucamarini et al.[19] proposed the twin-field (TF) QKD protocol. Based on single-photon interference between remote fields, this protocol breaks the linear bound between key rate and distance, further advancing the development of Measurement-device-independent quantum key distribution (MDI-QKD). In recent years, asynchronous MDI-QKD protocols based on asynchronous two-photon interference[20-22] have effectively reduced implementation complexity by relaxing strict synchronization requirements for photon arrival times. These protocols provide new technical pathways for the practical application of MDI-QKD. Despite significant breakthroughs in MDI-QKD, key generation still relies on successful photon interference. The success probability decreases exponentially with channel loss, leading to low key rates and limited fault tolerance and robustness in high-loss and long-distance scenarios. Moreover, a single successful interference event transmits only 1 bit of classical information, which fails to meet the demands of high-speed communication scenarios.

To address these issues, this paper proposes applying MERA to MDI-QKD (collectively referred to as MERA-MDI-QKD). By utilizing the hierarchical structure of MERA for lossless compression and decompression, the classical information carried by a single successful interference event is expanded into multi-level bit information of MERA. The main contributions of this paper include: 1) proposing an MDI-QKD protocol based on single-photon states compressed at the L-th layer of the MERA state to improve the key generation rate; 2) proposing an MDI-QKD protocol based on entangled states compressed at the $L-1$ layer of the MERA state to effectively mitigate the impact of high loss and noise interference in long-distance channels; 3) proposing an MDI-QKD protocol in hybrid mode, which can dynamically switch MDI-QKD schemes according to real-time channel conditions to achieve optimal performance adaptation in different scenarios.

The remainder of this paper is organized as follows: Section 2 introduces the basic

principles and encoding rules of MERA. Section 3 elaborates on the specific design concepts of the MERA-based MDI-QKD protocol. Section 4 presents the performance evaluation. Section 5 provides the security analysis. Section 6 concludes the paper.

2 Theoretical Foundation

This section primarily introduces the core theoretical foundation of the MERA-based MDI-QKD protocol proposed in this paper. It focuses on elucidating the basic principles of matrix product states (MPS) and MERA, while clarifying the encoding rules for key operators in the protocol. This establishes the theoretical basis for subsequent protocol design and analysis.

2.1 Matrix Product States

Matrix product states (MPS)[23] are a tensor network representation method used to efficiently describe the wave functions of one-dimensional quantum many-body systems. For a system composed of N qubits, the standard formulation of its MPS is shown in Eq. (1):

$$|\psi\rangle_{\mathrm{MPS}} = \sum_{i_1,i_2,\ldots,i_N} \mathrm{Tr}\left(A_{i_1}^{[1]} A_{i_2}^{[2]} \cdots A_{i_N}^{[N]}\right) |i_1 i_2 \cdots i_N\rangle, \tag{1}$$

Here, the boundary tensors $A_{i_1}^{[1]}$ and $A_{i_N}^{[N]}$ are second-order tensors, whereas the intermediate tensors (e.g., $A_{i_2}^{[2]}$) are third-order tensors. The symbol Tr denotes the matrix trace operation.

Currently, MPS can be prepared using various methods, including quantum circuits composed of consecutive controlled-NOT gates and single-qubit rotation gates[24], optical lattices in cold atom systems[25], or logarithmic-depth quantum circuits[26]. However, although MPS performs well for short-range entangled states, its sequential structure limits its ability to represent long-range entanglement. Specifically, the entanglement entropy is bounded by the bond dimension, which hinders the efficient representation of strong correlations between distant particles within the system. Due to these limitations, recent research has increasingly shifted toward tensor network methods that better capture long-range entanglement features, such as MERA or projected entangled pair states (PEPS).

2.2 Multiscale Entanglement Renormalization Ansatz (MERA)

MERA[27] is a tensor network with a hierarchical structure. It achieves efficient encoding of quantum states at different scales by introducing disentanglers U and isometries W. The expression for the MERA state is

$$|\varphi^{(l)}\rangle = W_l|\varphi^{(l-1)}\rangle$$
$$= \quad W_l W_{l-1} U_{l-1} W_{l-2} U_{l-2} \cdots W_1 U_1 |\varphi^{(0)}\rangle, \tag{2}$$

Here, the initial state $|\varphi^{(0)}\rangle$ is a pre-prepared MPS; $|\varphi^{(l)}\rangle$ denotes the compressed quantum state at the l-th layer, whereas $|\varphi^{(l-1)}\rangle$ represents the compressed quantum state at the $(l-1)$-th layer. The disentangler U constitutes a local unitary operation designed to eliminate short-range entanglement between adjacent degrees of freedom prior to coarse-graining, satisfying $UU^\dagger = U^\dagger U = I \otimes I$. The isometry W serves as a linear transformation that maps multiple local degrees of freedom to fewer degrees of freedom, satisfying $W^\dagger W = I$. Figure 1 illustrates the hierarchical structure of MERA, where rectangles represent the U operators and triangles denote the W operators.

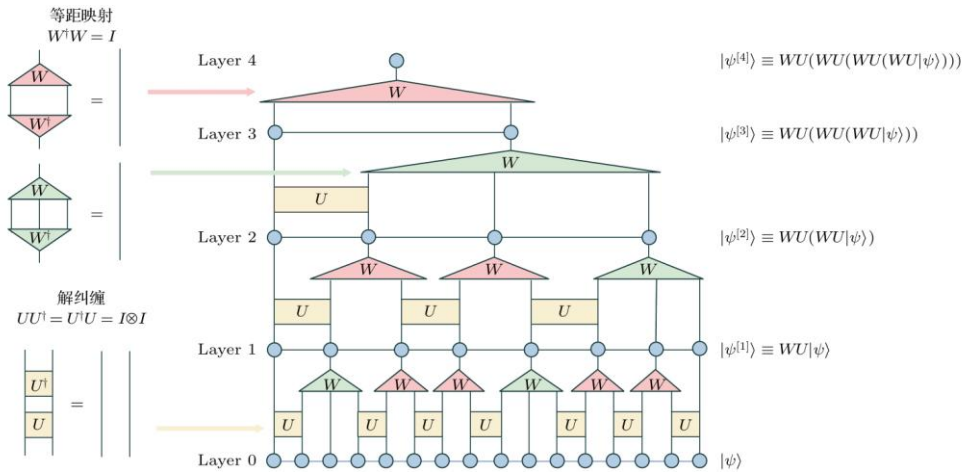

Fig. 1 The structure of MERA.

We consider the initial state in Figure 1 to be: $|\varphi^{(0)}\rangle = \frac{1}{\sqrt{16}} \times (|0000110111100110\rangle + \cdots + |1101111001011110\rangle)$ The specific steps for constructing the upper-layer state $|\varphi^{(1)}\rangle$ from the bottom-layer state $|\varphi^{(0)}\rangle$ are as follows.

1) **Initial Random Partitioning**: The bottom-layer particles $|\varphi^{(0)}\rangle$ are randomly interleaved and partitioned into several groups using binary or ternary encoding. This process lays the foundation for the subsequent unified transformation of each particle group.

2) **Application of the *U* Operator**: We apply the U operator to each partitioned group of particles. We use u_1, u_1, u_2, u_2, u_2, u_1, and u_2 in sequence. The matrix expressions for u_1 and u_2 are detailed in Section 2.3. This step eliminates short-range entanglement between particles within each group and reduces the complexity of subsequent transformations.

3) **Application of the *W* Operator**: After processing with the U operator, we apply the W operator to each group of particles. We use w_3, w_2, w_2, w_4, w_1, and w_1 in sequence.

The matrix expressions for each $w_i (i = 1,2,3,4)$ are detailed in Section 2.3. This maps each group of particles to effective degrees of freedom at a higher level, achieving state compression. The final result is the upper-layer state:

$$|\varphi^{(1)}\rangle = \frac{1}{\sqrt{8}}(|00101000\rangle + \cdots + |00011010\rangle).$$

The key advantage of MERA lies in its ability to simultaneously preserve intra-layer entanglement and inter-layer correlations. By employing *U* and *W* to eliminate short-range entanglement and establish long-range entanglement, it achieves robustness while maintaining high encoding efficiency. This provides an ideal theoretical framework for constructing high-capacity, interference-resistant QKD protocols.

2.3 Encoding Rules

Within the MERA framework, the layer-by-layer compression and decompression of quantum states are jointly realized by two types of operators, *U* and *W*. To facilitate the design and implementation of MERA-based MDI-QKD protocols, it is necessary to explicitly encode the operator types and their operational rules. Based on references [28,29] and protocol requirements, this paper defines the specific matrix forms of these two types of operators as follows:

$$u_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix},$$

$$u_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix},$$

$$w_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix},$$

$$w_2 = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix},$$

$$w_3 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & 0 \end{bmatrix},$$

$$w_4 = \begin{bmatrix} 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Notably, *W* and *U* are not fixed and can be optimized according to specific conditions. To simplify the handling of different operator types in numerical practice, this paper adopts a binary encoding strategy to classify and encode operators. This approach ensures that each operator corresponds to a unique binary sequence and introduces corresponding decompression rules to establish a clear mapping between high-level MERA state encoding and specific operations. *U*-type operators include two basic operations, each encoded with 1 bit; *W*-type operators comprise four basic operations, encoded with 2 bits. The specific encoding rules are as follows:

$$\mathrm{enc}(U_i) = \begin{cases} 0, & i = 1 \\ 1, & i = 2 \end{cases} \quad \mathrm{enc}(W_j) = \begin{cases} 00, & j = 1 \\ 01, & j = 2 \\ 10, & j = 3 \\ 11, & j = 4 \end{cases}$$

Here, $\mathrm{enc}(x)$ denotes the binary encoding of *x*.

During decompression, the receiver maps the received bit string back to the corresponding *W* or *U* operator based on the binary code. This process restores the original quantum state information layer by layer. Table 1 details the specific operations.

Table 1. Encoding table with decompression Rules for operator *W* and *U*.

Matrix	Binary coding	Unsqueezed state	Decompression encoding rule
U_1	0	—	—
U_2	1	—	—
W_1	00	$\|00\rangle$	000 (corresponding to $\|00\rangle$)
		$\|11\rangle$	001 (corresponding to $\|11\rangle$)
W_2	01	$\|01\rangle$	010 (corresponding to $\|01\rangle$)
		$\|10\rangle$	011 (corresponding to $\|10\rangle$)
W_3	10	$\|000\rangle$	100 (corresponding to $\|000\rangle$)
		$\|111\rangle$	101 (corresponding to $\|111\rangle$)
W_4	11	$\|000\rangle$	110 (corresponding to $\|000\rangle$)
		$\|111\rangle$	111 (corresponding to $\|111\rangle$)

3 MERA-Based MDI-QKD Protocol

To address the limited key rate of classical MDI-QKD in long-distance and high-noise channel environments, this paper proposes three improved MDI-QKD schemes based on the multiscale entanglement renormalization ansatz (MERA). These schemes employ the hierarchical entanglement structure of MERA to compress and encode quantum information, thereby enhancing the key generation rate and noise resistance of the protocol. This section details the implementation processes of these three schemes.

3.1 Protocol Initialization

In the MERA-based MDI-QKD protocol, the communicating parties (Alice and Bob) collaboratively design four MERA states with distinct topological structures in advance. This design considers practical conditions such as channel loss, noise levels, and security requirements. The number of bottom-layer particles in these MERA states can be flexibly configured according to the communication scale. A larger number of particles provides a greater potential key space, meeting the high key volume demands of large-scale quantum networks. Conversely, reducing the number of bottom-layer particles lowers the complexity of operator operations and improves protocol execution efficiency. Furthermore, the key generation efficiency can be dynamically optimized by adjusting the scope of the disentanglement operator *U* and the isometric mapping operator *W*.

To clearly elucidate the protocol principles, this paper defines four MERA structures, as shown in Figure 2 (denoted as Configurations A, B, C, and D), and establishes the following conventions.

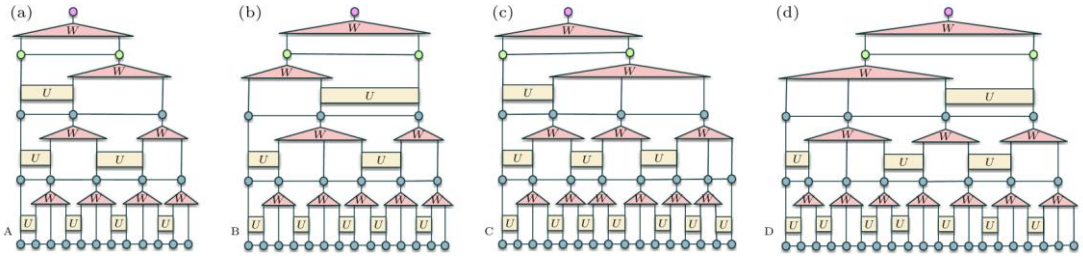

Fig. 2 Schematic diagram of the four MERA structures. Structures A and D are encoded as 0, while structures B and C are encoded as 1

Layer *L*: This layer comprises compressed single-photon quantum states. The compressed single-photon states at layer L for predefined configurations A and B are $|0\rangle$, whereas those for configurations C and D are $|1\rangle$. Furthermore, configurations A and D are encoded as the classical bit "0", while configurations B and C are encoded as the classical bit "1".

Layer $L-1$: This layer consists of compressed two-particle entangled states. The compressed entangled states at layer $L-1$ for predefined configurations A and B are $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, while those for configurations C and D are $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

3.2 Protocol Scheme

3.2.1 Scheme 1: MDI-QKD Based on Compressed Single-Photon States at Layer *L* of MERA States

Figure 3 illustrates the core process of quantum key distribution in Scheme 1. In this figure, blue spheres represent decoy states, while red, orange, green, and purple spheres denote quantum states from the four distinct MERA states (A, B, C, and D), respectively. Specifically, the spheres in Figures 3(a)-(e) represent the compressed single-photon states at layer L of the MERA states corresponding to each color. The spheres in Figure 3(f) represent the quantum states available for key establishment after decompressing the MERA states of the corresponding colors. A red dashed box indicates that Alice and Bob selected different bases, leading to the discarding of the current result. A green dashed box indicates that both Alice and Bob selected the X basis, with these measurement results used for eavesdropping detection. The specific steps are as follows:

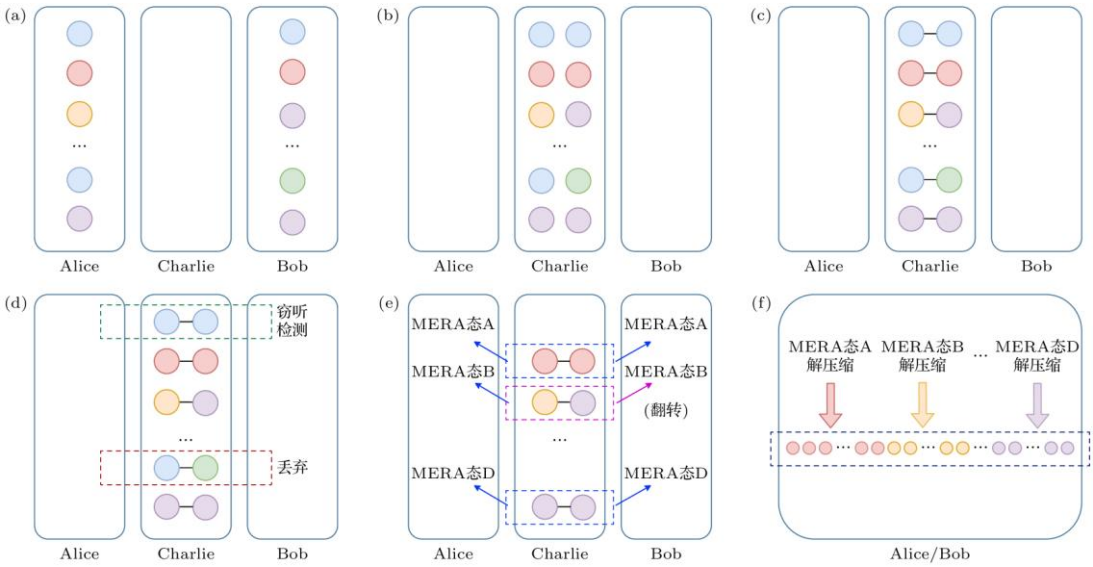

Fig. 3 Schematic of the MDI-QKD protocol based on a compressed single-photon state at layer L of a MERA state: (a) Quantum-state preparation; (b) transmission of the quantum states to Charlie; (c) Bell-state measurement; (d) basis-matching sifting; (e) MERA-structure matching; (f) MERA decompression and key extraction.

Step 1: Quantum State Preparation. Alice and Bob each independently and randomly select one state from four predefined MERA states. Compressed single-photon states are prepared at the L-th layer of the MERA, and decoy states are randomly inserted to enhance the security of the practical system. This study employs a decoy-state scheme comprising one signal state and two decoy states[30]. Alice and Bob modulate their light sources to three different intensities $\{\mu, \nu_1, \nu_2\}$, where μ represents the signal state intensity (i.e., the average number of photons per light pulse), and ν_1 and ν_2 denote the intensities of the two decoy states, satisfying $\mu > \nu_1 > \nu_2 \geqslant 0$. Regarding basis selection, only the signal intensity is encoded in the Z basis, while all decoy intensities are encoded in the X basis for subsequent eavesdropping detection. To ensure coordinated key generation, specific unitary matrices operate on the entangled states at the $(L-1)$-th layer. This operation ensures that the L-th layer of different MERA configurations yields predefined quantum states (see Section 3.1 for details).

The introduction of the decoy-state scheme in this protocol serves as a security measure against the non-ideal characteristics of light sources in physical implementations. This measure operates independently of the core MERA encoding logic. While MERA encoding manipulates ideal logical qubits at the algorithmic level, decoy states provide standardized security verification and parameter estimation capabilities at the physical level. This approach counters defects in real-world light sources and ensures the security of the protocol during actual deployment.

Step 2: Quantum State Transmission. After preparation, Alice and Bob transmit their photons through a quantum channel to a third-party measurement node, Charlie.

Step 3: Bell State Measurement. Charlie performs a joint Bell state measurement (BSM) on the received two-photon system and publicly announces the measurement results. This process reveals no specific bit information, thereby ensuring measurement-device independence. Based on the results announced by Charlie, Alice and Bob classify the outcomes into two classical events. If the result is $|\Phi^+\rangle$ or $|\Phi^-\rangle$, they record it as a "correlated" event. This indicates that the L-th layer single-photon states sent by Alice and Bob are both $|0\rangle$ or both $|1\rangle$. If the result is $|\Psi^+\rangle$ or $|\Psi^-\rangle$, they record it as an "anti-correlated" event. This indicates that the L-th layer single-photon states sent by Alice and Bob are orthogonal to each other; that is, one is $|0\rangle$ and the other is $|1\rangle$.

It is important to note that Charlie can only determine whether the L-th layer single-photon states sent by Alice and Bob are identical. He cannot ascertain the specific MERA configuration. An anti-correlated event indicates that Alice and Bob have selected different MERA configurations. In this case, Bob must perform a bit flip ($|0\rangle \leftrightarrow |1\rangle$) on his L-th layer compressed single-photon state. This step lays the foundation for the correct coordination of the MERA structure between both parties in subsequent steps.

Step 4: Basis Matching Sifting. Alice and Bob publicly compare their selected measurement bases (Z basis or X basis) via a classical channel. An event is retained only if both parties select the same measurement basis. Events involving the Z basis are used for final key generation, while events involving the X basis are used for channel eavesdropping detection. The basis matching sifting rules are detailed in Table 2.

Table 2. Sifting results of basis matching.

Basis chosen by Alice	Basis chosen by Bob	Retain or not	Reason
Z-basis	Z-basis	Retention	For key generation
X basis	X basis	Retention	For eavesdropping detection
Z-basis	X basis	Unreserved	Basis mismatch
X basis	Z-basis	Unreserved	Basis mismatch

Step 5: Match the MERA structure. After Charlie announces the BSM results, Alice and Bob publicly disclose the MERA structure codes they selected (codes A and D are encoded as "0", while codes B and C are encoded as "1"). Based on the BSM results and the rules defined in Table 3, both parties synchronously perform the necessary flip operations. This ensures the use of a consistent MERA structure during subsequent

decompression, thereby generating identical keys.

Table 3. Mapping relationship between Bell-state measurement results and bit flip transformations.

Alice/Bob basis	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$
Z-basis	Bit flip	Bit flip
X basis	Bit flip	No Turnover

Step 6: MERA decompression and key extraction. Based on the Bell state measurement results publicly announced by Charlie, and combined with the MERA private encoding rules pre-agreed upon by Alice and Bob, both parties independently perform logical-level decompression operations locally. This is achieved by applying the inverse operations of the MERA compression process layer by layer (using the W^{-1} and U^{-1} operators). They reconstruct the logical quantum state equivalent to the original multi-qubit entangled state. Finally, they obtain the classical key bit string through local measurements. To ensure the integrity of the quantum state under noisy channels, a multi-layer fidelity verification mechanism is introduced.

Define the ideal target state of the *l*-th layer as $|\phi_{\text{ideal}}^{(l)}\rangle$, and the quantum state obtained from actual decompression as $|\phi_{\text{real}}^{(l)}\rangle$. The fidelity of this layer is defined as

$$F_l = \left|\langle\phi_{\text{ideal}}^{(l)}|\phi_{\text{real}}^{(l)}\rangle\right|^2. \tag{3}$$

Set a fidelity threshold $F_{\text{threshold}}$. If $F_l \geqslant F_{\text{threshold}}$, the *l*-th layer is considered validated; otherwise, the data for that layer are discarded. If no layers pass validation during a decompression round, or if Alice and Bob share no commonly validated layers, all data from that round are discarded. This discard event is broadcast via a classical channel, and the key generation process restarts.

Among the layers passing fidelity validation, Alice and Bob determine a common set of valid layers, denoted as U_{layer}. They then generate the required key through the following steps.

(1) **Layer selection:** Both parties agree on a specific layer *l* from the set U_{layer}.

(2) **Binary sequence construction:** For each selected layer $l \in U_{\text{layer}}$, Alice and Bob convert the quantum state information of that layer into classical binary sequences. They ensure sequence consistency through coordination:

$$k_l = A_l = B_l, \tag{4}$$

Here, A_l and B_l denote the bit sequences obtained by Alice and Bob at the *l*-th layer, respectively.

(3) **Constructing the raw key:** Concatenate the bit sequences k_l generated from each

valid layer $l \in U_{\text{layer}}$ in descending order of layer indices to form the raw key K:

$$K = \|_{l \in U_{\text{layer}}} k_l, \tag{5}$$

Here, the symbol $\|$ denotes the concatenation operation.

(4) **Extracting the final key:** Repeat the aforementioned photon pair transmission and processing procedure n times, and concatenate the raw keys K_i generated in each round:

$$K_{\text{final}} = \|_{i=1}^{n} K_i. \tag{6}$$

Standard post-processing steps (including error correction and privacy amplification) are then performed on K_{final} to generate the final secure key.

3.2.2 Scheme 2: MDI-QKD Based on Compressed Entangled States at the $L-1$ Layer of MERA States

The core process of Scheme 2 for quantum key distribution is illustrated in Figure 4. In Figure 4, blue spheres represent decoy states, while red, orange, green, and purple spheres represent quantum states from four different MERA states (A, B, C, and D), respectively. Specifically, the spheres in Figures 4(a)—(e) denote the compressed entangled states at the $L-1$ layer of the MERA states corresponding to each color. The spheres in Figure 4(f) represent the quantum states available for key establishment after decompressing the MERA states of the corresponding colors. The specific steps are as follows:

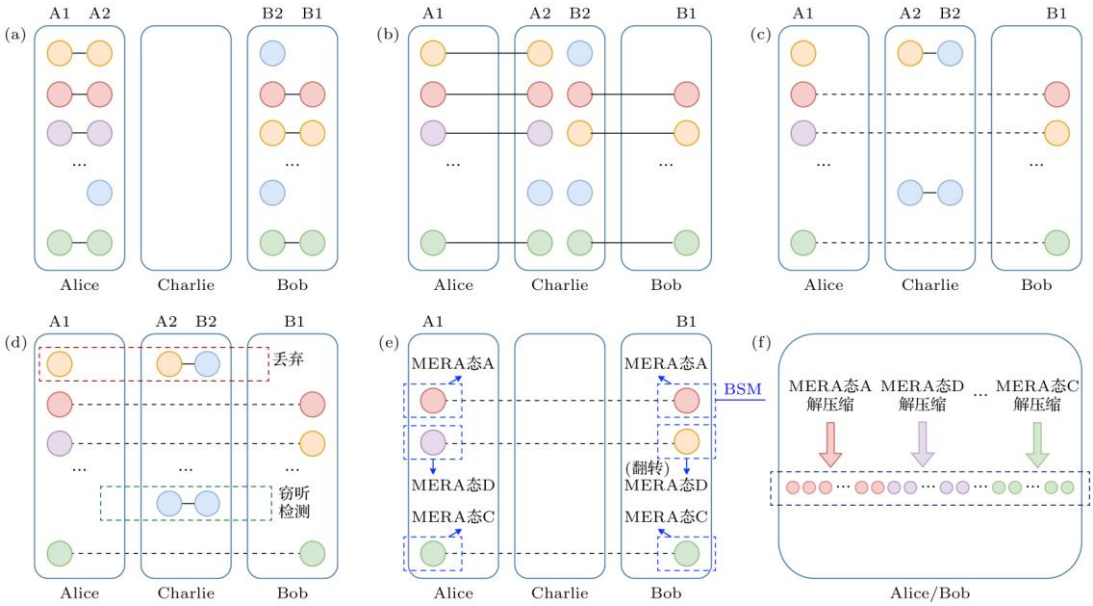

Fig. 4 Schematic of the MDI-QKD protocol based on a compressed entangled state at layer $L-1$ of a MERA state: (a) Quantum-state preparation; (b) transmission of the quantum states to Charlie; (c) Bell-state measurement (BSM); (d) basis-matching sifting; (e) MERA-structure matching; (f) MERA decompression and key extraction.

Step 1: Preparation of quantum states. Alice and Bob each independently and randomly select one state from four predefined MERA states. Using specific unitary

matrices, the $L-1$ layer of the MERA state is prepared into a predefined compressed entangled state. Furthermore, decoy states are randomly inserted using the decoy-state scheme described in Step 1 of Section 3.2.1 to facilitate subsequent eavesdropping detection.

Step 2: Distribution of quantum states. As shown in Fig. 4(b), after the quantum states are prepared, Alice and Bob retain photons A1 and B1, respectively, and transmit photons A2 and B2 to Charlie via quantum channels.

Step 3: Bell state measurement. Charlie performs Bell state measurements (BSM) on the photons received from Alice and Bob. Upon completion of the measurements, Charlie publicly announces only the measurement results. Alice and Bob then determine whether the event is correlated (the photon states of Alice and Bob are identical) or anti-correlated (the photon states of Alice and Bob are complementary).

Step 4: Basis matching and sifting. Alice and Bob publicly compare their basis choices via a classical channel. Events are classified into three categories and sifted based on the sources of the particles involved in the BSM. Case 1: Both photons in the BSM originate from entangled pairs (both using the Z basis). In this scenario, entanglement swapping causes the particles retained by Alice and Bob to form a new entangled state. These events are retained for key generation. Case 2: One photon in the BSM originates from an entangled pair, while the other is a decoy state (one using the Z basis and the other using the X basis). The results of such events and the corresponding photons are discarded and do not participate in subsequent key generation. Case 3: Both photons in the BSM are decoy states (both using the X basis). The BSM results of these events are used for eavesdropping detection.

Step 5: MERA structure matching. Alice and Bob locally measure their retained photons A1 and B1. Combining these measurements with the BSM correlation results announced by Charlie, they mutually infer the compressed entangled states at the $L-1$ layer held by the other party. Subsequently, both parties employ the same MERA structure matching method as in Scheme 1 (see Section 3.2.1 for details). By publicly exchanging limited encoding information, they coordinate to achieve a consistent MERA configuration, ensuring that both parties identify the same MERA state for decompression and key extraction.

Step 6: Fidelity verification and key establishment. This step is identical to Step 6 in Scheme 1 (see Section 3.2.1 for details). Based on the coordinated MERA structure, both parties perform layer-by-layer decompression and fidelity verification. They extract binary sequences from the verified layers and form the raw key K_{final} through cascading operations. Finally, a secure key is generated after error correction and privacy amplification.

3.2.3 Scheme 3: Hybrid Mode

To balance the key generation rate and noise resistance under different channel conditions, this paper further proposes an adaptive hybrid operation mode. This mode dynamically selects between MDI-QKD based on compressed single-photon states at the Lth layer of MERA states (Scheme 1) and MDI-QKD based on compressed entangled states at the $L-1$ layer of MERA states (Scheme 2), depending on real-time channel conditions.

Dynamic selection mechanism: Parameters such as the quantum bit error rate (QBER) and photon transmission efficiency of the quantum channel are monitored in real time.
1) When the channel quality is good (low QBER and high transmission efficiency), Scheme 1 is prioritized to increase the key generation rate.
2) When the channel quality is poor (high QBER and low transmission efficiency), the system switches to Scheme 2, leveraging the strong correlations of entangled states to enhance noise resistance.

Scheduling function: To quantify the aforementioned dynamic selection strategy, this paper defines a scheduling probability p, which represents the proportion of Scheme 1 used in communication. Correspondingly, $1-p$ represents the proportion of Scheme 2. This probability is dynamically calculated using the following formula:

$$p = \alpha \cdot \frac{1}{1+e^{k(\mathrm{QBER}-Q_{\mathrm{th}})}} + \beta \cdot \frac{\eta}{\eta_{max}}, \tag{7}$$

Here, α and β are weighting coefficients satisfying $\alpha+\beta=1$, used to balance the impact of QBER and transmission efficiency; Q_{th} is the preset QBER threshold; k is the adjustment coefficient; η is the measured channel transmission efficiency; and η_{max} is the theoretical maximum transmission efficiency.

Based on the aforementioned mechanism, the MDI-QKD protocol in hybrid mode executes the following steps.

Quantum State Preparation and Transmission: Alice and Bob randomly select, based on the calculated probability p from the scheduling function, to prepare and transmit either compressed single-photon states from the L-th layer of the MERA state or compressed entangled states from the $(L-1)$-th layer of the MERA state. During transmission, a decoy-state scheme, as described in Step 1 of Section 3.2.1, is employed to randomly insert decoy states for eavesdropping detection.

Bell State Measurement: Charlie performs BSM on the received quantum states. For single-photon states, he announces whether the result is an "identical state"; for entangled states, he announces whether the result is a "correlated state."

Base Matching Screening and MERA Structure Matching: Alice and Bob invoke the corresponding processing methods based on the type of quantum state actually used in the current round. If the single-photon state from the L-th layer of the MERA state is used, they execute the base matching screening and MERA structure matching methods identical to those in Scheme 1 (see Section 3.2.1 for details). If the entangled

state from the $(L-1)$-th layer of the MERA state is used, they execute the base matching screening and MERA structure matching methods identical to those in Scheme 2 (see Section 3.2.2 for details).

MERA Decompression and Key Extraction: This step is exactly the same as Step 6 in Scheme 1 (see Section 3.2.2 for details).

It is important to clarify that using the MERA structure itself does not increase information entropy. Instead, it serves as an efficient coding and scheduling framework. This framework significantly enhances the amount of effective secure information that can be extracted and utilized from each successful event in subsequent MDI-QKD quantum transmission. The core value of this design lies in significantly reducing the number of quantum channel uses and BSM operations required to generate a target-length key under given security standards. Consequently, it effectively counteracts channel loss and improves the practical performance of the protocol.

Notably, the security of this protocol stems from the separation of the "public MERA structure" and the "private coding rules" . The topological structure of the MERA is public. However, the *W*/*U* operators used for compression/decompression at each layer, as well as the mapping relationships between quantum states and classical bits, are secretly shared by Alice and Bob. Even if an eavesdropper intercepts the transmitted single-qubit states, they cannot determine the correct inverse operations due to the lack of private coding rules. Even if they luckily guess some operators correctly, the decompressed result remains the private entangled state between Alice and Bob. Since the eavesdropper does not hold the entangled partner particles, they cannot obtain effective information through local measurements. This dual guarantee of "classical private rules + quantum entanglement correlation" causes the eavesdropper's decompression error probability to grow exponentially with the number of layers. Ultimately, the probability of successfully stealing the key becomes negligible. Meanwhile, the increase in the key generation rate is not "creating random bits out of nothing." Instead, it leverages the entanglement compression characteristics of MERA to allow single-qubit transmission to efficiently carry the random information of original multi-qubit entangled states. This introduces no additional information leakage and fully meets the security and efficiency requirements of QKD.

The security source of the "private coding rules" in this protocol is as follows: Both parties first run a standard QKD protocol (such as BB84) to generate a short shared key. This short key serves as a "key seed" to derive the private coding rules required for this protocol. Therefore, the security of the private coding rules is ultimately guaranteed by the physical principles of standard QKD protocols. During protocol execution, these rules function as a pre-shared "codebook." They guide the communicating parties on how to efficiently extract longer classical bit sequences from the limited secure correlations established by each quantum transmission event. This process strictly

adheres to the principle of information conservation and does not increase the total entropy of secure information. Its core value lies in significantly improving the effective secure key output corresponding to the quantum resource consumption per unit of transmission, thereby enhancing the protocol's ability to resist channel loss.

4 Performance Evaluation

This paper aims to overcome bottlenecks such as the low key generation rate and weak long-distance communication capability of classical MDI-QKD. This section quantifies the protocol performance by constructing a mathematical model. It focuses on two core metrics: key generation rate and coding capacity. Simulation experiments are combined to verify the effectiveness of the scheme.

4.1 Key Generation Rate

4.1.1 Key Generation Rate of the MDI-QKD Protocol Based on Compressed Single-Photon States from the *L*-th Layer of MERA

Gain: In the Z basis, the successful gain Q^{rect} of the MDI-QKD protocol based on compressed single-photon states from the L-th layer of MERA is defined as the joint probability of successful qubit transmission and the generation of valid detection events. It can be expressed as

$$Q^{\text{rect}} = \sum_{n,m} Q_{n,m}^{\text{rect}}, \tag{8}$$

Here, $Q_{n,m}^{\text{rect}}$ denotes the gain when two legitimate users transmit n and m photons, respectively.

Quantum Bit Error Rate (QBER): Assuming the error rate in the horizontal basis (Z basis) is e^{rect}, the overall quantum bit error rate E^{rect} is given by

$$E^{\text{rect}} = \frac{1}{Q^{\text{rect}}} \sum_{n,m} Q_{n,m}^{\text{rect}} e_{n,m}^{\text{rect}}. \tag{9}$$

MERA Decompression Success Rate: During the key extraction process, the MERA state undergoes layer-by-layer decompression, with fidelity serving as the verification criterion. The probability of successful decompression at the l-th layer is defined as

$$P_l = Pr(F_l \geqslant F_{\text{th}}), \tag{10}$$

Here, $Pr(F_l \geqslant F_{\text{th}})$ denotes the probability that the fidelity value at the l-th layer falls within the range $F_l \geqslant F_{\text{th}}$.

Upper bound on recoverable secure bits: Let n be the number of qubits at the bottom layer of the MERA, and let the branching factor of the MERA be $b \in \{2,3\}$. The

maximum number of layers in the MERA is expressed as follows:

$$L = \lceil \log_b n \rceil. \tag{11}$$

Thus, the number of effective qubits contained in the l-th layer ($0 \leqslant l \leqslant L$) of MERA is

$$n_l = \lfloor \frac{n}{b^l} \rfloor. \tag{12}$$

Ideally, the total quantum state information contained within a MERA state compression can be expressed as

$$n^l_{\mathrm{MERA}} = \sum_{l=0}^{L} n_l. \tag{13}$$

Probabilistic Model for Successful Preparation of a Single MERA State: Assuming the entangled photon source follows a specific statistical distribution, the probability that the source generates *n* pairs of entangled photons is[31]

$$P'(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \tag{14}$$

Here, λ denotes the parameter of the entanglement source, defined as $\lambda = \sinh^2 \chi$.

The MERA state can be prepared using the schemes provided in Refs. [32,33]. First, the bottom-layer MPS state is prepared. Subsequently, the operators W and U are applied sequentially to generate the upper-layer MPS states layer by layer. The bottom-layer MPS state can be obtained by splicing entangled pairs using the fusion method described in Refs. [34,35]. To prepare an MPS state with a bottom-layer quantum number of m_0, at least $m_0 - 1$ entangled pairs must be generated, followed by $m_0 - 2$ fusion operations. Four logical Bell states are distinguished using *N*-photon encoding, achieving a single fusion success probability of $P_{\mathrm{fus}} = 1 - 1/4^N$ [36]. Therefore, the success probability for preparing a single MERA state is

$$P(1) = \sum_{n=m_0-1}^{\infty} \frac{(n+1)\,\lambda^n}{(1+\lambda)^{n+2}} P_{\mathrm{fus}}^{m_0-2} \sum_{l=1}^{L} P_{wu}(l), \tag{15}$$

Here, $P_{wu}(l)$ denotes the success probability of preparing the *l*-th layer of the MERA state using operators *W* and *U*.

Executing the compression operation for a single MERA layer is physically equivalent to implementing a specific quantum circuit configuration. This circuit primarily consists of linear optical controlled-phase gates and corresponding modulators. In the adopted MERA architecture with approximately *N* physical photons at the bottom layer, the disentanglement operator *U* and the isometry operator *W* at each layer act only on two or three adjacent quantum states. Their total number scales approximately linearly with the number of bottom-layer modes, reaching an order of magnitude of $O(N)$. The additional insertion loss introduced by one layer of MERA operations can be reasonably estimated as a constant on the order of a few dB.

Fiber Loss Model: For the two quantum channels transmitted from Alice and Bob to Charlie, the fiber loss models can be expressed respectively as:

$$\eta_a(L_{\mathrm{ac}}) = 10^{-\alpha L_{\mathrm{ac}}/10}, \eta_b(L_{\mathrm{bc}}) = 10^{-\alpha L_{\mathrm{bc}}/10}, \tag{16}$$

Here, α denotes the fiber attenuation coefficient, typically set to $0.2\mathrm{dB/km}$; L_{ac} and L_{bc} represent the communication distances from Alice and Bob to Charlie, respectively.

In the X basis, the communicating parties employ decoy states for eavesdropping detection and quantum bit error rate estimation, without involving MERA structure selection. The introduction of decoy states prevents eavesdroppers from distinguishing between signal states and decoy states, thereby ensuring protocol security.

In the MDI-QKD protocol based on MERA layer-L compressed single-photon states, the key generation rate depends not only on factors such as basis matching probability and quantum bit error rate but also on the success rate of layer-by-layer decompression of MERA states. Therefore, considering the capability of this protocol to generate multi-level keys in a single successful event, the key generation rate R_{si} is given by Eq. (17)[16,30]:

$$\begin{aligned} R_{\mathrm{si}} \geqslant \sum_{l=1}^{L} m_l P_l^{(A)} P_l^{(B)} \frac{n_{\mathrm{MERA}}^{l'}}{n_{\mathrm{MERA}}^{l}} \Big[& P(1) Y_{\mathrm{rect}}^{1,1} \left(1 - H_2(e_{\mathrm{X}}^{1,1})\right) \\ & - Q^{\mathrm{rect}} f\left(E^{\mathrm{rect}}\right) H_2\left(E^{\mathrm{rect}}\right) \Big], \end{aligned} \tag{17}$$

$$e_{\mathrm{X}}^{1,1} = \frac{1}{2} - \frac{t_{\mathrm{a}} t_{\mathrm{b}} \eta_{\mathrm{d}}^2 (1-e_{\mathrm{d}})^2 (1-Y_0)^2}{4 Y_{\mathrm{rect}}^{1,1}}, \tag{18}$$

$$\begin{aligned} Y_{\mathrm{rect}}^{1,1} = (1-Y_0)^2 [4 Y_0^2 (1 - t_{\mathrm{a}}\eta_{\mathrm{d}})(1 - t_{\mathrm{b}}\eta_{\mathrm{d}}) \\ + 2 Y_0 (t_{\mathrm{a}}\eta_{\mathrm{d}} + t_{\mathrm{b}}\eta_{\mathrm{d}} - \tfrac{3}{2} t_{\mathrm{a}} t_{\mathrm{b}} \eta_{\mathrm{d}}^2 + \tfrac{1}{2} t_{\mathrm{a}} t_{\mathrm{b}} \eta_{\mathrm{d}}^2)], \end{aligned} \tag{19}$$

Here, L denotes the number of layers in the MERA structure; m_l represents the number of qubits in the l-th layer of the MERA, which corresponds to the number of key bits extractable from that layer; $t_{\mathrm{a}} = \eta_{\mathrm{a}}(L_{\mathrm{ac}}) = 10^{-\alpha L_{\mathrm{ac}}/10}, t_{\mathrm{b}} = \eta_{\mathrm{b}}(L_{\mathrm{bc}}) = 10^{-\alpha L_{\mathrm{bc}}/10}$, where L_{ac} and t_{a} (L_{bc} and t_{b}) indicate the channel distance and transmission efficiency from Alice (Bob) to Charles, respectively; $P_l^{(\mathrm{A})}$ and $P_l^{(\mathrm{B})}$ denote the probabilities of successful decompression at the l-th layer of the MERA for Alice and Bob, respectively; η_{d} is the detector efficiency; e_{d} represents the polarization mismatch error; Y_0 is the background probability assumed to be independent of photon pulse detection, including detector dark counts and other background contributions; $n_{\mathrm{MERA}}^{l'}/n_{\mathrm{MERA}}^{l}$ indicates the ratio of the number of logical bits obtained per instance to the complete MERA state

information. In Scheme 1, ideally, $n_{\mathrm{MERA}}^{l'} = n_{\mathrm{MERA}}^{l}$. $P(1)$ is the probability of preparing a single MERA state; $Y_{\mathrm{rect}}^{1,1}$ is the probability that Charlie announces a successful event; $e_{\mathrm{X}}^{1,1}$ is the error rate in the *X* basis; Q^{rect} and E^{rect} represent the total gain and error rate in the Z basis, respectively, which can be measured directly[30]. Based on the multi-intensity decoy-state method proposed in Reference [30], optimal intensity values for signal and decoy states are selected to estimate the values of $Y_{\mathrm{rect}}^{1,1}$ and $e_{\mathrm{X}}^{1,1}$, as detailed in Eqs. (18) and (19).

The error correction efficiency function for the error rate is $f(E^{\mathrm{rect}}) > 1$. $H_2(E^{\mathrm{rect}})$ and $H_2(E^{\mathrm{diag}})$ correspond to the Shannon entropies for the *Z* basis and *X* basis, respectively, reflecting the uncertainty caused by qubit error rates. The formula is given by

$$H_2(x) = -x\log_2 x - (1-x)\log_2 (1-x). \tag{20}$$

4.1.2 Key Generation Rate of the MDI-QKD Protocol Based on Compressed Entangled States at the $L-1$ Layer of MERA

Building on the previously discussed MDI-QKD protocol utilizing compressed single-photon states at the *L*th layer of MERA, this study further investigates scenarios where Alice and Bob employ entangled states. A significant distinction from Scheme 1 is that in Scheme 2, Alice and Bob each utilize entangled states from the $L-1$ layer of MERA. Both parties retain one photon from their respective entangled pairs for subsequent local measurements, while transmitting the other photon through quantum channels to the relay node Charlie for Bell State Measurement (BSM). This process essentially constitutes entanglement swapping. By performing BSM on one photon from each of the two independent entangled pairs provided by Alice and Bob, the locally retained photons are projected into a definite entangled state, thereby establishing remote entanglement.

At the lth layer of MERA, the lattice spacing $r(l)$ between adjacent points is given by

$$r(l) = b^l, \tag{21}$$

Here, b denotes the branching factor of MERA. The correlation between these two points, $C(x,y)$, follows a power-law decay:

$$C(x,y) \equiv r^{-q}, r = r(l) = b^l, q > 0, \tag{22}$$

Here, q denotes the effective power-law exponent determined by the scaling dimension. According to References [37,38] and Equation (22), the bit error rate E_{ent} can be modeled as

$$E_{\mathrm{ent}} = \frac{1}{2}(1 - C(x,y)\eta(L)), \tag{23}$$

Here, $\eta(L)$ denotes the channel efficiency under the standard fiber-optic loss model.

When Alice and Bob generate n and m pairs of entangled photons, respectively, the joint probability of successfully performing entanglement swapping and detecting photons locally at both ends is given by Eq. (24)[31]:

$$\begin{aligned} Y_{n,m} = \\ [1-(1-Y_0)(1-\eta_{\mathrm{a}})^n][1-(1-Y_0)(1-\eta_{\mathrm{b}})^m] \\ \times [1-(1-Y_0)(1-\eta_{\mathrm{ac}})^n][1-(1-Y_0)(1-\eta_{\mathrm{bc}})^m], \end{aligned} \tag{24}$$

Here, η_{a} and η_{b} denote the local detector efficiencies of Alice and Bob, respectively. The terms $\eta_{\mathrm{ac}} = \eta_a(L_{\mathrm{ac}}) \cdot \eta_{\mathrm{c}}$ and $\eta_{\mathrm{bc}} = \eta_b(L_{\mathrm{bc}}) \cdot \eta_{\mathrm{c}}$ represent the product of the channel transmission efficiency from Alice and Bob to Charlie and the detector efficiency at Charlie's end. Y_0 indicates the detector dark count probability.

According to Reference [30], under asymptotic conditions, the quantum bit error rate $e_{\mathrm{ent}}^{1,1}$ for a single pair of entangled photons in the X basis is given by

$$e_{\mathrm{ent}}^{1,1} = \frac{1}{2} - \frac{\eta_{\mathrm{ac}}\eta_{\mathrm{bc}}\eta_{\mathrm{a}}\eta_{\mathrm{b}}(1-e_{\mathrm{d}})^2(1-Y_0)^2}{4Y_{1,1}}. \tag{25}$$

In summary, in the asymptotic regime, the key generation rate of the MDI-QKD protocol based on the compressed entangled state at the $L-1$ layer of MERA can be given by Eq. (26)[30,31]:

$$\begin{aligned} R_{\mathrm{ent}} = \sum_{l=1}^{L} m_l P_l^{(\mathrm{A})} P_l^{(\mathrm{B})} \frac{n_{\mathrm{MERA}}^{l''}}{n_{\mathrm{MERA}}^{l}} \Big[P(1) Y_{1,1} (1 - H_2(e_{\mathrm{ent}}^{1,1})) \\ - Q_{\mathrm{ent}} f(E_{\mathrm{ent}}) H_2(E_{\mathrm{ent}}) \Big], \end{aligned} \tag{26}$$

Here, L denotes the number of layers in the MERA structure; m_l represents the number of qubits at the l-th layer of the MERA; $P_l^{(\mathrm{A})}$ and $P_l^{(\mathrm{B})}$ are the decompression success rates at the l-th layer of the MERA for Alice and Bob, respectively; $Q_{\mathrm{ent}}^{1,1}$ and $e_{\mathrm{ent}}^{1,1}$ denote the gain and quantum bit error rate when Alice and Bob each generate a pair of entangled photons; Q_{ent} and E_{ent} represent the total gain and quantum bit error rate; $P(1)$ is the probability of preparing a single MERA state, as detailed in Eq. (15); and $n_{\mathrm{MERA}}^{l''}/n_{\mathrm{MERA}}^{l}$ indicates the proportion of logical qubits obtained relative to the complete MERA state information. In Scheme II, MERA decompression starts from layer $L-1$, so $n_{\mathrm{MERA}}^{l''} = n_{\mathrm{MERA}}^{l} - 1$.

4.1.3 Key Generation Rate in Hybrid Mode

In the hybrid mode, the overall key generation rate of the system, R_{hybrid}, is the weighted sum of Scheme I and Scheme II, expressed as

$$R_{\mathrm{hybrid}} = pR_{\mathrm{single}} + (1-p)R_{\mathrm{entangled}}, \tag{27}$$

Here, R_{single} and $R_{\text{entangled}}$ are given by Eq. (17) and Eq. (26), respectively; p denotes the dynamic scheduling probability, which is determined by the scheduling function in Eq. (7).

4.2 Encoding Capacity

Encoding capacity is a critical metric for evaluating the information transmission efficiency of QKD protocols. It is defined as the number of classical key bits carried per successful detection event. In this study, it refers to the theoretical upper bound of extractable effective key bits. This bound applies after a successful joint detection event, where both communication parties leverage the MERA hierarchical structure under unconditional security conditions. The enhancement of this upper bound arises because the MERA structure enables a single detection event to unlock encoded information across multiple layers.

In classical MDI-QKD protocols, each successfully transmitted photon generates at most 1 bit of key. Assuming that the communicating parties transmit a total of n photons (with Alice and Bob each sending $n/2$ photons), the effective encoding capacity is

$$K_{\text{effective}}^{\text{MDI-QKD}} = \frac{n}{2} \cdot P_{\text{basis}}, \tag{28}$$

Here, P_{basis} denotes the probability that both communicating parties select the Z basis, and $K_{\text{effective}}^{\text{BB84}}$ represents the number of generated effective bits.

The core advantage of the proposed MERA-based MDI-QKD protocol lies in its use of the hierarchical entanglement structure of MERA to compress and encode quantum information. Decryption enables layer-by-layer key extraction, allowing multiple levels of classical key information to be derived from each pair of successfully detected photons. Since Schemes 1, 2, and 3 share the same core encoding mechanism and differ only in the type of transmitted quantum states, we establish a unified encoding capacity model. The effective encoding capacity of the MERA-based MDI-QKD protocol can thus be expressed as

$$K_{\text{effective}}^{\text{MERA}} = \sum_{i=1}^{n/2} \sum_{l=1}^{L} m_{il} \cdot P_l^{(\text{A})} \cdot P_l^{(\text{B})} \cdot P_{\text{basis}}, \tag{29}$$

Here, n denotes the number of photons sent by Alice and Bob, respectively; m_{il} represents the number of effective key bits extractable from the MERA state corresponding to the i-th photon after decompression at the l-th layer; $P_l^{(\text{A})}$ and $P_l^{(\text{B})}$ are the probabilities of successful decompression at the l-th layer of the MERA for Alice and Bob, respectively; L is the total number of layers in the MERA structure; and P_{basis} is the probability that both communicating parties select the Z basis.

4.3 Experiments

The benchmarks for comparison in this study are the classical MDI-QKD protocol using standard three-intensity decoy states under the asymptotic security framework[16] and the hybrid-source MDI-QKD protocol[39]. Both protocols share the same security framework, decoy-state scheme, and standard device parameter model (0.2 dB/km fiber loss, typical detection efficiency, and dark count rate) with our proposed scheme, ensuring fair and valid comparisons. It should be noted that the 442 km MDI-QKD experiment reported by Liu et al.[40] represents an engineering milestone achieved with finite key lengths. Its customized high-performance device configuration and optimization goals for extreme distances differ in scope from the "theoretical performance exploration of coding schemes" focused on in this work; therefore, it was not directly included in the comparison. This experiment laid an important foundation for the long-distance practical application of MDI-QKD. Our proposed scheme complements these experimental results significantly. Future work may combine finite-key-length optimization with high-performance device technologies to further expand the long-distance application potential of MERA-MDI-QKD.

To visualize the simulation results more intuitively, we simulated four different MERA state configurations with a bottom-layer quantum number of 128 and $L = 6$ layers, using a standard symmetric channel model. The core parameters used in the simulation are listed in Table 4, with data sourced from references [16,30,36,38,41]. Here, p is the weight coefficient of the scheduling function; q is the power-law exponent of the correlation degree between two adjacent photons at the $L-1$-th layer of the MERA; P_{fus} is the single-step fusion success rate for the MPS state; f_{e} is the error correction efficiency factor; Y_0 is the detector dark count probability; e_{d} is the intrinsic error rate of the detector; and η_{d} is the detector efficiency. We assume that the detector efficiencies for Alice, Bob, and Charlie are equal, i.e., $\eta_{\mathrm{a}} = \eta_{\mathrm{b}} = \eta_{\mathrm{c}} = \eta_{\mathrm{d}}$.

Table 4. Simulation parameters.

η_{d}	e_{d}	Y_0	f_{e}	P_{fus}	q	p
14.5%	1.5%	6.02×10^{-6}	1.16	98.4%	0.35	50%

Figure 5 illustrates the variation trends of key generation rates for different MDI-QKD protocols over communication distances ranging from 0 to 400 km. The horizontal axis represents the total communication distance between Alice and Bob, while the vertical axis denotes the number of key bits generated per pulse. The blue solid line represents the classical MDI-QKD protocol proposed in Reference [16]. The green solid line indicates the MDI-QKD protocol employing hybrid sources within

the multimode interference modeling framework proposed in Reference [39], where one party uses a weak coherent pulse (WCP) source and the other uses a spontaneous parametric down-conversion (SPDC) source. The orange, red, and purple solid lines represent the MDI-QKD protocols proposed in this study, based on the compressed single-photon state at the Lth layer of the MERA state, the compressed entangled state at the $L-1$th layer of the MERA state, and the hybrid mode, respectively.

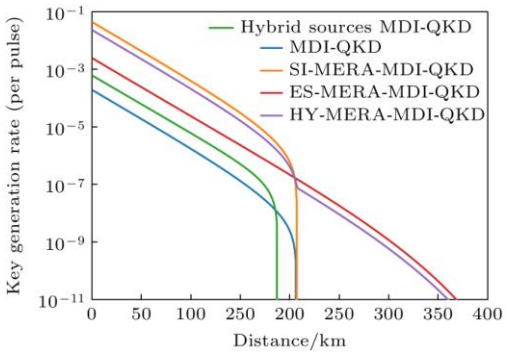

Fig. 5 Key generation rate versus distance for different MDI-QKD protocols.

Figure 5 illustrates that the key generation rates for all protocols exhibit a decaying trend as the communication distance increases. Classical MDI-QKD maintains a certain key generation rate over short to medium distances. However, its decay rate is rapid, with the key generation rate approaching zero at approximately 205 km, thereby preventing the generation of valid keys. Hybrid-source MDI-QKD outperforms standard MDI-QKD in the 0-180 km range. Nevertheless, its key generation rate decays rapidly beyond 180 km, indicating that its long-distance communication capability remains limited. In contrast, the proposed SI-MERA-MDI-QKD demonstrates the highest key generation rate within the 0-200 km range. For instance, at 150 km, the key generation rate of MDI-QKD is approximately 1.324×10^{-7} bit/pulse, whereas that of SI-MERA-MDI-QKD is approximately 3.036×10^{-5} bit/pulse. This represents an increase of approximately 22,931% in the key rate compared to MDI-QKD. Although the communication capability of ES-MERA-MDI-QKD in the 0-200 km range is lower than that of the other two MERA-based MDI-QKD schemes, it exhibits the most gradual decay trend. It maintains an effective key generation rate exceeding 10^{-11} bit/pulse at 350 km, thereby extending the effective communication distance to beyond 350 km. HY-MERA-MDI-QKD integrates the advantages of both SI-MERA-MDI-QKD and ES-MERA-MDI-QKD. It achieves a high key generation rate comparable to SI-MERA-MDI-QKD over short to medium distances while maintaining a slow decay characteristic similar to ES-MERA-MDI-QKD over long distances.

Figure 6 presents the key generation rates of different MDI-QKD protocols at communication distances of 50 km, 100 km, 200 km, and 300 km, clearly highlighting the performance differences among the protocols at specific distance points. At communication distances of 50 km and 100 km, the bar heights for the three proposed MERA-based MDI-QKD schemes are significantly higher than those of the other schemes. SI-MERA-MDI-QKD (orange bars) and HY-MERA-MDI-QKD (red bars) belong to the highest performance tier, followed by ES-MERA-MDI-QKD (green bars). At 200 km, a distinct performance gap emerges between the MERA-based MDI-QKD schemes and the other protocols. The key generation rate of MDI-QKD (blue bars) drops to 2.396×10^{-9} bit/pulse, while that of hybrid-source MDI-QKD (purple bars) approaches zero, making it difficult to generate valid keys. In contrast, the three MERA-based MDI-QKD protocols maintain effective key generation rates at the same order of magnitude, 10^{-7} bit/pulse, with clearly non-zero bar heights. At 300 km, only ES-MERA-MDI-QKD (green bars) and HY-MERA-MDI-QKD (red bars) sustain effective key generation rates, whereas the other protocols fail to produce valid keys.

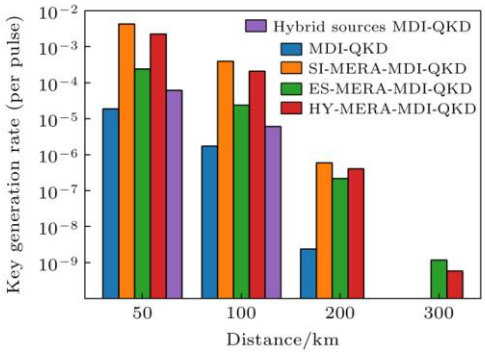

Fig. 6 Key generation rate at 50, 100, 200, and 300 km for different MDI-QKD protocols.

Figure 7 illustrates the variation in key generation rates with communication distance for various MDI-QKD protocols at detector efficiencies $\eta_{\mathrm{d}} = 0.1$, 0.2, 0.3, and 0.4. As η_{d} increases, the key generation rate curves for all protocols shift upward overall. The inflection points also shift to the right, thereby extending the communication distance. Furthermore, under any η_{d} condition, the three MERA-based schemes consistently demonstrate superior key generation capabilities compared to the benchmark protocols. Specifically, HY-MERA-MDI-QKD (purple curve) and ES-MERA-MDI-QKD (red curve) achieve longer effective communication distances. Taking $\eta_{\mathrm{d}} = 0.3$ as an example, SI-MERA-MDI-QKD (orange curve) maintains the highest key rate over the 0—240 km range, followed by HY-MERA-MDI-QKD and ES-MERA-MDI-QKD. Meanwhile, HY-MERA-MDI-QKD and ES-MERA-MDI-QKD sustain effective key generation rates above 10^{-11} bit/pulse at 400 km. In contrast, effective key generation for the other protocols terminates before 210 km.

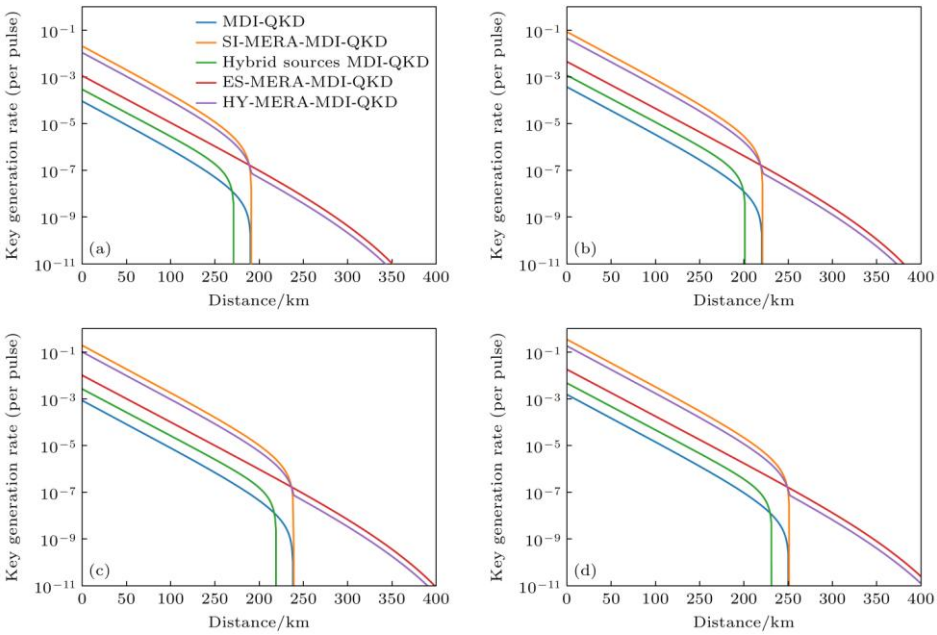

Fig. 7 Key generation rate as a function of communication distance for different detector efficiencies: (a) Detector efficiency = 0.1; (b) detector efficiency = 0.2; (c) detector efficiency = 0.3; (d) detector efficiency = 0.4.

Figure 8 illustrates the variation in key generation rates for different MDI-QKD protocols as a function of communication distance, under channel losses of 0.1 dB/km, 0.2 dB/km, 0.3 dB/km, and 0.4 dB/km. As shown in Figure 8, increasing channel loss causes the inflection points of the key rate curves for all protocols to shift leftward, thereby reducing the maximum communication distance. Nevertheless, the MERA-based MDI-QKD scheme consistently outperforms the comparative schemes in key generation performance across all tested loss conditions. Taking a channel loss of 0.4 dB/km as an example, the SI-MERA-MDI-QKD protocol (orange curve) maintains the highest key generation rate within the 0-100 km range, followed by HY-MERA-MDI-QKD (purple curve) and ES-MERA-MDI-QKD (red curve). Meanwhile, classical MDI-QKD fails to generate valid keys at approximately 100 km, whereas HY-MERA-MDI-QKD and ES-MERA-MDI-QKD sustain a key generation rate of approximately 10^{-11} bit/pulse at 170 km.

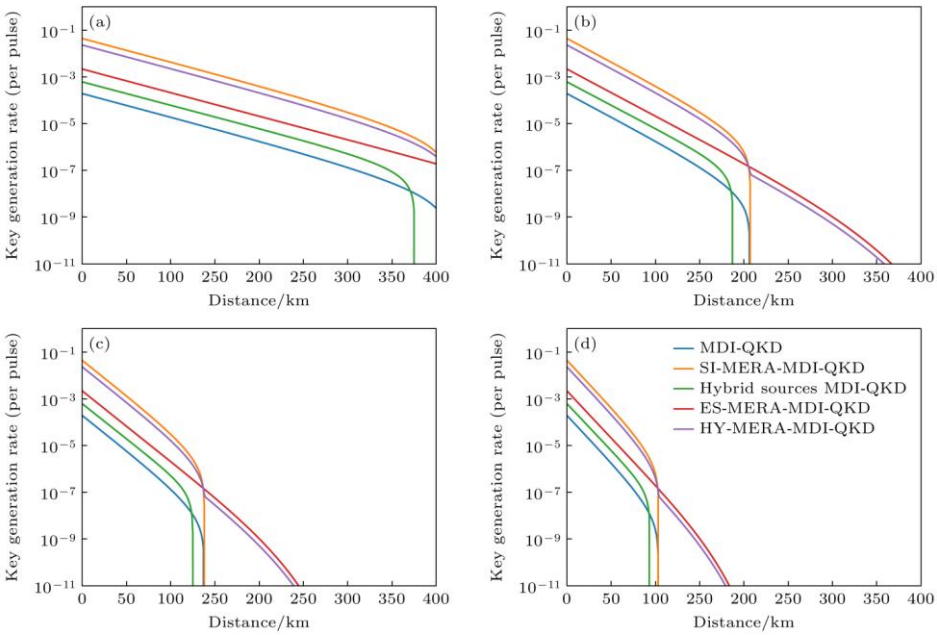

Fig. 8 Key generation rate as a function of communication distance under different channel losses: (a) 0.1 dB/km; (b) 0.2 dB/km; (c) 0.3 dB/km; (d) 0.4 dB/km.

Figure 9 illustrates the variation in classical bit encoding capacity as a function of the total number of transmitted photons (including decoy states) for the MERA-based MDI-QKD protocol and the MDI-QKD protocol from Reference [16] under three quantum bit error rate (QBER) conditions (QBER = 0%, 8%, and 10%). Overall, the curve for MERA-MDI-QKD remains consistently above that of the classical MDI-QKD protocol, regardless of whether errors are present. The performance gap between the two protocols widens linearly with the number of photons. For instance, when 500 photons are transmitted, MERA-MDI-QKD encodes approximately 27,610 classical bits under QBER = 0, whereas classical MDI-QKD encodes only about 125 classical bits. This represents an increase in encoding capacity by a factor of nearly 221. Even at QBER = 10%, the MERA-MDI-QKD protocol encodes more than 24,890 classical bits, while the classical MDI-QKD protocol encodes only 113 bits. By leveraging its hierarchical MERA structure, MERA-MDI-QKD enables each photon to encode 2—3 classical bits of information. As the number of layers increases, each successfully decompressed photon may encode more classical bits. This allows the encoding capacity of the MERA-MDI-QKD protocol to far exceed that of the standard MDI-QKD protocol. However, this improvement is not unlimited. Increasing the number of layers L leads to diminishing marginal returns and higher implementation complexity. Furthermore, lower-level entanglement is more susceptible to noise. Therefore, a trade-off is required when selecting L in practical applications.

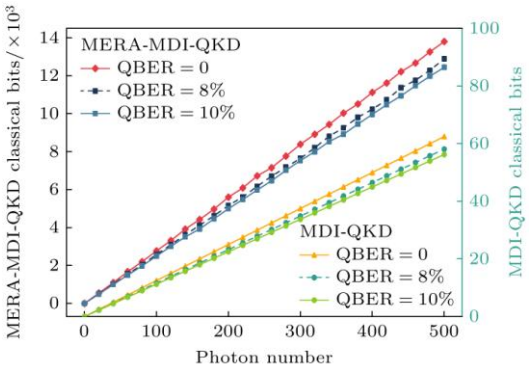

Fig. 9 The variation of the coding capacity of MDI-QKD proposed in Ref. [16] and MERA-based MDI-QKD with the total number of transmitted photons.

Integrating the aforementioned simulation results, the MERA-based MDI-QKD protocol comprehensively outperforms classical MDI-QKD schemes in terms of key generation rate, maximum communication distance, and robustness. Specifically, SI-MERA-MDI-QKD exhibits optimal performance and high key rates over short distances (0-200 km). ES-MERA-MDI-QKD demonstrates superior performance and strong noise resistance over long distances (greater than 200 km). HY-MERA-MDI-QKD achieves balanced performance across all distances. This approach provides multidimensional technical support for quantum secure communication in various scenarios, significantly advancing the practical implementation of MDI-QKD.

It is important to note that the numerical simulations in this study aim to theoretically reveal the potential and performance limits of MERA-based MDI-QKD protocols relative to traditional protocols regarding key rate and transmission distance. Therefore, the current simulation model primarily considers channel transmission loss and inherent detector parameters. It does not explicitly incorporate additional device losses introduced by the physical implementation of MERA into the total channel efficiency calculation framework. Modeling these relevant device losses and subsequently re-optimizing protocol parameters and system architecture constitute a clear and significant direction for future research.

5 Security Analysis

This section systematically analyzes the security of the three proposed MERA-based MDI-QKD schemes against typical attack models, including collective attacks, intercept-resend attacks, and Trojan horse attacks.

5.1 Collective Attacks

In a collective attack, the eavesdropper (Eve) independently performs identical joint operations on each transmission within the quantum channel. After the protocol

execution is complete, Eve performs collective measurements to maximize information acquisition. In MERA-based MDI-QKD protocols, the multi-layer entanglement structure of MERA is employed. Each transmitted quantum state effectively encodes redundant information for multiple bits. This inherent redundancy enhances robustness against collective attacks.

5.1.1 Security Analysis of MDI-QKD Based on MERA Layer *L* Compressed Single-Photon States Under Collective Attacks

In Scheme 1, Alice and Bob compress multi-bit information into single-photon states $|\varphi_0\rangle$ or $|\varphi_1\rangle$ at the L-th layer of MERA for transmission. They randomly insert decoy states $|\varphi^+\rangle$ or $|\varphi^-\rangle$ for eavesdropping detection. Eve's collective attack can be modeled as implementing unitary operations U_{AE} and U_{BE} on the two channels, respectively, while introducing her initial ancillary states $|0\rangle_{e1}$ and $|0\rangle_{e2}$. Let $|\varepsilon_{ji}\rangle_{e1}$ and $|\tau_{\ell k}\rangle_{e2}$ denote the components of Eve's ancillary states after attacking the Alice and Bob channels, respectively. The attack process can be formally expressed as

$$E_1 : |\varphi_i\rangle_{\mathrm{A}}|0\rangle_{e1} \xrightarrow{U_{\mathrm{AE}}} \sum_{j=0}^{1} |\varphi_j\rangle_{\mathrm{A}}|\varepsilon_{ji}\rangle_{e1}, \tag{30}$$

$$E_2 : |\varphi_k\rangle_{\mathrm{B}}|0\rangle_{e2} \xrightarrow{U_{\mathrm{BE}}} \sum_{l=0}^{1} |\varphi_l\rangle_{B}|\tau_{lk}\rangle_{e2}, \tag{31}$$

Here, $i,k \in 0,1$ denotes the basis indices of the quantum states sent by Alice or Bob, while j,l represents the signal state collapse branches potentially induced by Eve's interference. A successful Bell state measurement projects the quantum state of the entire composite system (including Eve's ancillary system) onto a subspace satisfying the correlation conditions. The ideal entangled state can be expressed as

$$|\Phi\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|\varphi_0\rangle_{\mathrm{A}}|\varphi_0\rangle_{\mathrm{B}} + |\varphi_1\rangle_{\mathrm{A}}|\varphi_1\rangle_{\mathrm{B}}). \tag{32}$$

After Eve performs the attack, the global quantum state evolves into

$$|\alpha^{(1)}_{\mathrm{ABe1e2}}\rangle = (U_{\mathrm{AE}} \otimes U_{\mathrm{BE}})(|\Phi\rangle_{\mathrm{AB}}|0\rangle_{e1}|0\rangle_{e2}). \tag{33}$$

If Charlie successfully measures the entanglement correlation, the projection satisfies $\langle\Phi|\alpha^{(1)}_{\mathrm{ABe1e2}}\rangle = 0$. To avoid introducing bit errors, the following condition must hold for all $i \neq j$ or $k \neq l$:

$$\langle \tau_{lk} | \varepsilon_{ji} \rangle = 0. \tag{34}$$

In summary, the auxiliary state components of Eve are mutually orthogonal if and only if zero bit errors occur. This implies that when the bit error rate is zero, Eve cannot obtain any distinguishing information about the original key bits from her auxiliary system. Conversely, if Eve attempts to steal information by making her auxiliary states non-orthogonal, she inevitably violates the aforementioned conditions. This violation leads to bit errors, which are subsequently detected by the legitimate communicating parties. Therefore, Protocol 1 is unconditionally secure against collective attacks: any eavesdropping activity translates into an observable increase in the bit error rate, thereby ensuring key security.

5.1.2 Security Analysis of MDI-QKD Based on Compressed Entangled States at the $L-1$ Layer of MERA Under Collective Attacks

In Protocol 2, Alice and Bob each employ compressed entangled states from the $L-1$ layer of the MERA. Alice uses one of the following two forms:

$$|\Phi^+\rangle_{\mathrm{A_1A_2}} = (|0\rangle_{\mathrm{A_1}}|0\rangle_{\mathrm{A_2}} + |1\rangle_{\mathrm{A_1}}|1\rangle_{\mathrm{A_2}})/\sqrt{2},$$

$$|\Psi^+\rangle_{\mathrm{A_1A_2}} = (|0\rangle_{\mathrm{A_1}}|1\rangle_{\mathrm{A_2}} + |1\rangle_{\mathrm{A_1}}|0\rangle_{\mathrm{A_2}})/\sqrt{2}.$$

Bob uses one of the following two forms:

$$|\Phi^+\rangle_{\mathrm{B_1B_2}} = (|0\rangle_{\mathrm{B_1}}|0\rangle_{\mathrm{B_2}} + |1\rangle_{\mathrm{B_1}}|1\rangle_{\mathrm{B_2}})/\sqrt{2},$$

$$|\Psi^+\rangle_{\mathrm{B_1B_2}} = (|0\rangle_{\mathrm{B_1}}|1\rangle_{\mathrm{B_2}} + |1\rangle_{\mathrm{B_1}}|0\rangle_{\mathrm{B_2}})/\sqrt{2}.$$

Alice and Bob retain particles $\mathrm{A_1}$ and $\mathrm{B_1}$, respectively, and transmit particles $\mathrm{A_2}$ and $\mathrm{B_2}$ to Charlie via quantum channels. Eve performs collective attacks on the Alice → Charlie and Bob → Charlie channels:

$$E_1 : |\varphi_i\rangle_{\mathrm{A_2}}|0\rangle_{e1} \xrightarrow{U_{\mathrm{A_2}E}} \sum_{j=0}^{1} |\varphi_j\rangle_{\mathrm{A_2}}|\varepsilon_{ji}\rangle_{e1}, \tag{35}$$

$$E_2 : |\varphi_k\rangle_{\mathrm{B_2}}|0\rangle_{e2} \xrightarrow{U_{\mathrm{B_2}E}} \sum_{l=0}^{1} |\varphi_l\rangle_{\mathrm{B_2}}|\tau_{lk}\rangle_{e2}. \tag{36}$$

At this point, the entire system, comprising the particles of Alice and Bob as well as the two auxiliary particles, is in the state:

$$|\alpha^{(1)}_{\mathrm{A_2B_2}e1e2}\rangle = (U_{\mathrm{B_2E}} \otimes U_{\mathrm{B_2E}})(|\varphi_i\rangle_{\mathrm{A_2}}|\varphi_k\rangle_{\mathrm{B_2}}|0\rangle_{e1}|0\rangle_{e2}). \quad (37)$$

If Charlie successfully measures the entanglement correlation, the projection satisfies $\langle\Phi|\alpha^{(1)}_{\mathrm{A_2B_2}e1e2}\rangle = 0$. To avoid introducing bit errors, the following condition holds for any $i \neq j$ or $k \neq \ell$:

$$\langle\tau_{lk}|\varepsilon_{ji}\rangle = 0. \quad (38)$$

Therefore, Protocol II also satisfies the security principle of "no error, no information" against collective attacks. Notably, since Charlie is untrusted in this protocol, any intentional publication of incorrect measurement results would immediately be detected. Such actions would cause the error rate in the decoy-state test to exceed the threshold.

5.1.3 Security Analysis of Hybrid-Mode MDI-QKD Against Collective Attacks

The hybrid protocol randomly selects either the compressed single-photon states from Protocol I or the compressed entangled states from Protocol II for each transmission round. This random switching essentially introduces an additional confusion mechanism. Eve cannot predict the encoding type used in each round, thereby making it difficult to optimize a unified attack strategy.

The maximum amount of information that Eve can obtain in Protocol III is

$$I_{\mathrm{E}}^{(3)} = pI_{\mathrm{E}}^{(1)} + (1-p)I_{\mathrm{E}}^{(2)}, \quad (39)$$

Here, p denotes the probability of employing Scheme 1; $I_{\mathrm{E}}^{(1)}$ and $I_{\mathrm{E}}^{(2)}$ represent the maximum information accessible to Eve in Scheme 1 and Scheme 2, respectively. Since Schemes 1 and 2 have been proven to prevent Eve from acquiring valid information under zero error rate conditions, Scheme 3 similarly ensures a security level where $I_{\mathrm{E}}^{(3)}$ is zero under the same conditions.

The hybrid mode not only preserves the security features of the first two schemes but also increases the uncertainty of Eve's attacks through random switching. For instance, if Eve attempts to attack single-photon states but encounters entangled state rounds, it becomes significantly more difficult for her to reconstruct valid information. Furthermore, the protocol can dynamically adjust the encoding scheme based on real-time monitoring of the error rate. When an abnormal increase in the error rate is detected, the system adaptively increases the proportion of entangled states, which offer stronger anti-interference capabilities, thereby further reducing the risk of information leakage.

5.2 Intercept-Resend Attack

5.2.1 MDI-QKD Based on Compressed Single-Photon States at the *L*-th Layer of MERA

1) **Source Structure**: Alice and Bob compress multi-bit information into single-photon states $\{|\phi_0\rangle, |\phi_1\rangle\}$ at the L-th layer of MERA and randomly insert decoy states $\{|\phi_+\rangle, |\phi_-\rangle\}$.

2) **Eve's Intercept-Resend**: Eve intercepts each photon, randomly selects the Z basis or X basis for measurement, and then prepares the corresponding state to resend to Charlie based on the measurement results.

3) **Error Rate Analysis**: When the measurement basis selected by Eve differs from that of the sender (with a probability of approximately 50%), there is a 50% probability that her measurement result will be inconsistent with the original quantum state. This leads to errors in Charlie's Bell state measurement results after resending. During security detection rounds, Alice and Bob publicly compare their measurement results for all decoy state rounds, allowing them to identify abnormal error rates. If an intercept-resend attack is present, the detected error rate will significantly exceed the protocol's security threshold.

In summary, in Scheme 1, any intercept-resend attack causes the error rate to exceed the security threshold. Alice and Bob can promptly terminate the protocol and discard the relevant data upon detecting abnormal error rates, thereby ensuring key security.

5.2.2 MDI-QKD Based on Compressed Entangled States at the $L-1$ Layer of MERA

In Scheme 2, when Eve intercepts the entangled photons sent by Alice or Bob (denoted as A_2 or B_2, respectively) and performs measurements, she inevitably destroys the original entanglement relationship. Subsequently, Eve faces a choice between two resending strategies.

1) **Resending Single-Photon States**: Eve prepares corresponding single-photon states based on the qubit information obtained from her measurements and sends them to Charlie. However, this operation destroys the entanglement correlation that should have been established between Alice and Bob, making it difficult for Charlie's BSM to observe valid entanglement events.

2) **Resending Entangled States**: Eve attempts to "forge" an entangled state photon, aiming to maintain some form of entanglement between the resent photon and the other photon retained by the sender to facilitate effective BSM. However, since Eve cannot obtain complete information about the entangled pairs shared by Alice and Bob, it is practically impossible for her to prepare a quantum state consistent with the original entangled state.

Therefore, regardless of the resending strategy Eve adopts, the probability of her

restoring the original entanglement is extremely low. During eavesdropping detection, due to Eve's disruption, Alice and Bob will either observe a severe loss of entanglement correlation (e.g., Charlie detects almost no valid entangled states) or an error rate far exceeding the threshold Q_{th}. Upon detecting either of these anomalies, Alice and Bob will terminate the protocol and discard all data.

5.2.3 MDI-QKD Based on the MERA Hybrid Mode

The hybrid mode further enhances the protocol's resistance to attacks by randomly switching encoding schemes. Without knowing whether the current round uses Scheme 1 or Scheme 2, Eve finds it difficult to select the optimal counter-strategy. If Eve treats the state as a single-photon state and performs measurements, but the round actually involves an entangled state, her operation is equivalent to measuring one half of an entangled pair. As analyzed in Scheme 2 above, this immediately destroys the entanglement correlation and is detected, and vice versa. If Eve attempts to optimize strategies for both scenarios separately, such as by performing a joint measurement that covers both single-photon and entangled states, she faces a fundamental limitation. Due to the differences in their representations in Hilbert space (one being a single-particle state and the other a two-particle entangled state), no current measurement method can accommodate both without reducing the correct discrimination rate. By publicly comparing the results of randomly inserted single-photon decoy states and entangled decoy states, Alice and Bob can determine that an attack has occurred if they detect abnormal error rates or loss of correlation.

5.3 Trojan Horse Attack

A Trojan horse attack (THA) involves Eve injecting strong coherent pulses into Alice's (or Bob's) port and collecting light reflected and scattered by the modulator to steal partial information. The target of the attack is the photons intended for transmission into the channel. The core characteristic of this attack is that Eve attempts to acquire the key through an optical side channel without interfering with the normal transmission of the quantum channel, thereby bypassing the randomness defense inherent in the quantum states.

Based on the MERA-MDI-QKD protocol model using compressed single photons introduced in Section 4.1.1, and the rigorous analysis of MDI-QKD-THA by Tan et al.[42], this paper incorporates THA into the MERA-MDI-QKD protocol. We correct the single-photon X-basis error rate and gain, obtaining the lower bound of the key generation rate as shown in Equation (40):

$$R_{\mathrm{si}}^{\mathrm{THA}} \geqslant \sum_{l=1}^{L} m_l P_l^{(\mathrm{A})} P_l^{(\mathrm{B})} \frac{n_{\mathrm{MERA}}^{l'}}{n_{\mathrm{MERA}}^{l}} \times \left[P(1) Y_{\mathrm{rect}}^{1,1} \left(1 - H_2(e_{\mathrm{X,T}}^{1,1})\right) - Q^{\mathrm{rect}} f\left(E^{\mathrm{rect}}\right) H_2\left(E^{\mathrm{rect}}\right) \right], \quad (40)$$

Here, $n_{\mathrm{MERA}}^{l'}/n_{\mathrm{MERA}}^{l}$ denotes the proportion of logical qubits obtained relative to the complete MERA state information; $P_l^{(\mathrm{A})}, P_l^{(\mathrm{B})}$ represent the probabilities of successful decompression at the l-th layer of the MERA for Alice and Bob, respectively; $P(1)$ is the probability of preparing a single MERA state; $Y_{\mathrm{rect}}^{1,1}$ is the probability that Charlie announces a successful event; $e_{\mathrm{X,T}}^{1,1}$ indicates the error rate considering the THA; and Q^{rect} and E^{rect} denote the total gain and total error rate in the Z basis, respectively. Similarly, for MERA-MDI-QKD based on compressed entangled states, $e_{\mathrm{ent}}^{1,1}$ is replaced by the error rate considering the THA.

When the THA model is considered, the bias introduced by the THA can be determined using the trace distance (which also applies to entangled pairs). The error introduced by the THA is

$$e_{\mathrm{X,T}}^{1,1} = \quad e_{\mathrm{X}}^{1,1} + 4\Delta'(1-\Delta')\left(1 - 2e_{\mathrm{X}}^{1,1}\right) + 4\sqrt{\Delta'(1-\Delta')e_{\mathrm{X}}^{1,1}\left(1 - e_{\mathrm{X}}^{1,1}\right)}, \quad (41)$$

$$\Delta = \frac{1}{2}\left[1 - \mathrm{e}^{(-2\mu_{\mathrm{out}})}\cos^2(\mu_{\mathrm{out}})\right], \quad (42)$$

$$\Delta' = \Delta / Y_{\mathrm{rect}}^{1,1}, \quad (43)$$

Here, $e_{\mathrm{X}}^{1,1}$ denotes the bit error rate in the absence of attacks; μ_{out} represents the average number of photons injected by Eve into Alice or Bob and reflected back; Δ indicates the trace distance deviation introduced by the THA. Consequently, we can directly substitute $e_{\mathrm{X,T}}^{1,1}$ from Eq. (41) into Eq. (40) to obtain the lower bound of the secure key rate for the MERA-MDI-QKD protocol under THA.

To evaluate the resistance of the proposed MERA-based MDI-QKD protocol against THA, we analyzed the secure key generation rate in the presence of THA through numerical simulations. Previous studies have shown that information leakage from intensity modulators affects the key rate more significantly than that from phase modulators[42,43]. Therefore, we performed simulations using data where the average number of Trojan horse photons reflected from the intensity modulator per pulse is

$\mu_{\mathrm{THA}} = 1.818 \times 10^{-12}$. The results are presented in Figure 10.

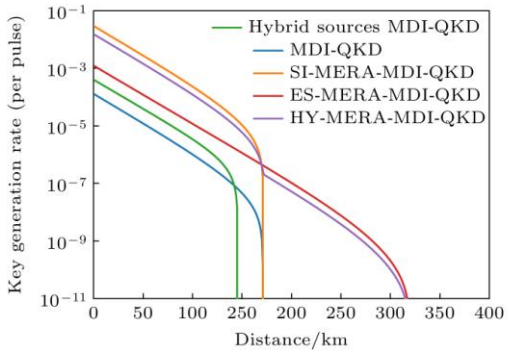

Fig. 10 Dependence of key generation rate on communication distance for different MDI-QKD protocols considering Trojan-horse attacks.

Figure 10 illustrates the variation in key generation rates for different MDI-QKD protocols as a function of communication distance, considering THA. As shown in Figure 10, the key generation rates for all protocols gradually decrease with increasing communication distance. Under THA with $\mu_{\mathrm{out}} = 1.818 \times 10^{-12}$, the key generation rate for classical MDI-QKD (blue curve) drops rapidly at approximately 170 km, while that for hybrid-source MDI-QKD (green curve) declines sharply at around 145 km, indicating that both are more sensitive to THA. Under the same THA conditions, although the effective key generation rate for MDI-QKD based on compressed single-photon states at the *L*th layer of MERA (orange curve) also drops rapidly at approximately 170 km, its key generation rate remains two orders of magnitude higher than that of classical MDI-QKD within the 0-170 km range. This demonstrates that the proposed scheme offers stronger information leakage suppression and greater practical value over short to medium distances. MDI-QKD based on compressed entangled states at the $L-1$th layer of MERA (red curve) and hybrid-mode MDI-QKD based on MERA (purple curve) can further extend the transmission limit to approximately 320 km under the same attack intensity.

In summary, the MERA-based MDI-QKD protocols proposed in this paper distribute key information across entangled states at different hierarchical levels by leveraging the multiscale entanglement structure of MERA. This makes it difficult for Eve to obtain the complete key through a single attack. Consequently, the protocols maintain superior secure key generation rates in the face of THA, and different MERA state encodings provide better defense against THA than classical MDI-QKD protocols.

6 Conclusion

This paper proposes three MERA-based MDI-QKD schemes: MDI-QKD based on compressed single-photon states at the *L*th layer of MERA states, MDI-QKD based on

compressed entangled states at the $L-1$th layer of MERA states, and MDI-QKD in hybrid mode. By introducing MERA hierarchical encoding into the MDI-QKD framework, we achieve the encoding and transmission of multi-bit information using single photons. Furthermore, a multi-layer fidelity verification mechanism effectively enhances the robustness of the protocol in noisy channels. This paper elaborates on the construction principles and procedures of the aforementioned protocols, designs four MERA structures, and provides a complete operational workflow including steps such as quantum state preparation, Bell state measurement, basis sifting, structure comparison, information decoding, and key extraction. Performance analysis results indicate that, compared with classical MDI-QKD protocols, the coding efficiency of the proposed MERA-based MDI-QKD protocols improves by nearly 221 times. Moreover, the two schemes based on compressed entangled states at the $L-1$th layer of MERA and hybrid-mode MDI-QKD can maintain effective key generation at a distance of 350 km, extending the effective communication distance of classical MDI-QKD protocols by approximately 150 km.

It should be noted that although the MERA structure used in our numerical simulations has 128 underlying particles, existing studies have demonstrated the preparation of large-scale MERA structures with up to 243 underlying particles[44]. With the continuous development of optical devices and entanglement preparation technologies, there is still room for expanding the scale of MERA, which can further enhance the information carrying capacity and noise resistance of the proposed protocols.

Future work will focus on studying the feasibility of experimental implementation of MERA-MDI-QKD, including physical implementation schemes for MERA tensor networks and optimization of multi-bit concurrent error correction algorithms. Meanwhile, we will extend the core concept of MERA encoding in this protocol to other quantum key distribution architectures, such as asynchronous MDI-QKD, to meet the demands for higher rates and broader coverage in quantum secure communication. In addition, the MERA joint operation framework presented in this paper is universal and can be extended to DI-QKD scenarios. Future research may focus on constraints such as real-world device efficiency and channel loss, exploring MERA-based entangled state optimization and efficient Bell inequality detection schemes to facilitate the long-distance practical application of DI-QKD.

References

[1] Bennett C H, Brassard G 1984 *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* pp 175-179

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Zapatero V, Leent T, Arnon-Friedman R, Liu W, Zhang Q, Weinfurter H, Curty M 2023 *npj Quantum Information* **9** 10

[4] Wang W, Lütkenhaus N 2022 *Phys. Rev. Res.* **4** 043097

[5] Ding H J, Liu J Y, Zhou X Y, Zhang C H, Li J, Wang Q 2023 *Phys. Rev. Appl.* **19** 044022

[6] Zhang Y, Ding X, Li Y, et al. 2025 *Phys. Rev. Lett.* **134** 210801

[7] Chen J P, Zhang C, Liu Y, et al. 2020 *Phys. Rev. Lett.* **124** 070501

[8] Wang S, Yin Z Q, He D Y, et al. 2022 *Nat. Photonics* **16** 154

[9] Liu Y, Zhang W J, Jiang C, et al. 2023 *Phys. Rev. Lett.* **130** 210801

[10] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G 2006 *Phys. Rev. A* **73** 022320

[11] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photonics* **4** 686

[13] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V 2007 *Phys. Rev. Lett.* **98** 230501

[14] Rosenfeld W, Burchardt D, Garthoff R, Redeker K, Ortegel N, Rau M, Weinfurter H 2017 *Phys. Rev. Lett.* **119** 010402

[15] Woodhead E, Acín A, Pironio S 2021 *Quantum* **5** 443

[16] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[17] Inamori H 2002 *Algorithmica* **34** 340

[18] Vidal G 2007 *Phys. Rev. Lett.* **99** 220405

[19] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400

[20] Xie Y M, Lu Y S, Weng C X, et al. 2022 *PRX Quantum* **3** 020315

[21] Zeng P, Zhou H, Wu W, Ma X 2022 *Nat. Commun.* **13** 3903

[22] Shao S F, Zhou L, Lin J, Minder M, Ge C, Xie Y M, Shen A, Yan Z, Yin H L, Yuan Z 2025 *Phys. Rev. X* **15** 021066

[23] Perez-Garcia D, Verstraete F, Wolf M M, Cirac J I 2007 *Quantum Info. Comput.* **7** 401

[24] Ran S J 2020 *Phys. Rev. A* **101** 032310

[25] Zhou L, Choi S, Lukin M D 2021 *Phys. Rev. A* **104** 032418

[26] Malz D, Styliaris G, Wei Z Y, Cirac J 2024 *Phys. Rev. Lett.* **13** 2

[27] Cincio L, Dziarmaga J, Rams M M 2008 *Phys. Rev. Lett.* **100** 240603

[28] Lai H, Huang Z, Ren L, Pieprzyk J, Zhao Q, Kwek L 2025 *Phys. Rev. A* **111** 022603

[29] Lai H, Ren L, Huang Z R, Wan L C 2024 *Acta Phys. Sin.* **73** 230301
[30] Xu F, Curty M, Qi B, Lo H K 2013 *New J. Phys.* **15** 113007
[31] Ma X, Fung C H F, Lo H K 2007 *Phys. Rev. A* **76** 012307
[32] Vidal G 2008 *Phys. Rev. Lett.* **101** 110501
[33] Pomarico D 2023 *Dynamics* **3** 622
[34] Browne D E, Rudolph T 2005 *Phys. Rev. Lett.* **95** 010501
[35] Wei Z Y, Malz D, González-Tudela A, Cirac J I 2021 *Phys. Rev. Res.* **3** 023021
[36] Qi J, Yu C Q, Yuan R Y, Yang Z, Ren B C 2025 *Opt. Laser Technol.* **192** 113385
[37] Scherer A, Sanders B C, Tittel W 2011 *Opt. Express* **19** 3004
[38] Pfeifer R N C, Evenbly G, Vidal G 2009 *Phys. Rev. A* **79** 040301
[39] Deng J J, Lu F Y, Zhong Z Q, et al. 2025 *Phys. Rev. Appl.* **24** 044045
[40] Liu J Y, Ma X, Ding H J, Zhang C H, Zhou X Y, Wang Q 2023 *Phys. Rev. A* **108** 022605
[41] Erkilic O, Conlon L, Shajilal B, Kish S, Tserkis S, Kim Y S, Lam P K, A S 2023 *npj Quantum Inf.* **9** 29
[42] Tan H, Li W, Zhang L, Wei K, Xu F 2021 *Phys. Rev. Appl.* **15** 064038
[43] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z L, Shields A J 2015 *Phys. Rev. X* **5** 031030
[44] Berezutskii A V, Luchnikov I A, Fedorov A K 2025 *Phys. Rev. Res.* **7** 013063