Title	Scalable and verifiable quantum secret sharing with photonic efficiency via quasicausal cones in the multiscale entanglement renormalization ansatz framework
Author(s)	Hong Lai, Zhongrui Huang, Li Ren, Josef Pieprzyk, Qibin Zhao and Leongchuan Kwek

Scalable and verifiable quantum secret sharing with photonic efficiency via quasicausal cones in the multiscale entanglement renormalization ansatz framework

Hong Lai [1,2,*] Zhongrui Huang [1] Li Ren,[1] Josef Pieprzyk [3,4] Qibin Zhao [5] and Leongchuan Kwek[2,6,7,8]

[1]*School of Computer and Information Science, Southwest University, Chongqing 400715, China*

[2]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*

[3]*Data61, CSIRO, Sydney, New South Wales 2122, Australia*

[4]*Institute of Computer Science, Polish Academy of Sciences, Warsaw 01-248, Poland*

[5]*RIKEN Center for Advanced Intelligence Project, Tokyo 103-0027, Japan*

[6]*MajuLab, UMI No. 3654, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore 117543, Singapore*

[7]*National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore*

[8]*Quantum Science and Engineering Centre, Nanyang Technological University, Singapore 639798, Singapore*

(Received 29 October 2024; accepted 22 January 2025; published 5 February 2025)

Quantum secret sharing (QSS) is set to revolutionize secure communication. However, achieving practical implementations that balance efficiency, security, and flexibility remains a significant challenge. To address this issue, we propose an innovative QSS scheme that integrates a verification mechanism for the distribution process by leveraging quasicausal cones within the multiscale entanglement renormalization ansatz framework. This approach ensures the secure dissemination of entangled photons across a multiuser network while enhancing the integrity of the quantum state against disturbances. A key feature of our scheme is the application of quasicausal cones, which improve the system's fault tolerance and recovery precision, preserving quantum state coherence and stability even in the presence of errors or losses. The recursive and hierarchical design of our framework enables it to dynamically adapt to fluctuations in network size and the number of participants, making it well suited for large-scale quantum networks. Furthermore, our method reduces the costs associated with photon transmission and storage, enhancing resource allocation within expansive quantum networks. The strategic incorporation of quasicausal cones represents a major advancement, streamlining the flow of quantum information and minimizing the overall resource footprint. By flexibly accommodating varying network sizes and configurations, our scheme marks a significant step towards efficient large-scale QSS, underscoring the critical role of quasicausal cones in advancing quantum communication technologies.

DOI: 10.1103/PhysRevA.111.022603

I. INTRODUCTION

Quantum communication is experiencing rapid advancements, driven by its superior security and transmission rates compared to classical methods. Initially limited to point-to-point connections between two users [1], the potential for enhanced communication performance grows significantly as network scale expands, resulting in an exponential increase in the amount of stored information with the growth of the network. The development of large multipartite entangled states presents both a fundamental scientific challenge and a crucial technological milestone for enabling effective quantum communication. Over time, quantum communication has evolved from simple two-user systems to sophisticated multiuser networks, facilitated by the creation of tailored multipartite entangled states [2,3].

Secret sharing is a cryptographic primitive involving multiple users, where secret information is distributed among several participants by a dealer and only an authorized set of participants can collaboratively reconstruct the original secret [4,5]. Quantum secret sharing (QSS) offers enhanced security by leveraging quantum entanglement to protect the secret from eavesdropping and dishonest participants, making it a promising solution for secure information storage in the quantum era [6]. Traditional secret-sharing methods have greatly benefited from quantum technologies, particularly the use of entanglement, a vital resource in quantum information theory [7–13]. However, as the shared entangled state scale expands, communication performance can be significantly enhanced, and the amount of storable information increases exponentially with the accessible entangled state's growth. The creation of larger multipartite entangled states is not only a fundamental scientific challenge but also the key technology enabling quantum communication. Despite considerable research on QSS, optimizing quantum communication costs during transmission, storage, and recovery have received little focus.

Recent advances have addressed some of these inefficiencies. Senthoor and Sarvepalli [14] proposed universal communication-efficient quantum threshold secret-sharing schemes to reduce communication costs. Subsequently, they introduced a general class of communication-efficient QSS schemes, including both threshold and nonthreshold

*Contact author: hlai@swu.edu.cn

variants [15]. Qin *et al.* [16] presented an efficient, secure, and flexible QSS scheme for eight users, leveraging a continuous-variable eight-partite bound entanglement state, which demonstrated a higher key rate with flexible user combinations. Chehimi *et al.* [17] propose a groundbreaking quantum semantic communication framework, leveraging the latest advancements in quantum machine learning and quantum semantic representations. Their framework focuses on extracting and embedding only the most relevant information from classical data into minimal, high-dimensional quantum states. These quantum states are then communicated over quantum channels with high precision, ensuring both quantum communication fidelity and semantic fidelity are maintained. This approach optimizes data transmission by minimizing unnecessary information, improving the efficiency and accuracy of quantum communication systems.

Despite these advancements, scaling QSS schemes to large many-body quantum states and optimizing verification and fault tolerance remain significant challenges. These issues stem from the high demand for quantum resources and the complexity of managing entanglement across multiple participants. As quantum networks grow in size and complexity, the need for scalable and robust QSS schemes becomes increasingly critical. The multiscale entanglement renormalization ansatz (MERA) framework presents a promising solution to these challenges. Originally developed for simulating quantum many-body systems [18–23], the MERA organizes and compresses quantum information hierarchically, making it highly suitable for QSS. We find that one of the key features of the MERA is the use of quasicausal cones, which efficiently track the propagation of quantum information across layers.

In this context, we propose a novel design for QSS by incorporating quasicausal cones into the quantum network architecture. Using these quasicausal cones, defined in the framework of a hierarchical quantum network with the MERA, we are able to optimally distribute entanglement across multiple layers of the network. The quasicausal cone structure ensures efficient propagation of entanglement, allowing for faster recovery of distributed quantum states and reducing communication latency. This approach provides an efficient mechanism for interconnecting more users while balancing communication efficiency and resource constraints. As such, it shows the potential to implement QSS with an even larger number of users, offering a versatile communication structure that adapts to changing network demands. This combination of advanced entanglement generation techniques and scalable network architecture paves the way for practical large-scale QSS systems.

The primary contributions of this paper are summarized as follows.

(i) *Definition of quasicausal cones.* We define quasicausal cones as regions of influence within the MERA network, which enable selective reconstruction of quantum states without needing to process the entire system. This concept serves as a foundational mechanism for scalability, verifiability, and fault tolerance in our scheme.

(ii) *Scalability through quasicausal cones.* The hierarchical structure of the MERA network, where the depth grows logarithmically with the size of the quantum state, allows the scheme to handle larger quantum states and more participants. By utilizing quasicausal cones, the flow of quantum information is confined to specific paths, reducing operational complexity while maintaining efficiency.

(iii) *Fault tolerance through quasicausal cones.* The quasicausal cone structure enhances fault tolerance, ensuring that even in the event of partial qubit loss or participant failure, the recovery of the original quantum state remains robust. The shared quantum states distributed along the quasicausal cones enable dynamic adjustments, preventing global errors.

(iv) *Verification through quasicausal cones.* The quasicausal cones keeps the natural structure of a MERA network, built by alternating layers of unitary U and isometric W operations, inherently provides a mechanism for verifying participants' secret shares. The presence of common photons in both U and W operations allows for layer validation during the recovery process, achieving verification.

The rest of the paper is organized as follows. Section II details the mathematical formulation of quasicausal cones within the MERA. Section III describes our QSS based on quasicausal cones. The performance analysis is presented in Sec. IV. Section V summarizes the paper.

II. BACKGROUND

This section provides a comprehensive overview of the multiscale entanglement renormalization ansatz algorithm and the critical concept of the quasicausal cone in quantum networks.

A. Entanglement renormalization

Let us define the Hilbert space before renormalization as

$$H \equiv \bigotimes_{s\in\mathcal{L}} H_s, \tag{1}$$

where s represents a site on the lattice $\mathcal{L}$. After renormalization, the Hilbert space transforms into

$$H' \equiv \bigotimes_{s'\in\mathcal{L}'} H'_{s'}, \tag{2}$$

where s' refers to a renormalized site on the new lattice $\mathcal{L}'$.

Through the coarse-graining process, each postrenormalization site s' corresponds to a set of sites $\{s\}$ (referred to as a block $B \subset \mathcal{L}$) in the original lattice. The relationship between the pre- and postrenormalized Hilbert spaces is described by the linear map [see Figs. 1(b) and 1(c)]

$$w : H'_{s'} \to H_B = \bigotimes_{s\in B} H_s, \tag{3}$$

where w is an isometry that satisfies $w^\dagger w = I$ (see Fig. 1). The isometry ensures that the inner product in the smaller Hilbert space is preserved when mapped to the larger space:

$$\begin{aligned} &|\psi\rangle \to w|\psi\rangle, \quad |\phi\rangle \to w|\phi\rangle, \\ &w^\dagger w = I \Rightarrow \langle\phi|\psi\rangle = \langle\phi|w^\dagger w|\psi\rangle. \end{aligned} \tag{4}$$

The isometry w forms the foundation of the hierarchical structure crucial to multiscale approaches such as the MERA. While w is not invertible, in some contexts, an inverse

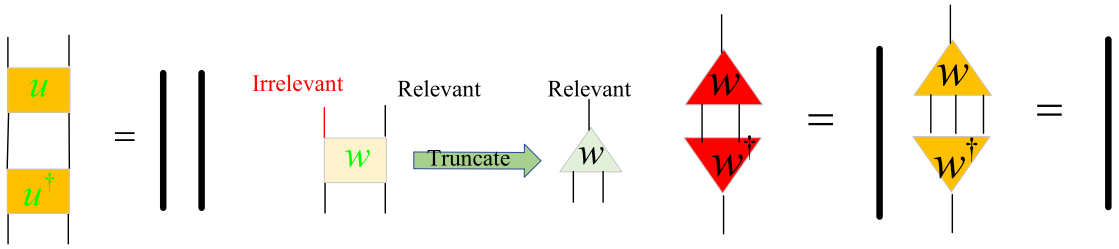

FIG. 1. (a) Detailed action of the isometry W and disentanglers U within the MERA framework, illustrating the role of $W^\dagger$ in the coarse-graining process. The black vertical lines represent the identity matrix of order 2, indicating the layer where these operations occur. (b) Binary isometric operation involving two-qubit transformations. (c) Ternary isometric operation, pertaining to three-qubit processing.

mapping w' can be defined

$$w' : \bigotimes_{s\in B} H_s \to H'_{s'}. \tag{5}$$

The coarse-graining process, which involves unitary transformations combined with projections, reorganizes degrees of freedom within blocks into high-energy short-range components (discarded) and low-energy long-range components (retained).

B. Disentanglers and coarse graining

In the next step, short-range entanglement is reduced using local unitary transformations called disentanglers. These transformations are applied across block boundaries, for example, in one-dimensional systems

$$U = \bigotimes_{i\in\partial} u_i, \quad u_i u_i^\dagger = u_i^\dagger u_i = I, \tag{6}$$

where u_i is a local unitary operator [see Fig. 1(a)]. This disentangling minimizes short-range entanglement before further coarse graining.

Thus, entanglement renormalization involves two essential steps: boundary disentangling $|\Psi\rangle \to U|\Psi\rangle$ and coarse graining $U|\Psi\rangle \to WU|\Psi\rangle$. As the process continues, short-range entanglement is progressively reduced, while long-range entanglement properties of the quantum state are extracted at each iteration.

C. Multiscale entanglement renormalization ansatz

One of the central ideas of the MERA is to efficiently compress and renormalize quantum states by redistributing entanglement across different scales [21]. The MERA is particularly effective for systems with long-range entanglement, and its hierarchical structure allows quantum states to be systematically coarse grained across multiple layers.

The MERA employs two essential components: disentanglers U, i.e., local unitary transformations that minimize entanglement within a local region while preserving global properties of the quantum state, and isometries W, i.e., operations that preserve the norm of quantum states and are used in the coarse-graining process to compress information while maintaining the integrity of the system's entanglement structure. The hierarchical structure of MERA efficiently encodes ground states of quantum many-body systems, particularly in critical systems or those with scale invariance, due to its logarithmic scaling in computational complexity [24–26]. Notably, at the base layer of a MERA network, the system is described as a matrix product state (MPS), which is defined as follows (from [27]).

Definition 1. An MPS representation of any many-body state is defined as

$$|\psi\rangle = \sum_{s_1 s_2 \cdots s_{n-1} s_n} \sum_{a_1 a_2 \cdots a_{n-2} a_{n-1}} A^{s_1}_{a_1} A^{s_2}_{a_1 a_2} \cdots A^{s_{n-1}}_{a_{n-2} a_{n-1}} A^{s_n}_{a_{n-1}} \times |s_1 s_2 \cdots s_{n-1} s_n\rangle,$$

where $A^{s_1}_{a_1}$ and $A^{s_n}_{a_{n-1}}$ represent rank-2 tensors, while $A^{s_2}_{a_1 a_2}, \cdots, A^{s_{n-1}}_{a_{n-2} a_{n-1}}$ represent rank-3 tensors.

The above relation can be simplified as

$$|\psi\rangle = \sum_{s_1 s_2 \cdots s_n} A^{s_1} A^{s_2} \cdots A^{s_{n-1}} A^{s_n} |s_1 s_2 \cdots s_{n-1} s_n\rangle.$$

In contrast to the MPS [27], the bond dimensions in the MERA do not need to increase as the system size grows. Moreover, the MERA facilitates the extraction of critical properties, such as operator scaling dimensions, for one-dimensional systems [28].

Using the three-photon many-body state $|\psi\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |011\rangle + |110\rangle)$ as an example, one of the representations (which is not unique) of the MPS that corresponds to the many-body state $|\psi\rangle$ is

$$\begin{aligned} |\Psi\rangle = &\begin{pmatrix} \frac{1}{\sqrt{3}} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} |001\rangle \\ &+ \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} |011\rangle \\ &+ \begin{pmatrix} 0 & \frac{1}{\sqrt{3}} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} |110\rangle, \end{aligned} \tag{7}$$

where the coefficient (i.e., the probability amplitude) $\frac{1}{\sqrt{3}}$ for states $|001\rangle$, $|011\rangle$, and $|110\rangle$) is written as the product of three matrices.

D. Quasicausal cone in the MERA

Building upon Vidal's causal cone framework [21], we introduce the quasicausal cone as an efficient method for tracking the flow of entanglement and information within the network. This approach facilitates the transition from simulation to quantum communication by ensuring that quantum information follows paths sufficient to reconstruct the original quantum state (recoverability principle). In the context of the MERA, we define the quasicausal cone through the following four essential points.

(i) Starting point. The quasicausal cone must begin at the first node of the initial layer, ensuring that the quantum information enters the network at the correct location.

(ii) Propagation through operations U and W. The quantum information should propagate through nodes influenced by disentanglers U and isometries W, allowing for proper compression, decompression, entanglement, and disentanglement of quantum information.

(a) Disentanglers U. These affect two adjacent nodes, performing disentangling operations in the downward direction and entangling operations in the upward direction.

(b) Isometries W. These affect either two or three nodes [see Fig. 1(c)]. In the downward direction, W compresses information, while in the upward direction, it decompresses information.

(iii) End point. The quasicausal cone must conclude at the last node of the initial layer.

(iv) Recoverability principle. The quantum information along the quasicausal cone path must be sufficient to reconstruct the original quantum state.

Note that the quasicausal cone described in the paper is inherently asymmetric. This asymmetry arises due to the random selection of disentangling and isometric operations in our scheme, particularly the use of binary and ternary isometric operations. These random choices result in quantum states between layers that lack symmetry.

We present the main procedure for constructing the quasicausal cone in a MERA network in Algorithm 1.

The quasicausal cone exhibits four key properties.

(i) Nonuniqueness. The unitary (U) and binary or ternary (W) operations are selected at each layer randomly. This randomness in selecting the U and W leads to variability in the specific operations and entangled photons involved in reconstructing the quantum state. Consequently, the quasicausal cone is not unique (see Fig. 2).

(ii) Locality and limited influence. Each entangled photon at lower layers of the MERA only affects a restricted set of qubits in the higher layers. As a result, the communication needed to measure local observables is confined to the quasicausal cone of the corresponding qubits, reducing overall communication costs.

(iii) Recursive nature. As the quantum state propagates downward, the quasicausal cone expands with each layer. The action of W compresses the state, reducing the number of effective degrees of freedom, while the disentanglers U distribute information across a broader set of qubits.

(iv) Stability of the quasicausal cone structure. Information in the MERA follows well-defined paths, ensuring that local operations affect only a finite number of entangled photons.

ALGORITHM 1. Quasicausal cone in the MERA network.

Input: n (number of particles)
Output: Quasicausal cone path *causal_cone*
$D_{\max} \leftarrow \lceil \log_2(n) \rceil$
$D_{\min} \leftarrow \lceil \log_3(n) \rceil$
$D \leftarrow$ RANDOMLAYER($D_{\min}, D_{\max}$)
causal_cone $\leftarrow [0]$
current_node $\leftarrow 0$
for *layer* $\leftarrow 1$ to D **do**
  if ISBINARYLAYER(*layer*) **then**
    current_node $\leftarrow$ APPLYDISENTANGLERU (*current_node*, 2)
    next_node $\leftarrow$ APPLYISOMETRYW(*current_node*, 2)
  else
    current_node $\leftarrow$ APPLYDISENTANGLERU (*current_node*, 2)
    next_node $\leftarrow$ APPLYISOMETRYW(*current_node*, 3)
  end if
  APPEND (*causal_cone*, *next_node*)
  current_node $\leftarrow$ *next_node*
end for
return *causal_cone*

This structure stabilizes the propagation of information, preventing the spread of global errors and localizing the effects of perturbations within the system.

Figure 2 illustrates the structure of a quasicausal cone in a MERA network. Note that the quasicausal cone does not span the entire system, but maintains a finite width as it traverses multiple layers. Furthermore, as the number of layers increases, the entanglement between photons follows a power-law relationship, as depicted in Fig. 3. This implies that although the entanglement may weaken, it does not completely vanish.

E. Applications of quasicausal cones in quantum secret sharing

The concept of causal cones, originally developed for quantum simulations [21], can be extended to quantum network communication. We introduce the notion of the quasicausal cone, which is particularly beneficial in applications like QSS in the next section. By organizing the propagation of entangled photons along a quasicausal cone, quantum resources are distributed efficiently and locally, optimizing network performance in terms of scalability, fault tolerance, and security. Furthermore, it reduces communication overhead by limiting operations to those within the quasicausal cone, thus minimizing the overall communication cost in quantum networks.

III. QUANTUM SECRET SHARING BASED ON THE QUASICAUSAL CONE IN THE MERA

In this section we develop a quantum-secret-sharing scheme by leveraging the quasicausal cone of the MERA. The scheme involves three primary roles: the dealer, participants, and the combiner.

Dealer. The dealer holds a secret, represented as a matrix product state $|\psi\rangle$ of n photons. This state is encoded

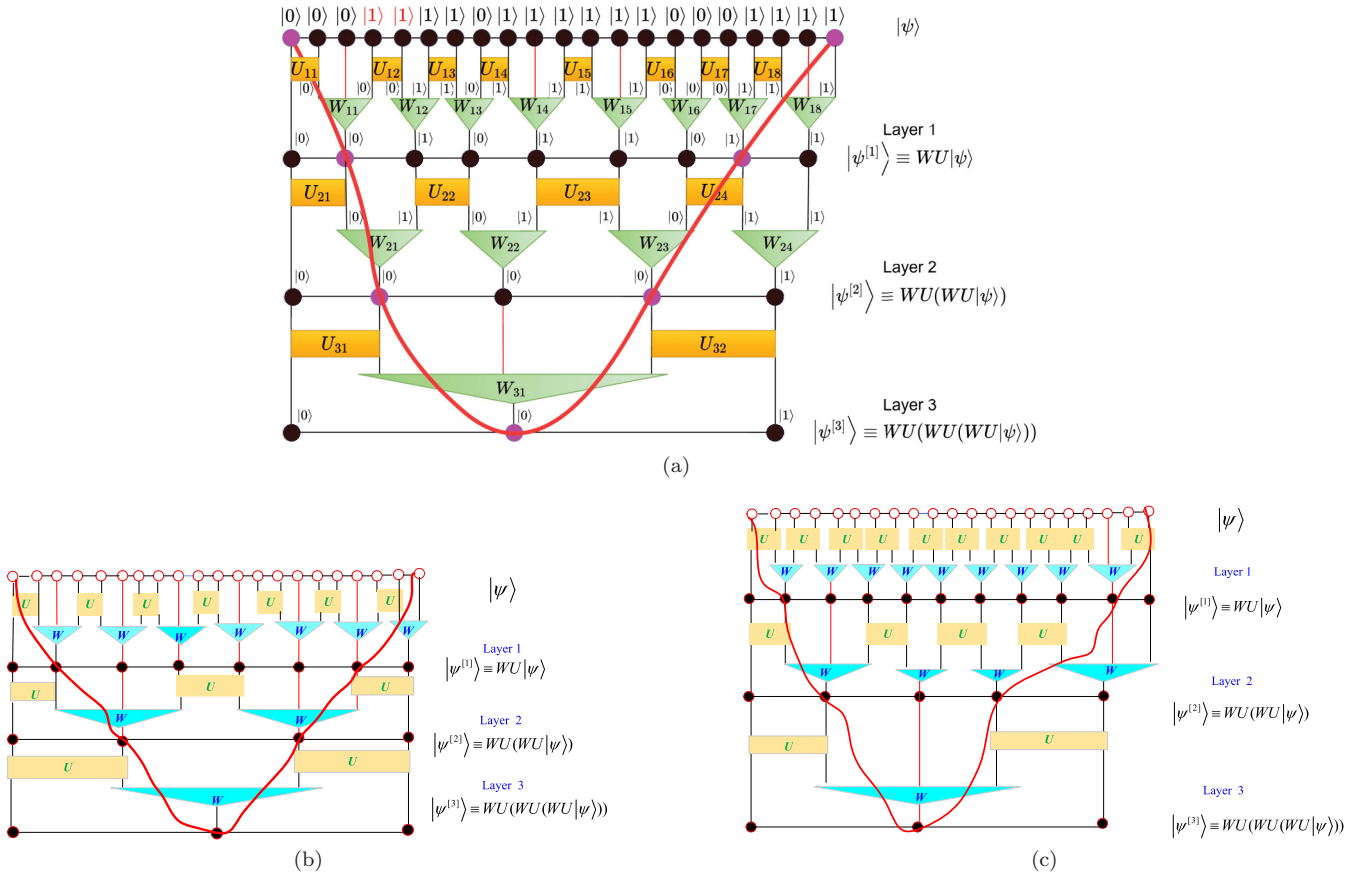

FIG. 2. (a) Schematic representation of a quasicausal cone within a MERA network. The red path illustrates the propagation of influence from a single entangled photon through successive layers of the network. As the qubit's influence moves downward, it only impacts a specific subset of qubits in the lower layers, thereby demonstrating the causal structure of the MERA. In (a)–(c) the red vertical lines specifically indicate ternary isometric operations that involve three-qubit processes. (b) and (c) Two variations of the quasicausal cones of the MERA network, obtained by using different choices of the isometry W and disentangler U. These variations lead to different ways in which the quantum information is renormalized and distributed across the layers.

across L layers of the MERA using disentangling operators $U^{[l]}$ and isometry operators $W^{[l]}$. The dealer computes the shares of $|\psi\rangle$ and distributes them to $L+1$ participants. The access structure of the secret requires the participation of all $L+1$ participants, thus constituting an $(L+1, L+1)$ secret-sharing scheme.

Participants. The participants receive both quantum and classical secret shares from the dealer, transmitted through quantum and classical channels, respectively.

Combiner. The combiner is the participant located at the initial layer of the quasicausal cone. The combiner collaborates with the dealer to predetermine whether the state obtained through the $W^{\dagger}$ operation is $|10\rangle$ or $|01\rangle$, or alternatively $|00\rangle$ or $|11\rangle$, depending on whether W_{li} $(l = 1, 2, \ldots, L)$ in the layer's position is even or odd.

The quasicausal cone's structure, consisting of alternating layers of unitary U and isometric W operations, allows for the verification of participants' secret shares in a downward-to-upward manner, ensuring the integrity of the recovery process. The recursive nature of the MERA network, whose depth scales logarithmically with system size, significantly reduces quantum communication overhead by focusing solely on the essential parts of the network required for state reconstruction.

As a result, this approach provides an efficient, fault-tolerant, verifiable, and scalable solution for QSS, making it suitable for practical applications in quantum networks. The detailed steps of the QSS scheme are described as follows.

Step 1: Initialization of the shared state and identification of the quasicausal cone. The MERA of L layers is initialized with the shared quantum state at the initial layer denoted by $|\psi\rangle$. Each layer applies unitary operations U and isometry operations W, compressing $|\psi\rangle$ while encoding correlations between qubits through the quasicausal cone to higher layers (see Fig. 2). These correlations are distributed as entangled photons among participants in the network. The state in the lth layer is represented as

$$|\psi^l\rangle = W^l U^l |\psi^{l-1}\rangle, \tag{8}$$

where $|\psi^0\rangle = |\psi_{\text{secret}}\rangle$ is the original layer state. The quasicausal cone shows which qubits are involved in the propagation of quantum information through layers, as represented by the red curve in Fig. 2. This recursive encoding efficiently compresses the quantum information, preserving its essential features across layers.

The dealer initiates the distribution of entangled photons by identifying the quasicausal cone associated with the state

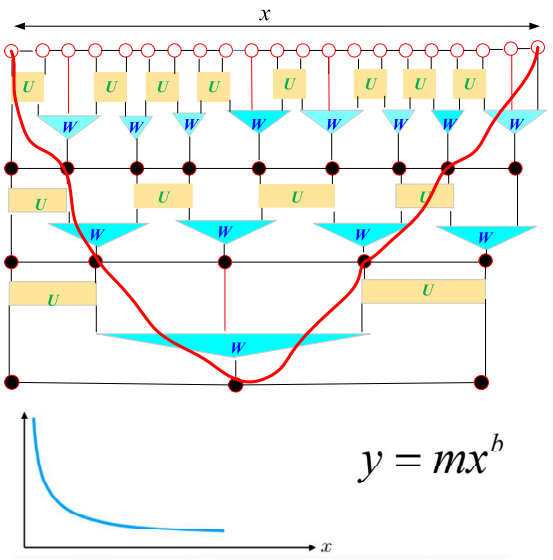

FIG. 3. Quasicausal cone in a MERA network capturing power-law correlations, where $x > 0$, $b < 0$, and $m > 0$.

$|\psi\rangle$. As depicted in Fig. 4 and traced by the red curve, this cone highlights the critical entangled photons and operations necessary for reconstructing the state $|\psi\rangle$. By focusing on the relevant photons within the cone, this quasicausal structure significantly reduces the number of operations required.

Step 2: Distribution of secret shares along the quasicausal cone. Entangled photons are distributed to participants as secret shares based on their positions in each layer of the quasicausal cone. The transmission of these photons is safeguarded through the use of decoy particles. For instance, if two entangled photons are located in the second layer of the quasicausal cone, both photons are assigned to the same participant. If only one entangled photon exists in a given layer, that photon is assigned to the corresponding participant.

Following this distribution strategy, most participants receive two entangled photons, with one participant receiving only one. Those who receive two photons utilize one for recovering the shared secret state and the other to verify the honesty of the participants and the correctness of the recovered secret. Meanwhile, the unitary operations U and

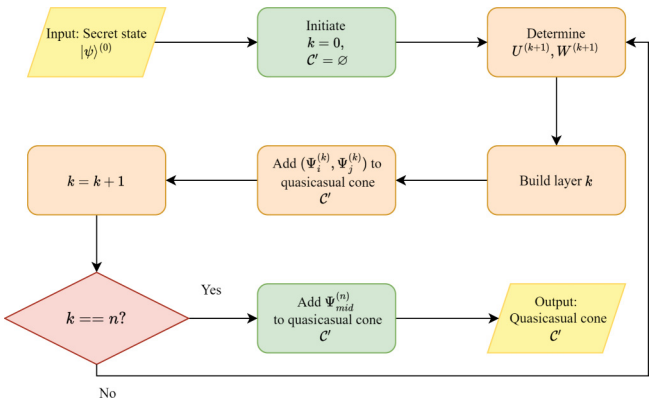

FIG. 4. Flowchart for a quasicausal cone in a quantum network.

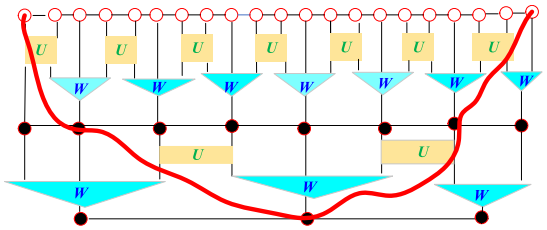

FIG. 5. Possible way to draw causal cones when the number of participants decreases based on Fig. 2.

isometry operations W for each layer are transmitted to the corresponding participants via classical channels.

Step 3: Verification and recovery of the shared state. After receiving the entangled photons along the quasicausal cone, all participants collaboratively recover the shared state $|\psi_{\text{secret}}\rangle$, following a process that proceeds from the lower layers upward.

Specifically, during this process, with their classical and quantum shares, the combiner uses all participants' information to verify the honesty of the other participants. If all participants are deemed honest, the combiner proceeds with recovering the secret state. Otherwise, the recovery process is aborted.

The Appendix provides a detailed illustration of the complete computation process for implementing our scheme.

IV. PERFORMANCE ANALYSIS

The quasicausal cone provides a significant advantage for efficient quantum information processing in QSS, particularly when dynamic adjustments to the number of participants or the scale of the network are required. By utilizing entangled photons along quasicausal cone pathways, the honesty of participants can be verified, ensuring that only legitimate participants can reconstruct the secret. This approach enhances the security of the QSS scheme.

Furthermore, distributing quantum states along these pathways reduces the number of required qubits, which in turn lowers quantum storage costs. This results in more efficient utilization of quantum resources, thereby achieving a quantum advantage in QSS. We further describe these properties in QSS.

A. Dynamic properties in QSS using quasicausal the cone

In a QSS scheme utilizing the quasicausal cone, the system is designed to dynamically adapt to changes in the number of participants being added or removed (see Figs. 5 and 6) through adjustments in the frequency of binary and ternary isometric operations, as well as various disentanglement operation matrices. By fine-tuning both isometric and disentanglement operations, the shared state can be effectively distributed across different layers to various participants, ensuring that the secret can only be recovered when all participants cooperate. The detailed processes are outlined in the following.

Isometric operators in the MERA network. Let the isometric operator W^l at layer l of the MERA network act on either two or three qubits, depending on whether it is binary or ternary.

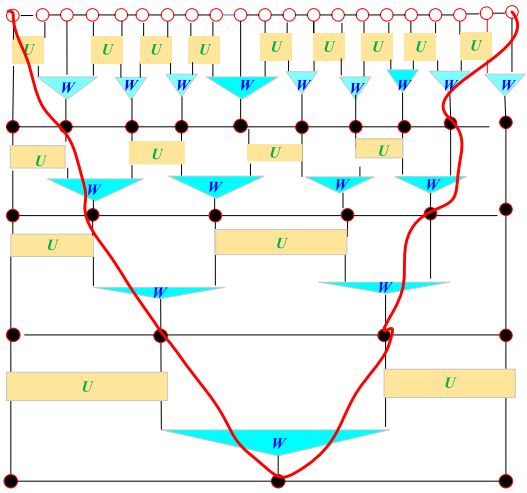

FIG. 6. Possible way to draw causal cones when the number of participants increases based on Fig. 2.

The operator is defined as

$$W^l : \mathcal{H}_2^{\otimes n} \to \mathcal{H}_2^{\otimes n'},$$

where $\mathcal{H}_2$ is the Hilbert space of a qubit and n and n' are the dimensions of the input and output states, respectively, at layer l. Specifically, he binary isometric operator acts on two qubits at a time

$$W^l_{\text{binary}} : \mathcal{H}_2 \otimes \mathcal{H}_2 \to \mathcal{H}_2$$

and the ternary isometric operator acts on three qubits

$$W^l_{\text{ternary}} : \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2 \to \mathcal{H}_2.$$

This flexibility allows our scheme to alternate between binary and ternary isometric operators depending on the number of participants and the required quantum operations for state reconstruction.

Step 1. Reassessing the network structure. The total number of layers L of the MERA is given by $L = \log_2(n)$ for the binary MERA or $L = \log_3(n)$ for the ternary MERA, where n represents the number of photons in the many-body state in the scheme. As the number N of participants increases, the MERA network is restructured into a quasiconic configuration to accommodate additional layers (see Fig. 6). Entangled photons along the cone of each new layer, together with the U and W operations for that layer, are distributed to the new participants. Conversely, when participants leave, the MERA is adjusted to form a quasiconic configuration with fewer layers (see Fig. 5). This refined structure presents the increase or reduction in the network as symmetrical steps because two isometric operations are used in our scheme

Step 2. Adjusting the hierarchy of operations. The operations U^l and W^l, which act at each layer l, need to be modified. For instance, in the case where a new participant is added, new operators W^{l+1} and U^{l+1} must be introduced at layer $l+1$ to integrate the new participant.

If $N \to N+1$, the change in hierarchy can be modeled as

$$U^{[l]}(N+1) = U^{[l]}(N) \oplus U^{[l]}_{\text{new}}(N+1),$$
$$W^{[l]}(N+1) = W^{[l]}(N) \oplus W^{[l]}_{\text{new}}(N+1),$$

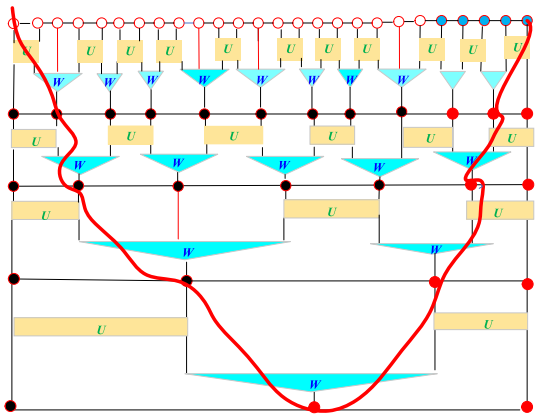

FIG. 7. Possible way to draw causal cones when the number of many-body states increases based on Fig. 2.

where $U^{[l]}_{\text{new}}(N+1)$ and $W^{[l]}_{\text{new}}(N+1)$ account for the new participant's state and $\oplus$ represents the addition of new information. Note that the focus here is on the overall U and W for a particular layer rather than specific mathematical expressions of U and W within that layer.

Step 3. Share redistribution. When participants are added or removed, shares (such as entangled photons and W and U) must be redistributed to participants involved.

B. Scalability in our QSS using the quasicausal cone

Assume the initial state $|\psi\rangle$ consists of n qubits. The depth D of the MERA network scales logarithmically with n as $D \sim \log_2(n)$ for the binary MERA or $D \sim \log_3(n)$ for the ternary MERA. This logarithmic scaling ensures that our scheme remains scalable, a critical feature for the practical deployment of QSS schemes in large-scale quantum networks. Leveraging the hierarchical and logarithmic properties of the MERA structure and the efficiency of quasicausal cones, our scheme enables dynamic and secure secret sharing across an expanding number of participants and an increasing number of qubits in the shared many-body state (see Figs. 5–8). This scalability supports efficient resource usage and robust

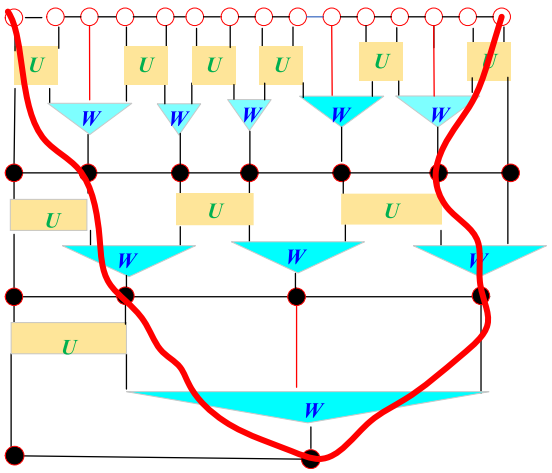

FIG. 8. Possible way to draw causal cones when the number of many-body states decreases based on Fig. 2.

security, making the scheme adaptable to the evolving needs of quantum communication networks.

The key aspects of scalability in our scheme are as follows.

(i) Handling larger networks. As the number of participants increases, our scheme integrates new members without significantly increasing complexity or resource consumption, due to the quasicausal cone in the MERA. For example, participants can be added dynamically by updating only part of the network.

(ii) Efficient resource management. Our scheme efficiently manages quantum resources, minimizing the number of photons required as the network grows. This reduces transmission and storage costs, crucial for managing fragile and costly quantum resources.

(iii) Dynamic reconfiguration. Participants in quantum networks may join or leave dynamically. Our scheme adjusts secret shares without requiring a full system reconstruction. For example, when a participant leaves, the quasicausal cone can be modified to exclude them while preserving the network's integrity.

(iv) Maintaining security in expanding networks. Ensuring security becomes increasingly challenging as networks grow. Our scalable QSS scheme ensures the secure distribution of quantum states, protecting the confidentiality of the shared secret as the network expands.

(v) Supporting quantum network expansion. As quantum networks expand over larger distances and more participants, our scalable QSS scheme enables the growth of robust and secure quantum communication infrastructures.

The design of quantum networks can leverage the multilayer structure of the MERA to recursively handle entanglement swapping, generating entangled states from local to remote scales. This hierarchical structure not only enhances the scalability of quantum networks but also effectively reduces resource consumption.

C. Layered verification mechanism in our QSS using the quasicausal cone

In our QSS scheme, the layered structure of the MERA allows participants to verify and recover information through entanglement and renormalization operations at different layers. This design enables information verification at each layer, ensuring the honesty of each participant.

Let the participants in the scheme be indexed as $P_1, P_2, \ldots, P_N$, where P_N is the highest index and P_1 is the lowest. Each participant holds their classical secret shares and quantum secret shares, which are used to verify the honesty of their peers through the bottom-up nature of the verification process in a layered MERA network.

Define the quasicausal cone C_q as the layered structure of information held by the participants, where each layer corresponds to a different set of participants and their associated quantum states.

Proof. Let P_k represent a participant in the scheme. Each participant P_k $(k = 2, 3, \ldots, N)$ holds two quantum states $|\psi_1^{k-1}\rangle$ and $|\psi_2^{k-1}\rangle$. To verify the honesty of the $(k+1)$th participant, P_1 combines the information from P_{k+1} with one of the quantum states $|\psi_1^{k-1}\rangle$ that P_k possesses.

Let the secret share of P_{k+1} be denoted by S_{k+1}. Using the information provided by S_{k+1} and the quantum state $|\psi_1^{k-1}\rangle$, the participant P_1 can reconstruct the state $|\psi_2^{k-1}\rangle$ as $|\psi_2^{k-1}\rangle = f(|\psi_1^{k-1}\rangle, S_{k+1})$, where $f(\cdot)$ is a reconstruction function that takes the quantum state and secret share as inputs.

Once P_1 has reconstructed the state $|\psi_2^{k-1}\rangle$, it compares the reconstructed state with the original state $|\psi_2^{k-1}\rangle$ from P_{k+1}. If the condition $|\psi_2^{k-1}\rangle = |\tilde{\psi}_2^{k-1}\rangle$ holds, where $|\tilde{\psi}_2^{k-1}\rangle$ is the reconstructed state, then the participant P_{k+1} is considered honest. If the states do not match, P_{k+1} is deemed dishonest.

This verification process can be applied iteratively from P_N to P_2. For example, P_1 can use the information from P_4 and the quantum state $|\psi_3^1\rangle$ to verify P_4's honesty. Similarly, P_1 can verify P_3 and so on, creating a layer of verification across the scheme.

The verification of each participant's honesty relies on the transmission of photons, which carry the quantum states $|\psi_1^{k-1}\rangle$ and $|\psi_2^{k-1}\rangle$. These photons are distributed according to the layers of the quasicausal cone, ensuring that each participant has the necessary information to perform the verification. ■

D. Fault tolerance in our QSS using the quasicausal cone

The fault tolerance of our QSS can be formally described through the mathematical relationships governing its operations. By leveraging hierarchical entanglement, effective error-correcting operations, information redundancy, and careful transmission design, the MERA framework maintains robustness against errors. Each of these aspects contributes to the overall reliability and stability of quantum information within the network, ensuring effective recovery and preservation of quantum states despite local perturbations. A detailed discussion follows.

Hierarchical entanglement structure. The MERA structure consists of layers of isometric and unitary transformations that establish a hierarchy of entanglement. Let us denote the quantum state at layer l by $|\psi^l\rangle$. The transition between layers can be represented as $|\psi^{[l]}\rangle = W^{[l]}U^{[l]}|\psi^{[l-1]}\rangle$. This hierarchical structure allows for error correction since each layer encapsulates the entanglement information of the previous layer, enabling recovery even if lower layers are perturbed.

Error-correcting operations U and W. The disentangling operations U and isometries W work effectively to limit error propagation. If a local error E occurs at layer l, we can model this as $|\tilde{\psi}^l\rangle = E|\psi^l\rangle$. After the error occurs, the subsequent state becomes

$$|\tilde{\psi}^{l+1}\rangle = U^{[l]}W^{[l]}|\tilde{\psi}^l\rangle = U^{[l]}W^{[l]}E|\psi^l\rangle.$$

The isometric and unitary operations are structured so that the norm of the error is contained, i.e.,

$$\|U^{[l]}W^{[l]}E\| \leqslant \|U^{[l]}W^{[l]}\| \times \|E\|.$$

This signifies that the norm of the error in the transformed state $|\tilde{\psi}^{l+1}\rangle$ is bounded by the product of the norms of $U^{[l]}W^{[l]}$ and E. This inequality shows isometric properties, i.e., the norm of $W^{[l]}$ typically is equal to 1, meaning it does not increase error magnitude, and error containment, i.e., the product $\|U^{[l]}W^{[l]}\| \times \|E\|$ effectively caps how large the error can grow as it propagates. Therefore, any local error E is

controlled as it ascends through the layers, limiting its disruptive potential.

By limiting error growth at each transformation, our scheme ensures that even if an error occurs, it will not overwhelm the entire quantum state or the encoded secret. This containment maintains the integrity of the encoded information and protects against severe disruptions in higher layers of the hierarchical structure. In essence, this inequality serves as a mathematical safeguard. It limits the spread and growth of errors across layers, ensuring that any local error does not lead to significant degradation of the entangled state. This control mechanism is essential for the robustness of the MERA-based QSS, enhancing its resilience to errors in real-world applications.

Local error correction and information redundancy. The MERA introduces redundancy to mitigate the effects of local errors. For any qubit error at site i, the corrected state can be approximated by leveraging the surrounding nodes $|\hat{\psi}^l\rangle = R_i(|\tilde{\psi}^l\rangle)$, where R_i represents a recovery operation that utilizes information from neighboring qubits to correct the error. The redundancy helps to ensure that the overall stability of the quantum state remains intact.

Error recovery in compression and decompression. As information is transmitted through the MERA structure, errors are filtered out during the compression and decompression phases. The downward flow can be described as

$$|\psi_{\text{compressed}}\rangle = \mathcal{C}(|\psi^l\rangle) = \prod_{j=1}^{m} W_j U_j |\psi^{l-j}\rangle,$$

where $\mathcal{C}$ is a compression operation involving the disentangling and isometric operations U_j and W_j over l layers. During upward transmission

$$|\psi_{\text{recovered}}\rangle = \mathcal{D}(|\psi_{\text{compressed}}\rangle) = \prod_{l=1}^{m} U_j^\dagger W_l^\dagger |\psi_{\text{compressed}}\rangle.$$

The redundancy and layered operations effectively reconstruct the original quantum state, filtering out transmission errors.

V. SECURITY AGAINST COLLUSION ATTACKS BY DISHONEST PARTICIPANTS

In this section we provide a rigorous mathematical analysis of the security measures embedded in our QSS scheme, particularly focusing on its resistance to collusion attacks by dishonest participants. By leveraging the layered structure of quasicausal cone in the MERA, this scheme imposes inherent constraints on information accessibility, allowing for secure verification and ensuring that no subset of colluding participants can reconstruct the secret without full cooperation. The detailed analysis proceeds are as follows.

Entanglement constraints imposed by the layered structure of the MERA. In our QSS scheme, each participant's share of the secret is represented by a quantum state $|\psi^i\rangle$ forming a hierarchical structure, with the root node containing the secret state $|\psi_{\text{secret}}\rangle$. Due to the recursive nature of the MERA structure, each layer's state is linked to the previous layer through isometric operators W and disentangling unitary operators U. This process imposes specific entanglement constraints at each layer.

For example, the isometric operator W^l at level l compresses the lower-dimensional state at level $l-1$ to a higher-dimensional state at level l. Mathematically, this can be represented as $|\psi^{l-1}\rangle = U_l^\dagger W_l^\dagger |\psi^l\rangle$. This hierarchical compression limits the potential for colluding participants to retrieve complete information from the higher layers, as each layer restricts information based on the quasicausal cone structure.

Information irreversibility in the compression process. The quasicausal cone structure of the MERA introduces irreversible information loss in each step as higher layers are compressed into lower layers. The dimensionality of each layer is reduced, ensuring that any subset of participants at level $l-1$ can only access a limited view, represented by the reduced density matrix ρ_S, which lacks sufficient rank to reconstruct the full state of $|\psi^l\rangle$: $\text{rank}(|\psi^l\rangle\langle\psi^l|) < \text{rank}(\rho_S)$. This irreversibility ensures that unauthorized participants cannot recover lower-layer information, bolstering the scheme's resistance to partial recovery by colluding subsets.

Layer dependence in the verification process. The hierarchical structure and causal cone dependence allow for sequential layer-by-layer verification, enhancing security against dishonest participants. For instance, participant P_1, acting as the secret combiner, can verify information integrity from lower levels. Sequential verification detects any tampering and identifies dishonest participants, ensuring secure information transmission.

Constraints imposed by the ω operators on unauthorized recovery. The operators W in the MERA necessitate complete knowledge across all layers for full state reconstruction. The decompression process relies on sequential operations from the top down, where the operator chain $\mathcal{C}(W)$ defines full information access: $\mathcal{C}(\omega) = W_1 U_1 W_2 U_2 \cdots W_N U_N$. If any operator W_i or U_i is missing, the chain is incomplete and recovery of $|\psi_{\text{secret}}\rangle$ is blocked, preventing unauthorized access.

Cooperativity requirement for full secret recovery. To fully recover $|\psi_{\text{secret}}\rangle$, cooperation from all participants is necessary. The complete reconstruction condition is expressed by the tensor product

$$|\psi_{\text{secret}}\rangle = \bigotimes_{i=1}^{N} \mathcal{C}(\omega)|\psi_i\rangle,$$

where $\mathcal{C}(\omega)$ is the chain across all layers. Any subset $S \subset \{P_1, \ldots, P_N\}$ fails to reconstruct the secret due to incomplete operator chains:

$$\bigotimes_{i\in S} \mathcal{C}(\omega)|\psi_i\rangle \neq |\psi_{\text{secret}}\rangle.$$

This cooperativity requirement ensures that only with full participation can the secret be recovered, making the scheme robust against collusion and unauthorized access.

A. Efficiency of the quasicausal cone approach

The quasicausal cone plays a central role in enhancing the efficiency of our QSS scheme by reducing the quantum communication cost associated with state recovery. This efficiency arises from limiting the information processing to the qubits

TABLE I. Comparison of QSS approaches and their advantages.

Reference	Key techniques	Communication efficiency	Fault tolerance	Scalability	Dynamic	Verifiability
[6]	GHZ	No	No	No	No	No
[13]	MERA	Yes	No	Yes	Yes	No
[14]	Staircase codes	Yes	No	No	No	No
[15]	Extended CSS codes	Yes	No	No	No	No
[16]	High-dimensional entangled state	Yes	No	No	No	No
This work	Quasicausal cone	Yes	Yes	Yes	Yes	Yes

and operations within the cone, thus avoiding unnecessary computation over irrelevant parts of the quantum network.

The efficiency of the quasicausal cone approach is reflected in the number of entangled photons that need to be processed for state recovery. The number of entangled photons on the quasicausal cone falls within the range $[2\lfloor\log_3(n)\rfloor + 1, 2\lfloor\log_2(n)\rfloor + 1]$, where n represents the number of photons in the many-body state in the scheme. The lower bound $2\lfloor\log_3(n)\rfloor + 1$ corresponds to the case where ternary isometric operators are predominantly used in the MERA network. The upper bound $2\lfloor\log_2(n)\rfloor + 1$ applies when binary isometric operators are used. Thus, the total number of entangled photons required for recovering the quantum state grows logarithmically with the number of participants, ensuring scalability of the scheme.

B. Quantum communication cost

The quantum communication cost refers to the amount of quantum information, in the form of quantum states or entangled photons, that needs to be sent to the participants during the secret recovery process. Since the quasicausal cone reduces the number of operations and qubits involved in state recovery, the quantum communication cost C_q is minimized.

Mathematically, the quantum communication cost can be expressed as $C_q(N) = \sum_{i=1}^{N} \mathcal{Q}_i$, where $\mathcal{Q}_i$ ($Q_i \in \{1, 2\}$) represents the number of quantum states sent to participant P_i during the recovery process. Since $\mathcal{Q}(n)$ grows logarithmically with n, the total quantum communication cost for n participants remains efficient even as the number of participants increases.

To highlight the advantages of our approach, we compare its quantum communication efficiency, fault tolerance, and other key features with several relative QSS schemes [6,13–16]. Table I provides a detailed comparison between different QSS models, demonstrating the benefits of employing the quasicausal cone in terms of efficiency, scalability, fault tolerance, and dynamic adaptability.

Our quasicausal cone method provides a significant improvement in quantum communication efficiency by reducing the number of entangled photons and qubits required for state recovery. Additionally, the logarithmic growth of quantum communication costs relative to the number of participants ensures scalability, making this approach ideal for large-scale quantum networks. By combining fault tolerance, dynamic adaptability, and verifiability, our scheme proves superior in terms of both performance and practicality.

VI. CONCLUSION AND FUTURE WORK

This paper introduces a novel quantum-secret-sharing scheme leveraging the quasicausal cone structure within the MERA framework. By utilizing the quasicausal cone, the scheme significantly reduces the number of transmitted photons, minimizing both transmission and storage costs while enhancing security. The proposed scheme is dynamic, scalable, verifiable, and fault tolerant, ensuring reliable quantum state recovery even in cases of participant or qubit loss.

Scalability is achieved through the logarithmic growth of network complexity, enabling efficient secret sharing among a large number of participants. The quasicausal cone efficiently identifies essential nodes for state reconstruction, while the parameters W and U allow for dynamic adjustments to optimize performance. This design provides a robust scalable solution for quantum communication, ensuring secure and reliable state recovery across diverse network configurations.

Building on this foundation, future work should explore the unique properties of the MERA to enhance many-body entangled state secret sharing. Specifically, we propose extending the current framework to enable the simultaneous sharing of multiple many-body entangled states. Leveraging the layered structure of the MERA, where each layer represents a many-body entangled state, participants could collaboratively reconstruct the states at each layer, ultimately sharing the tensor product of these entangled states. This approach has the potential to inspire new protocols for secure communication, offering both theoretical insights and practical advancements in quantum communication networks.

Despite these advancements, several experimental challenges remain, particularly in scaling QSS schemes to larger networks while maintaining resource efficiency and robustness against noise. The proposed MERA-based framework addresses these challenges by confining quantum information propagation to specific quasicausal paths, thereby minimizing the quantum resources required for entanglement distribution and recovery. Furthermore, the hierarchical structure of the MERA, characterized by logarithmic scaling of the network depth, enables scalability without significant increases in complexity. Its fault-tolerant features, such as entanglement redundancy across layers, mitigate the effects of noise and qubit loss, ensuring resilience under realistic experimental conditions.

To advance this work, several key milestones and technical challenges have been identified. First, the framework

must be generalized to support the encoding and reconstruction of multiple many-body entangled states, which will require adapting the isometric and unitary transformations at each layer. Second, optimizing the allocation of entanglement resources to balance redundancy and efficiency is critical for practical deployment. Finally, developing experimental protocols to test the robustness of the scheme under real-world conditions, such as photon loss and limited qubit connectivity, will be essential. These steps will guide both the theoretical development and experimental realization of the framework, ensuring its viability for large-scale QSS systems.

ACKNOWLEDGMENTS

H.L. was supported by the National Natural Science Foundation of China (Grant No. 61702427); the Natural Science Foundation of Chongqing, China (Grant No. CSTB2022NSCQ-MSX0749), funded by China Scholarship Council (Grant No. 202306990061); and the Southwest University's 2022 School-Level Teaching Reform Program (Grant No. 2022JY086). Q.Z. was supported partially by RIKEN Quantum project. L.K. was supported by the National Research Foundation, Singapore and the Ministry of Education, Singapore.

APPENDIX: EXAMPLE OF OUR PROPOSED SCHEME

As an illustration, let us consider Fig. 2 to introduce the specific steps mentioned above, where the initial state is given by

$$|\psi\rangle = \frac{1}{\sqrt{21}}(|000001101111110001111\rangle + |11111111111111111111\rangle + \cdots + |01010101010101010101\rangle). \tag{A1}$$

At the first layer adjacent to the initial layer, participants receive photons entangled via the actions of $U^{[1]}$ and $W^{[1]}$. These operations transform the original state $|\psi\rangle$ into a new state $|\psi^{[1]}\rangle$, which is a compressed version of the initial state. The entangled photons contain the necessary information to invert these transformations.

By using disentangling operators $U_{11}, U_{12}, \ldots, U_{18}$ and isometry operators $W_{11}, W_{12}, \ldots, W_{18}$ [13], which are in the forms

$$u_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix}, \quad u_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \quad w_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix},$$

$$w_2 = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \quad w_3 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & 0 \end{bmatrix},$$

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

we can obtain the first layer. When $u_1, u_2, \ldots, u_6$ are applied to the states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, the following results can be obtained:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u_1} |00\rangle, \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{u_1} |01\rangle, \tag{A2}$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u_2} |11\rangle, \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{u_2} |10\rangle. \tag{A3}$$

Equations (A2) and (A3) show that different disentangling operators can compress different entangled states into the same product state. Since u_1 and u_2 are unitary operators, their inverses are given by $u_1^{-1} = u_1^\dagger$ and $u_2^{-1} = u_2^\dagger$. Consequently, we obtain the relationships

$$|00\rangle \xrightarrow{u_1^\dagger} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |01\rangle \xrightarrow{u_1^\dagger} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{A4}$$

$$|11\rangle \xrightarrow{u_2^\dagger} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |10\rangle \xrightarrow{u_2^\dagger} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{A5}$$

Equations (A4) and (A5) demonstrate that the same product state can be decompressed into different entangled states by applying different disentangling operators.

The procedure for constructing the first layer is outlined in detail as follows (note that the order of the equations corresponds to the states that are identical in the first layer, rather than the sequence in which the entangled states appear). Specifically, the operations U_{11}, U_{12}, U_{17}; U_{14}, U_{16}; U_{13}, U_{15}, U_{18}; W_{11}, W_{16}; W_{14}, W_{15}, W_{18}; W_{12}, W_{17}; and W_{13} are applied in the same manner.

For simplicity, we illustrate the computation by selecting one representative operation from each group as follows:

$$U_{11}\left(\frac{\sqrt{2}}{2}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\right)=\begin{bmatrix}\frac{1}{\sqrt{2}}&0&0&\frac{1}{\sqrt{2}}\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\\\frac{1}{\sqrt{2}}&0&0&-\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=|00\rangle, \tag{A6}$$

$$U_{16}\left(\frac{\sqrt{2}}{2}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}\right)=\begin{bmatrix}\frac{1}{\sqrt{2}}&0&0&\frac{1}{\sqrt{2}}\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\\\frac{1}{\sqrt{2}}&0&0&-\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}0\\\frac{\sqrt{2}}{2}\\\frac{\sqrt{2}}{2}\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=|01\rangle, \tag{A7}$$

$$U_{13}\left(\frac{\sqrt{2}}{2}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\right)=\begin{bmatrix}\frac{1}{\sqrt{2}}&0&0&-\frac{1}{\sqrt{2}}\\0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\\frac{1}{\sqrt{2}}&0&0&\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{\sqrt{2}}{2}\\0\\0\\\frac{\sqrt{2}}{2}\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=|11\rangle, \tag{A8}$$

$$W_{11}\left(\frac{\sqrt{2}}{2}(|000\rangle+|111\rangle)\right)=\frac{\sqrt{2}}{2}\begin{bmatrix}1&0&0&0&0&0&0&1\\0&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&0\end{bmatrix}\begin{bmatrix}\frac{\sqrt{2}}{2}\\0\\0\\0\\0\\0\\0\\\frac{\sqrt{2}}{2}\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}=|0\rangle, \tag{A9}$$

$$W_{14}\left(\frac{\sqrt{2}}{2}(|000\rangle+|111\rangle)\right)=\frac{\sqrt{2}}{2}\begin{bmatrix}0&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&0\\1&0&0&0&0&0&0&1\end{bmatrix}\begin{bmatrix}\frac{\sqrt{2}}{2}\\0\\0\\0\\0\\0\\0\\\frac{\sqrt{2}}{2}\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}=|1\rangle, \tag{A10}$$

$$W_{13}\left(\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)\right)=\frac{\sqrt{2}}{2}\begin{bmatrix}0&1&1&0\\1&0&0&1\end{bmatrix}\begin{bmatrix}0\\\frac{\sqrt{2}}{2}\\\frac{\sqrt{2}}{2}\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}=|0\rangle, \tag{A11}$$

$$W_{12}\left(\frac{\sqrt{2}}{2}(|01\rangle+|10\rangle)\right)=\frac{\sqrt{2}}{2}\begin{bmatrix}1&0&0&1\\0&1&1&0\end{bmatrix}\begin{bmatrix}0\\\frac{\sqrt{2}}{2}\\\frac{\sqrt{2}}{2}\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}=|1\rangle. \tag{A12}$$

Hence, the disentangling and isometry operations transform the initial 21-photon entangled state into the compressed state of the first layer, completing the first stage of compression.

Following the same methodology, the second and third layers are constructed by applying the unitary transformations U_{21}, U_{22}, U_{23}, U_{24}, U_{31}, and U_{32} and the disentangling operations W_{21}, W_{22}, W_{23}, W_{24}, and W_{31}. These operations facilitate the progression to the subsequent level of the quantum network architecture.

The many-body state $|\psi\rangle$ in Eq. (A1) is progressively compressed through the operators W and U. In the photon distribution for the four-participant set $\{P_1, P_2, P_3, P_4\}$, the dealer sends the photons $\psi_1^{(0)}$ and $\psi_{21}^{(0)}$ (note that the superscript denotes the layer number and the subscript indicates the specific entangled photon within that layer) from the original layer to P_1, the photons $\psi_2^{(1)}$

and $\psi_8^{(1)}$ from the first layer to P_2, the photons $\psi_2^{(2)}$ and $\psi_4^{(2)}$ from the second layer to P_3, and the photon $\psi_2^{(3)}$ from the third layer to P_4 via quantum channels. Meanwhile, the dealer transmits $U_{11}, U_{12}, \ldots, U_{18}$ and $W_{11}, W_{12}, \ldots, W_{18}$ to P_2, U_{22}, U_{23}, U_{24} and W_{21}, W_{22}, W_{23} to P_3, and W_{31} to P_4 through classical channels. The transmission of the photons is protected by the use of decoy particles.

The distribution of entangled photons requires careful communication between participants. Since the photons hold the quantum correlations necessary for recovery, participants in adjacent layers must ensure that the correct operations are applied to the photons. This communication is crucial for synchronizing the application of inverse operations across layers.

Similarly, we use Fig. 2(a) to illustrate the verification and recovery process in our QSS scheme. First, participant P_1 uses their secret shares, that is, the photon $\psi_2^{(3)}$ (i.e., $|0\rangle$) from the third layer, and applies the operators U_{31}, U_{32}, and W_{31}, performing the following computations.

First, with the operator W_{31}, P_1 can obtain

$$W_{31}^{\dagger}|0\rangle = \frac{\sqrt{2}}{2}\begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \frac{\sqrt{2}}{2}(|000\rangle + |111\rangle). \tag{A13}$$

Next, with the outcome from Eq. (A13), the photon $\psi_1^{(0)}$ from P_1, and the two photons $\psi_2^{(2)}$ and $\psi_4^{(2)}$ from P_3, P_1 can confirm that $\psi_3^{(2)}$ is $|0\rangle$. Moreover, with the recovered state $|000\rangle$, P_1 verifies whether $|0\rangle$ is equal to $\psi_4^{(2)}$. If they are equal, then P_4 is deemed honest and proceeds to the next step of recovery. Otherwise, the recovery process is terminated.

Next, with W_{21}, W_{22}, W_{23}, and W_{24} and the recovered information from P_3 and P_4, P_1 can further recover by computing

$$W_{21}^{\dagger}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{A14}$$

The same computation applies to W_{22}, W_{23}, and W_{24}.

Finally, with $\psi_2^{(1)}$ and the dealer's classical information, P_1 confirms the recovery using W_{21}, W_{22}, W_{23}, W_{24}. Additionally, P_1 verifies whether $|1\rangle$ is equal to $\psi_4^{(2)}$. If they are equal, then P_3 is deemed honest and the process continues. Otherwise, the recovery is terminated. Finally, P_1 follows the same method to recover and verify. If P_2 is honest, the shared state $|\psi\rangle$ is fully recovered and confirmed as correct.

Note that the inherent structure of the MERA network, built by alternating layers of unitary U and isometric W operations, naturally provides a mechanism for both layer verification and fault tolerance during the recovery of quantum states. By utilizing entangled photons shared between these operations, the network can dynamically verify the correctness of the recovery process and detect faults. This built-in structure not only enhances the reliability of quantum communication but also optimizes resource usage by maintaining efficient compression and recovery processes throughout the network.

[1] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, The evolution of quantum key distribution networks: On the road to the qinternet, IEEE Commun. Surv. Tut. **24**, 839 (2022).

[2] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent multiparty quantum communication, Phys. Rev. Lett. **114**, 090501 (2015).

[3] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B.Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling *et al.*, A trusted node-free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).

[4] A. Shamir, How to share a secret, Commun. ACM **22**, 612 (1979).

[5] G. R. Blakley, *International Workshop on Managing Requirements Knowledge, New York, 1979* (IEEE Computer Society, Washington, DC, 1979), pp. 313–317.

[6] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[7] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A **63**, 042301 (2001).

[8] A. Karlsson, M. Koashi, and N. Imoto, Quantum entanglement for secret sharing and secret splitting, Phys. Rev. A **59**, 162 (1999).

[9] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, Absolute maximal entanglement and quantum secret sharing, Phys. Rev. A **86**, 052335 (2012).

[10] S. Bagherinezhad and V. Karimipour, Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers, Phys. Rev. A **67**, 044302 (2003).
[11] Y. Tian, J. Wang, G. Bian, J. Chang, and J. Li, Dynamic multi-party to multi-party quantum secret sharing based on Bell states, Adv. Quantum Technol. **7**, 2400116 (2024).
[12] G.-D. Li, W.-C. Cheng, Q.-L. Wang, L. Cheng, Y. Mao, and H.-Y. Jia, Quantum secret sharing enhanced: Utilizing W states for anonymous and secure communication, arXiv:2402.02413.
[13] H. Lai, J. Pieprzyk, and L. Pan, Dynamic hierarchical quantum secret sharing based on the multiscale entanglement renormalization ansatz, Phys. Rev. A **106**, 052403 (2022).
[14] K. Senthoor and P. K. Sarvepalli, Theory of communication efficient quantum secret sharing, IEEE Trans. Inf. Theory **68**, 3164 (2022).
[15] K. Senthoor and P. K. Sarvepalli, Communication efficient quantum secret sharing via extended CSS codes, IEEE J. Sel. Areas Commun. **42**, 1818 (2024).
[16] Y. Qin, J. Cheng, J. Ma, D. Zhao, Z. Yan, X. Jia, C. Xie, and K. Peng, Efficient and secure quantum secret sharing for eight users, Phys. Rev. Res. **6**, 033036 (2024).
[17] M. Chehimi, C. Chaccour, C. K. Thomas, and W. Saad, Quantum semantic communications for resource-efficient quantum networking, IEEE Commun. Lett. **28**, 803 (2024).
[18] G. Carleo and M. Troyer, Solving the quantum many-body problem with artificial neural networks, Science **355**, 602 (2017).
[19] L. Cincio, J. Dziarmaga, and M. M. Rams, Multiscale entanglement renormalization ansatz in two dimensions: Quantum Ising model, Phys. Rev. Lett. **100**, 240603 (2008).
[20] E. M. Stoudenmire, Learning relevant features of data with multi-scale tensor networks, Quantum Sci. Technol. **3**, 034003 (2018).
[21] G. Vidal, Class of quantum many-body states that can be efficiently simulated, Phys. Rev. Lett. **101**, 110501 (2008).
[22] A. Franco-Rubio and G. Vidal, Entanglement and correlations in the continuous multi-scale entanglement renormalization ansatz, J. High Energy Phys. 12 (2017) 129.
[23] K. Garg, Z. Ahmed, and A. Thomasen, Qubit frugal entanglement determination with the deep multi-scale entanglement renormalization ansatz, arXiv:2404.08548.
[24] T. Barthel and Q. Miao, Scaling of contraction costs for multiscale entanglement renormalization including tensor Trotterization and variational Monte Carlo, Phys. Rev. B **111**, 045104 (2025).
[25] G. Evenbly and G. Vidal, Entanglement renormalization in two spatial dimensions, Phys. Rev. Lett. **102**, 180406 (2009).
[26] G. Evenbly and G. Vidal, Algorithms for entanglement renormalization, Phys. Rev. B **79**, 144108 (2009).
[27] W. W. Ho, S. Choi, H. Pichler, and M. D. Lukin, Periodic orbits, entanglement, and quantum many-body scars in constrained models: Matrix product state approach, Phys. Rev. Lett. **122**, 040603 (2019).
[28] V. Giovannetti, S. Montangero, and R. Fazio, Quantum multiscale entanglement renormalization ansatz channels, Phys. Rev. Lett. **101**, 180503 (2008).