




Dynamic hierarchical quantum secret sharing based on the multiscale entanglement renormalization ansatz

Hong Lai ^{1,*}, Josef Pieprzyk ^{2,3} and Lei Pan ⁴

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

²*Data61, CSIRO, Sydney, New South Wales 2122, Australia*

³*Institute of Computer Science, Polish Academy of Sciences, Warsaw 01-248, Poland*

⁴*School of Information Technology, Deakin University, Geelong, Victoria 3220, Australia*



(Received 8 June 2022; accepted 18 October 2022; published 2 November 2022)

Tensor networks offer a novel and powerful tool for solving a variety of problems in mathematics, data science, and engineering. One such network is the multiscale entanglement renormalization ansatz (MERA). The MERA exhibits a hierarchical structure of layers, where each layer corresponds to a particular length (or energy) scale. The structure can be easily constructed using isometric and disentangler transformations. The following question arises: Is it possible to use the MERA to build hierarchical quantum secret sharing (HQSS)? The paper answers the question in the affirmative. In particular, it shows how a hierarchy of participant trust and authority relates to a MERA structure. The structure consists of binary and ternary MERA modules, which generate secret shares for participants. Because a binary MERA can be replaced by its ternary sibling and vice versa, our HQSS scheme is dynamic, allowing promotion and demotion of participants from the different layers but also enrollment of new ones and disenrollment of old ones from the same layer. The correctness and security of our dynamic hierarchical quantum secret sharing scheme are discussed.

DOI: [10.1103/PhysRevA.106.052403](https://doi.org/10.1103/PhysRevA.106.052403)

I. INTRODUCTION

Threshold secret sharing was introduced independently by Shamir [1] and Blakley [2]. The Shamir scheme applies polynomial interpolation, while the Blakley scheme uses geometric objects. In both schemes, there is a group of n participants. Each participant holds their share. The schemes allow recreating a secret by any t participants. In many applications, however, some participants are more trustworthy than others. For example, in the banking industry, a branch head is more trustworthy than a clerk. To deal with such circumstances, hierarchical secret sharing (HSS) has been proposed. There are many HSS solutions in the literature. In the Kothari scheme [3], the secret is a scalar and shares are linear varieties. In the Tassa scheme [4], polynomial derivatives are used to achieve different levels of authorization (trust). Farras and Padró [5] used the properties of hierarchically minimal vectors to construct an ideal HSS. Based on Birkhoff interpolation, Traverso *et al.* [6] presented their dynamic and verifiable HSS. Recently, Chen *et al.* [7] designed a multipartite HSS, which is based on polymatroid-based techniques and linear algebraic techniques. Zhang *et al.* [8] proposed a decentralized and fair hierarchical threshold secret sharing using blockchain. Yuan *et al.* [9] constructed a hierarchical multisecret sharing scheme. Their scheme is based on linear homogeneous recurrence relations and a one-way function.

A quantum variant of HSS was first studied by Wang *et al.* [10]. In their hierarchical quantum secret sharing (HQSS) scheme, participant authorizations belong to one of two pos-

sible levels. The follow-up works explore various entangled states, including six-qubit cluster states, eight-qubit cluster states, nonmaximally four-qubit cluster states, and arbitrary two-qubit states via the cluster state [11–16]. All the above HQSS schemes allow sharing a single secret only. However, in many applications, there is a need to handle multiple secrets. This is the case where groups with different authorization levels wish to share their secrets among themselves. For instance, in a drug company, directors may need to share highly sensitive information about a new drug formula with managers about a production plan and workers about a work timetable roster.

Qin *et al.* [17] designed their HQSS using a special high-dimensional entangled state. At different authorization levels, participants share secrets in different ways. The hierarchy of secrets means that participants at the i th level can collectively recover the secret on the level but also all secrets from levels below, i.e., $i - 1, \dots, 1$; conversely, secrets above the i th level are not accessible. This secret sharing is static and does not allow participants to be promoted (i.e., moved to a higher level of hierarchy) or demoted (i.e., dropped to a lower level). Mishra *et al.* [18] proposed their dynamic hierarchical quantum secret sharing (DHQSS) that permits the movement of participants up and down along a hierarchical structure.

Tensor networks developed in [19–21] offer an exciting and new approach to solving various problems in mathematics, data science, machine learning, and quantum key distribution [22–31]. In particular, the multiscale entanglement renormalization ansatz (MERA) is a fascinating refinement of tensor networks [32,33]. It provides solutions to error correction [34,35] and machine learning [36,37] problems. Tensors in the MERA are organized in layers,

*Corresponding author: h lai@swu.edu.cn

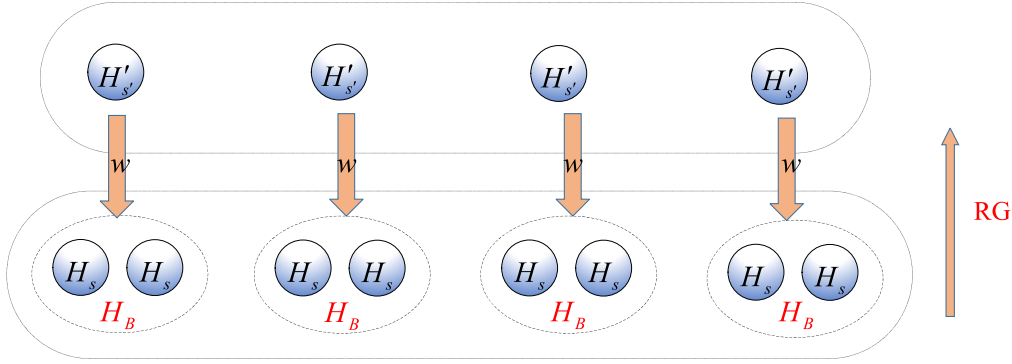


FIG. 1. Hilbert space coarse graining with one block equal to two sites.

where each layer corresponds to a different length (or energy) scale. In other words, using entanglement renormalization and isometric operations, a layer (hierarchical) structure of the MERA is formed with a new state.

Inspired by the new developments in quantum secret sharing, we investigate the potential of the MERA in designing new DHQSS. Note that the MERA exhibits an inherent hierarchical structure. Each level of the structure corresponds to an appropriate length scale. The MERA seems to be a suitable tool for quantum many-body state sharing. In addition, both the binary MERA and the ternary MERA allow the movement of participants from the different layers up and down along a hierarchical structure. Additionally, new participants from the same layer can be enrolled and old ones from the same layer can be disenrolled. Our MERA-based solution shares the advantages of the schemes of Qin *et al.* [17] and Mishra *et al.* [18]. Note that the MERA is also a high-dimensional entangled state. Lancien *et al.* pointed out in [38] that a high-dimensional entangled state is more robust against noise than a low-dimensional one [39]. Another advantage of the application of entangled states is better security. Shares held by participants are unknown before measuring a state of a particle that carries a share. Even a dealer does not know participant shares. Note that in classical secret sharing, the dealer knows all shares. This means that QSS offers a higher security level.

The rest of the paper is organized as follows. Section II introduces the background. Section III describes our HDQSS. The correctness of our HQMBSS is proven in Sec. IV. Performance analysis is presented in Sec. V. Section VI summarizes the paper.

II. BACKGROUND

This section presents two main building blocks of our schemes. We first introduce entanglement renormalization, which includes coarse-graining transformation and boundary deforming. Next we define the multiscale entanglement renormalization ansatz and discuss its properties.

A. Entanglement renormalization

We define the Hilbert space before renormalization as

$$H \equiv \bigotimes_{s \in \mathcal{L}} H_s, \quad (1)$$

where s indicates a site on lattice \mathcal{L} . The renormalized Hilbert space is defined as

$$H' \equiv \bigotimes_{s' \in \mathcal{L}'} H'_{s'}. \quad (2)$$

In the spirit of coarse graining (see Fig. 1), one site s' after renormalization corresponds to multiple sites $\{s\} \equiv \mathcal{B} \subset \mathcal{L}$ (called a block) before renormalization. We relate the Hilbert spaces (before normalization and after normalization) according to the linear mapping

$$w : H'_{s'} \rightarrow H_{\mathcal{B}} = \bigotimes_{s \in \mathcal{B}} H_s, \quad (3)$$

where w is called an isometry such that $w^\dagger w = I$. Here isometry refers to the mapping of the inner product (modulus) preservation, that is,

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

The isometry w guarantees that the inner product of two quantum states in a small space is equal to the inner product of their images mapped to a large space. Note that in Sec. III, the isometry w is used to design a hierarchical structure for quantum state secret sharing. Obviously, w is not an invertible mapping, but it can induce an inverse mapping w' as

$$w' : \bigotimes_{s \in \mathcal{B}} H_s \rightarrow H'_{s'}. \quad (5)$$

The way of induction is to shrink the indicators on different sides of the tensor (the following will not distinguish between the two in terms of notation, that is, we uniformly use the symbol H_s ; see Fig. 1). In fact, it is equivalent to unitary plus projection (or projection). That is, we take a certain unitary transformation of several columns, similar to the truncation operation in the singular value decomposition. Its physical interpretation is to recombine and distribute the degrees of freedom of the block into short-range, high-energy, and irrelevant parts and long-range, low-energy, and relevant parts before discarding the former and outputting merely the latter as shown in Fig. 2.

We divide the original lattice into different blocks so that each block \mathcal{B} corresponds to $w_{\mathcal{B}}$. By mapping each block, the original quantum state can be coarse grained into a new state

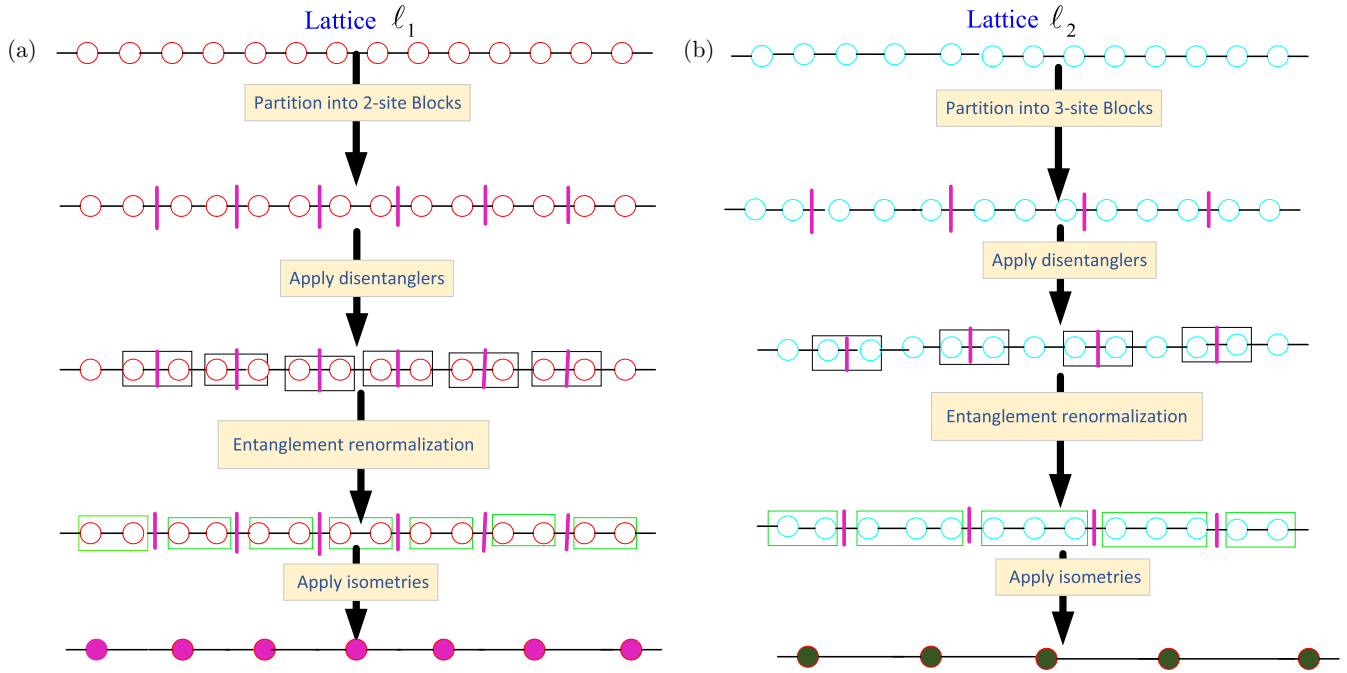


FIG. 2. Flow chart of the real-space renormalization-group transformation for (a) the binary MERA and (b) the ternary MERA.

in a subspace, that is,

$$W = \bigotimes_B w_B, \quad |\Psi\rangle \rightarrow |\Psi'\rangle = W|\Psi\rangle. \quad (6)$$

Therefore, the role of w is to select a subspace \mathcal{H}'_s such that $|\Psi'\rangle$ obtained by projection contains all relevant properties of $|\Psi\rangle$.

The disadvantage of the above coarse graining is that entanglement between blocks is “roughly” truncated. This issue leads us to the following question: Can short-range entanglement between blocks be manually weakened by a local unitary transformation before coarse graining? The answer is yes. To be exact, for all n adjacent sites on both sides of the partition boundary ∂ (for a one-dimensional system $n = 2$), an n -qubit unitary gate u_i is applied to address the problem, which is

$$U = \bigotimes_{i \in \partial} u_i, \quad (7)$$

$$u_i u_i^\dagger = u_i^\dagger u_i = I \otimes I, \quad (8)$$

where u_i is called a reversible disentangler (see Fig. 3). Disentanglers preserve information and the dimension of the state space of the sites. Isometries pack two or three sites into one, keep the ground-state properties, and project high-dimension states in the low-energy subspace.

One may ask the following question: Does a random application of the disentangling (unitary) transformation change the properties of the original quantum state? One can argue that a local unitary transformation can only alter a short-range entanglement. In addition, a short-range entanglement is inherently unimportant for the state after coarse graining. Consequently, such a local unitary transformation is allowed when necessary. Moreover, disentangling transformation reorganizes or adjusts the border between blocks, while entangled degrees are on the same side of the border.

We take an example from the work in [40] to explain how disentanglers work. The example includes four spin- $\frac{1}{2}$ ($r_1 s_1 s_2 r_2$) particles in a chain and an isometry matrix w that is used to coarse grain the two middle particles. A whole many-body state is described by

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_{r_1}|1\rangle_{s_1} + |1\rangle_{r_1}|0\rangle_{s_1}) \frac{1}{\sqrt{2}}(|0\rangle_{r_2}|1\rangle_{s_2} + |1\rangle_{r_2}|0\rangle_{s_2}) \\ &= \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle). \end{aligned}$$

Obviously, pairwise spins of particles (r_1, s_1) and (r_2, s_2) are in maximally entangled states, which is the worst case. It means that the following reduced density matrix is in the maximally mixed state:

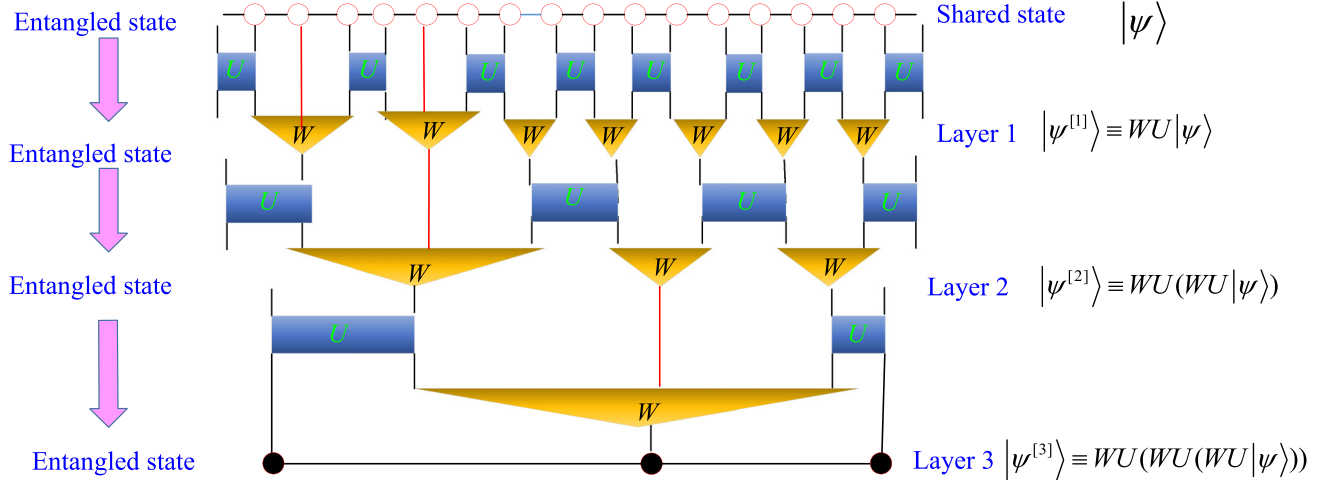
$$\begin{aligned} \rho_{s_1 s_2} &= \text{Tr}_{r_1 r_2} \rho = \text{Tr}_{r_1 r_2} |\psi\rangle\langle\psi| \\ &= \frac{1}{4}(|00\rangle\langle 00| + |11\rangle\langle 11| + |10\rangle\langle 10| + |01\rangle\langle 01|). \end{aligned}$$

Coarse graining causes many errors if we want to retain the whole state space. Thus, we use a disentangler u that operates on the pairs (r_1, s_1) and (s_2, r_2). The disentangler is in the form

$$u = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (9)$$

When the disentangler u given by Eq. (9) operates on $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, the outcome is

$$\begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle. \quad (10)$$



(1) the binary and ternary MERA are alternatively used to design layers for participants with different rights in our DHQMBSS scheme.

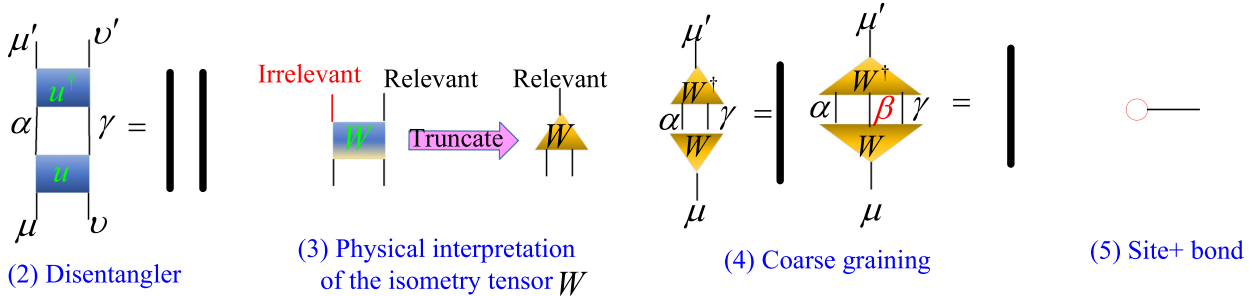


FIG. 3. Illustration of our proposed DHQMBSS based on the binary and the ternary MERA.

In other words, we have

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

As demonstrated above, once the disentangler u is applied on $|\psi\rangle$, the state of the four spins becomes $|0000\rangle$. Consequently, the corresponding reduced density matrix is

$$\rho_{s_1 s_2} = |00\rangle\langle 00|.$$

To sum up, entanglement renormalization consists of the following two steps: (1) boundary deforming $|\Psi\rangle \rightarrow U|\Psi\rangle$ and (2) coarse graining $U|\Psi\rangle \rightarrow WU|\Psi\rangle$.

The entanglement between sites after coarse graining actually reflects the (longer-range) entanglement between blocks before coarse graining. Therefore, with the iteration of the entanglement renormalization group (ERG), the short-range entanglement is continuously renormalized while the long-range entanglement properties of the quantum state are gradually extracted (the data in Ref. [34] show this effect well). That is to say, different ERG layers contain entangled information of different length scales of the original quantum state. In other words, different entanglement renormalization layers contain entangled information of different length scales of the original quantum state (see Figs. 2 and 3).

Definition 1 (matrix product state [22]). A matrix product state (MPS) representation of any many-body state is defined

as

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

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

The above relation can be simplified as

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

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

$$\begin{aligned} |\Psi\rangle &= \left(\frac{1}{\sqrt{3}} \quad 0\right) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |001\rangle \\ &+ \left(\frac{1}{\sqrt{3}} \quad 0\right) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |011\rangle \\ &+ \left(0 \quad \frac{1}{\sqrt{3}}\right) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} |110\rangle, \end{aligned} \quad (12)$$

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.

B. Multiscale entanglement renormalization ansatz

Definition 2 (multiscale entanglement renormalization ansatz [41–44]). The MERA consists of a series of alternately arranged unitary matrices (disentangler operators) and isometric matrices of different scales.

We use two different types of MERA, i.e., binary and ternary. Figure 2 shows the flow charts of the real-space renormalization-group transformation for the binary and the ternary MERA. They will be used in our proposed scheme (see Sec. III). Compared to a binary MERA, a ternary MERA scales as a lower power of the bond dimension. In contrast, if local entanglement needs to be removed, then the binary MERA is more effective. Hence, the binary MERA can lower the bond dimension. Moreover, the choices for the block size can be used to design a dynamic hierarchical quantum secret sharing.

III. DESIGN OF DYNAMIC HIERARCHICAL QUANTUM MANY-BODY STATE SHARING FROM MERA

In the section we present our dynamic hierarchical quantum many-body state sharing (DHQMSS) scheme using the MERA. Our scheme targets theory innovation and its applications, where access to a document or secret key must be handled jointly by participants assigned to different layers of quantum secret sharing. Moreover, participants at different layers have different range entanglement. The number of participants and shared secrets may vary for different layers. A shared state (secret) at a certain layer is recovered by all participants at the layer. To determine the final state, however, participants need classical information provided by a dealer. Note that any participant from a higher layer is able to obtain shared secrets by participants at lower layers. The converse does not hold (see Fig. 3).

Importantly, both the binary MERA and the ternary MERA are viable alternatives to produce intermediate states in our scheme. The dealer is able to dynamically adjust secret sharing parameters and execute enrollment and disenrollment operations to accept new participants and remove the unwanted ones from the same layer. Moreover, the promotion and demotion of participants from the different layers are allowed in our scheme.

A. Description of DHQMSS

In our secret sharing scheme, both the binary MERA and the ternary MERA are used to design the hierarchical structure (see Fig. 3), which is our theoretical innovation in this paper. Both MERA versions apply similar disentanglers U . There are, however, subtle differences in functionalities of the isometries W . The MERA modules in Fig. 3 are constructed for a lattice \mathcal{L} made of $N = 16$ sites. For a two-to-one (binary) MERA, its tensors are of types (1,2) and (2,2). The (1,2) tensors are called an isometry W matrix and the (2,2) tensors are called a disentangler U . The following relations hold:

$$\sum_{\alpha,\gamma} (W)_{\alpha\beta\gamma}^\mu (W^\dagger)_{\mu'}^{\alpha\gamma} = I_{\mu\mu'},$$

$$\sum_{\alpha,\gamma} (U)_{\alpha\gamma}^{\mu\nu} (U^\dagger)_{\mu'\nu'}^{\alpha\gamma} = I_{\mu\mu'} I_{\nu\nu'}.$$

For a three-to-one (ternary) MERA, the isometries W are of type (1,3), but the disentanglers U are still of type (2,2). Similarly, the following relations hold:

$$\sum_{\alpha,\beta,\gamma} (W)_{\alpha\beta\gamma}^\mu (W^\dagger)_{\mu'}^{\alpha\beta\gamma} = I_{\mu\mu'},$$

$$\sum_{\alpha,\gamma} (U)_{\alpha\gamma}^{\mu\nu} (U^\dagger)_{\mu'\nu'}^{\alpha\gamma} = I_{\mu\mu'} I_{\nu\nu'}.$$

Note that the concept of isometric matrix can be extended to isometric tensors $w(w_1, w_2)$, where $w(w_1, w_2)$ satisfies the condition

$$w : \mathbb{V}_{\text{in}} \rightarrow \mathbb{V}_{\text{out}}, \quad ww^\dagger = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (13)$$

In our DHQMSS, the secret is a many-body state such as the MPS that is prepared by $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. The entangled state in the MPS is first disentangled by U and then the long range is compressed into $|0\rangle$ or $|1\rangle$ by W to obtain $|\psi^{[l]}\rangle$. The disentangler U and isometry matrix W (note that U and W have many choices, a detailed introduction in the latter example), $|0\rangle$ and $|1\rangle$, respectively, are public, but which exact U and W are used for short-range and long-range entanglement are private.

Moreover, it is assumed that there are n layers, and each participant is assigned to one of these layers. For the j th layer, there are l_j participants denoted by $\text{Bob}_{j,1}, \text{Bob}_{j,2}, \dots, \text{Bob}_{j,l_j}$ who can share a quantum many-body state $|\psi\rangle$. Recovery of $|\psi\rangle$ requires the collaboration of all l_j participants at the same layer or cooperation of alternative participants at a proper combination of different layers. In addition, a participant at the j th layer can acquire the shared secrets at lower layers, while secrets at higher layers are not accessible. A more detailed description is given below.

Step 1: Generation of hierarchical states and shares. The dealer, Alice, first prepares the shared entangled state $|\psi\rangle$ of $m = 2^n$ photons (here n and m denote the number of layers and entangled photons of the shared many-body state, respectively) and the number of participants is determined based on a practical setting (because the binary MERA and the ternary MERA are viable alternatives, which affects the number of participants). Alice first transforms $|\psi\rangle$ into a new state $|\psi^{[1]}\rangle \equiv (WU)|\psi\rangle$. Then she allocates a single entangled photon of $|\psi^{[1]}\rangle$ to a single participant from the first layer. Each participant holds their photon as an individual share.

Using the same method, Alice allocates shares [i.e., $|0\rangle$'s or $|1\rangle$'s, which are prepared by compressing the long-range entangled photons in terms of $|\psi^{[l]}\rangle \equiv \underbrace{(WU \dots (WU)}_j |\psi\rangle)$] to the

participants from the j th layer, where $j = 1, 2, \dots, n$. Moreover, in the processing of the renormalization group (see Fig. 3), the isometry matrix W and the disentangler U may differ on the photons of the lattices from the same layer. To be exact, $U(u_1, u_2, u_3, u_4, u_5, u_6)$ and $W(w_1, w_2, w_3, w_4)$, which are unique option sets on $|\psi\rangle$, are defined as

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

$$\begin{aligned}
 u_2 &= \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \\
 u_3 &= \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad u_4 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \\
 u_5 &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}, \quad u_6 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \end{bmatrix}, \\
 w_1 &= \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}, \\
 w_2 &= \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \\
 w_3 &= \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}, \\
 w_4 &= \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}.
 \end{aligned}$$

Note that $u_1, u_2, u_3, u_4, u_5, u_6$ and w_1, w_2, w_3, w_4 can be chosen by the dealer at random. The reason to define the six disentangler matrices and four isometric matrices is that the two kinds of two-photon entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and one kind of three-photon entangled state $\frac{1}{\sqrt{3}}(|000\rangle + |111\rangle)$ are used; these two-photon entangled states can be disentangled into one of two states of their own or one of the other states, so, six disentangler matrices are needed [see Eqs. (14)–(17) and (22)–(25)]. Meanwhile, renormalized two-photon entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and three-photon entangled states $\frac{1}{\sqrt{3}}(|000\rangle + |111\rangle)$ are mapped into a single photon with the help of isometric matrices, and to guarantee the security of our scheme, the different two-photon and three-photon entangled states must have the same probability to be compressed into $|0\rangle$ or $|1\rangle$ [see Eqs. (30)–(35)].

Summing up, given an entangled state $|\psi\rangle$, the dealer iteratively transforms it using the disentanglers and isometric matrices. As a result, Alice obtains a sequence of hierarchical states

$$|\psi\rangle \xrightarrow{WU} |\psi^{[1]}\rangle \xrightarrow{WU} |\psi^{[2]}\rangle \xrightarrow{WU} \dots \xrightarrow{WU} |\psi^{[n]}\rangle, \quad (14)$$

where $|\psi^{[j]}\rangle \equiv \underbrace{(WU \dots (WU)}_j |\psi\rangle)$ and $j = 1, 2, \dots, n$.

Step 2: Share distribution. Alice sends appropriate shares to the participants $\text{Bob}_{j,1}, \text{Bob}_{j,2}, \dots, \text{Bob}_{j,l_j}$ from the l_j ($j = 1, 2, \dots, n$) layer via a quantum channel. The transmission of

the sequences is protected by the decoy particles. The detailed process is described in the next step.

Step 3: Decoy particles for eavesdropping detection. The dealer prepares decoy particles for randomly chosen bases $B_z = \{|0\rangle, |1\rangle\}$ and $B_x = \{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The decoy particles are subsequently inserted into the shared state sequence randomly, recording the particle positions and initial states. Upon the receipt of the participants' acknowledgment of receiving the particles, Alice, the dealer, announces the positions of the decoy particles and tells the participants about a collection of bases to measure decoy particles.

After the measurement is accomplished, the participants inform Alice about their outcomes via an authenticated broadcast channel. Alice computes the error rate by comparing the initial states of the decoy particles with participant measurements. If the error rate is higher than a certain threshold, the protocol is aborted; otherwise, it continues. Note that we assume that the dealer is honest and follows the protocol faithfully. This implies that l_j participants at the j th layer are able to reconstruct the many-body state $|\psi^{[j]}\rangle$.

Step 4: Secret recovery. After receiving the entangled photon sequences from the MPS state, the participants at the j th layer use the basis $\{|0\rangle, |1\rangle\}$ to measure their particles. Prior to a recovery of the state $|\psi\rangle$, the participants $\text{Bob}_{j,1}, \text{Bob}_{j,2}, \dots, \text{Bob}_{j,l_j}$ need to mutually verify their identities. If the verification is positive, then they can proceed with the recovery of $|\psi^{[j]}\rangle$, $j = 1, 2, \dots, n$. To obtain the many-body state $|\psi\rangle$, the dealer needs to send the specific U and W to the participants who can use U and W to obtain U^\dagger and W^\dagger . Finally, according to Eq. (12), the collection of $\text{Bob}_{j,1}, \text{Bob}_{j,2}, \dots, \text{Bob}_{j,l_j}$ can recover the many-body state $|\psi\rangle$.

B. Examples

Here we are going to illustrate our secret sharing. Figure 3 is also helpful. Suppose that there are 17 participants who are assigned to three layers of hierarchy. At the first layer, there are nine participants denoted by $\text{Bob}_{1,1}, \text{Bob}_{1,2}, \dots, \text{Bob}_{1,9}$. At the second layer, there are five participants, denoted by $\text{Bob}_{2,1}, \text{Bob}_{2,2}, \dots, \text{Bob}_{2,5}$. Three participants $\text{Bob}_{3,1}, \text{Bob}_{3,2}$, and $\text{Bob}_{3,3}$ are at the third layer. Further we assume that our shared many-body state is a matrix product state in the form $|\psi\rangle = \sum_{s_1 \dots s_{16}} A^{[1]} A^{[2]} \dots A^{[15]} A^{[16]} |s_1 s_2 \dots s_{15} s_{16}\rangle$, where $A^{[1]}, A^{[16]}$ are vectors; $A^{[2]}, A^{[3]}, \dots, A^{[15]}$ are all order-3 tensors of dimension $d_p \times d_c \times d_c$; d_p is the physical dimension; and d_c is the bond dimension. Note that the MPS formalism is particularly suited for describing sequential schemes for the generation of multipartite states.

For the shares of $\text{Bob}_{1,1}, \text{Bob}_{1,2}, \dots, \text{Bob}_{1,9}$, Alice first performs operations $U(u_1, u_2, u_3, u_4, u_5, u_6)$ and $W(w_1, w_2, w_3, w_4)$, which are defined in step 1 on $|\psi\rangle$. She obtains $|\psi^{[1]}\rangle$. Note that $u_1, u_2, u_3, u_4, u_5, u_6$ and w_1, w_2, w_3, w_4 can be chosen at random. In the MPS, it is assumed that any entanglement between two sites is either $\frac{\sqrt{2}}{2}(|00\rangle + |11\rangle)$ or $\frac{\sqrt{2}}{2}(|01\rangle + |10\rangle)$ [45]. The vectors can be

equivalently represented as

$$\frac{\sqrt{2}}{2}(|00\rangle + |11\rangle) = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad \frac{\sqrt{2}}{2}(|01\rangle + |10\rangle) = \frac{\sqrt{2}}{2} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

When operations u_1 and u_2 are performed on the vectors to achieve disentanglement we obtain

$$u_1 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle, \tag{15}$$

$$u_3 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle, \tag{16}$$

$$u_1 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle, \tag{17}$$

$$u_4 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle. \tag{18}$$

The above calculations in Eqs. (14)–(17) can be abbreviated as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u_1} |00\rangle, \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{u_3} |00\rangle, \tag{19}$$

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{u_1} |01\rangle, \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u_4} |01\rangle. \tag{20}$$

Because $u_1, u_3,$ and u_4 are unitary, their inverses are $u_1^{-1} = u_1^\dagger, u_3^{-1} = u_3^\dagger,$ and $u_4^{-1} = u_4^\dagger.$ Thus we obtain the relations

$$|00\rangle \xrightarrow{u_1^\dagger} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |00\rangle \xrightarrow{u_3^\dagger} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{21}$$

$$|01\rangle \xrightarrow{u_1^\dagger} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |01\rangle \xrightarrow{u_4^\dagger} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{22}$$

Similarly, we have

$$u_2 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle, \tag{23}$$

$$u_5 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle, \tag{24}$$

$$u_2 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle, \tag{25}$$

$$u_6 \left(\frac{\sqrt{2}}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle. \tag{26}$$

As before, we abbreviate Eqs. (22)–(25) as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u_2} |11\rangle, \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{u_5} |11\rangle, \tag{27}$$

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{u_2} |10\rangle, \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u_6} |10\rangle. \tag{28}$$

As $u_2, u_5,$ and u_6 are unitary, their inverses are $u_2^{-1} = u_2^\dagger, u_5^{-1} = u_5^\dagger,$ and $u_6^{-1} = u_6^\dagger.$ We can write the relations

$$|11\rangle \xrightarrow{u_2^\dagger} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |11\rangle \xrightarrow{u_5^\dagger} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad (29)$$

$$|10\rangle \xrightarrow{u_2^\dagger} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |10\rangle \xrightarrow{u_6^\dagger} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (30)$$

According to Eqs. (20), (21), (28), and (29), if $|00\rangle, |01\rangle, |10\rangle,$ and $|11\rangle$ are known, the corresponding entangled vector can be calculated. However, according to Eq. (20), the vectors corresponding to $|00\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle);$ according to Eq. (21), the vectors corresponding to $|01\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle);$ according to Eq. (28), the vectors corresponding to $|11\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle);$ according to Eq. (29), the vectors corresponding to $|10\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$ which suggests the decoding is not unique. Removing their uncertainty requires specific information on $U(u_1, u_2, u_3, u_4, u_5, u_6).$

When the operations w_1 and w_2 are performed on any long-range entangled states $\frac{\sqrt{2}}{2}(|00\rangle + |11\rangle)$ or $\frac{\sqrt{2}}{2}(|01\rangle + |10\rangle)$ and w_3 and w_4 are performed on long-range entangled states $\frac{\sqrt{2}}{2}(|000\rangle + |111\rangle),$ we obtain

$$w_1\left(\frac{\sqrt{2}}{2}(|00\rangle + |11\rangle)\right) = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle, \quad (31)$$

$$w_1\left(\frac{\sqrt{2}}{2}(|01\rangle + |10\rangle)\right) = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle, \quad (32)$$

$$w_2\left(\frac{\sqrt{2}}{2}(|00\rangle + |11\rangle)\right) = \frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle, \quad (33)$$

$$w_2\left(\frac{\sqrt{2}}{2}(|01\rangle + |10\rangle)\right)$$

$$= \frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle, \quad (34)$$

$$w_3\left(\frac{\sqrt{2}}{2}(|000\rangle + |111\rangle)\right) = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle, \quad (35)$$

$$w_4\left(\frac{\sqrt{2}}{2}(|000\rangle + |111\rangle)\right) = \frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle. \quad (36)$$

Alice determines

$$|\psi^{[1]}\rangle = \sum_{s'_1 \dots s'_9} A_1^{[1]} \dots A_1^{[9]} |s'_1 \dots s'_9\rangle$$

and sends $|s'_1\rangle, \dots, |s'_9\rangle$ to $\text{Bob}_{1,1}, \text{Bob}_{1,2}, \dots, \text{Bob}_{1,9},$ respectively. Communication is done via a quantum channel with decoy states. The $A_1^{[1]}, A_1^{[2]}, \dots, A_1^{[9]}$ are obtained by U and $W,$ which are transmitted via an authenticated classical channel. In a similar way, Alice calculates shares and distributes them to $\text{Bob}_{2,1}, \text{Bob}_{2,2}, \dots, \text{Bob}_{2,5}$ and $\text{Bob}_{3,1}, \text{Bob}_{3,2}, \text{Bob}_{3,3}.$

For step 4, $\text{Bob}_{i,q}$ knows his W and measures his particles (see Fig. 4). The following relations hold:

$$w_1^\dagger |0\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \frac{\sqrt{2}}{2}(|00\rangle + |11\rangle),$$

$$w_1^\dagger |1\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \frac{\sqrt{2}}{2}(|01\rangle + |10\rangle),$$

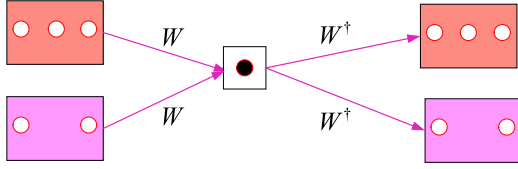


FIG. 4. Graphical presentation of how the isometry W and the noninjectivity of W^\dagger would work in the binary and the ternary MERA.

$$w_2^\dagger|0\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{bmatrix} = \frac{\sqrt{2}}{2}(|01\rangle + |10\rangle),$$

$$w_2^\dagger|1\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \frac{\sqrt{2}}{2}(|00\rangle + |11\rangle),$$

$$w_3^\dagger|0\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \frac{\sqrt{2}}{2}(|000\rangle + |111\rangle),$$

$$w_4^\dagger|1\rangle = \frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix} = \frac{\sqrt{2}}{2}(|000\rangle + |111\rangle).$$

Taking into account the above relations and information about u_1, u_2, u_3, u_4, u_5 , and u_6 , $\text{Bob}_{i,q}$ can recover $|\psi\rangle$. It is important to note that the secret MPS $|\psi\rangle$ can only be recovered jointly by all participants from the i th layer. Each $\text{Bob}_{i,q}$ can also discover his own secret share s_k with $k = 1, 2, \dots, i - 1$ based on his own measurement outcome.

IV. CORRECTNESS OF DHQMSS

Theorem 1. Given a shared MPS $|\psi\rangle$, shares $|s_{iq}\rangle$ are held by participants $\text{Bob}_{i,q}$ at the i th layer, where $i = 1, 2, \dots, n$ and $q = 1, 2, \dots, l_i$, and W and U . Then all participants at the i th layer can collectively recover the state $|\psi^{[i]}\rangle$ and further recover $|\psi\rangle$.

Proof. According to step 4, participants at the i th layer, i.e., $\text{Bob}_{i,1}, \text{Bob}_{i,2}, \dots, \text{Bob}_{i,l_i}$, measure the particles $|s_{i1}s_{i2}\dots s_{i,l_i}\rangle$ to obtain the many-body state in the i th layer, i.e., $|\psi^{[i]}\rangle$. Moreover, based on $|s_{i1}s_{i2}\dots s_{i,l_i}\rangle$ and W^\dagger , $\text{Bob}_{i,1}, \text{Bob}_{i,2}, \dots, \text{Bob}_{i,l_i}$ can obtain the long-range entangled state. Then, according to U^\dagger , the states from the long-range entanglement can be further recovered and so can

their corresponding short-range entangled state. Therefore, the participants $\text{Bob}_{i,q}$ at the i th layer can easily derive $|\psi\rangle$ based on Eq. (13), and Theorem 1 is proved. ■

Theorem 2. Given a shared MPS $|\psi\rangle$, shares $|s_{iq}\rangle$ are held by participants $\text{Bob}_{i,q}$ at the i th layer, where $i = 1, 2, \dots, n$ and $q = 1, 2, \dots, l_i$, and W and U . Then all participants at the i th layer can recover jointly the secret states at $|\psi^{[i-1]}\rangle, |\psi^{[i-2]}\rangle, \dots, |\psi^{[1]}\rangle$.

Proof. As described in the proof of Theorem 1, $\text{Bob}_{i,q}$ at the i th layer can recover $|\psi^{[i]}\rangle$. Then, according to Eq. (13) and Fig. 3, with W^\dagger and U^\dagger , $\text{Bob}_{i,q}$ can further derive $s_{(i-1)j}, s_{(i-2)j}, \dots, s_{1j}$. Therefore, by combining the measured results of n particles, $\text{Bob}_{i,q}$ can obtain the secrets $|\psi^{[i-1]}\rangle, |\psi^{[i-2]}\rangle, \dots, |\psi^{[1]}\rangle$. This concludes the proof. ■

V. PERFORMANCE ANALYSIS

In this section we investigate the confidentiality and security of the shared secrets at different layers of hierarchy. We also discuss the dynamic property of our scheme that allows us to enroll new participants and disenroll old ones and the promotion and demotion of participants.

A. Confidentiality at single layer

Before discussing the confidentiality at a single layer, we need to make clear which parameters are public and which are secret. In our DHQMSS, the secret is a many-body state such as the MPS which is prepared by $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$; the entangled state in the MPS is first disentangled by $U(u_1, u_2, u_3, u_4, u_5, u_6)$ and then the long-range entangled state is compressed into $|0\rangle$ or $|1\rangle$ by W to obtain $|\psi^{[i]}\rangle$. Here $U(u_1, u_2, u_3, u_4, u_5, u_6)$, $W(w_1, w_2, w_3, w_4)$, $|0\rangle$, and $|1\rangle$ are public, but which exact $U(u_1, u_2, u_3, u_4, u_5, u_6)$ and $W(w_1, w_2, w_3, w_4)$ chosen by the dealer Alice are used for short-range and long-range entanglement are private. Also, there are three kinds of general attackers, that is, an outsider who is not a participant but who knows the public parameters and wants to guess or compute secret elements, a single dishonest participant who knows all public information and their own secret share, and a group of colluding and dishonest participants who know public information and their own secret shares.

Participants at the i th layer $\text{Bob}_{i,1}, \text{Bob}_{i,2}, \dots, \text{Bob}_{i,l_i}$ measure the particles $|s_{i1}s_{i2}\dots s_{i,l_i}\rangle$ in $|\psi^{[i]}\rangle$ to obtain quantum bits of the i th layer as their shares. Here $|\psi^{[i]}\rangle$ is the maximally entangled state generated by Alice and the particles $|s_{i1}s_{i2}\dots s_{i,l_i}\rangle$ are obtained by randomly choosing $W(w_1, w_2, w_3, w_4)$. To be exact, according to Eqs. (30)–(35), the state $|0\rangle$ corresponds to w_1, w_2, w_3 and the state $|1\rangle$ corresponds to w_1, w_2, w_4 , respectively. Therefore, to quantify the protocol's security, we present a function of our protocol's input parameters $W(w_1, w_2, w_3, w_4)$ as follows:

$$\Pr(w) = \begin{cases} \frac{1}{3} & \text{for } w = w_k, \quad k = 1, 2, 3, 4 \\ \frac{2}{3} & \text{for } w \neq w_k, \quad k = 1, 2, 3, 4, \end{cases}$$

that is to say, the correct probability that the attacker Eve can guess is $\frac{1}{3}$ for $|0\rangle$ and $|1\rangle$, respectively.

Moreover, to recover the secret $|\psi\rangle$, Eve needs to guess a correct $U(u_1, u_2, u_3, u_4, u_5, u_6)$ based on Eqs. (20), (21), (28), and (29). To be exact, according to Eq. (20), the state $|00\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$; according to Eq. (21), the state $|01\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$; according to Eq. (28), the state $|11\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$; according to Eq. (29), the state $|10\rangle$ can be decoded into two entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. That is, (u_1, u_3) , (u_1, u_4) , (u_2, u_5) , and (u_2, u_6) can correspond to the same state with probability $\frac{1}{2}$. Therefore, to quantify the protocol's security, we present a function of our protocol's input parameters $U(u_1, u_2, u_3, u_4, u_5, u_6)$ as

$$\Pr(u) = \begin{cases} \frac{1}{2} & \text{for } u = u_m, \quad m = 1, 2, \dots, 6 \\ \frac{1}{2} & \text{for } u \neq u_m, \quad m = 1, 2, \dots, 6. \end{cases}$$

This means that the correct probability that the attacker Eve can guess is $\frac{1}{2}$ for $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, respectively.

Therefore, any $l_i - 1$ participants in the i th layer cannot recover the secret $|\psi\rangle$. This is because our scheme needs classical information to further remove uncertainty when all participants work together. The detailed explanation is as follows. For example, if the unknown state for the l_i th participant is $|0\rangle$, then each of the $l_i - 1$ states can be correctly guessed with probability $\frac{1}{3}$ and then according to Fig. 3 she needs to guess a correct $U(u_1, u_2, u_3, u_4, u_5, u_6)$ [(u_1, u_3) , (u_1, u_4) , (u_2, u_5) , and (u_2, u_6) can correspond the same state] with probability $\frac{1}{2}$ and the probability of correctly decoding becomes $\frac{1}{2} \times \frac{1}{3} = \frac{1}{6}$. Consequently, for all states in the i th layer, the correct probability for all states is $1/6^{(l_i-1)}$. Therefore, the probability of the many-body state $|\psi\rangle$ is $1/6^{(l_i-1)}$. Therefore, based on any participant's or a group of colluding and dishonest participants' state or states, they cannot deduce other participants' states. Based on this short discussion, we conclude that the confidentiality in one layer of our proposed scheme is against the three kinds of general attackers.

B. Confidentiality at different layers

As proved in Theorem 2, participants can access the shared secret states at lower layers, i.e., a participant in the i th layer knows the secret states $|\psi^{[i-1]}\rangle, |\psi^{[i-2]}\rangle, \dots, |\psi^{[1]}\rangle$. We will prove that the participants cannot obtain the shared many-body state at a higher layer, i.e., the participants in the i th layer cannot obtain $|\psi^{[i+1]}\rangle, |\psi^{[i+2]}\rangle, \dots, |\psi^{[n]}\rangle$.

We recall the MERA entangled state generated by Alice in Sec. III. As explained in Theorem 2, the i th quantum bits of the states $|\psi^{[i-1]}\rangle, |\psi^{[i-2]}\rangle, \dots, |\psi^{[1]}\rangle$ can be deduced from the states of the particles $|s_{i1}s_{i2} \dots s_{il_i}\rangle$. However, the i th quantum bits of the secret state $|\psi^{[i+1]}\rangle, |\psi^{[i+2]}\rangle, \dots, |\psi^{[n]}\rangle$ cannot be deduced from the particles $|s_{i1}s_{i2} \dots s_{il_i}\rangle$. This is because $W(w_1, w_2, w_3, w_4)$ and correct (u_1, u_3) , (u_1, u_4) , (u_2, u_5) , and (u_2, u_6) can correspond to the same state, without the classical information, and the participants from the i th layer cannot obtain the corresponding correct states.

C. Security against measurement attacks

A measurement attack can be launched by an adversary, Eve, who is eavesdropping on a quantum channel. This means that Eve measures transmitted photons. According to step 3 of our secret sharing scheme (see Sec. III), transmitted photons are protected by decoy photons. Since during transmission decoy photons are randomly interleaved with secret sharing photons, Eve is unable to tell apart decoy photons from secret sharing ones. If Eve decides to eavesdrop, then she needs to measure photons and select one of two bases at random. The probability of a correct guess is $\frac{1}{2}$ (a more detailed analysis is the same as in Sec. V A). Since in our DHQMSS scheme U and W are adjustable, the measurement attacks are analyzed based on the example in Sec. III B. In the example, (u_1, u_3) , (u_1, u_4) , (u_2, u_5) , and (u_2, u_6) correspond to the same states, respectively, so the probability of Eve correctly guessing them is $\frac{1}{2}$, respectively. Also, $|0\rangle$ and $|1\rangle$ correspond to three different isometric matrices, respectively, so the probability of Eve correctly guessing them is $\frac{1}{3}$, respectively (a more detailed analysis is the same as in Sec. V A). For a single transmitted state $|0\rangle$ or $|1\rangle$, the probability of correctly decoding becomes $\frac{1}{2} \times \frac{1}{3} = \frac{1}{6}$. In other words, the error rate is $1 - \frac{1}{6} = \frac{5}{6}$. Therefore, the error rate of decoy particles is $\frac{1}{2} \times \frac{5}{6} = \frac{5}{12}$. According to the current quantum technology, the noise rate in a typical quantum channel ranges from 2% to 8.9% [46–49]. This result is significantly lower than the expected value $\frac{5}{12} \approx 41.7\%$, so Eve's measurements can be easily detected.

D. Security against intercept-and-resend attacks

In this attack, Eve intercepts and resends transmitted MPS photons via a quantum channel. Eve measures an MPS photon sent by Alice using the any basis $\{|\xi_0\rangle, |\xi_1\rangle\}$ ($B_z = \{|0\rangle, |1\rangle\}$ or $B_x = \{|+\rangle, |-\rangle\}$). Depending on her measurement outcome, Eve sends to Bob her own MPS whose state is prepared using either B_z or B_x . We can define their projection operators as follows:

$$P(\xi_0) = |\xi_0\rangle \langle \xi_0|, \quad P(\xi_1) = |\xi_1\rangle \langle \xi_1|. \quad (37)$$

According to Azuma and Ban's work [50], explicit forms of $P(\xi_0)$ and $P(\xi_1)$ are taken into consideration. Also referring to the work in [51], an arbitrary rotation matrix of group $SU(2)$, which is defined by a set of three generators T_k , and T_k satisfy the Lie algebra $[T_i, T_j] = i\epsilon_{ijk}T_k$, with $\epsilon_{123} = 1$. The element of $SU(2)$ is given by the matrix $U = \exp(i\mathbf{T} \cdot \boldsymbol{\omega})$, where $\boldsymbol{\omega}$ is a vector that has components ω_k in a given coordinate frame and $T_k = \frac{1}{2}\sigma_k$, $k = x, y, z$, with standard Pauli matrices $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and these Pauli matrices satisfy the relation $\sigma_i\sigma_j = \delta_{ij} + i\epsilon_{ijk}\sigma_k$. According to three angles θ , φ , and ψ , the Euler parametrization $V(\alpha, \beta, \gamma)$ of any matrix of $SU(2)$ transformation is defined as

$$\begin{aligned} V(\alpha, \beta, \gamma) &= \exp\left(-\frac{i}{2}\alpha\sigma_z\right) \exp\left(-\frac{i}{2}\beta\sigma_y\right) \exp\left(-\frac{i}{2}\gamma\sigma_z\right) \\ &= \begin{bmatrix} e^{-i(\alpha+\gamma)/2} \cos(\beta/2) & -e^{-i(\alpha-\gamma)/2} \sin(\beta/2) \\ e^{i(\alpha-\gamma)/2} \sin(\beta/2) & e^{i(\alpha+\gamma)/2} \cos(\beta/2) \end{bmatrix}, \end{aligned} \quad (38)$$

where $0 \leq \alpha < 4\pi$, $0 \leq \beta < 4\pi$, and $0 \leq \gamma < 4\pi$. According to [50], $P(\xi_0)$ and $P(\xi_1)$ can be written in the following form:

$$P(\xi_0) = V(\alpha, \beta, \gamma) \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} V^\dagger(\alpha, \beta, \gamma) \\ = \begin{bmatrix} \cos^2(\beta/2) & (1/2)e^{-i\alpha} \sin(\beta) \\ (1/2)e^{i\alpha} \sin(\beta) & \sin^2(\beta/2) \end{bmatrix}, \quad (39)$$

$$P(\xi_1) = V(\alpha, \beta, \gamma) \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} V^\dagger(\alpha, \beta, \gamma) \\ = \begin{bmatrix} \sin^2(\beta/2) & -(1/2)e^{-i\alpha} \sin(\beta) \\ -(1/2)e^{i\alpha} \sin(\beta) & \cos^2(\beta/2) \end{bmatrix}. \quad (40)$$

When Eve measures using the basis of either $|\xi_0\rangle$ or $|\xi_1\rangle$, she assumes that Alice transmits a classical bit 0 or 1, respectively. We follow the work of Azuma and Ban [50] and define P_t as the probability of the event that Eve makes a correct guess of a key bit sent by Alice, where $t \in \{x, y\}$ is known to both Alice and Bob_{*j,1*}, Bob_{*j,2*}, ..., Bob_{*j,l_j*}.

Here Q_t is defined as the probability of the event that Alice and Bob fail to detect the Eve measurement when both of them apply the t basis. The probabilities P_t and Q_t can be written as

$$P_t = \frac{1}{2} \sum_{i \in \{0,1\}} \langle i_t | P(\xi_i) | i_t \rangle, \\ Q_t = \frac{1}{2} \sum_{i \in \{0,1\}} \sum_{j \in \{0,1\}} [\langle i_t | P(\xi_j) | i_t \rangle]^2 \quad \text{for } t \in \{x, y\}. \quad (41)$$

They can be transformed into the following forms (where $t \in \{x, y\}$):

$$P_x = \frac{1}{2}(1 + \cos \alpha \sin \beta), \\ Q_x = \frac{1}{8}[5 + \cos(2\alpha) - 2 \cos^2 \alpha \cos(2\beta)], \\ P_y = \frac{1}{2}(1 + \sin \alpha \sin \beta), \\ Q_y = \frac{1}{8}[5 - \cos(2\alpha) - 2 \sin^2 \alpha \cos(2\beta)]. \quad (42)$$

It is reasonable to assume that Eve selects her eavesdropping strategy so that $P_x = P_y$, implying that $\sin \alpha = \cos \alpha$. Without loss of generality, we can assume that $\alpha \in [0, 2\pi)$. Thus, we get that α implies either $\pi/4$ or $5\pi/4$. For the case $\alpha = \pi/4$, we obtain

$$P_x = P_y = \frac{1}{2}[1 + (1/\sqrt{2}) \sin \beta]. \quad (43)$$

Likewise, we assume that $\beta \in [0, 2\pi)$. As $P_x = P_y$, we get

$$P_x = P_y \in \left\{ \frac{2 - \sqrt{2}}{4}, \frac{2 + \sqrt{2}}{4} \right\}. \quad (44)$$

For the case $\alpha = 5\pi/4$, the following relation holds:

$$P_x = P_y = \frac{1}{2} \left[1 - \left(\frac{1}{\sqrt{2}} \right) \sin \beta \right]. \quad (45)$$

As $P_x = P_y$, we get

$$P_x = P_y \in \left\{ \frac{2 - \sqrt{2}}{4}, \frac{2 + \sqrt{2}}{4} \right\}. \quad (46)$$

The above considerations are done under a reasonable assumption that Eve's strategy is symmetric or $P_x = P_y$. Eve's

optimum intercept-and-resend attacks occur when $\alpha = \pi/4$ and $\beta = \pi/2$ and when $\alpha = 5\pi/4$ and $\beta = 3\pi/2$. In the case of the optimal attack, Eve guesses correctly a key bit with a probability close to 0.8535. The probability that Alice and Bob fail to detect Eve's eavesdropping is $\frac{3}{4}$. When Alice sends n qubits, Bob detects the send-and-intercept attack with a probability $1 - 0.8535^n$. On the other hand, Alice and Bob discover eavesdropping with a probability $1 - (\frac{3}{4})^n$.

E. Security against entangle-and-measure attacks

We assume that Eve prepares a new state by entangling the MPS with an auxiliary state $|0_E\rangle$, i.e., $|\Psi'\rangle$. The attack cannot be detected when Bob_{*j,1*}, Bob_{*j,2*}, ..., Bob_{*j,l_j*} use the B_z basis for their measurements. Recall that our transmitted photons are compressed by W and U in order to implement the layer hierarchy. This means that even if Eve obtains a compressed photon, she cannot extract any useful information without knowing detailed W and U . Furthermore, Eve's entanglement eavesdropping can be discovered by Bob_{*j,1*}, Bob_{*j,2*}, ..., Bob_{*j,l_j*} when they check whether or not the condition $\prod_{n=1}^N j_{n_i}^x = 1$ holds. Note that $\prod_{n=1}^N j_{n_i}^x$ is equal to either 0 or 1 with equal probability. For $|\Psi'\rangle$, the relation $j_{E_i}^x \prod_{n=1}^N j_{n_i}^x = 1$ holds (but not for $\prod_{n=1}^N j_{n_i}^x$) [52]. Thus, our scheme is secure against the entangle-and-measure attack.

F. Security against collusion attacks

Dishonest participants may collude to steal other participants' secret information. However, in our scheme, photons are not transmitted one by one among the participants. Instead, the dealer, Alice, transmits photons to each participant directly via dedicated quantum channels. Therefore, there is no chance for a dishonest participant to transmit the forged particles to other participants and steal their secret share information. Therefore, our scheme can resist the dishonest participants' collusion attack.

G. Participant enrollment and disenrollment from the same layer

The scheme allows new participants from the same layer to join. To facilitate this, the dealer only needs to modify the binary and ternary MERA numbers and adjust isometric matrices used. After such modification, new shares are issued. When participants from the same layer need to be removed, again the dealer needs to reduce or modify the structure of the binary and the ternary MERA and adjust selection of isometric matrices. After such modification, old shares become void. Recall our analysis from Sec. IV. It ensures that our scheme provides the confidentiality of the shared quantum state and shares or photons held by participants. Let us consider enrollment and disenrollment operations.

Enrollment. We claim that our scheme can be easily updated to accommodate a new participant from the same layer because the QSS hierarchical structure use a collection of binary and ternary MERA modules. If a new participant from the same layer joins, the collection is upgraded from a binary to a ternary MERA or alternatively a ternary MERA can be extended to two binary MERA modules. There is a need to

regenerate shares only for participants affected by the change, which is implemented by replacing $\sum_{\alpha,\beta,\gamma}(w)_{\alpha\beta\gamma}^\mu(w^\dagger)_{\mu'}^{\alpha\beta\gamma} = I_{\mu\mu'}$ with $\sum_{\alpha,\gamma}(w)_{\alpha\gamma}^\mu(w^\dagger)_{\mu'}^{\alpha\gamma} = I_{\mu\mu'}$.

Disenrollment. This is because the binary and the ternary MERA are alternately used. For the elastic use, when an old participant from the same layer resigns or terminates, we can change the construction of one binary MERA into that of a ternary MERA in generating the state shares without affecting the number of other layers, and only two participants' shares are changed in that layer. The root cause is the change of the isometric matrices, that is, $\sum_{\alpha,\gamma}(w)_{\alpha\gamma}^\mu(w^\dagger)_{\mu'}^{\alpha\gamma} = I_{\mu\mu'}$ is replaced with $\sum_{\alpha,\beta,\gamma}(w)_{\alpha\beta\gamma}^\mu(w^\dagger)_{\mu'}^{\alpha\beta\gamma} = I_{\mu\mu'}$. Moreover, it is easy to generalize the action or termination of a certain number of old participants from the same layer.

Updating the many-body state. A shared many-body state is usually dynamically generated in a streaming manner. Assume that we need to append a new many-body state to the original one. We want to avoid the decomposition of the original tensor. This improves efficiency and reduces the cost of preparing and measuring a many-body state. We use the idea of the authors of [53]. Given two many-body states $\mathcal{A} \in R^{I_1 \times I_2 \times \dots \times I_N}$ and $\mathcal{B} \in R^{I_1 \times I_2 \times \dots \times I_N}$, the addition of the two states $\mathcal{C} = \mathcal{A} + \mathcal{B}$ is performed as

$$C_n(i_n) = \begin{cases} (\mathcal{A}_1(i_1)\mathcal{B}_1(i_1)), & n = 1 \\ \begin{bmatrix} \mathcal{A}_n(i_n) & 0 \\ 0 & \mathcal{B}_n(i_n) \end{bmatrix}, & n = 2, 3, \dots, N-1 \\ \begin{bmatrix} \mathcal{A}_N(i_N) \\ \mathcal{B}_N(i_N) \end{bmatrix}, & n = N, \end{cases}$$

where $\mathcal{C}(i_1, i_2, \dots, i_N) = \mathcal{C}_1(i_1), \mathcal{C}_2(i_2), \dots, \mathcal{C}_N(i_N)$. The subtraction of \mathcal{B} from \mathcal{A} (i.e., $\mathcal{C} = \mathcal{A} - \mathcal{B}$) is shown by

$$C_n(i_n) = \begin{cases} (-\mathcal{A}_1(i_1)\mathcal{B}_1(i_1)), & n = 1 \\ \begin{bmatrix} \mathcal{A}_n(i_n) & 0 \\ 0 & \mathcal{B}_n(i_n) \end{bmatrix}, & n = 2, 3, \dots, N-1 \\ \begin{bmatrix} \mathcal{A}_N(i_N) \\ \mathcal{B}_N(i_N) \end{bmatrix}, & n = N. \end{cases}$$

It is assumed that the original many-body state is \mathcal{A} and the new state is the many-body state \mathcal{B} . Note that if \mathcal{A} and \mathcal{B} are not of the same order or dimension (requiring zero filling to make them of the same order and dimension), then the above-mentioned addition and subtraction of many-body states can be performed. Therefore, the update of the many-body state in our scheme is feasible.

H. Participant promotion from the different layers

In practice, a participant from the different layers who is assigned to the i th layer should have an option to be promoted to the $(i+1)$ th, $(i+2)$ th, \dots , n th layers. This is possible due to the scheme's flexibility in using binary and ternary MERA modules. If a participant needs to be promoted, the number of ternary MERA modules can be easily reduced at the i th layer. This feature allows producing a new share for the participant at the $(i+1)$ th layer. However, the promotion number of participants at the i th layer to the $(i+1)$ th, $(i+2)$ th, \dots , n th layers is limited. On the one hand, this is because our hierarchical structure does not allow us to have too many participants at the $(i+1)$ th, $(i+2)$ th, \dots , n th layers. On the other hand, if too many participants at layer i are promoted to the $(i+1)$ th, $(i+2)$ th, \dots , n th layers, the remaining participants at the i th layer may not be able to compute their secret state. Therefore, our scheme provides limited competitive places for top performers who are at the i th layer to the $(i+1)$ th, $(i+2)$ th, \dots , n th layers.

I. Scheme hierarchy

The hierarchy of our QSS is inherited from a tree structure of MERA modules. It implies that a participant at the i th layer is less powerful than a participant at the $(i+1)$ th layer. Note that any participant at the i th layer has a unique superior from the $(i+1)$ th layer.

J. Secret recovery control

In many practical secret sharing applications, the secret recovery needs to be controlled by the dealer. For instance, heads of an army can launch nuclear weapons only if the state president gives a "go ahead." A bank transfer of a large lump sum transaction is allowed only if two clerks put their shares together along with the branch manager's approval. Such control of secret recovery is possible in our scheme. Recall that the secret in our scheme is a many-body state such as an MPS, which is determined by both $|\psi^{[1]}\rangle, |\psi^{[2]}\rangle, \dots, |\psi^{[n]}\rangle$ and W and U . The dealer can easily control the timing of secret recovery by withholding the classical parts W and U from participants. The dealer gives her "OK" by publishing the classical part W and U . Table I compares our work with other similar schemes from [7–9,12–14,17,18].

TABLE I. Comparison of our scheme with the schemes in [7–9,12–14,17,18].

Work	Secret	Way to realize hierarchy	Features
Ref. [8]	classical	blockchain	fair, hierarchical
Ref. [9]	classical	linear homogeneous recurrence relations	hierarchical
Ref. [12]	quantum	specify participant level	hierarchical
Ref. [13]	quantum	specify participant level	hierarchical
Ref. [17]	quantum	special high-dimensional entangled state	hierarchical
Ref. [7]	quantum	linear algebraic techniques	hierarchical
Ref. [14]	quantum	specify participant level	hierarchical
Ref. [18]	quantum	tree	dynamic, hierarchical, promotability, controllable
present paper	quantum	MERA	dynamic, hierarchical, promotability, controllable

VI. CONCLUSION

We have proposed a DHQSS scheme based on a hierarchical structure built from MERA modules. Depending on an authorization or trust of a participant, the participant is assigned to an appropriate layer in our scheme hierarchy. As there is a binary MERA as well as a ternary MERA, the scheme hierarchy can be easily adapted to a current need for secret recovery. The dynamic nature of the secret sharing hierarchy permits participants from the same layer to join (enrollment) and resign (disenrollment). Also, the scheme allows a certain number of participants from the different layers to be promoted or demoted.

Our scheme fills a research gap in the design of HQSS schemes, whose hierarchy can grow and shrink depending on demands. This characteristic is very useful in many practical applications. Also, we have only considered binary and ternary as in the paper in terms of the method proposed by

Evenbly and Vidal. Moreover, the special high-dimensional entangled states, i.e., the MERA, suggested in this work may be applicable to other quantum cryptography protocols and inspire more study in this direction in future work.

ACKNOWLEDGMENTS

H.L. was supported by the National Natural Science Foundation of China (Grant No. 61702427), the Fundamental Research Funds for the Central Universities (Grant No. XDJK2020B027), the General Program of Chongqing Natural Science Foundation (Grant No. CSTB2022NSCQ-MSX0749), the Venture & Innovation Support Program for Chongqing Overseas Returnees (Grant No. cx2018076), and in part by the 1000-Plan of Chongqing by Southwest University (Grant No. SWU116007). J.P. was supported by Polish National Science Center Grant No. 2018/31/B/ST6/03003.

-
- [1] A. Shamir, How to share a secret, *Commun. ACM* **22**, 612 (1979).
- [2] G. R. Blakley, Proceedings of American Federation of Information Processing Societies National Computer Conference [Int. J. Commun. Netw. Syst. Sci. **7**, 313 (1979)].
- [3] S. C. Kothari, in *Advances in Cryptology*, edited by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science Vol. 196 (Springer, Berlin, 1984), pp. 231–241.
- [4] T. Tassa, Hierarchical threshold secret sharing, *J. Cryptol.* **20**, 237 (2007).
- [5] O. Farras and C. Padró, Ideal hierarchical secret sharing schemes, *IEEE Trans. Inf. Theory* **58**, 3273 (2012).
- [6] G. Traverso, D. Demirel, and J. Buchmann, Dynamic and verifiable hierarchical secret sharing, in *Information Theoretic Security. ICITS 2006*, edited by A. Nascimento and P. Barreto, Lecture Notes in Computer Science, Vol 10015 (Springer, Cham, 2016).
- [7] Q. Chen, C. Tang, and Z. Lin, Efficient explicit constructions of multipartite secret sharing schemes, *IEEE Trans. Inf. Theory* **68**, 601 (2022).
- [8] E. Zhang, M. Li, S.-M. Yiu, J. Du, J.-Z. Zhu, and G.-G. Jin, Fair hierarchical secret sharing scheme based on smart contract, *Inf. Sci.* **546**, 166 (2021).
- [9] J. Yuan, J. Yang, C. Wang, X. Jia, F.-W. Fu, and G. Xu, A new efficient hierarchical multi-secret sharing scheme based on linear homogeneous recurrence relations, *Inf. Sci.* **592**, 36 (2022).
- [10] X.-W. Wang, L.-X. Xia, Z.-Y. Wang, and D.-Y. Zhang, Hierarchical quantum-information splitting, *Opt. Commun.* **283**, 1196 (2010).
- [11] X.-W. Wang, D.-Y. Zhang, S.-Q. Tang, X.-G. Zhan, and K.-M. You, Hierarchical quantum information splitting with six-photon cluster states, *Int. J. Theor. Phys.* **49**, 2691 (2010).
- [12] X.-W. Wang, D.-Y. Zhang, S.-Q. Tang, and L.-J. Xie, Multi-party hierarchical quantum-information splitting, *J. Phys. B* **44**, 035505 (2011).
- [13] M.-Q. Bai and Z.-W. Mo, Hierarchical quantum information splitting with eight-qubit cluster states, *Quantum Inf. Process.* **12**, 1053 (2013).
- [14] J.-Y. Peng and Z.-W. Mo, Hierarchical and probabilistic quantum state sharing with a nonmaximally four-qubit cluster state, *Int. J. Quantum Inf.* **11**, 1350004 (2013).
- [15] G. Xu, C. Wang, and Y.-X. Yang, Hierarchical quantum information splitting of an arbitrary two-qubit state via the cluster state, *Quantum Inf. Process.* **13**, 43 (2014).
- [16] X.-W. Zha, N. Miao, and H.-F. Wang, Hierarchical quantum information splitting of an arbitrary two-qubit using a single quantum resource, *Int. J. Theor. Phys.* **58**, 2428 (2019).
- [17] H. Qin, W. K. S. Tang, and R. Tso, Hierarchical quantum secret sharing based on special high-dimensional entangled state, *IEEE J. Sel. Top. Quantum Electron.* **26**, 1 (2020).
- [18] S. Mishra, C. Shukla, A. Pathak, R. Srikanth, and A. Venugopalan, An integrated hierarchical dynamic quantum secret sharing protocol, *Int. J. Theor. Phys.* **54**, 3143 (2015).
- [19] M. Navascués, S. Singh, and A. Acín, Connector Tensor Networks: A Renormalization-Type Approach to Quantum Certification, *Phys. Rev. X* **10**, 021064 (2020).
- [20] S.-J. Ran, E. Tirrito, C. Peng, X. Chen, L. Tagliacozzo, G. Su, and M. Lewenstein, *Tensor Network Contractions: Methods and Applications to Quantum Many-Body Systems*, Lecture Notes in Physics Vol. 964 (Springer Nature, Cham, 2020).
- [21] J. Biamonte, Lectures on quantum tensor networks. [arXiv:1912.10049](https://arxiv.org/abs/1912.10049).
- [22] 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).
- [23] B. Sutherland, Quantum many-body problem in one dimension: Ground state, *J. Math. Phys.* **12**, 246 (1971).
- [24] G. Carleo and M. Troyer, Solving the quantum many-body problem with artificial neural networks, *Science* **355**, 602 (2017).
- [25] R. Islam, R. Ma, P. M. Preiss, M. E. Tai, A. Lukin, M. Rispoli, and M. Greiner, Measuring entanglement entropy in a quantum many-body system, *Nature (London)* **528**, 77 (2015).
- [26] S. Cheng, L. Wang, T. Xiang, and P. Zhang, Tree tensor networks for generative modeling, *Phys. Rev. B* **99**, 155131 (2019).

- [27] K. Chabuda, J. Dziarmaga, T. J. Osborne, and R. Demkowicz-Dobrzański, Tensor-network approach for quantum metrology in many-body quantum systems, *Nat. Commun.* **11**, 250 (2020).
- [28] S. J. Ran, Z. Z. Sun, S. M. Fei, G. Su, and M. Lewenstein, Tensor network compressed sensing with unsupervised machine learning, *Phys. Rev. Res.* **2**, 033293 (2020).
- [29] D. Liu, S.-J. Ran, P. Wittek, J. Peng, R. B. García, G. Su, and M. Lewenstein, Machine learning by unitary tensor network of hierarchical tree structure, *New J. Phys.* **21**, 073059 (2019).
- [30] Q. Zhang, H. Lai, and J. Pieprzyk, Quantum-key-expansion protocol based on number-state-entanglement-preserving tensor network with compression, *Phys. Rev. A* **105**, 032439 (2022).
- [31] H. Lai, J. Pieprzyk, L. Pan, and M. A. Orgun, Two types of dynamic quantum state secret sharing based on tensor networks states, *Physica A* **582**, 126257 (2021).
- [32] L. Cincio, J. Dziarmaga, and M. M. Rams, Multiscale Entanglement Renormalization Ansatz in Two Dimensions: Quantum Ising Model, *Phys. Rev. Lett.* **100**, 240603 (2008).
- [33] E. M. Stoudenmire, Learning relevant features of data with multi-scale tensor networks, *Quantum Sci. Technol.* **3**, 034003 (2018).
- [34] G. Vidal, Class of Quantum Many-Body States That Can Be Efficiently Simulated, *Phys. Rev. Lett.* **101**, 110501 (2008).
- [35] K. Furuya, N. Lashkari, and M. Moosa, Renormalization group and approximate error correction, [arXiv:2112.05099](https://arxiv.org/abs/2112.05099).
- [36] J. A. Reyes and E. M. Stoudenmire, Multi-scale tensor network architecture for machine learning, *Mach. Learn.* **2**, 035036 (2021).
- [37] S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi, and A. Amirlatifi, *Proceedings of the 2020 International Joint Conference on Neural Networks* (IEEE, Piscataway, 2020), pp. 1–8.
- [38] C. Lancien, O. Gühne, R. Sengupta, and M. Huber, Relaxations of separability in multipartite systems: Semidefinite programs, witnesses and volumes, *J. Phys. A: Math. Theor.* **48**, 505302 (2015).
- [39] M. Epping, H. Kampermann, C. Macciavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, *New J. Phys.* **19**, 093012 (2017).
- [40] L. Cincio, Strongly correlated systems, Ph.D. thesis, Jagiellonian University, 2011.
- [41] G. Vidal, Entanglement Renormalization, *Phys. Rev. Lett.* **99**, 220405 (2007).
- [42] G. Evenbly and G. Vidal, Entanglement Renormalization in Two Spatial Dimensions, *Phys. Rev. Lett.* **102**, 180406 (2009).
- [43] G. Evenbly and G. Vidal, Algorithms for entanglement renormalization, *Phys. Rev. B* **79**, 144108 (2009).
- [44] S.-J. Ran, A. Piga, C. Peng, G. Su, and M. Lewenstein, Few-body systems capture many-body physics: Tensor network approach, *Phys. Rev. B* **96**, 155120 (2017).
- [45] T.-C. Wei, R. Raussendorf, I. Affleck, Some aspects of Affleck–Kennedy–Lieb–Tasaki models: Tensor network, physical properties, spectral gap, deformation, and quantum computation, in *Entanglement in Spin Chains*, edited by A. Bayat, S. Bose, and H. Johannesson, Quantum Science and Technology (Springer, Cham, 2022), pp. 89–125.
- [46] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, Practical free-space quantum key distribution over 10 km in daylight and at night, *New J. Phys.* **4**, 43 (2002).
- [47] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Quantum Cryptography with Entangled Photons, *Phys. Rev. Lett.* **84**, 4729 (2000).
- [48] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, Quantum key distribution over 67 km with a plug&play system, *New J. Phys.* **4**, 41 (2002).
- [49] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Single Photon Quantum Cryptography, *Phys. Rev. Lett.* **89**, 187901 (2002).
- [50] H. Azuma and M. Ban, The intercept/resent attack and the collective attack on the six-state protocol of the quantum key distribution, [arXiv:1912.00196](https://arxiv.org/abs/1912.00196).
- [51] J. J. Sakurai and J. Napolitano, in *Modern Quantum Mechanics*, edited by J. Person, 2nd ed. (Addison-Wesley, Boston, 2014), Vol. 39.
- [52] B. A. Nguyen, Quantum exam, *Phys. Lett. A* **350**, 174 (2006).
- [53] H. Liu, L. T. Yang, Y. Guo, X. Xie, and J. Ma, An incremental tensor-train decomposition for cyber-physical-social big data, *IEEE Trans. Big Data* **7**, 341 (2018).