Quantum-key-expansion protocol based on number-state-entanglement-preserving tensor network with compression

Qiang Zhang,[1] Hong Lai,[1,*] and Josef Pieprzyk[2,3]
[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*

(Received 30 October 2021; accepted 7 March 2022; published 24 March 2022)

Quantum-key-distribution (QKD) protocols allow exchanging a cryptographic key between two parties. With the development of the Internet, however, all forms of communications consume a huge number of cryptographic keys. Improving the secure key rate of QKD is becoming increasingly important. Quantum compression and key expansion are two ways to increase the secure key rate. In this paper, we propose a quantum-key-expansion (QKE) protocol. A series of singlet states are compressed by number-state-entanglement-preserving tensors and disentanglers to obtain a compressed two-body-entangled state. The cryptographic key is expanded by the number-state-entanglement-preserving tensor network. The advantages of the proposed QKE protocol over the classical-key-expansion algorithm in the key-expansion method, the key length, and the security are discussed in this study. Moreover, due to the structure of the number-state-preserving compression tensor network, our protocol can resist the intercept-resend attack, entanglement-and-measurement attack, and coherent attack.

DOI: 10.1103/PhysRevA.105.032439

I. INTRODUCTION

There are two classes of quantum-key-distribution (QKD) protocols. The first class is prepare-and-measure protocols, such as the Bennett-Brassard 1984 (BB84) QKD [1], the Bennett 1992 (B92) QKD [2], the decoy-state QKD [3], the measurement-device-independent (MDI) QKD [4,5], the round-robin differential phase shift (RRDPS) QKD [6], and the twin-field (TF) QKD [7] in which the present farthest distance is up to 833 km [8]. For the general prepare-and-measure protocols, a sender, Alice, prepares quantum states and sends them to a receiver, Bob, who performs the measurement on his received quantum states. While Bob can avoid performing the measurements [9], the second class is entangle-based protocols, such as the Ekert 1991 (E91) QKD [10] and the Bennett-Brassard-Mermin 1992 (BBM92) QKD [11]. For the general entangle-based protocols, a pair of entangled photons is prepared by Alice or a third party [12]. One photon is kept by Alice and the other is sent to Bob. Then Alice and Bob measure their photons. The entangle-based protocols have recently attracted more attention from the research community. Zhang *et al.* [13] have proposed a QKD protocol based on two Bell entangled states. Tchoffo *et al.* [14] have designed a novel QKD protocol based on entangled photons with a pseudorandom basis. Works [15–17] have shown how to use high-dimensional entangled states to construct QKD protocols.

With the development of the Internet, a large amount of data is generated and communicated in a pretty short time. Thus it is critical in modern digital technology to compress data into the smallest possible space [18]. In the quantum domain, storing large amounts of data in the smallest possible space is urgent because of the high cost of storing data and the requirement for sophisticated error correction techniques, due to limited quantum storage resources [19]. However, quantum compression can effectively utilize valuable quantum resources while reducing quantum memory [18], which is important for both quantum computing and quantum communication [20]. In particular, in quantum communication, quantum compression can reduce the quantum memory requirements of quantum networks and facilitate the communication between nodes in the network [21,22].

On the other hand, all forms of communication consume a huge number of secret keys in reality [23]. As a result, key expansion is an effective means of increasing the key rate in the communication process. Key expansion is commonly used in classical cryptography to improve security [24]. The expanded key is used to encrypt the same piece of plain text in algorithms such as the advanced encryption standard (AES) [25]. The disadvantage of this method is that, if a specific round key is known, all round keys become easier to crack [26]. Quantum key expansion (QKE) can overcome this disadvantage. The general QKE protocol used the standard QKD protocol to generate a short secure seed key, which is then used to complete the key expansion. Thus QKE can provide higher security than AES [27,28]. Hwang *et al.* [29] proposed a QKD protocol without public announcement of bases (PAB), which can be seen as a QKE scheme. This protocol first uses a BB84 protocol to share a secure key as the encoding base between Alice and Bob. Then, Alice prepares the signal state and sends it to Bob, who measures the received signal state by the shared base sequence. As long as Eve does not know the base, Alice and Bob can use this base sequence to repeatedly complete the key-distribution process. However, the disadvantage is that the eavesdropper Eve can obtain

[*] Corresponding author: hlai@swu.edu.cn

the key information by fixing a base to measure the signal state and inferring the base information from the information transferred between Alice and Bob [23]. Based on the QKD without PAB protocol, Ji *et al.* [30] showed that the QKE protocol is a powerful tool for enhancing the maximum distance of key distribution. Likewise, Wang [31] proposed a QKE protocol without measurement mismatch, which costs almost zero classical communication and consumes fewer qubits than that in the standard protocols. Vlachos *et al.* [27] prepared the seed key as the initial state of the quantum cellular automata and obtain a larger key by changing the period of quantum cellular automata states. Luo *et al.* [32] and Hsu *et al.* [33] used the seed key to the postprocessing of the standard QKD protocol, in order to produce a larger key. Recently, Arrazola *et al.* [24] and Tahmasbi *et al.* [34] consumed the seed key to generate the expansion key from the covert communication, respectively.

In this paper, we investigate quantum compression and its application for a design of more efficient QKE protocols. In particular, we focus our attention on singlet states, which can be compressed by a tensor network (TN). There are several TN models that include the matrix product state (MPS) [35], tree tensor network (TTN) [36], projected entangled pair state (PEPS) [37], and multiscale entanglement renormalization ansatz (MERA) [38]. TN models are a key component of current quantum physics [39]. They provide an effective and accurate way to simulate strongly correlated quantum systems.

Note that, due to their good compression features, quantum tensor networks have been recently used in machine learning [40–42]. Using a minimal number of parameters, TN can get close to or even beat classical machine learning. This is achieved by reducing the dimension of data from exponential to polynomial. Bai *et al.* [21] have used a local compression protocol to build a TTN model that may theoretically perform lossless compression of the AKLT state [43]. Evenbly [44] has suggested a number-state-preserving tensor network with a MERA structure.

In this paper, we extend number-state-preserving tensor network into number-state-entanglement-preserving tensor network with quantum compression. Our TN model is then applied to singlet states. A resulting entangled photon pair is used to perform the QKD protocol. We verify theoretically that our compression model has a matching number-state-entanglement-preserving tensor so a compression process for singlet states can be completed. We demonstrate that our compression model scales well.

The rest of the paper is organized as follows. Section II introduces necessary background. Section III provides details of number-state-entanglement-preserving tensor networks. Section IV describes our QKE protocol. Section V presents the security analysis. Section VI concludes the paper and discusses future research.

II. PRELIMINARIES

A. Number-state-preserving compression tensors

Consider a lattice with L sites, where each site is described by a local Hilbert space of dimension 2. The base state of every site is denoted as $|z\rangle \in \{|0\rangle, |1\rangle\}$, where $|0\rangle = [1, 0]^{\mathrm{T}}$, $|1\rangle = [0, 1]^{\mathrm{T}}$. Then, the number state is defined as [44]

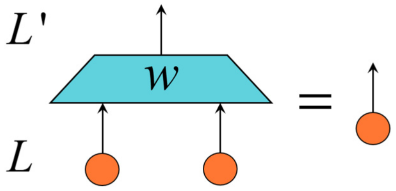

FIG. 1. Illustration of the number-state-preserving compression tensor w.

$$|Z^L\rangle = \bigotimes_{k=0}^{L-1} |z^k\rangle, \tag{1}$$

where $k = 0, 1, \ldots, L-1$ is the lattice position.

A number-state-preserving compression tensor can be regarded as a mapping from one number state to another [44]. For example, the number-state-preserving compression tensor w is defined as follows:

$$w = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}. \tag{2}$$

Then, applying w to a number state $|Z^2\rangle = |z^0\rangle \otimes |z^1\rangle$, we obtain

$$|0\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle \xrightarrow{w} |0\rangle, \quad |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle \xrightarrow{w} |1\rangle. \tag{3}$$

A number-state-preserving compression tensor w can alternatively be expressed as a direction-determined tensor (see Fig. 1), where the index contains the input and output edges. The lattice L represents the input side, while the lattice L' representsthe output side.

B. Disentangler

Vidal [38] has proposed the concept of disentangler. It is a unitary transformation that removes short-range entanglement [45]. For example, given a disentangler u as follows:

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

where $uu^\dagger = u^\dagger u = I$, then, for the state $1/\sqrt{2}(|00\rangle + |11\rangle)$, we obtain

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{u} |00\rangle. \tag{4}$$

This means that u disentangles $1/\sqrt{2}(|00\rangle + |11\rangle)$ into a product state $|00\rangle$.

III. NUMBER-STATE-ENTANGLEMENT-PRESERVING TENSOR NETWORK

A number-state-preserving compression tensor input is kept as a direct product state as indicated in Sec. II A. We will now expand it to cover a case of an entangled state. For example, given an input state that consists of one singlet state and two spin-1/2 photons, i.e., $|L\rangle \otimes 1/\sqrt{2}(|01\rangle - |10\rangle) \otimes |R\rangle$, where $|L\rangle, |R\rangle \in \{|0\rangle, |1\rangle\}$. Similar to Eqs. (2) and (3), we define number-state-preserving tensors w_1 and w_2 as follows:

$$w_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \tag{5}$$

where

$$\begin{aligned} &|0\rangle|0\rangle, |1\rangle|1\rangle \xrightarrow{w_1} |0\rangle, \quad |0\rangle|1\rangle, |1\rangle|0\rangle \xrightarrow{w_1} |1\rangle, \\ &|0\rangle|0\rangle, |1\rangle|1\rangle \xrightarrow{w_2} |1\rangle, \quad |0\rangle|1\rangle, |1\rangle|0\rangle \xrightarrow{w_2} |0\rangle. \end{aligned} \tag{6}$$

We define $W_1 := w_1 \otimes w_1$ and $W_2 := w_2 \otimes w_2$. They output entangled states. For $|L\rangle = |0\rangle$, we choose W_1 and obtain

$$\begin{aligned} &|0\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |0\rangle \xrightarrow{W_1} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \\ &|0\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |1\rangle \xrightarrow{W_1} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \end{aligned} \tag{7}$$

For $|L\rangle = |1\rangle$, we use W_2 and get

$$\begin{aligned} &|1\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |0\rangle \xrightarrow{W_2} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \\ &|1\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |1\rangle \xrightarrow{W_2} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \end{aligned} \tag{8}$$

Next, we apply different numbers of single states as an initial input. We explore ways we can design a number-state-entanglement-preserving tensor network using number-state-compression-preserving tensors and disentanglers.

Example 1. Eight-particle input states composed of three singlet states. Suppose $|L\rangle = 0$ and $|R\rangle = 0$; the initial input state is defined as

$$\begin{aligned} |\Psi_I\rangle &= |0\rangle \otimes \bigotimes_{i=1}^{3} |\Psi_i^-\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}\bigg[\frac{1}{\sqrt{2}}(|0010\rangle - |0100\rangle) \otimes \frac{1}{\sqrt{2}}(|1010\rangle - |1100\rangle) \\ &\quad - \frac{1}{\sqrt{2}}(|0011\rangle - |0101\rangle) \otimes \frac{1}{\sqrt{2}}(|0011\rangle - |0101\rangle)\bigg]. \end{aligned} \tag{9}$$

According to $|L\rangle = |0\rangle$ and Eqs. (6) and (7), we first apply a tensor w_1 layer (see Fig. 2) to $|\Psi_I\rangle$. The output is

$$\begin{aligned} |\Psi_1^o\rangle &= W_1|\Psi_I\rangle \\ &= \frac{1}{\sqrt{2}}\bigg[\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \\ &\quad - \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\bigg], \end{aligned} \tag{10}$$

where the index o of $|\Psi_1^o\rangle$ means the output and $W_1 = \bigotimes_{i=1}^4 w_1$ is the tensor product of all w_1 in the first layer.

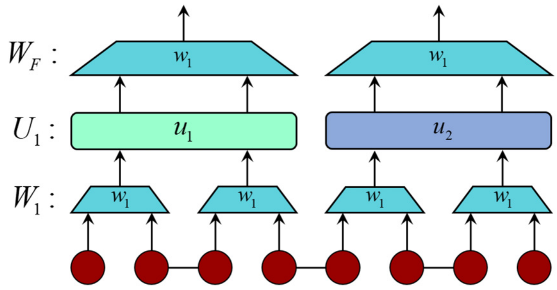

FIG. 2. Three layer number-state-entanglement-preserving tensor network. The choice of W_1 is determined by state $|L\rangle$; if $|L\rangle = |0\rangle$, then $W_1 = \bigotimes_{i=1}^4 w_1$; otherwise, $W_1 = \bigotimes_{i=1}^4 w_2$. The layer U_1 disentangles the output of W_1 and produces a result that we want. Finally, W_F outputs the compressed entangled state.

Similar to Eq. (4), we define disentanglers

$$u_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{11}$$

and

$$u_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \tag{12}$$

and obtain the product state

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xrightarrow{u_1} |01\rangle, \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xrightarrow{u_1} |00\rangle, \\ &\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xrightarrow{u_2} |01\rangle, \quad \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \xrightarrow{u_2} |11\rangle. \end{aligned} \tag{13}$$

Using $U_1 = u_1 \otimes u_2$, we remove short-range entanglement of $|\Psi_1^o\rangle$ and get

$$\begin{aligned} |\Psi_2^o\rangle = U_1|\Psi_1^o\rangle &= \frac{1}{\sqrt{2}}(|0111\rangle - |0001\rangle) \\ &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \otimes |1\rangle. \end{aligned} \tag{14}$$

At last, we apply a final tensor $W_F = w_1 \otimes w_1$ and obtain a compressed entangled state

$$|\Psi_F\rangle = W_F|\Psi_2^o\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle). \tag{15}$$

A three layer number-state-entanglement-preserving tensor network is shown in Fig. 2.

Example 2. 16-particle input states composed of seven singlet states. We set $|L\rangle = |0\rangle$ and $|R\rangle = |0\rangle$ and the initial input is $|\Phi_I\rangle = |0\rangle \otimes \bigotimes_{i=1}^{7} |\Psi_i^-\rangle \otimes |0\rangle$. As $|L\rangle = |0\rangle$ and according to Eqs. (6) and (7), we first apply a tensor w_1 layer to $|\Phi_I\rangle$. The result is

$$\begin{aligned}
|\Phi_1^o\rangle &= W_1|\Phi_I\rangle \\
&= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) - \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \\
&\quad \times \otimes \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) - \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \\
&\quad + \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) - \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\
&\quad \times \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\
&\quad + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) - \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
&\quad \times \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),
\end{aligned} \tag{16}$$

where $W_1 = \bigotimes_{i=1}^{8} w_1$. Similar to Example 1, we set disentanglers as

$$u_3 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{17}$$

and

$$u_4 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}. \tag{18}$$

We obtain a product state

$$\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \xrightarrow{u_3} |10\rangle, \quad \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \xrightarrow{u_3} |11\rangle, \quad \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \xrightarrow{u_4} |10\rangle, \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xrightarrow{u_4} |00\rangle. \tag{19}$$

Combining Eqs. (13) and (19) and applying $U_1 = u_1 \otimes u_2 \otimes u_3 \otimes u_2$ for $|\Phi_1^o\rangle$, we get

$$|\Phi_2^o\rangle = U_1|\Phi_1^o\rangle = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0111\rangle - |0001\rangle) \otimes \frac{1}{\sqrt{2}}(|1111\rangle - |1001\rangle) - \frac{1}{\sqrt{2}}(|0101\rangle - |0011\rangle) \otimes \frac{1}{\sqrt{2}}(|1011\rangle - |1100\rangle)\right]. \tag{20}$$

Further, we use $W_2 = \bigotimes_{i=1}^{4} w_1$ to compress $|\Phi_2^o\rangle$ again and we obtain

$$|\Phi_3^o\rangle = W_2|\Phi_2^o\rangle = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) - \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) \otimes \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)\right]. \tag{21}$$

We use $U_2 = u_3 \otimes u_4$ to remove a short-range entanglement of $|\Phi_3^o\rangle$. We get

$$|\Phi_4^o\rangle = U_2|\Phi_2^o\rangle = |1\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes |0\rangle. \tag{22}$$

Finally, we apply the tensor $W_F = w_1 \otimes w_1$ and obtain a compressed entangled state $|\Phi_F\rangle = W_F|\Phi_4^o\rangle = 1/\sqrt{2}(|10\rangle - |01\rangle)$. A five layer number-state-entanglement-preserving tensor network is shown in Fig. 3. Now we are ready to discuss a generic case.

Proposition 1. The internal entangled state in $|\Psi_I\rangle$ is unaffected by the boundary state choices $|L\rangle$ and $|R\rangle$.

Proof. If there are n single states, the initial input state is defined as

$$\begin{aligned}|\Psi_I\rangle &= |L\rangle \otimes \bigotimes_{i=1}^{n} |\Psi_i^-\rangle \otimes |R\rangle \\ &= \frac{1}{2}\Bigg\{\left[|L\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |0\rangle\right] \otimes \left[|1\rangle \otimes \bigotimes_{i=3}^{n-3} |\Psi_i^-\rangle \otimes |0\rangle\right] \otimes \left[|1\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |R\rangle\right] \\ &\quad - \left[|L\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |0\rangle\right] \otimes \left[|1\rangle \otimes \bigotimes_{i=3}^{n-3} |\Psi_i^-\rangle \otimes |1\rangle\right] \otimes \left[|0\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |R\rangle\right] \\ &\quad - \left[|L\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |1\rangle\right] \otimes \left[|0\rangle \otimes \bigotimes_{i=3}^{n-3} |\Psi_i^-\rangle \otimes |0\rangle\right] \otimes \left[|1\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |R\rangle\right] \\ &\quad + \left[|L\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |1\rangle\right] \otimes \left[|0\rangle \otimes \bigotimes_{i=3}^{n-3} |\Psi_i^-\rangle \otimes |1\rangle\right] \otimes \left[|0\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |R\rangle\right]\Bigg\}. \end{aligned} \tag{23}$$

Obviously, while different choices for $|L\rangle$ and $|R\rangle$ affect the result of $|L\rangle \otimes 1/\sqrt{2}(|01\rangle - |10\rangle) \otimes |0\rangle$ and number-state-preserving tensors, they have no effect on the internal entanglement state such as $|1\rangle \otimes \bigotimes_{i=3}^{n-3} |\Psi_i^-\rangle \otimes |0\rangle$. This proves the proposition.

Proposition 2. Given $n = 2^\ell - 1$ singlet states, then there is a collection of disentanglers.

Proof (by induction for ℓ). (1) Assume that $\ell = 1$. Then the input state is $|L\rangle \otimes 1/\sqrt{2}(|01\rangle - |10\rangle) \otimes |R\rangle$. After the action of W, a compressed entanglement state is $1/\sqrt{2}(|L'R'\rangle - |\bar{L}'\bar{R}'\rangle)$ and there is a disentangler u that satisfies

$$\frac{1}{\sqrt{2}}(|L'R'\rangle - |\bar{L}'\bar{R}'\rangle) \xrightarrow{u} |L'R'\rangle.$$

(2) Assume that $\ell = 2$ and $n = 3$. This case is an eight-particle input state composed of three singlet states (Example 1). Thus there is an appropriate disentangler.

(3) Assume $\ell = k$, $n = 2^k - 1$, and the input state is $|L\rangle \otimes \bigotimes_{i=1}^{2^k-1} |\Psi_i^-\rangle \otimes |R\rangle$. After the action of the number-state-preserving W, there is a disentangler that meets the proposition.

When $\ell = k + 1$, the input state is $|L\rangle \otimes \bigotimes_{i=1}^{2^{k+1}-1} |\Psi_i^-\rangle \otimes |R\rangle$, which could be represented as follows:

$$\begin{aligned}&|L\rangle \otimes \bigotimes_{i=1}^{2^{k+1}-1} |\Psi_i^-\rangle \otimes |R\rangle \\ &\quad = |L\rangle \otimes |\Psi_L\rangle \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes |\Psi_R\rangle \otimes |R\rangle \\ &\quad = \frac{1}{\sqrt{2}}[(|L\rangle \otimes |\Psi_L\rangle \otimes |0\rangle) \otimes (|1\rangle \otimes |\Psi_R\rangle \otimes |R\rangle) \\ &\qquad - (|L\rangle \otimes |\Psi_L\rangle \otimes |1\rangle) \otimes (|0\rangle \otimes |\Psi_R\rangle \otimes |R\rangle)], \end{aligned} \tag{24}$$

where $|\Psi_L\rangle = \bigotimes_{i=1}^{2^k-1} |\Psi_i^-\rangle$ and $|\Psi_R\rangle = \bigotimes_{i=2^k+1}^{2^{k+1}-1} |\Psi_i^-\rangle$. Due to the fact that the disentangler exists when the input state is $|L\rangle \otimes \bigotimes_{i=1}^{2^k-1} |\Psi_i^-\rangle \otimes |R\rangle$, the matching disentanglers can also be found when the input state is $|L\rangle \otimes \bigotimes_{i=1}^{2^k-1} |\Psi_i^-\rangle \otimes |0\rangle(|1\rangle)$ or $(|1\rangle)|0\rangle \otimes \bigotimes_{i=2^k+1}^{2^{2k}-1} |\Psi_i^-\rangle \otimes |R\rangle$. This indicates that Proposition 2 is correct.

According to Propositions 1 and 2, we theoretically prove that our model is scalable. Algorithm. 1 shows details of compression.

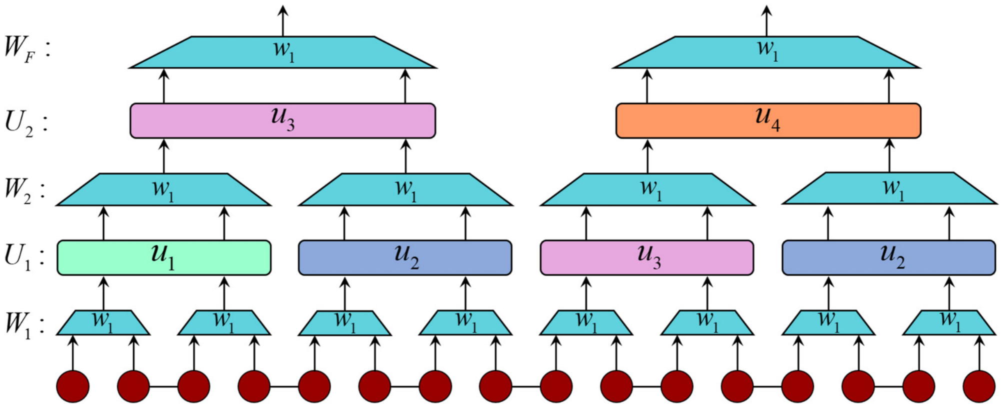

FIG. 3. Five layer number-state-entanglement-preserving tensor network. The choice of W_1 and W_2 is determined by state $|L\rangle$; if $|L\rangle = |0\rangle$, then $W_1 = \bigotimes_{i=1}^{8} w_1$ and $W_2 = \bigotimes_{i=1}^{4} w_1$. Otherwise, if $|L\rangle = |1\rangle$, then $W_1 = \bigotimes_{i=1}^{8} w_2$ and $W_2 = \bigotimes_{i=1}^{4} w_2$. The layers U_1 and U_2 disentangle the output of W_1 and W_2. Finally, W_F outputs the compressed entangled state.

Algorithm 1: Compression algorithm

```
Input: $n$ singlet states $|\Psi^-\rangle$, $|L\rangle$, $|R\rangle$
Output: $|\Psi_F\rangle$
initialize $w_1, w_2, u_1, u_2, u_3, u_4$;
calculate $|\Psi_I\rangle \leftarrow |L\rangle \otimes \bigotimes_{i=1}^{n} |\Psi_i^-\rangle \otimes |R\rangle$;
calculate the number of layer $l$;
if $|L\rangle = |0\rangle$ and $|R\rangle = |0\rangle$ or $|R\rangle = |1\rangle$ then
    $N \leftarrow n+1$;
    initialize the output: $|\Psi_F\rangle \leftarrow |\Psi_I\rangle$;
    for $i = 1$ to $l/2$ do
        $W \leftarrow \bigotimes_{i=1}^{N} w_1$;
        $U \leftarrow u_1 \otimes \bigotimes_{i=1}^{N/4-1} (u_2 \otimes u_3)_i \otimes u_4$;
        $|\Psi_F\rangle \leftarrow U \times W \times |\Psi_F\rangle$;
        $N \leftarrow N/2$;
    end
else
    $N \leftarrow n+1$;
    initialize the output: $|\Psi_F\rangle \leftarrow |\Psi_I\rangle$;
    for $i = 1$ to $l/2$ do
        $W \leftarrow \bigotimes_{i=1}^{N} w_2$;
        $U \leftarrow u_1 \otimes \bigotimes_{i=1}^{N/4-1} (u_2 \otimes u_3)_i \otimes u_4$;
        $|\Psi_F\rangle \leftarrow U \times W \times |\Psi_F\rangle$;
        $N \leftarrow N/2$;
    end
end
if $|L\rangle = |0\rangle$ and $|R\rangle = |0\rangle$ or $|R\rangle = |1\rangle$ then
    $|\Psi_F\rangle \leftarrow w_1 \otimes w_1 \times |\Psi_F\rangle$;
else
    $|\Psi_F\rangle \leftarrow w_2 \otimes w_2 \times |\Psi_F\rangle$;
end
```

IV. QUANTUM-KEY-EXPANSION PROTOCOL

A. Our protocol

In this section, we design a QKE protocol that applies our compression algorithm. We assume that an eavesdropper, Eve, knows everything about the key preparation except the initial state $|\Psi_I\rangle$ and the structure of the number-state-entanglement-preserving tensor network. Further, suppose that Alice and Bob have agreed on n singlet states, $|L\rangle$, and $|R\rangle$.

Step 1. Initial-state compression. Assume that an agreed initial state is

$$|\Psi_I\rangle = |L\rangle \otimes \bigotimes_{i=1}^{n} |\Psi_i^-\rangle \otimes |R\rangle, \tag{25}$$

where $|\Psi_i^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$. Alice compresses the $|\Psi_I\rangle$ using Algorithm. 1 and obtains the compressed entangled state

$$|\Psi_F\rangle = \frac{1}{\sqrt{2}}(|L_F\rangle|R_F\rangle - |L_F'\rangle|R_F'\rangle), \tag{26}$$

where $|L_F\rangle(|R_F\rangle) = |0\rangle(|1\rangle)$ and $|L_F'\rangle(|R_F'\rangle) = |1\rangle(|0\rangle)$.

Step 2. Key generation. Using the compressed entangled state $|\Psi_F\rangle$, Alice and Bob complete the QKD. For example, the first photon in Eq. (26) is kept by Alice and the second photon is sent to Bob via a quantum channel. Alice and Bob choose one of two bases randomly to measure each photon they receive. After measurement, they tell each other what basis they have used. This is done via a classical channel. As in the BB84 and BBM92 protocols, Alice and Bob keep the measurement result if it matches the correct basis. Otherwise, they discard it [1,11].

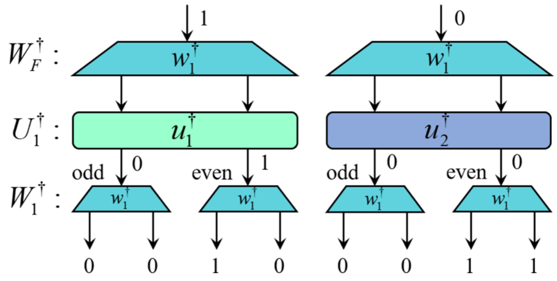

FIG. 4. Illustration of key generation. Assume the measurement result of Eq. (15) is $|10\rangle$. Then, use $|10\rangle$ as the input of $W_F^\dagger$ and output the entangled state $(|01\rangle + |10\rangle) \otimes (|00\rangle + |11\rangle)$. $U_1^\dagger$ disentangles the state into a product state $|0100\rangle$. The state as the input for $w_1^\dagger$ of $W_1^\dagger$ at the odd site decodes $|0\rangle(|1\rangle)$ into $|00\rangle(|01\rangle)$ and decodes $|0\rangle(|1\rangle)$ into $|11\rangle(|10\rangle)$ at the even site. Finally, according to the site of $w_1^\dagger$ at the $W_1^\dagger$ layer, we determine the generated key bits 00100011.

Next, Alice publishes a small number of photons chosen at random. This allows Bob to determine an error rate of quantum channel. If the error rate is lower than a predetermined threshold, they conclude that communication is reliable and free from outside interference. Finally, Alice informs Bob about the number of layers in this tensor network, $|L\rangle$, $|R\rangle$ and the rule for decompressing the compressed entangled state. The communication is done over a classical channel. Example 1 from Sec. III shows how to extract a secure cryptographic key from the compressed entangled state $|\Psi_F\rangle = 1/\sqrt{2}(|10\rangle - |01\rangle)$ [see Eq. (15)].

Assume that the measurement result is $|10\rangle$. First, we consider $|10\rangle$ as the input of the final tensor $W_F^\dagger := w_1^\dagger \otimes w_1^\dagger$ as follows:

$$W_F^\dagger|10\rangle = w_1^\dagger|1\rangle \otimes w_1^\dagger|0\rangle = (|01\rangle + |10\rangle) \otimes (|00\rangle + |11\rangle). \tag{27}$$

Next, we take $(|01\rangle + |10\rangle) \otimes (|00\rangle + |11\rangle)$ as the input of $U^\dagger = u_1^\dagger \otimes u_2^\dagger$ and obtain

$$\begin{aligned} &U^\dagger[(|01\rangle + |10\rangle) \otimes (|00\rangle + |11\rangle)] \\ &\quad = u_1^\dagger(|01\rangle + |10\rangle) \otimes u_2^\dagger(|00\rangle + |11\rangle) \\ &\quad = |01\rangle \otimes |00\rangle. \end{aligned} \tag{28}$$

Finally, we consider $|01\rangle \otimes |00\rangle$ as the input of $W_1^\dagger = w_1^\dagger \otimes w_1^\dagger \otimes w_1^\dagger \otimes w_1^\dagger$ and obtain

$$\begin{aligned} W_1^\dagger|0100\rangle &= w_1^\dagger|0\rangle \otimes w_1^\dagger|1\rangle \otimes w_1^\dagger|0\rangle \otimes w_1^\dagger|0\rangle \\ &= (|00\rangle + |11\rangle) \otimes (|01\rangle + |10\rangle) \\ &\quad \times \otimes(|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle). \end{aligned} \tag{29}$$

We assume the following encoding for $w_1^\dagger$ of $W_1^\dagger$ at the odd site (see Fig. 4). We encode $|00\rangle(|01\rangle)$ into $|0\rangle(|1\rangle)$, respectively. Likewise, encoding for $w_1^\dagger$ of $W_1^\dagger$ at the even site is $|0\rangle(|1\rangle)$ for $|11\rangle(|10\rangle)$, respectively. Consequently, both Alice and Bob can establish a common cryptographic key 00100011. Key generation is shown in Fig. 4.

TABLE I. Efficiency of different protocols.

Protocol	$\mathcal{Q}$	$\mathcal{R}$	b	$\mathcal{E}(\%)$
BB84 [1]	0.5	1	1	25%
BBM92 [11]	1	1	1	50%
Example 1	8	8	1	88.9%
Example 2	16	16	1	94.1%
QKD without PAB [29]	1	1	0	100%

B. Information transmission efficiency

From the point of view of information theory, the information transmission efficiency $\mathcal{E}$ of a QKD protocol is defined as follows [46]:

$$\mathcal{E} = \frac{\mathcal{Q}}{\mathcal{R} + b}, \tag{30}$$

where $\mathcal{Q}$ is the number of bits in the key, $\mathcal{R}$ is the number of qubits, and b is the number of classical bits interchanged between communication parties. In the BB84 protocol, $\mathcal{Q} = 0.5$, $\mathcal{R} = 1$, and $b = 1$. $b = 1$ is used to indicate whether Alice and Bob use the same measuring base [47]. Thus the efficiency of BB84 is 25%. In the BBM92 protocol, $\mathcal{Q} = 1$, $\mathcal{R} = 1$, and $b = 1$. The efficiency is 50%. Theoretically, the QKE protocol (i.e., QKD without PAB) proposed by Hwang *et al.* [29] is capable of reaching 100% efficiency [23] with $\mathcal{Q} = 1$ and $\mathcal{R} = 1$. Due to the elimination of the measurement base announcement, $b = 0$.

However, while the protocol we proposed compresses $|\Psi_I\rangle$ into $|\Psi_F\rangle$, and the QKD process of $|\Psi_F\rangle$ can be done in the same way as the BBM92 protocol, this does not imply that our protocol's efficiency is comparable to the BBM92 protocol. For example, in the case of Example 1, the initial state $|\Psi_I\rangle$ contains eight photons, $\mathcal{R} = 8$. Then, decompressing the compressed entangled state can generate eight bits secure key, $\mathcal{Q} = 8$. Alice and Bob need one bit to indicate the information of the base, $b = 1$. Thus the efficiency of our protocol is 88.9%. Likewise, in the case of Example 2, the efficiency is 94.1%. The efficiency $\mathcal{E}$ of different protocols is shown in Table I. As the number of photons in $|\Psi_I\rangle$ increases, the efficiency of our protocol tends to 100%.

To compare the length of generated security keys among different protocols, we ran simulations on QuVis [48] for BB84, BBM92, QKD without PAB, and Example 1. The experiment setup is as follows. (1) Alice sends polarized photons to Bob at random. (2) Eve uses random bases to eavesdrop the quantum channel between Alice and Bob, except for the QKD protocol without PAB. (3) The experiment is completed by "fast forward 100 photons" (i.e., a fast simulation of 100 single-photon sending processes). (4) The number of photons in the experiment is 100 to 1000. (5) The experiment of Example 1 is completed by decompressing the key obtained from BBM92. (6) Parameters measured in this experiment are the value of N key (N_k) for each protocol. The result of experiments shows that our protocol can generate larger security keys than BB84, BBM92, and QKD without PAB. The result is shown in Fig. 5.

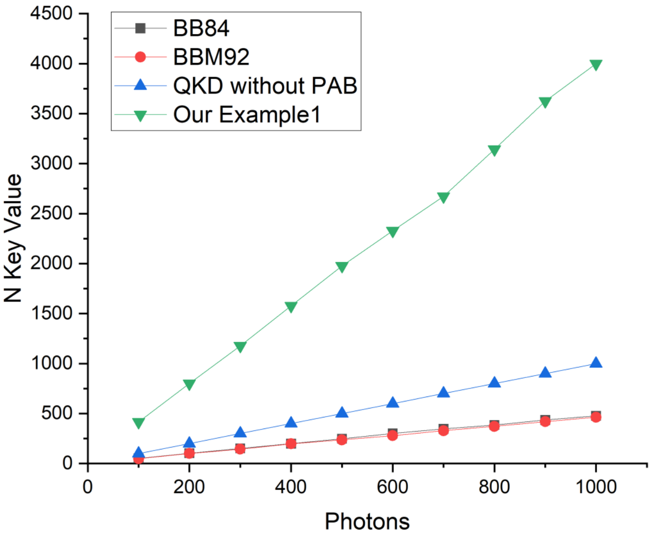

FIG. 5. Length of the secure key generated by different protocols. The results show that our protocol can generate larger security keys compared to the traditional BB84, BBM92, or QKE protocol, i.e., QKD without PAB.

C. Distinction between classical-key expansion and our protocol

Compared with the classical-key-expansion method, such as the AES key-expansion algorithm, our protocol has advantages in terms of the key-expansion method, the key length, and the security. The details are as follows.

Key-expansion method. The method for AES key expansion is to use the initial key to generate the round key for the process of encryption and decryption by mathematical computation [49]. The extended round key can be used timely in encryption. However, the disadvantage is that, if a specific round of keys is known, all round keys become easier to crack [26]. In contrast, the quantum compression method used in our protocol can improve this problem, because the secure key generated by our protocol is random.

Key length. If the key can be extended to any length, the key-extension approach is more effective [50]. The AES key-expansion method has three different lengths of keys, namely AES-128, AES-192, and AES-256 [25]. As a result, the length of each round of key expansion is also 128, 192, and 256, respectively. In contrast, the key generated by our protocol satisfies the power of 2 which tends more to this requirement.

Security. When executing the subkey expansion, AES performs the three operations SubBytes, ShiftRows, and MixColumns [25,26]. Key cracking becomes more complex as a result of these operations. Thus the security of the AES key-expansion method comes from the computational complexity. Theoretically, however, this complexity can be broken by quantum computers [49]. In contrast, the security of our protocol is guaranteed by the quantum compression and the number-state-entanglement-preserving tensor network, which we discuss in Sec. V.

We display the distinction between classical-key expansion and our protocol in Table II.

TABLE II. Comparison between the classical-key-expansion method in AES algorithm and our protocol.

Features	Classical-key expansion	Our protocol
Method	Mathematical computation	Quantum compression and quantum entanglement
Key length	128,192,256	The power of 2
Security	Computational complexity	Quantum compression and the tensor network

V. SECURITY ANALYSIS

As we have discussed in Sec. IV A, Alice and Bob use compressed entangled states to complete the standard QKD process, such as BBM92. We can obtained the secure key by decompressing the measured result. Thus the BBM92 protocol ensures the security of the compressed state in the communication process. In this section, we focus on the security analysis of the proposed number-state-entanglement-preserving tensor network and discuss three types of attack: intercept-resend attack, entanglement-and-measurement attack, and coherent attack. Eve has no knowledge about the initial state $|\Psi_I\rangle$ and the structure of the number-state-entanglement-preserving tensor network.

Intercept-resend attack. In this attack, Eve measures each photon on a randomly chosen basis. Then, she resends the resulting state to Bob. For the case of Example 1, the compressed state is $|\Psi_F\rangle = 1/\sqrt{2}(|10\rangle - |01\rangle)$. Alice holds the first photon and sends the second photon to Bob. Eve intercepts the second photon and measures it. Assume her measurement result is $|0\rangle$. However, without the knowledge of the initial state and the structure of the tensor network, she cannot be sure whether the result is $|10\rangle$ or $|00\rangle$. As we have discussed in Sec. IV A, the measurement result between Alice and Bob is $|10\rangle$. If the result of Eve is $|00\rangle$, she cannot obtain any information about the cryptographic key. If the result of Eve is $|10\rangle$, without the knowledge about the tensor network, she also cannot obtain any information about the cryptographic key.

Entanglement-and-measurement attack. In this attack, Eve prepares ancillary state $|\epsilon\rangle$ to entangle with each photon she intercepts. For the case of Example 1, Eve entangles the ancillary state $|\epsilon\rangle$ with the sent photon using a unitary transformation $U_{B\epsilon}$, and she obtains the combined state as follows:

$$|\Psi_C\rangle = U_{B\epsilon}|\Psi_F\rangle|\epsilon\rangle = U_{B\epsilon}\frac{1}{\sqrt{2}}(|1_A0_B\rangle - |0_A1_B\rangle)|\epsilon\rangle. \quad (31)$$

For example, if $U_{B\epsilon}$ is a CNOT (controlled-NOT) transformation, the ancillary state $|\epsilon\rangle = |0_\epsilon\rangle$ and then the combined state $|\Psi_C\rangle = 1/\sqrt{2}(|1_A0_B0_\epsilon\rangle - |0_A1_B1_\epsilon\rangle)$. However, without the knowledge about the initial state and the structure of the tensor network, the combined states Eve can guess are $1/\sqrt{2}(|0_A0_B0_\epsilon\rangle + |1_A1_B1_\epsilon\rangle)$, $1/\sqrt{2}(|0_A0_B0_\epsilon\rangle - |1_A1_B1_\epsilon\rangle)$, $1/\sqrt{2}(|1_A0_B0_\epsilon\rangle + |0_A1_B1_\epsilon\rangle)$, and $1/\sqrt{2}(|1_A0_B0_\epsilon\rangle - |0_A1_B1_\epsilon\rangle)$. Considering the measurement result of Eve is $|0_\epsilon\rangle$, she cannot be sure whether the result between Alice and Bob is $|1_A0_B\rangle$ or $|0_A0_B\rangle$. If she chooses $|0_A0_B\rangle$, she cannot obtain any information about the cryptographic key. If she chooses $|1_A0_B\rangle$, without the knowledge about the tensor network, she cannot obtain any information about the cryptographic key.

Coherent attack. In this attack, Eve can prepare an arbitrary joint state $|\epsilon_E\rangle$ of the ancilla, which then interacts with the photons before being measured jointly. Consider Alice and Bob share n pairs of compressed entangled states. Eve treats n photons that Alice sent to Bob as a single quantum system, denoted as $|S_{AB}\rangle$. Then, Eve interacts the joint state $|\epsilon_E\rangle$ with $|S_{AB}\rangle$ by a unitary transformation U_{BE}. The combined state is $U_{BE}|S_{AB}\rangle|\epsilon_E\rangle$. Assuming that Eve can obtain the encoded information of all n photons by a single joint measurement, she has a certain probability to get the correct structure of the number-state-entanglement-preserving tensor network. Consider an initial state $|\Psi_I\rangle$ contains $2n + 2 = 2^\ell$ particles and the number of compression layers is $\log_2(2n + 2) - 1 = \ell - 1$. Assume that Eve can guess the number of compression layers with a probability of $1/(\ell - 1)$.

Let $|L\rangle = |0\rangle$ and all number-state-preserving tensors are w_1. Eve can guess a number-state-preserving tensor with a probability of 1/2. She successfully guesses a single disentangler with a probability of 1/4. As the total number of disentanglers is $2^\ell/2 - 2$, Eve is able to guess all of them with a probability of $(1/4)^{2^\ell/2-2}$. Summing up, Eve is able to get the correct number-state-preserving-tensor network with a probability of $1/[2^{2^\ell-3}(\ell - 1)]$. Further, as we discuss in Sec. IV, a cryptographic key generation process in our QKD protocol is controlled by tensor positions (odd or even in Fig. 4) in compression layers $W_1^\dagger$. The probability that Eve obtains the correct rule of $w_1^\dagger$ in $W_1^\dagger$ is $2^{\log_2 2^\ell/2} = 2^{\ell-1}$. Hence Eve can get a cryptographic key with a probability of

$$P = \frac{1}{2^{2^\ell-3}(\ell - 1)2^{\ell-1}}. \quad (32)$$

The larger ℓ, the smaller probability of Eve's guesses. For the Example 1, the initial state $|\Psi_I\rangle$ contains eight particles, and $\ell = 3$. The probability that Eve can obtain the cryptographic key is $P = 1/2^8 = 1/128$. Likewise, for the Example 2, $|\Psi_I\rangle$ contains 16 particles, and $\ell = 4$. The probability that Eve can obtain the cryptographic key is $P = 1/(3 \times 2^{16}) = 1/196608$. Hence the larger the initial state, the exponentially decreasing probability of success of Eve's guess.

VI. CONCLUSION

In this paper, we have proposed a QKE protocol that applies number-state-entanglement-preserving tensor networks with quantum compression. In this protocol, we have exploited different choices for $|L\rangle$ and $|R\rangle$ that allow us to construct randomized number-state-preserving tensors and disentanglers. As a result, we can obtain various number-state-entanglement-preserving tensor networks with randomized compression. The compression model is scalable as it works for the cases, where the number of input photons is a power of 2. Compared with the traditional BB84, BBM92, and the QKE protocol, our protocol can generate longer secure keys using a smaller number of entangled photons, which can increase the cryptographic key generation rate. Further, we compared the distinction between the classical AES key expansion algorithm and our protocol on key expansion method, key length, and security. The result shows that our protocol has a better performance than the classical-key-expansion method. In addition, we discussed the security of our protocol in intercept-resend attack, entanglement-and-measurement attack, and coherent attack. Due to the structure of the number-state-entanglement-preserving tensor network, our protocol can resist intercept-resend attack and entanglement-and-measurement attack. For coherent attack, the larger the initial state, the exponentially decreasing probability of success of Eve's guess.

ACKNOWLEDGMENTS

Q.Z. and H.L. have been supported by the National Natural Science Foundation of China (Grant No. 61702427) and the Fundamental Research Funds for the Central Universities (Grant No. XDJK2020B027), the Venture & Innovation Support Program for Chongqing Overseas Returnees (Grant No. cx2018076), and the financial support in part by the National Natural Science Foundation of China (Grants No. 62032019 and No. 61732019) and the Capacity Development Grant of Southwest University (Grant No. SWU116007). J.P. has been supported by Australian Research Council (ARC) Grant No. DP180102199 and Polish National Science Center (NCN) Grant No. 2018/31/B/ST6/03003.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[2] C. H. Bennett, Quantum Cryptography Using Any Two Nonorthogonal States, Phys. Rev. Lett. **68**, 3121 (1992).

[3] H. K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[4] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[5] H. K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[6] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature (London) **509**, 475 (2014).

[7] M. Lucamarini, Z. L. Yuan, J. F. Dynes *et al.*, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[8] S. Wang, Z. Q. Yin, D. Y. He *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photon. **16**, 154 (2022).

[9] G. J. Fan-Yuan, F. Y. Lu, S. Wang *et al.*, Measurement-device-independent quantum key distribution for nonstandalone networks, Photon. Res. **9**, 1881 (2021).

[10] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[11] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[12] S. K. Joshi, D. Aktas, S. Wengerowsky *et al.*, A trusted node-free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).

[13] C. Y. Zhang and Z. J. Zheng, Entanglement-based quantum key distribution with untrusted third party, Quantum Inf. Process. **20**, 1 (2021).

[14] M. Tchoffo and A. G. Tene, Privacy amplification of entanglement parametric-down conversion based quantum key distribution via quantum logistic map for photon bases choice, Chaos Solitons Fractals **140**, 110110 (2020).

[15] M. Doda, M. Huber, G. Murta *et al.*, Quantum Key Distribution Overcoming Extreme Noise: Simultaneous Subspace Coding Using High-Dimensional Entanglement, Phys. Rev. Appl. **15**, 034003 (2021).

[16] X. M. Hu, W. B. Xing, B. H. Liu *et al.*, Efficient Generation of High-Dimensional Entanglement through Multipath Down-Conversion, Phys. Rev. Lett. **125**, 090503 (2020).

[17] X. M. Hu, W. B. Xing, B. H. Liu *et al.*, Efficient distribution of high-dimensional entanglement through 11 km fiber, Optica **7**, 738 (2020).

[18] C. J. Huang, H. Ma, Q. Yin *et al.*, Realization of a quantum autoencoder for lossless compression of quantum data, Phys. Rev. A **102**, 032412 (2020).

[19] Y. Yang, G. Chiribella, and D. Ebler, Efficient Quantum Compression for Ensembles of Identically Prepared Mixed States, Phys. Rev. Lett. **116**, 080501 (2016).

[20] C. R. Fan, B. Lu, X. T. Feng *et al.*, Efficient multi-qubit quantum data compression, Quantum Eng. **3**, e67 (2021).

[21] G. Bai, Y. Yang, and G. Chiribella, Quantum compression of tensor network states, New J. Phys. **22**, 043015 (2020).

[22] A. Pepper, N. Tischler, and G. J. Pryde, Experimental Realization of a Quantum Autoencoder: The Compression of Qutrits via Machine Learning, Phys. Rev. Lett. **122**, 060501 (2019).

[23] Y. Yang, L. Luo, and G. Yin, A new secure quantum key expansion scheme, Int. J. Theor. Phys. **52**, 2008 (2013).

[24] J. M. Arrazola and R. Amiri, Secret-key expansion from covert communication, Phys. Rev. A **97**, 022325 (2018).

[25] J. Daemen and V. Rijmen, AES proposal: Rijndael, 1999 (to be published).

[26] J. Yan and F. Chen, *An Improved AES Key Expansion Algorithm*, International Conference on Electrical, Mechanical and Industrial Engineering (Atlantis Press, Dordrecht, 2016), p. 113.

[27] P. Vlachos and I. G. Karafyllidis, Simulation of quantum key expansion using quantum cellular automata, Comput. Phys. Commun. **180**, 251 (2009).

[28] W. Y. Kon and C. C. W. Lim, Provably secure symmetric private information retrieval with quantum cryptography, Entropy **23**, 54 (2021).

[29] W. Y. Hwang, I. G. Koh, and Y. D. Han, Quantum cryptography without public announcement of bases, Phys. Lett. A **244**, 489 (1998).

[30] S. Ji, H. Lee, and G. L. Long, Secure quantum key expansion between two parties sharing a key, J. Korean Phys. Soc. **51**, 1245 (2007).

[31] X. B. Wang, An efficient protocol for secure and deterministic quantum key expansion, Int. J. Quantum Inf. **4**, 955 (2006).

[32] Z. Luo and I. Devetak, Efficiently implementable codes for quantum key expansion, Phys. Rev. A **75**, 010303(R) (2007).

[33] K. C. Hsu and T. A. Brun, Family of finite geometry low-density parity-check codes for quantum key expansion, Phys. Rev. A **87**, 062332 (2013).

[34] M. Tahmasbi and M. R. Bloch, Framework for covert and secret key expansion over classical-quantum channels, Phys. Rev. A **99**, 052329 (2019).

[35] F. Verstraete and J. I. Cirac, Matrix product states represent ground states faithfully, Phys. Rev. B **73**, 094423 (2006).

[36] Y. Y. Shi, L. M. Duan, and G. Vidal, Classical simulation of quantum many-body systems with a tree tensor network, Phys. Rev. A **74**, 022320 (2006).

[37] F. Verstraete, M. M. Wolf, and D. Perez-Garcia *et al.*, Criticality, the Area Law, and the Computational Power of Projected Entangled Pair States, Phys. Rev. Lett. **96**, 220601 (2006).

[38] G. Vidal, Entanglement Renormalization, Phys. Rev. Lett. **99**, 220405 (2007).

[39] J. Biamonte and V. Bergholm, Tensor networks in a nutshell, arXiv:1708.00006 [Contemp. Phys. (to be published)].

[40] Z. Y. Han, J. Wang, H. Fan *et al.*, Unsupervised Generative Modeling Using Matrix Product States, Phys. Rev. X **8**, 031012 (2018).

[41] D. Liu, S. J. Ran, P. Wittek *et al.*, Machine learning by unitary tensor network of hierarchical tree structure, New J. Phys. **21**073059 (2019).

[42] S. Cheng, L. Wang, and P. Zhang, Supervised learning with projected entangled pair states, Phys. Rev. B **103**, 125117 (2021).

[43] I. Affleck, T. Kennedy, E. H. Lieb *et al.*, Rigorous Results on Valence-Bond Ground States in Antiferromagnets, Phys. Rev. Lett. **59**, 799 (1987).

[44] G. Evenbly, Number-state preserving tensor networks as classifiers for supervised learning, arXiv:1905.06352.

[45] A. J. Ferris and G. Vidal, Variational Monte Carlo with the multiscale entanglement renormalization ansatz, Phys. Rev. B **85**, 165147 (2012).

[46] A. Cabello, Quantum Key Distribution in the Holevo Limit, Phys. Rev. Lett. **85**, 5635 (2000).

[47] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, Phys. Rev. A **65**, 032302 (2002).

[48] A. Kohnle, C. Benfield, D. Cassettari *et al.*, QuVis: The Quantum Mechanics Visualization Project, 2018 (to be published).

[49] A. B. Al-Ghamdi, A. Al-Sulami, and A. O. Aljahdali, On the security and confidentiality of quantum key distribution, Security Privacy **3**, e111 (2020).

[50] M. Al-Muhammed, A novel key expansion technique using diffusion, Comput. Fraud Security **2018**, 12 (2018).