Quantum Information and Computation, Vol. 15, No. 3&4 (2015) 0200–0234

GROUND STATE BLIND QUANTUM COMPUTATION ON AKLT STATE

TOMOYUKI MORIMAE
ASRLD Unit, Gunma University,
1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan
morimae@gmail.com

VEDRAN DUNJKO
School of Engineering and Physical Sciences, Heriot-Watt University
Edinburgh EH14 4AS, U.K.

School of Informatics, The University of Edinburgh
Edinburgh EH8 9AB, U.K.

Division of Molecular Biology, Ruer Bošković Institute
Bijenička cesta 54, P.P. 180, 10002 Zagreb, Croatia

ELHAM KASHEFI
School of Informatics, The University of Edinburgh
Edinburgh EH8 9AB, U.K.

Received August 26, 2013
Revised July 28, 2014

The blind quantum computing protocols (BQC) enable a classical client with limited quantum technology to delegate a computation to the quantum server(s) in such a way that the privacy of the computation is preserved. Here we present a new scheme for BQC that uses the concept of the measurement based quantum computing with the novel resource state of Affleck-Kennedy-Lieb-Tasaki (AKLT) chains leading to more robust computation. AKLT states are physically motivated resource as they are gapped ground states of a physically natural Hamiltonian in condensed matter physics. Our BQC protocol can enjoy the advantages of AKLT resource states (in a multiserver setup), such as the cooling preparation of the resource state, the energy-gap protection of the quantum computation. It also provides a simple and efficient preparation of the resource state in linear optics with biphotons.

Keywords: delegated quantum computing, measurement-based quantum computing, AKLT model
Communicated by: I Cirac & J Eisert

1 Introduction

In a future, at the time when a scalable quantum computer is realized, there will be much demand for the blind quantum computation [1, 2, 3, 4], since the quantum computer must be super-expensive and super-fragile, and therefore only limited number of servers can possess it. In particular, it is likely that a client (Alice) who has only a classical computer or a primitive quantum instrument which is not sufficient for the universal quantum computation will ask a quantum server (Bob) to perform her quantum computation on his fully-fledged quantum computer. Bob runs his quantum computer according to Alice's input and instructions, and finally returns the final output of the quantum computation to Alice. The crucial point in the blind quantum computation is that Alice does not want Bob to learn her input, the algorithm she wants to run, and the final output of the computation. For example, if Alice wants to factor a large integer by using Shor's factoring algorithm [5], the blind quantum computation must be performed in such a way that Bob cannot know her input (the large integer), the output of the computation (a prime factor), and even the fact that he is factoring.

For the classical computation, Feigenbaum [6] introduced the notion of "computing with encrypted data", and showed that for some functions f, an instance x can be efficiently encrypted into $z = E_k(x)$ in such a way that Alice can recover $f(x)$ efficiently from k and $f(z)$ computed by Bob. Moreover Abadi, Feigenbaum and Killian showed that no **NP**-hard function [7] can be computed blindly if unconditional security is required, unless the polynomial hierarchy collapses at the third level [8, 9]. Even restricting the security condition to be only computational [a], the question of the possibility of blind computing, also known as fully homomorphic encryption, remined open for 30 years [10].

Unlike classical computing, quantum mechanics could overcome the limitation of computational security. An example of the blind quantum computation was first proposed by Childs [1] where the quantum circuit model is adopted, and the register state is encrypted with quantum one-time pad scheme [11] so that Bob who performs quantum gates learns nothing about information in the quantum register. In this method, however, Alice needs to have a quantum memory and the ability to apply local Pauli operators at each step. Similarly the protocol proposed by Arrighi and Salvail [2] requires multi-qubit preparations and measurements while Aharonov, Ben-Or and Eban's protocol [4] requires a constant-sized quantum computer with memory.

On the other hand, in Broadbent, Fitzsimons and Kashefi's protocol [3], adapted to the one-way quantum computation [12, 13] all Alice needs is a classical computer and a very weak quantum instrument, which emits random single-qubit states. In particular, she does not require any quantum memory and the protocol is unconditionally secure. In their scheme, Alice's quantum instrument emits states $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\xi}|1\rangle)$, where

$$\xi \in \mathcal{A} = \left\{ \frac{k\pi}{4} \middle| k = 0, ..., 7 \right\}$$

is a random number which is secret to Bob, and each state is directly sent to Bob. Bob keeps all these states in his quantum memory, and creates the spacial resource state, which is alike to the two-dimensional cluster state and called "the brickwork state" [3], by applying the controlled-Z (CZ) operation among appropriate qubits in the received states. Alice calculates, by using her classical computer, the direction in which a qubit should be measured, and instructs the direction to Bob after some modifications such that (i) the byproduct operators emerged from the previous Bob's measurements are compensated, (ii) the random ξ is canceled, and (iii) the true direction and the true measurement outcomes, which reveal Alice's input, algorithm and output, remain secret to Bob. Bob does the measurement on the brickwork state according to the instruction from Alice, and sends the measurement result

[a] A crypto-system is unconditionally secure (also refereed to as "information-theoretically secure") if it is secure even when the adversary has unlimited computing power. A weaker notion is computational security where the adversary power is restricted to efficient computation.

to Alice for the next measurement. After repeating such two-way classical communications between Alice and Bob, their measurement-based quantum computation is finally finished, and Bob returns the final result (classical or quantum) of the computation to Alice. As is shown in [3], Bob learns nothing about Alice's input, the algorithm she wants to run, and the final output of the computation.

In the recent active interaction between condensed matter physics and quantum information science, plenty of novel resource states for the measurement-based quantum computation beyond the cluster state have been proposed [14, 15, 16, 17, 18, 19, 20, 21, 24, 22, 23, 25]. These new resource states have several interesting features and advantages over the cluster state. For example, some of those resource states are gapped ground states of their parent Hamiltonians, and therefore they can be easily prepared by cooling condensed matter systems and the measurement-based quantum computation can be protected from noise by the energy gap [15, 16, 17, 18, 19, 20, 24, 21, 22, 23]. In particular, Affleck-Kennedy-Lieb-Tasaki (AKLT) states [26] are physically motivated important resource states [15, 16, 17, 18, 19, 20, 21, 22, 23], since they are gapped ground states of a physically natural Hamiltonian which has long been studied in condensed matter physics, and exhibit many novel features, such as the one-dimensional Haldane phase [27], the diluted antiferromagnetic order detected by the string order parameter [28], and the effective spin-1/2 degree of freedom (edge state) appearing on the boundary of the chain [29]. Furthermore, it was shown recently that the preparation of the AKLT resource states is more efficient and simpler than that of the cluster state in linear optics with biphotons [30].

It is, however, not obvious that these novel resource states also admit blind quantum computation like the cluster state. They have drastically different properties compared to the cluster state or graph states in general, such as the local purity, the correlation property, and the entanglement property [15, 16, 17, 18, 19, 20, 21, 24, 22, 23]. Furthermore, the actual computation over these new resources, such as the way of measurements and the way of compensating byproducts, are also strongly different from those over the cluster state [15, 16, 17, 18, 19, 20, 21, 24, 22, 23].

In this paper, we show for the first time that the ground state measurement-based blind quantum computation is possible with AKLT resource states. As we will see later, this is not a straightforward generalization of the blind quantum computation on the cluster state, although it borrows the general idea from [3]. Hence a new proof of security for the blind quantum computation with AKLT states was also required. As a result, our new protocol can enjoy the advantages of the AKLT resource states (in a multiserver setup), namely the easy preparation of the resource state by cooling condensed matter systems, the natural protection of the quantum computation by the energy gap. It also provides a simple and efficient preparation of the resource state in linear optics with biphotons.

More precisely, we propose two methods, the single-server protocol and the double-server protocol. In the single-server protocol (Fig. 1), there are two parties, called Alice and Bob. Alice, the client, has a classical computer and a quantum instrument which is not sufficient for the universal quantum computation, whereas Bob, the server, has a universal quantum computer. Alice's quantum instrument emits random four-qubit states so-called "Dango states" each of which is directly sent to Bob through the quantum channel (Fig. 1 (a)), and Bob stores all of them in his quantum memory. Each Dango state hides certain random number which is secret to Bob, and these secret numbers are used later for the blind quantum computation. From Dango states, Bob creates the resource state, which is unitary equivalent to an AKLT state (Fig. 1 (b)). Alice calculates the angle in which a particle should be measured by using her classical computer, and sends the angle to Bob through the classical channel. Bob performs the measurement according to Alice's information, and returns the result of the measurement to Alice. They repeat this two-way classical communication (Fig. 1 (c)) until they finish the computation. Bob finally sends the final output of the quantum computation to Alice. The whole protocol can be done in such a way that Bob learns nothing about Alice's input, output, and algorithm. Recently an efficient scheme for preparation of AKLT state with biphotons was proposed in [30] and it seems that our single-server protocol can be adapted to such a scheme but we leave it as an open question what the best implementation is.

As we argue later, the single-server protocol cannot enjoy the energy-gap protection in condensed-matter systems, since Bob cannot prepare any natural parent Hamiltonian without knowing hidden angles in Dango states. Moreover, although Alice's quantum instrument is too primitive to perform the universal quantum computation, and it does not seem to be hard to implement this instrument in certain optical setups, it would be ideal if we can make Alice completely classical. Therefore, similar to [3], we consider an extension of the protocol to the double-server protocol. In the double-server protocol (Fig. 2), there are three parties Alice, Bob1, and Bob2. Alice, the client, has only a classical computer, whereas Bob1 and Bob2, servers, have universal quantum computers. Furthermore, Bob1 and Bob2 share many Bell pairs but they have no classical or quantum channel between them. Settings analogous to the entangled, but classically non-communicating servers have recently been drawing a considerable attention in a related context. This scenario has been considered in e.g. [40] as a means of establishing 'classical control over quantum systems' for verifying quantum computation, with a purely classical client. Here, we will however only consider the robustness of the multiserver blind quantum computation as the first step towards feasible verification scheme.

In the double-server protocol, Bob1 first creates AKLT resource states (Fig. 2 (a)). Bob1 next adiabatically turns off the interaction between some particles and others in his resource state, and teleports these particles to Bob2 by consuming Bell pairs. Bob1 sends Alice the result of the measurement in the teleportation through the classical channel (Fig. 2 (b)). Note that due to the lack of any communication (classical or quantum) channels between Bob1 and Bob2, the teleportation procedure from Bobs' point of view can be seen as a usage of a totally mixed channel where only Alice knows how to correct the output of the channel. Next, Alice calculates the angle in which particles should be measured by using her classical computer, and sends Bob2 the angle which is the sum of the calculated angle plus a random angle through the classical channel (Fig. 2 (c)). Bob2 performs the measurement in that angle and sends the result of the measurement to Alice (Fig. 2 (d)). Alice sends the previous random angle to Bob1 (Fig. 2 (e)), and Bob1 does the single-qubit rotation which compensates that random angle (Fig. 2 (f)). Bob1 and Bob2 repeat this two-way classical communication with Alice until they finish the computation. The whole protocol can be done in such a way that two Bobs learn nothing about Alice's input, output, and algorithm. As we will argue later, the scheme of double servers proposed in [3] where Bob1 prepares random states and Bob2 performs the measurement that compensates that random angle, will not lead to a ground state BQC protocol without affecting the privacy condition. While our new protocol can fully benefit from the energy-gap protection in condensed-matter systems, without revealing any information about Alice's secret computation.

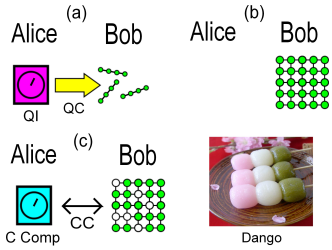

Fig. 1. (Color online.) The single-server protocol. (a): Alice's quantum instrument (QI) emits many four-qubit states so-called "Dango" states each of which is directly sent to Bob through the quantum channel (QC). Bob stores all of them in his quantum memory. (b): From these Dango states, Bob creates the resource state. (c): Alice calculates the angle in which a particle should be measured by using her classical computer (C Comp) and sends the angle to Bob through the classical channel (CC). Bob performs the measurement and returns the result of the measurement to Alice. They repeat this two-way classical communication until they finish the computation. Bob finally sends the final output of the computation to Alice.

This paper is organized as follows. In Sec. 2, we briefly review the concept of correlation space [16, 17, 18] which is used throughout this paper in order to describe measurement-based quantum computation on AKLT states. We also briefly review the AKLT model and measurement-based quantum computing with AKLT resource. In Sec. 3, we explain the single-server protocol. We show the blindness of the single-server protocol in Sec. 4. We also explain the double-server protocol in Sec. 5 and show its blindness in Sec. 6. We finish with a discussion in Sec. 7 which also highlights open problems.

2 Quantum computation in correlation space

In this section, we will briefly review the concept of correlation space [16, 17, 18], which is used throughout this paper. For details see Refs. [16, 17, 18].

Let us consider the matrix-product state of a quantum state in the d^N-dimensional Hilbert space

$$\sum_{l_1=1}^{d}...\sum_{l_N=1}^{d}\langle L|A[l_N]...A[l_1]|R\rangle|l_N\rangle\otimes...\otimes|l_1\rangle,$$

where $|L\rangle$ and $|R\rangle$ are two-dimensional complex vectors and A's are two-dimensional complex matrices. Let us assume that the first qudit of the matrix-product state is projected onto

$$|\theta,\phi\rangle=\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle.$$

Then, the matrix-product state becomes

$$\sum_{l_2=1}^{d}...\sum_{l_N=1}^{d}\langle L|A[l_N]...A[l_2]A[\theta,\phi]|R\rangle|l_N\rangle\otimes...\otimes|l_2\rangle\otimes|\theta,\phi\rangle,$$

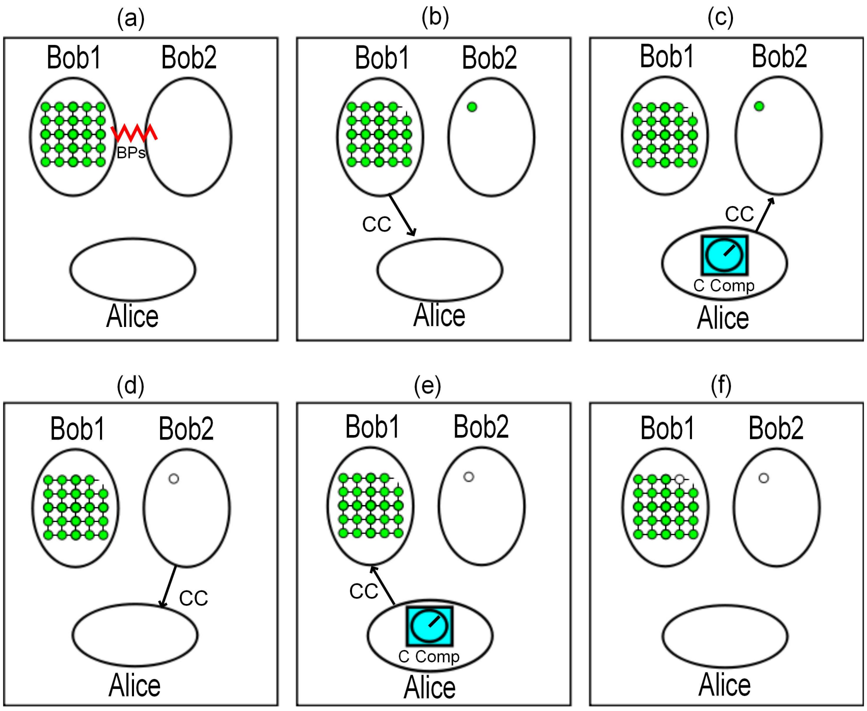

Fig. 2. (Color online.) The double-server protocol. (a): Bob1 creates AKLT resource states. Bob1 and Bob2 share Bell pairs (BPs). (b): Bob1 adiabatically turns off the interaction between some particles and others in his resource state, and teleports these isolated particles to Bob2 by consuming Bell pairs. Bob1 also sends Alice the result of the measurement in the teleportation. (c): Alice calculates the angle in which particles should be measured by using her classical computer (C Comp) and sends Bob2 the angle which is the sum of thus calculated angle and a random angle. (d): Bob2 performs the measurement in that angle and sends the result of the measurement to Alice. (e): Alice sends Bob1 the previous random angle. (f): Bob1 implements the single-qubit rotation which compensates the random rotation.

where

$$A[\theta,\phi]=\cos\frac{\theta}{2}A[0]+e^{-i\phi}\sin\frac{\theta}{2}A[1].$$

If $A[0]$ and $A[1]$ are appropriately chosen in such a way that $A[\theta,\phi]$ is unitary, we can "simulate" the unitary rotation $A[\theta,\phi]|R\rangle$ of $|R\rangle$ in the linear space where $|L\rangle$, $|R\rangle$, and A's live. This linear space is called "correlation space" [16, 17, 18]. In the general framework of measurement-based quantum computation, which is called the computational tensor network [16, 17, 18], universal quantum computation is performed in this correlation space. Note that in the one-way quantum computing model, the correlation space and the physical space are the same. This separation between the correlation space and the physical space will allow us to use many new resource states for measurement-based quantum computing. One such resource state is the AKLT state [15].

Let us consider the one-dimensional open-boundary chain of N qutrits. The AKLT Hamiltonian [26] is defined by

$$H_{AKLT}(\beta)\equiv\sum_{j=1}^{N-1}h_{j+1,j}(\beta),$$

where

$$h_{j+1,j}(\beta)\equiv\frac{1}{2}[\mathbf{S}_{j+1}\cdot\mathbf{S}_j-\beta(\mathbf{S}_{j+1}\cdot\mathbf{S}_j)^2]+\frac{1}{3}$$

and $\mathbf{S}_j\equiv(S_j^x,S_j^y,S_j^z)$ is the spin-1 operator on site j defined by

$$\begin{aligned}
S_j^x &\equiv \frac{1}{\sqrt{2}}\begin{pmatrix}0&1&0\\1&0&1\\0&1&0\end{pmatrix},\\
S_j^y &\equiv \frac{-i}{\sqrt{2}}\begin{pmatrix}0&1&0\\-1&0&1\\0&-1&0\end{pmatrix},\\
S_j^z &\equiv \begin{pmatrix}1&0&0\\0&0&0\\0&0&-1\end{pmatrix}.
\end{aligned}$$

If $-1<\beta<1$, the system is in the gapped Haldane phase [27]. In particular, if $\beta=-1/3$, Each $h_{j+1,j}(-1/3)$ is the projection operator onto the eigenspace of the total spin operator of two spin-1/2 particles corresponding to the eigenvalue 2. For $\beta=-1/3$, the ground states are called AKLT states [26] and explicitly written in the following matrix product form [26, 15]:

$$|AKLT^{N,L,R}\rangle\equiv\frac{\sqrt{2}}{\sqrt{3^N}}\sum_{l_1=1}^{3}...\sum_{l_N=1}^{3}\langle L|A[l_N]...A[l_1]|R\rangle|l_N\rangle\otimes...\otimes|l_1\rangle, \quad (1)$$

where

$$\begin{aligned}
|1\rangle &\equiv -\frac{1}{\sqrt{2}}\Big(|S_z=+1\rangle-|S_z=-1\rangle\Big),\\
|2\rangle &\equiv \frac{1}{\sqrt{2}}\Big(|S_z=+1\rangle+|S_z=-1\rangle\Big),\\
|3\rangle &\equiv |S_z=0\rangle,
\end{aligned}$$

$|S_z = k\rangle$ ($k \in \{-1, 0, +1\}$) are eigenvectors of the z-component S_z of the spin-1 operator, $|L\rangle$ and $|R\rangle$ are two-dimensional complex vectors, and $\{A[1], A[2], A[3]\}$ are 2×2 matrices defined by

$$\begin{aligned} A[1] &\equiv X, \\ A[2] &\equiv XZ, \\ A[3] &\equiv Z. \end{aligned}$$

Here, X and Z are Pauli operators over qubits. Note that the ground states of the AKLT Hamiltonian are four-fold degenerate, and each ground state is specified with $|L\rangle$ and $|R\rangle$, which represent two qubit edge states. The AKLT states are frustration free, since

$$h_{j+1,j}(-1/3)|AKLT^{N,L,R}\rangle = 0$$

for any $|L\rangle$ and $|R\rangle$, and for all $j = 1, ..., N-1$.

The AKLT model has long been studied in condensed matter physics since it can describe the one-dimensional Haldane phase [27] of a qutrit chain, which exhibits the spectral gap [26], the diluted antiferromagnetic order detected by the string order parameter [28], and the effective spin-1/2 degree of freedom, namely the edge state, appearing on the boundary of the chain [29]. Furthermore, the AKLT model has recently been attracting much attentions in the field of quantum information, because of its connections to the matrix product representation [31, 32, 33], the localizable entanglement [34, 35], and the measurement-based quantum computation [15, 19, 16, 20, 21]. Indeed, it was shown in Refs. [15, 19, 20, 21] that the measurement-based quantum computation is possible on the AKLT chains or other ground states in the gapped Haldane phase ($-1 < \beta < 1$).

We briefly review universal measurement-based quantum computation on AKLT states [15]. Assume that a qutrit of Eq. (1) is measured in the basis $\mathcal{M}(\phi) = \{|\alpha(\phi)\rangle, |\beta(\phi)\rangle, |\gamma\rangle\}$, where

$$\begin{aligned} |\alpha(\phi)\rangle &= \frac{1+e^{i\phi}}{2}|1\rangle + \frac{1-e^{i\phi}}{2}|2\rangle, \\ |\beta(\phi)\rangle &= \frac{1-e^{i\phi}}{2}|1\rangle + \frac{1+e^{i\phi}}{2}|2\rangle, \\ |\gamma\rangle &= |3\rangle. \end{aligned}$$

Then, following operations are implemented in the correlation space according to the measurement result [15].

$$\begin{aligned} |\alpha(\phi)\rangle &: \quad Xe^{i\phi Z/2}, \\ |\beta(\phi)\rangle &: \quad XZe^{i\phi Z/2}, \\ |\gamma\rangle &: \quad Z. \end{aligned}$$

Now assume that the unitary operation

$$V = |3\rangle\langle 1| + |1\rangle\langle 2| + |2\rangle\langle 3|$$

is applied on a qutrit and that qutrit is measured in the basis $\mathcal{M}(\phi)$. Then, following operations are implemented in the correlation space according to the measurement result [15].

$$
\begin{aligned}
|\alpha(\phi)\rangle &: \quad XZe^{-i\phi X/2}, \\
|\beta(\phi)\rangle &: \quad Ze^{-i\phi X/2}, \\
|\gamma\rangle &: \quad X.
\end{aligned}
$$

In this way, any single-qubit Z and X rotations are possible up to some Pauli byproducts. By appropriately changing the sign of ϕ (adapting measurements of the physical qutrits), these byproducts can be moved forward so that they are corrected in the final stage of the computation over the correlation space. Although the gate operation implemented in the AKLT MBQC is not deterministic, a polynomial overhead is sufficient to reduce the failure probability to exponentially small.

3 Single-sever Blind Quantum Computing Protocol

As said before, in the single-server BQC protocol (Fig. 1), Alice has a classical computer and a quantum instrument that emits random four-qubit states called "Dango states". Depending on the desired computation and the input size, Alice will send $(2 \times N \times M)$ Dango states directly to Bob through a one-way quantum channel that they initially share. Bob stores all of them in his quantum memory to creates the resource state, called "rotated AKLT states". The procedure of preparing such an initial state is explained in the Blind state preparation Subsection below.

Next, Alice calculates the angle in which a particle of a rotated AKLT state should be measured. Recall that this is a qutrit measurement that will induce a qubit operation over the correlation space. Moreover the calculated angle should compensate for the initial random rotation of the Dango states and byproduct operation of the previous measurement. Finally an additional random rotation will be added to hide the true result of the measurement from Bob. Bob performs the measurement according to Alice's information (sent via a classical channel to him), and returns the result of the measurement to Alice. They repeat this two-way classical communication until they finish the computation. Bob finally sends the final output of the quantum computation to Alice. The exact protocol is given in the Blind computation Subsection below where we describe how a blind arbitrary X and Z rotation in the correlation space can be performed. Next we describe how two-qubit entangling operation of CZ can be performed in regular places. The rotation operators are also performed in regular interval, and hence the overall structure of the actual underlying computation remains hidden to Bob. These set of operators define a universal set of gates for quantum computing.

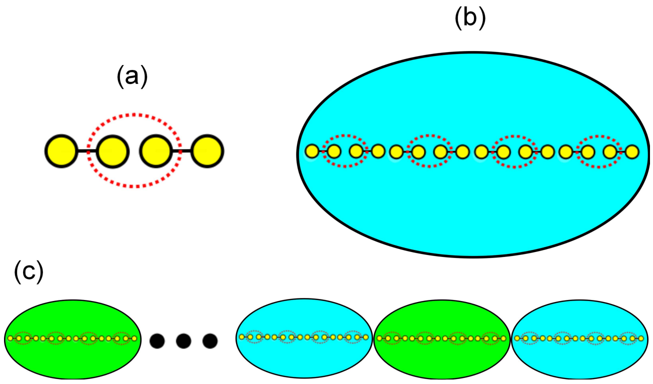

Fig. 3. (Color online.) (a): A Dango state. Two yellow circles connected by a bond are qubits which consist of the Bell state. The operator $(I - |\eta_1\rangle\langle\eta_1|)T_{Z/X}(\xi)$ acts on two qubits in the red dotted circle. (b): A Z-Dango chain for $n = 4$. (c): A Combo chain $|C_b\rangle$. Z-Dango chains are colored in blue, whereas X-Dango chains are colored in green.

3.1 Blind state preparation

Denote the Bell basis by

$$\begin{aligned}
|\eta_1\rangle &\equiv \frac{1}{\sqrt{2}}\Big(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle\Big),\\
|\eta_2\rangle &\equiv \frac{1}{\sqrt{2}}\Big(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle\Big),\\
|\eta_3\rangle &\equiv \frac{1}{\sqrt{2}}\Big(|1\rangle\otimes|0\rangle + |0\rangle\otimes|1\rangle\Big),\\
|\eta_4\rangle &\equiv \frac{1}{\sqrt{2}}\Big(|1\rangle\otimes|0\rangle - |0\rangle\otimes|1\rangle\Big).
\end{aligned}$$

The full state preparation is described in Protocol 1. Assume Alice's desired computation is composed of a sequence of X and Z-rotations and CZ operations. Depending on the number of the required operators and the size of the input, Alice will choose integer values N and M. Then Alice's quantum instrument emits $N\times M$ "Z-Dango states" and $N\times M$ "X-Dango states" defined as (see Fig. 3 (a))

$$\begin{aligned}
|D_Z(\xi^Z_{a,b})\rangle &\equiv (I\otimes(I-|\eta_1\rangle\langle\eta_1|)\otimes I)(I\otimes T_Z(\xi^Z_{a,b})\otimes I)|\eta_1\rangle\otimes|\eta_1\rangle,\\
|D_X(\xi^X_{a,b})\rangle &\equiv (I\otimes(I-|\eta_1\rangle\langle\eta_1|)\otimes I)(I\otimes T_X(\xi^X_{a,b})\otimes I)|\eta_1\rangle\otimes|\eta_1\rangle,
\end{aligned}$$

where $(a,b)\in\{1,...,N\}\times\{1,...,M\}$, $\xi^{Z/X}_{a,b}\in\mathcal{A}\equiv\Big\{\frac{k\pi}{4}\Big|k=0,...,7\Big\}$ are independently and uniformly distributed random numbers which are secret to Bob, and the two qubit operators $T_Z(\xi^Z_{a,b})$ and $T_X(\xi^X_{a,b})$ are defined by

$$\begin{aligned}
T_Z(\xi^Z_{a,b}) &\equiv |00\rangle\langle 00| + e^{i\xi^Z_{a,b}}|01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|,\\
T_X(\xi^X_{a,b}) &\equiv \Big(\frac{1+e^{i\xi^X_{a,b}}}{2}|\eta_2\rangle + \frac{1-e^{i\xi^X_{a,b}}}{2}|\eta_4\rangle\Big)\langle\eta_2| + \Big(\frac{1-e^{i\xi^X_{a,b}}}{2}|\eta_2\rangle + \frac{1+e^{i\xi^X_{a,b}}}{2}|\eta_4\rangle\Big)\langle\eta_4|\\
&\quad +|\eta_1\rangle\langle\eta_1| + |\eta_3\rangle\langle\eta_3|.
\end{aligned}$$

Alice sends all these Dango states to Bob, and records all $\{\xi_{a,b}^{Z/X}\}$ for the later use [36]. Bob arranges all the Dango states in a lattice with $2N$ columns and M rows.

Alice chooses a parameter $n < N$. We call a collection of n Dango states, sent by Alice to be kept in Bob's memory, " (k,b)th Z-Dango chain states" or "(k,b)th X-Dango chain states" defines as (see Fig. 3 (b))

$$\begin{aligned} |B_{k,b}^Z\rangle &\equiv \bigotimes_{j=1}^{n} |D_Z(\xi_{(k-1)n+j,b}^Z)\rangle, \\ |B_{k,b}^X\rangle &\equiv \bigotimes_{j=1}^{n} |D_X(\xi_{(k-1)n+j,b}^X)\rangle, \end{aligned}$$

where $k = 1, ..., N/n$ and $b = 1, ..., M$. A Z-Dango chain state is used for the implementation of a single-qubit Z-rotation whereas an X-Dango chain state is used for the implementation a single-qubit X-rotation. However, to hide the actual structure of the computation Alice will work with a regular one-dimensional chain, called "Combo chain state" $|C_b\rangle$, composed of N/n Z-Dango chain states and N/n X-Dango chain states (Fig. 3 (c)) with two-edge qubits projected on $|R^*\rangle$ and $|L\rangle$ states, respectively (Fig. 4 (a)):

$$|C_b\rangle \equiv \langle R^*|\langle L|\Big(|B_{N/n,b}^X\rangle \otimes |B_{N/n,b}^Z\rangle \otimes ... \otimes |B_{2,b}^X\rangle \otimes |B_{2,b}^Z\rangle \otimes |B_{1,b}^X\rangle \otimes |B_{1,b}^Z\rangle\Big)$$

$(b = 1, ..., M)$. Here, $|L\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ and $|R\rangle = |0\rangle$. However, $|R\rangle$ could be any arbitrary state depending on Alice's desired input using the uploading method [38].

Now in order to entangle qubits of the Combo chain to create the desired resource state, Bob will perform the following operators. Let us define the PEPS operation to be [31, 32, 33]

$$P \equiv \frac{1}{\sqrt{2}} \sum_{l=1}^{3} \sum_{i=0}^{1} \sum_{j=0}^{1} A_{i,j}[l] |l\rangle\langle i| \otimes \langle j|,$$

which creates a qutrit from two qubits, where $A_{i,j}[l]$ is (i,j)-element of the matrix $A[l]$. Consider the following unitary operators acting on a qutrit

$$\begin{aligned} U(\xi_{a,b}^{Z/X}) &\equiv \Big(\frac{1+e^{i\xi_{a,b}^{Z/X}}}{2}|1\rangle + \frac{1-e^{i\xi_{a,b}^{Z/X}}}{2}|2\rangle\Big)\langle 1| + \Big(\frac{1-e^{i\xi_{a,b}^{Z/X}}}{2}|1\rangle + \frac{1+e^{i\xi_{a,b}^{Z/X}}}{2}|2\rangle\Big)\langle 2| + |3\rangle\langle 3|, \\ V &\equiv |3\rangle\langle 1| + |1\rangle\langle 2| + |2\rangle\langle 3|. \end{aligned}$$

It is easy to verify that

$$\begin{aligned} PT_Z(\xi_{a,b}^{Z/X}) &= U(\xi_{a,b}^{Z/X})P, \\ PT_X(\xi_{a,b}^{Z/X}) &= V^\dagger U(\xi_{a,b}^{Z/X})VP. \end{aligned}$$

Bob has to apply the filtering operation $I - |\eta_1\rangle\langle\eta_1|$. In order to do so, he performs the measurement $\{|\eta_1\rangle\langle\eta_1|, I - |\eta_1\rangle\langle\eta_1|\}$ to every pair of two qubits in the Combo chain which is specified by a dotted blue circle in Fig. 4 (b). If $|\eta_1\rangle\langle\eta_1|$ is realised, two qubits are just removed from the chain (Fig. 4 (c)). Next Bob applies the PEPS operation P to each pair of two qubits in order to obtain qutrits (Fig. 4 (d), (e), (f)) [39]. This PEPS operation is done deterministically since $I-|\eta_1\rangle\langle\eta_1|$ is already applied to every pair of qubits. Therefore Bob has created a new one-dimensional chain of qutrits (Fig. 4 (f)) called "rotated AKLT state":

$$|RAKLT_b^{2N,L,R}(\{\xi_{a,b}^{Z/X}\})\rangle = \mathcal{U}_b(\{\xi_{a,b}^{Z/X}\})|AKLT^{2N,L,R}\rangle,$$

where

$$\begin{aligned}\mathcal{U}_b(\{\xi_{a,b}^{Z/X}\}) \quad \equiv \quad & \Big\{V^\dagger U(\xi_{N,b}^X)V\otimes...\otimes V^\dagger U(\xi_{N-n+1,b}^X)V\Big\}\otimes\Big\{U(\xi_{N,b}^Z)\otimes...\otimes U(\xi_{N-n+1,b}^Z)\Big\}\\ & \vdots\\ & \otimes\Big\{V^\dagger U(\xi_{n+n,b}^X)V\otimes...\otimes V^\dagger U(\xi_{n+1,b}^X)V\Big\}\otimes\Big\{U(\xi_{n+n,b}^Z)\otimes...\otimes U(\xi_{n+1,b}^Z)\Big\}\\ & \otimes\Big\{V^\dagger U(\xi_{n,b}^X)V\otimes...\otimes V^\dagger U(\xi_{1,b}^X)V\Big\}\otimes\Big\{U(\xi_{n,b}^Z)\otimes...\otimes U(\xi_{1,b}^Z)\Big\}\end{aligned}$$

(for simplicity, we have assumed that all filterings give $|\eta_1\rangle\langle\eta_1|$). We call a qutrit which is rotated by $U(\xi_{a,b}^Z)$ "Z-prerotated qutrit" and a qutrit which is rotated by $V^\dagger U(\xi_{a,b}^X)V$ "X-prerotated qutrit". Other qutrits are called "plain qutrits". The "(k,b)th Z/X-prerotated AKLT subsystem" is defined to be the set of Z/X-prerotated qutrits in bth prerotated AKLT chain corresponding to particles of (k,b)th Z/X-Dango chain.

Algorithm 1: Blind State Preparation

- Alice sends Bob parameter values N, M and $n<N$.
- Alice sends Bob $N\times M$ many Z-Dango states $|D_Z(\xi_{a,b}^Z)\rangle$ where $(a,b)\in\{1,...,N\}\times\{1,...,M\}$.
- Alice sends Bob $N\times M$ many X-Dango states $|D_X(\xi_{a,b}^X)\rangle$ where $(a,b)\in\{1,...,N\}\times\{1,...,M\}$.
- Bob arranges the received Z-Dango states in M rows of N/n Z-Dango chains $|B_{k,b}^Z\rangle$ where $k=1,2,...,N/n$, $b=1,...,M$.
- Bob arranges the received X-Dango states in M rows of N/n X-Dango chains $|B_{k,b}^X\rangle$ where $k=1,2,...,N/n$, $b=1,...,M$.
- Bob arranges the Dango chains in M rows of Combo chains $|C_b\rangle\equiv|B_{N/n,b}^X\rangle\otimes|B_{N/n,b}^Z\rangle\otimes...\otimes|B_{1,b}^X\rangle\otimes|B_{1,b}^Z\rangle$.
- Bob applies filtering and PEPS operators to create M rows of rotated AKLT states $|RAKLT_b^{2N,L,R}(\{\xi_{a,b}^{Z/X}\})\rangle$, where $b=1,...,M$.

See also Fig. 4.

3.2 Blind computation protocol

A single blind Z-rotation is performed using a Z-Dango chain state. Let us assume that Alice wants to perform the Z-rotation $\exp\left[\frac{iZ}{2}\theta_{k,b}^Z\right]$ with $\theta_{k,b}^Z\in\mathcal{A}$, using the (k,b)th Z-Dango chain [37]. The step by step operation is given in Protocol 2. Note that we implement the desired Z-rotation using qutrit measurements. However, the third outcome $|\gamma\rangle$ leads to the

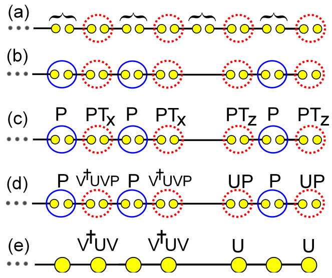

Fig. 4. (Color online.) (a): A chain $|C\rangle$. (b): The filtering operation is applied to every pair of qubits which is indicated by a blue dotted circle. (c): $|\eta_1\rangle\langle\eta_1|$ is realized on the seventh and eighth qubits. (d): The PEPS P is applied to every pair of two qubits. (e): It is equivalent to (d). (f): It is equivalent to (e). Now large yellow circles are qutrits.

failure as it implements only the trivial Pauli Z. The probability that Alice fails to implement her desired Z-rotation in a single Z-Dango chain is $1/3^n$, which is small for sufficiently large n. Similarly a blind X rotation could be applied (see Protocol 3) where again, the probability that Alice fails to implement her desired X-rotation in a single X-Dango chain is $1/3^n$. Note that these protocols are designed in such a way to follow the construction of the AKLT computation of Sec. 2, while canceling the prerotation that was added to the resource state for the purpose of blindness.

Let us finally explain how the two-qubit operation of controlled-Z (CZ) is performed. In order to perform CZ gates blindly, CZ gates are periodically implemented with the period that is independent of Alice's input and the algorithm. In this case, Bob learns nothing from the period. Because of the periodic implementation of CZ gates, Alice sometimes experiences an unwanted CZ gate. However, Alice can cancel the effect of an unwanted CZ gate by implementing the trivial identity operation (plus Pauli byproduct operations) until she arrives at the next CZ gate which cancels the previous one. This is possible due to the following commutation rules.

$$\begin{aligned} CZ(I\otimes X)CZ &= Z\otimes X, \\ CZ(I\otimes Z)CZ &= I\otimes Z, \\ CZ(X\otimes I)CZ &= X\otimes Z, \\ CZ(Z\otimes I)CZ &= Z\otimes I. \end{aligned}$$

In Protocol 4, we explain how to implement the CZ gate plus Z-rotation

$$\Big(\exp\Big[\frac{iZ}{2}\theta^Z_{k,b}\Big]\otimes\exp\Big[\frac{iZ}{2}\theta^Z_{k',b'}\Big]\Big)CZ$$

between (k,b)th and (k',b')th Z-prerotated AKLT subsystems, where $\theta^Z_{k,b},\theta^Z_{k',b'}\in\mathcal{A}$. Note that the local Z rotations are required to cancel the prerotations of qutrits. The probability that Alice fails to implement the CZ gate in this algorithm is $(5/9)^n$, which is small for large n.

Algorithm 2: Blind Z Rotation

Initially the flag parameter (known to both Alice and Bob) is set $\tau = 1$. For $j = 1 \cdots n$ Alice and Bob perform the following steps.

(I) Alice sends Bob the angle

$$\phi^Z_{(k-1)n+j,b} \equiv \tau\theta^Z_{k,b} + \xi^Z_{(k-1)n+j,b} + \pi r^Z_{(k-1)n+j,b} \pmod{2\pi},$$

where $r^Z_{(k-1)n+j,b} \in \{0,1\}$ is a random number which is secret to Bob. If there is the X byproduct before this step, $\theta^Z_{k,b}$ should be replaced with $-\theta^Z_{k,b}$ in order to compensate this byproduct operator. However, Z byproduct commutes trivially with the operation implemented in the correlation space, and therefore it can be corrected at the end of computation.

(II) Bob measures the jth Z-prerotated qutrit of the (k,b)th Z-prerotated AKLT subsystem in the basis

$$\mathcal{M}(\phi^Z_{(k-1)n+j,b}) \equiv \{|\alpha(\phi^Z_{(k-1)n+j,b})\rangle, |\beta(\phi^Z_{(k-1)n+j,b})\rangle, |\gamma\rangle\},$$

where

$$\begin{aligned} |\alpha(\phi^Z_{(k-1)n+j,b})\rangle &\equiv \frac{1+\exp\left[i\phi^Z_{(k-1)n+j,b}\right]}{2}|1\rangle + \frac{1-\exp\left[i\phi^Z_{(k-1)n+j,b}\right]}{2}|2\rangle, \\ |\beta(\phi^Z_{(k-1)n+j,b})\rangle &\equiv \frac{1-\exp\left[i\phi^Z_{(k-1)n+j,b}\right]}{2}|1\rangle + \frac{1+\exp\left[i\phi^Z_{(k-1)n+j,b}\right]}{2}|2\rangle, \\ |\gamma\rangle &\equiv |3\rangle. \end{aligned}$$

and sends the result to Alice.

- If the measurement result is $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$,

$$R^\alpha_Z(\tau\theta^Z_{k,b}, r^Z_{(k-1)n+j,b}) \equiv \exp\left[\frac{-i\tau\theta^Z_{k,b}}{2}\right] X Z^{r^Z_{(k-1)n+j,b}} \exp\left[\frac{iZ}{2}\tau\theta^Z_{k,b}\right]$$

  is implemented in the correlation space and Alice sets $\tau = 0$.
- If the measurement result is $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$,

$$R^\beta_Z(\tau\theta^Z_{k,b}, r^Z_{(k-1)n+j,b}) \equiv \exp\left[\frac{-i\tau\theta^Z_{k,b}}{2}\right] X Z^{r^Z_{(k-1)n+j,b}+1} \exp\left[\frac{iZ}{2}\tau\theta^Z_{k,b}\right]$$

  is implemented in the correlation space and Alice sets $\tau = 0$.
- If the measurement result is $|\gamma\rangle$, Z is implemented in the correlation space.

The probability of obtaining each result is $1/3$.

(III) Bob does the measurement $\{|1\rangle, |2\rangle, |3\rangle\}$ on the next plain qutrit if any.

Algorithm 3: Blind X Rotation

Initially the flag parameter (known to both Alice and Bob) is set $\tau = 1$. For $j = 1 \cdots n$ Alice and Bob perform the following steps.

(I) Alice sends Bob the angle

$$\phi^X_{(k-1)n+j,b} \equiv \tau\theta^X_{k,b} + \xi^X_{(k-1)n+j,b} + r^X_{(k-1)n+j,b}\pi \pmod{2\pi},$$

where $r^X_{(k-1)n+j,b} \in \{0,1\}$ is a random number which is secret to Bob. If there is the Z byproduct operator before this step, $\theta^X_{k,b}$ should be replaced with $-\theta^X_{k,b}$ in order to compensate this byproduct operator. However, X byproduct commutes trivially with the operation implemented in the correlation space, and therefore it can be corrected at the end of computation.

(II) Bob applies V on the jth X-prerotated qutrit of the (k,b)th X-prerotated AKLT subsystem, and does the measurement in the basis

$$\mathcal{M}(\phi^X_{(k-1)n+j,b}) \equiv \{|\alpha(\phi^X_{(k-1)n+j,b})\rangle, |\beta(\phi^X_{(k-1)n+j,b})\rangle, |\gamma\rangle\},$$

where

$$\begin{aligned}
|\alpha(\phi^X_{(k-1)n+j,b})\rangle &\equiv \frac{1+\exp\left[i\phi^X_{(k-1)n+j,b}\right]}{2}|1\rangle + \frac{1-\exp\left[i\phi^X_{(k-1)n+j,b}\right]}{2}|2\rangle,\\
|\beta(\phi^X_{(k-1)n+j,b})\rangle &\equiv \frac{1-\exp\left[i\phi^X_{(k-1)n+j,b}\right]}{2}|1\rangle + \frac{1+\exp\left[i\phi^X_{(k-1)n+j,b}\right]}{2}|2\rangle,\\
|\gamma\rangle &\equiv |3\rangle.
\end{aligned}$$

and sends the result to Alice.

- If the measurement result is $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$,

$$R^\alpha_X(\tau\theta^X_{k,b}, r^X_{(k-1)n+j,b}) \equiv \exp\left[\frac{-i\tau\theta^X_{k,b}}{2}\right] X^{r^X_{(k-1)n+j,b}+1} Z \exp\left[\frac{-iX}{2}\tau\theta^X_{k,b}\right]$$

  is implemented in the correlation space and Alice sets $\tau = 0$.

- If the measurement result is $|\beta(\phi^X_{(k-1)n+j,b})\rangle$,

$$R^\beta_X(\tau\theta^X_{k,b}, r^X_{(k-1)n+j,b}) \equiv \exp\left[\frac{-i\tau\theta^X_{k,b}}{2}\right] X^{r^X_{(k-1)n+j,b}} Z \exp\left[\frac{-iX}{2}\tau\theta^X_{k,b}\right]$$

  is implemented in the correlation space and Alice sets $\tau = 0$.

- If the measurement result is $|\gamma\rangle$, X is implemented.

The probability of obtaining each result is 1/3.

(III) Bob performs the measurement $\{|1\rangle, |2\rangle, |3\rangle\}$ on the next plain qutrit if any.

Algorithm 4: Controlled-Z followed by Blind Z-rotations

Initially the flag parameters (known to both Alice and Bob) are set $\tau=1$, $\tau'=1$ and $\epsilon=1$. For $j=1\cdots n$ Alice and Bob perform the following steps.

(I) If $\epsilon=0$, skip this step. Bob applies the unitary operation

$$\begin{aligned} W &\equiv \frac{|1,1\rangle+|1,2\rangle+|2,1\rangle-|2,2\rangle}{2}\langle 1,1|+\frac{|1,1\rangle+|1,2\rangle-|2,1\rangle+|2,2\rangle}{2}\langle 1,2| \\ &+\frac{|1,1\rangle-|1,2\rangle+|2,1\rangle+|2,2\rangle}{2}\langle 2,1|+\frac{-|1,1\rangle+|1,2\rangle+|2,1\rangle+|2,2\rangle}{2}\langle 2,2| \\ &+|1,3\rangle\langle 1,3|+|2,3\rangle\langle 2,3|+|3,1\rangle\langle 3,1|+|3,2\rangle\langle 3,2|+|3,3\rangle\langle 3,3| \end{aligned}$$

between jth Z-prerotated qutrit of (k,b)th Z-prerotated AKLT subsystem and jth Z-prerotated qutrit of (k',b')th Z-prerotated AKLT subsystem.

(II) Alice sends Bob the angles

$$\begin{aligned} \phi^Z_{(k-1)n+j,b} &= \tau\theta^Z_{k,b}+\xi^Z_{(k-1)n+j,b}+r^Z_{(k-1)n+j,b}\pi \pmod{2\pi}, \\ \phi^Z_{(k'-1)n+j,b'} &= \tau'\theta^Z_{k',b'}+\xi^Z_{(k'-1)n+j,b'}+r^Z_{(k'-1)n+j,b'}\pi \pmod{2\pi}, \end{aligned}$$

where $r^Z_{(k-1)n+j,b}, r^Z_{(k'-1)n+j,b'}\in\{0,1\}$ are random numbers. If there is any byproduct which contains X before this step, the sign of $\theta^Z_{k,b}$ or $\theta^Z_{k',b'}$ should be appropriately changed. However, Z byproduct commutes trivially with the operation implemented in the correlation space, and therefore it can be corrected at the end of computation.

(III) Bob does the measurement $\mathcal{M}(\phi^Z_{(k-1)n+j,b})$ (the same as that of Protocol 1) on the jth Z-prerotated qutrit of the (k,b)th Z-prerotated AKLT subsystem and the measurement $\mathcal{M}(\phi^Z_{(k'-1)n+j,b'})$ on the jth Z-prerotated qutrit of the (k',b')th Z-prerotated AKLT subsystem. The operation implemented in the correlation space is summarized as follows:

$$\begin{aligned} |\alpha(\phi^Z_{(k-1)n+j,b})\rangle\otimes|\alpha(\phi^Z_{(k'-1)n+j,b'})\rangle &: \Big[R^\alpha_Z(\tau\theta^Z_{k,b},r^Z_{(k-1)n+j,b})\otimes R^\alpha_Z(\tau'\theta^Z_{k',b'},r^Z_{(k'-1)n+j,b'})\Big]CZ^\epsilon \\ |\alpha(\phi^Z_{(k-1)n+j,b})\rangle\otimes|\beta(\phi^Z_{(k'-1)n+j,b'})\rangle &: \Big[R^\alpha_Z(\tau\theta^Z_{k,b},r^Z_{(k-1)n+j,b})\otimes R^\beta_Z(\tau'\theta^Z_{k',b'},r^Z_{(k'-1)n+j,b'})\Big]CZ^\epsilon \\ |\alpha(\phi^Z_{(k-1)n+j,b})\rangle\otimes|\gamma\rangle &: R^\alpha_Z(\tau\theta^Z_{k,b},r^Z_{(k-1)n+j,b})\otimes Z \\ |\beta(\phi^Z_{(k-1)n+j,b})\rangle\otimes|\alpha(\phi^Z_{(k'-1)n+j,b'})\rangle &: \Big[R^\beta_Z(\tau\theta^Z_{k,b},r^Z_{(k-1)n+j,b})\otimes R^\alpha_Z(\tau'\theta^Z_{k',b'},r^Z_{(k'-1)n+j,b'})\Big]CZ^\epsilon \\ |\beta(\phi^Z_{(k-1)n+j,b})\rangle\otimes|\beta(\phi^Z_{(k'-1)n+j,b'})\rangle &: \Big[R^\beta_Z(\tau\theta^Z_{k,b},r^Z_{(k-1)n+j,b})\otimes R^\beta_Z(\tau'\theta^Z_{k',b'},r^Z_{(k'-1)n+j,b'})\Big]CZ^\epsilon \\ |\beta(\phi^Z_{(k-1)n+j,b})\rangle\otimes|\gamma\rangle &: R^\beta_Z(\tau\theta^Z_{k,b},r^Z_{(k-1)n+j,b})\otimes Z \\ |\gamma\rangle\otimes|\alpha(\phi^Z_{(k'-1)n+j,b'})\rangle &: Z\otimes R^\alpha_Z(\tau'\theta^Z_{k',b'},r^Z_{(k'-1)n+j,b'}) \\ |\gamma\rangle\otimes|\beta(\phi^Z_{(k'-1)n+j,b'})\rangle &: Z\otimes R^\beta_Z(\tau'\theta^Z_{k',b'},r^Z_{(k'-1)n+j,b'}) \\ |\gamma\rangle\otimes|\gamma\rangle &: Z\otimes Z \end{aligned}$$

(IV) If the Z-rotation by $\theta^Z_{k,b}$ is implemented in the preivous step, then Alice sets $\tau=0$. If the z-rotation by $\theta^Z_{k',b'}$ is implemented in the previous step, then Alice sets $\tau'=0$. If the CZ is implemented in the previous step, then Alice sets $\epsilon=0$.

(V) Bob does the measurement $\{|1\rangle,|2\rangle,|3\rangle\}$ on the next plain qutrit if any.

3.3 Ground state computing

In the single-server protocol, it is not easy for Bob to enjoy the energy-gap protection, since Bob cannot prepare any natural parent Hamiltonian without knowing $\{\xi_{a,b}^{Z/X}\}$. This is understood as follows.

Let us consider the span

$$\Big\{ \ |RAKLT_b^{2N,L,R}(\{\xi_{a,b}^{Z/X}\})\rangle \ \Big| \ \xi_{a,b}^{Z/X} \in \mathcal{A}, \ a=1,...,N \ \Big\}$$

of all rotated AKLT states. As is shown below, the dimension of the span is 2^{2N}. Therefore, if Bob does not know $\{\xi_{a,b}^{Z/X}\}$, he must prepare an unnatural Hamiltonian with exponentially-degenerated ground states.

Let us show that the dimension of the span is 2^{2N}. Let

$$|\psi_{2N}\rangle = |\phi_0\rangle \otimes \Big(\bigotimes_{i=1}^{2N} |\phi_i\rangle\Big) \otimes |\phi_{2N+1}\rangle,$$

where $|\phi_0\rangle$ and $|\phi_{2N+1}\rangle$ are qubit states, and $|\phi_i\rangle$ $(i=1,...,2N)$ are qutrit states. Let

$$\mathbf{U}_{\vec{\xi}} = I_2 \otimes \mathcal{U}_b(\{\xi_{a,b}^{Z/X}\}) \otimes I_2$$

be a grobal unitary operator, where I_2 is the identity operator on a single qubit. Let E is a global unitary operator which works as

$$E|\psi_{2N}\rangle = |AKLT^{2N,L,R}\rangle.$$

From Lemma below and the fact that $E^\dagger$ is unitary,

$$\begin{aligned}
\dim\Big(\mathrm{span}\Big\{\mathbf{U}_{\vec{\xi}} E|\psi_{2N}\rangle\Big\}_{\vec{\xi}}\Big) &= \dim\Big(\mathrm{span}\Big\{(\mathbf{U}_{\vec{\xi}} E)^\dagger|\psi_{2N}\rangle\Big\}_{\vec{\xi}}\Big) \\
&= \dim\Big(\mathrm{span}\Big\{E^\dagger \mathbf{U}_{\vec{\xi}}^\dagger|\psi_{2N}\rangle\Big\}_{\vec{\xi}}\Big) \\
&= \dim\Big(\mathrm{span}\Big\{\mathbf{U}_{\vec{\xi}}^\dagger|\psi_{2N}\rangle\Big\}_{\vec{\xi}}\Big) \\
&= \dim\Big(\mathrm{span}\Big\{\mathbf{U}_{\vec{\xi}}|\psi_{2N}\rangle\Big\}_{\vec{\xi}}\Big) \\
&= 2^{2N}.
\end{aligned}$$

Lemma 1 *Let $\{V_1, \dots V_r\}$ be a set of r operators, and let $|\phi\rangle$ be a state in their domain. Then*

$$dim\Big(span\Big\{V_i|\phi\rangle\Big\}_i\Big) = dim\Big(span\Big\{V_i^\dagger|\phi\rangle\Big\}_i\Big).$$

Proof: Recall that $\dim\Big(\mathrm{span}\Big\{V_i|\phi\rangle\Big\}_i\Big)$ is equal to the rank of the Gram matrix of the set of vectors $\{V_i|\phi\rangle\}_i$. Also note that if G_A is the Gram matrix of the set of vectors $\{V_i|\phi\rangle\}_i$ and G_B is the Gram matrix of the set of vectors $\{V_i^\dagger|\phi\rangle\}_i$, then $G_A = G_B^*$. Finally, let us remind that $\mathrm{rank}(A) = \mathrm{rank}(A^*)$ for all matrices A.

4 Blindness of the single-server protocol

In this section, we show the blindness of the single-server protocol (composed of Protocols 2, 3, 4). Informally speaking, a protocol is defined to be blind if Bob, given all the classical and quantum information during the protocol, cannot learn anything about the Alice's actual computational angles, input and the output [3]. In the original paper for the blind quantum computation over the cluster states [3] blindness is formally defined in terms of the independence of classical and quantum states of Bob from Alice's secret. Here we adapt the definition to our setting but we omit a formal proof of the equivalences between the two definitions. Note that since random numbers are independent with each other, the combinations of gates are also secure.

Definition 1 *A single-server protocol is blind if*

(S1) The conditional probability distribution of Alice's nontrivial computational angles, given all the classical information Bob can obtain during the protocol, and given the measurement results of any POVMs which Bob may perform on his system at any stage of the protocol, is uniform,

and

(S2) The register state in the correlation space is one-time padded to Bob.

In order to show (S1), we have to show three lemmas.

In the following we define Φ, Θ, Ξ and R to be independently and uniformly distributed random variables, corresponding to the angles sent by Alice to Bob, Alice's secret computational angle, random prerotation and a hidden binary parameter, respectively. From the construction of the protocol, the following relation is satisfied:

$$\Phi = \Theta + \Xi + R\pi \pmod{2\pi}.$$

We denote by ρ_Ξ the state that Alice sends to Bob parametrized by Ξ. The most general method Bob may resort to in order to learn Alice's secret computational angles is described by a POVM measurement $\{\Pi_j\}_{j=1}^m$ on ρ_Ξ. This POVM can depend on all classical messages received from Alice. Let $O \in \{1, ..., m\}$ be the random variable corresponding to the result of the POVM measurement. Bob's knowledge about Alice's secret angles is given by the conditional probability distribution of $\Theta = \theta$ given $O = j$ and $\Phi = \phi$:

$$P(\Theta = \theta | O = j, \Phi = \phi).$$

Lemma 2 *If ρ_Ξ is a Dango state $|D_{Z/X}(\Xi)\rangle\langle D_{Z/X}(\Xi)|$, then $P(\Theta = \theta | O = j, \Phi = \phi) = \frac{1}{8}$ for any $\theta, \phi \in \mathcal{A}$, $j \in \{1, ..., m\}$, and POVM on ρ_Ξ.*

Proof: From Bayes' theorem, we have

$$\begin{aligned} P(\Theta = \theta | O = j, \Phi = \phi) &= \frac{P(O = j | \Theta = \theta, \Phi = \phi) P(\Theta = \theta, \Phi = \phi)}{P(O = j, \Phi = \phi)} \\ &= \frac{P(O = j | \Theta = \theta, \Phi = \phi) P(\Theta = \theta) P(\Phi = \phi)}{P(O = j | \Phi = \phi) P(\Phi = \phi)} \\ &= \frac{1}{8} \frac{\mathrm{Tr}\big[\Pi_j \frac{1}{2} \sum_r \rho_{\phi - \theta - r\pi}\big]}{\mathrm{Tr}\big[\Pi_j \frac{1}{8} \frac{1}{2} \sum_{\theta, r} \rho_{\phi - \theta - r\pi}\big]}. \end{aligned}$$

If ρ_Ξ is a Dango state $|D_{Z/X}(\Xi)\rangle\langle D_{Z/X}(\Xi)|$, we obtain

$$\frac{1}{2}\sum_r \rho_{\phi-\theta-r\pi} = \frac{1}{2}\frac{1}{8}\sum_{\theta,r}\rho_{\phi-\theta-r\pi}$$

for any $\phi,\theta\in[0,2\pi]$, and hence $P(\Theta=\theta|O=j,\Phi=\phi)=1/8$. The above equation is valid since

$$|D_Z(\xi)\rangle\langle D_Z(\xi)| = \big[I\otimes(I-|\eta_1\rangle\langle\eta_1|)\otimes I\big]\frac{1}{4}\begin{pmatrix} 1 & e^{-i\xi} & 1 & 1\\ e^{i\xi} & 1 & e^{i\xi} & e^{i\xi}\\ 1 & e^{-i\xi} & 1 & 1\\ 1 & e^{-i\xi} & 1 & 1\end{pmatrix}\oplus\mathbf{0}_{12}\big[I\otimes(I-|\eta_1\rangle\langle\eta_1|)\otimes I\big],$$

where $\mathbf{0}_{12}$ is the 12×12 zero matrix and the 4×4 matrix is in the basis $\{|0000\rangle,|0011\rangle,|1100\rangle,|1111\rangle\}$, and there exists a unitary which maps $(I\otimes T_Z(\xi)\otimes I)|\eta_1\rangle\otimes|\eta_1\rangle$ to $(I\otimes T_X(\xi)\otimes I)|\eta_1\rangle\otimes|\eta_1\rangle$.
■

Lemma 3 *Consider a collection of L states $\{\rho_{\Xi_l}\}_l$ such that for each $l=1,\ldots,L$ we have*

$$P\Big(\Theta_l=\theta_l\Big|O^l=j,\Phi_l=\phi_l\Big)=\frac{1}{8}$$

where Φ_l, Θ_l, Ξ_l and R_l are defined as before. Also, O^l are the random variables corresponding to (arbitrary) POVMs performed on individual systems. Then for any global POVM performed on the entire collection of L states we have

$$P\Big(\Theta=(\theta_1,...,\theta_L)\Big|O=j,\Phi=(\phi_1,...,\phi_L)\Big)=\frac{1}{8^L}$$

where O is the random variable corresponding to the outcome of the global POVM.

Proof: Similar to the previous proof, from Bayes' theorem, we have

$$\begin{aligned} &P\Big(\Theta=(\theta_1,...,\theta_L)\Big|O=j,\Phi=(\phi_1,...,\phi_L)\Big)\\ =\;& \frac{P\Big(O=j\Big|\Theta=(\theta_1,...,\theta_L),\Phi=(\phi_1,...,\phi_L)\Big)P\Big(\Theta=(\theta_1,...,\theta_L),\Phi=(\phi_1,...,\phi_L)\Big)}{P\Big(O=j,\Phi=(\phi_1,...,\phi_L)\Big)}\\ =\;& \frac{P\Big(O=j\Big|\Theta=(\theta_1,...,\theta_L),\Phi=(\phi_1,...,\phi_L)\Big)P\Big(\Theta=(\theta_1,...,\theta_L)\Big)P\Big(\Phi=(\phi_1,...,\phi_L)\Big)}{P\Big(O=j\Big|\Phi=(\phi_1,...,\phi_L)\Big)P\Big(\Phi=(\phi_1,...,\phi_L)\Big)}\\ =\;& \frac{1}{8^L}\frac{\mathrm{Tr}\Big[\Pi_j\bigotimes_{i=1}^L\frac{1}{2}\sum_{r_i}\rho_{\phi_i-\theta_i-r_i\pi}\Big]}{\mathrm{Tr}\Big[\Pi_j\bigotimes_{i=1}^L\frac{1}{8}\frac{1}{2}\sum_{\theta_i,r_i}\rho_{\phi_i-\theta_i-r_i\pi}\Big]}. \end{aligned}$$

Let us define two local operators acting on lth state ρ_{Ξ_l} by

$$\begin{aligned} \Pi_j^l &\equiv \mathrm{Tr}_{1,\ldots,l-1,l+1,\ldots,L}\Big[\Pi_j\bigotimes_{i=1}^{l-1}\frac{1}{2}(\sum_{r_i}\rho_{\phi_i-\theta_i-r_i\pi})\bigotimes_{i=l+1}^{L}\frac{1}{2}(\sum_{r_i}\rho_{\phi_i-\theta_i-r_i\pi})\Big],\\ \tilde{\Pi}_j^l &\equiv \mathrm{Tr}_{1,\ldots,l-1,l+1,\ldots,L}\Big[\Pi_j\bigotimes_{i=1}^{l-1}\frac{1}{8}\frac{1}{2}(\sum_{\theta_i,r_i}\rho_{\phi_i-\theta_i-r_i\pi})\bigotimes_{i=l+1}^{L}\frac{1}{8}\frac{1}{2}(\sum_{\theta_i,r_i}\rho_{\phi_i-\theta_i-r_i\pi})\Big]. \end{aligned}$$

The partial trace is a CPTP superoperator, hence the above operators are non-negative operators, and since

$$\begin{aligned}\sum_{j=1}^m \Pi_j^l &= I,\\ \sum_{j=1}^m \tilde{\Pi}_j^l &= I,\end{aligned}$$

hence $\{\Pi_j^l\}_{j=1}^m$ and $\{\tilde{\Pi}_j^l\}_{j=1}^m$ are local POVMs on lth state.

Let O^l and $\tilde{O}^l$ be the random variables which correspond to the results of the POVMs $\{\Pi_j^l\}_{j=1}^m$ and $\{\tilde{\Pi}_j^l\}_{j=1}^m$, respectively. Then, we have

$$\begin{aligned}
&P\Big(\Theta=(\theta_1,...,\theta_L)\Big|O=j,\Phi=(\phi_1,...,\phi_L)\Big)\\
&= \frac{1}{8^L}\frac{\mathrm{Tr}_l\Big[\Pi_j^l\frac{1}{2}\sum_{r_l}\rho_{\phi_l-\theta_l-r_l\pi}\Big]}{\mathrm{Tr}_l\Big[\tilde{\Pi}_j^l\frac{1}{8}\frac{1}{2}\sum_{\theta_l,r_l}\rho_{\phi_l-\theta_l-r_l\pi}\Big]}\\
&= \frac{1}{8^L}\frac{P(O^l=j|\Phi_l=\phi_l,\Theta_l=\theta_l)}{P(\tilde{O}^l=j|\Phi_l=\phi_l)}\\
&= \frac{1}{8^L}\frac{P(O^l=j|\Phi_l=\phi_l,\Theta_l=\theta_l)}{P(O^l=j|\Phi_l=\phi_l)}\frac{P(O^l=j|\Phi_l=\phi_l)}{P(\tilde{O}^l=j|\Phi_l=\phi_l)}\\
&= \frac{1}{8^{L-1}}\frac{P(O^l=j|\Phi_l=\phi_l,\Theta_l=\theta_l)P(\Phi_l=\phi_l)P(\Theta_l=\theta_l)}{P(O^l=j|\Phi_l=\phi_l)P(\Phi_l=\phi_l)}\frac{P(O^l=j|\Phi_l=\phi_l)}{P(\tilde{O}^l=j|\Phi_l=\phi_l)}\\
&= \frac{1}{8^{L-1}}\frac{P(O^l=j|\Phi_l=\phi_l,\Theta_l=\theta_l)P(\Phi_l=\phi_l,\Theta_l=\theta_l)}{P(O^l=j,\Phi_l=\phi_l)}\frac{P(O^l=j|\Phi_l=\phi_l)}{P(\tilde{O}^l=j|\Phi_l=\phi_l)}\\
&= \frac{1}{8^{L-1}}P(\Theta_l=\theta_l|\Phi_l=\phi_l,O^l=j)\frac{P(O^l=j|\Phi_l=\phi_l)}{P(\tilde{O}^l=j|\Phi_l=\phi_l)}\\
&= \frac{1}{8^L}\frac{P(O^l=j|\Phi_l=\phi_l)}{P(\tilde{O}^l=j|\Phi_l=\phi_l)}.
\end{aligned}$$

Note that $P(O^l=j|\Phi_l=\phi_l)$ and $P(\tilde{O}^l=j|\Phi_l=\phi_l)$ are independent of θ_l, and hence

$$P\Big(\Theta=(\theta_1,...,\theta_L)\Big|O=j,\Phi=(\phi_1,...,\phi_L)\Big)$$

is also independent of θ_l. The same result holds for any $l=1,...,L$, hence the proof is completed. ■

Recall that a single X/Z Dango chain is used for the implementation of a fixed X/Z rotation. The following lemma shows this information does not help Bob to learn about Alice's secret.

Lemma 4 *Under the assumptions of Lemma 3, assume that Θ takes values with a non-zero probability only in a subset K, i.e. $\Theta\in K\subset\mathcal{A}^{\times L}$. Then*

$$P\Big(\Theta=\theta\Big|O=j,\Phi=(\phi_1,...,\phi_L),\Theta\in K\Big)=\frac{1}{|K|}$$

for any $\theta\in K$, $(\phi_1,...,\phi_L)\in\mathcal{A}^{\times L}$, $j\in\{1,...,m\}$, and POVM on $\bigotimes_{i=1}^L\rho_{\Xi_i}$.

Proof: Similar to the previous proofs, we have

$$
\begin{aligned}
P\Big(\Theta=\theta\Big|O=j,\Phi=(\phi_1,...,\phi_L),\Theta\in K\Big) &= \frac{P\Big(\Theta=\theta,\Theta\in K\Big|O=j,\Phi=(\phi_1,...,\phi_L)\Big)}{P\Big(\Theta\in K\Big)}\\
&= \frac{P\Big(\Theta=\theta\Big|O=j,\Phi=(\phi_1,...,\phi_L)\Big)}{P\Big(\Theta\in K\Big)}\\
&= \frac{1/8^L}{|K|/8^L}.
\end{aligned}
$$

■

Theorem 1 *The single-server protocol satisfies (S1).*

Proof: Bob receives $2NM$ Dango states, and therefore there are $2NM$ secret angles $\{\xi_{a,b}^{Z/X}\}_{(a,b)=(1,1)}^{(N,M)}$. Bob also receives $2NM$ angles $\{\phi_{a,b}^{Z/X}\}_{(a,b)=(1,1)}^{(N,M)}$ from Alice. Let $\Theta,\Phi\in\mathcal{A}^{\times 2NM}$ be random variables, and $O\in\{1,...,m\}$ be the random variable which corresponds to the result of the POVM measurement which Bob performs on his system. Since Bob knows that Alice tries the same rotation many times in a single Z/X-AKLT subsystem until she succeeds, and that after the success of the rotation Alice implements the trivial identity operation on the rest of qutrits in the Z/X-AKLT subsystem, Bob can assume that Θ takes values only in a subset K: $\Theta\in K\subset\mathcal{A}^{\times 2NM}$, where $|K|=8^{2NM/n}$.

From Lemma 1, 2, and 3, we have the following equality $\forall\theta\in K$, $\forall\phi_{a,b}^{Z/X}\in\mathcal{A}$, $(a=1,...,N)$, $(b=1,...,M)$, $j\in\{1,...,m\}$, and for any POVM

$$
P\Big(\Theta=\theta\Big|O=j,\Phi=\{\phi_{a,b}^{Z/X}\}_{(a,b)=(1,1)}^{(N,M)},\Theta\in K\Big)=\frac{1}{|K|}
$$

■

Theorem 2 *The single-server protocol satisfies (S2).*

Proof: It is easy to see

- When $R_Z^\alpha(\theta_{k,b}^Z,r_{(k-1)n+j,b}^Z)$ or $R_Z^\beta(\theta_{k,b}^Z,r_{(k-1)n+j,b}^Z)$ is implemented in the correlation space, the byproduct $XZ^{r^Z_{(k-1)n+j,b}}$ or $XZ^{r^Z_{(k-1)n+j,b}+1}$ occurs, respectively. If Bob has no information about the value of $r_{(k-1)n+j,b}^Z$, he cannot know whether the byproduct Z appears or not.
- When $R_X^\alpha(\theta_{k,b}^X,r_{(k-1)n+j,b}^X)$ or $R_X^\beta(\theta_{k,b}^X,r_{(k-1)n+j,b}^X)$ is implemented in the correlation space, the byproduct $X^{r^X_{(k-1)n+j,b}+1}Z$ or $X^{r^X_{(k-1)n+j,b}}Z$ occurs, respectively. If Bob has no information about the value of $r_{(k-1)n+j,b}^X$, he cannot know whether the byproduct X appears or not.

Note that we assume Alice's computation is implemented via a regular structure hence it contains both X and Z rotations. Therefore both byproducts of Pauli X and Z operators will appear leading to the full one-time padding of the computation in the correlation space. In fact, we can show that Bob cannot have any information about the values of $\{r_{(k-1)n+j,b}^{Z/X}\}$ by showing similar proofs as those for $\{\theta_{k,b}^{Z/X}\}$. However, it is easy to consider that $\theta_{k,b}^{Z/X}$ takes values only 0 or π in the above proofs leading to the exchange of the role of $\{r_{(k-1)n+j,b}^{Z/X}\}$ and $\{\theta_{k,b}^{Z/X}\}$.

5 Double-server protocol

In this section, we will explain the double-server protocol (Fig. 2). There are two advantages behind the new protocol: Alice could be completely classical and more importantly the resource state preparation and computation could be done more robustly using the energy-gap protection. To achieve these new features while keeping the security requirement intact, it is assumed that the two servers, Bob1 and Bob2, share many Bell pairs but have no classical or quantum channel between them. As we will discuss later it is an interesting open question (both from the practical and theoretical perspective) whether this assumption could be relaxed.

In the double-server protocol, Bob1 first creates AKLT resource states (without any random rotation), hence the preparation and storage of the state could be performed using ground state energy-gap protection as described in details in [15]. Next, depending on Alice's desired gates, Bob1 adiabatically turns off the interaction between some particles and the rest of particles in his resource state, and teleports these particles to Bob2 by consuming Bell pairs. Bob1 sends Alice the result of the measurement in the teleportation through the classical channel. Note that due to the lack of any communication (classical or quantum) channels between Bob1 and Bob2, the teleportation procedure from Bobs' point of view can be seen as a usage of a totally mixed channel where only Alice knows how to correct the output of the channel.

Next, Alice calculates the angle in which particles should be measured by using her classical computer, and sends Bob2 the angle which is the sum of the calculated angle plus the compensation for the byproduct and a random angle to hide the actual angle of the computation. Bob2 performs the measurement in that angle and sends the result of the measurement to Alice. Next, Alice sends the previous random angle to Bob1 and he does the single-qubit rotation which compensates the added random angle. Bob1 and Bob2 repeat this two-way classical communication with Alice until they finish the computation.

We define a (k, b)th AKLT subsystem ($k = 1, ..., N/n$, $b = 1, ..., M$) to be the collection of n qutrits of the bth AKLT chain with column index $(k-1)n+1, (k-1)n+2, ..., (k-1)n+n$ (Fig. 5 (a)). A single-qubit rotation is implemented in a single AKLT subsystem. Let us assume that Alice wants to perform the single-qubit Z-rotation $\exp\left[\frac{iZ}{2}\theta_{k,b}^{Z}\right]$ with $\theta_{k,b}^{Z} \in \mathcal{A}$ using (k, b)th AKLT subsystem (Protocol 5). The protocol for implementing an arbitrary X-rotation is similar and is given in the Appendix C. Finally, in order to perform blind CZ gates, similar to the single-sever protocol, Bob1 periodically implements CZ gates. In order to keep the register state in the ground space, the interactions are adiabatically turned off before each CZ gate. Unwanted CZ gates are canceled in the same way as that in the single-server protocol. Note that while for simplicity we present each gate separately however our generic construction with regular rotation and entangling gates will prevent any leakage of the information of the underlying structure of the computation obtained via composition.

Algorithm 5: Double-server Blind Z rotation

Initially the flag parameter (known to only Alice) is set $\tau = 1$. Alice sets her secret parameter $\epsilon^Z_{k,b} = 0$ and also chooses random numbers $\delta^Z_{k,b} \in \mathcal{A}$. Alice sends Bob1 parameter values N, M and $n < N$. Bob1 creates M AKLT chains $|AKLT^{N,L,R}_b\rangle$, where $b = 1, ..., M$ (see Equation 1) of N qutrits arranged in an array of N columns and M rows. For $j = 1 \cdots n/2$ Alice, Bob1, and Bob2 repeat (I)-(VI).

(I) Bob1 adiabatically turns off the interaction which acts on the jth qutrit of (k, b)th AKLT subsystem and applies $P^\dagger$ to the isolated qutrit in order to convert the qutrit into the pair of two qubits (Fig. 5 (b)). (The application of $P^\dagger$ can be done deterministically. For the physical implementation of $P^\dagger$, see Appendix 1.)

(II) Bob1 teleports the created two qubits to Bob2 by consuming two Bell pairs (Fig. 5 (c)). These two teleported qubits are affected by a two-qubit Pauli error $E \otimes E' \in \{I, X, Z, XZ\} \otimes \{I, X, Z, XZ\}$ (Fig. 5 (d)). Bob1 sends Alice the result of the measurement in the teleportation and hence only Alice and Bob1 knows which error appears.

(III) Bob2 applies the filtering operation $\{I - |\eta_1\rangle\langle\eta_1|, |\eta_1\rangle\langle\eta_1|\}$ to the received two qubits, and sends the result to Alice.

- If the Pauli error is $I \otimes I$, $X \otimes X$, $Z \otimes Z$, or $XZ \otimes XZ$, the probability of realizing $|\eta_1\rangle\langle\eta_1|$ is 0.
- If the Pauli error is $I \otimes Z$, $X \otimes XZ$, $Z \otimes I$, or $XZ \otimes X$, $|\eta_1\rangle\langle\eta_1|$ is realized with the probability 1/3. If $|\eta_1\rangle\langle\eta_1|$ is realized, Z is implemented in the correlation space.
- If the Pauli error is $I \otimes X$, $X \otimes I$, $Z \otimes XZ$, or $XZ \otimes Z$, $|\eta_1\rangle\langle\eta_1|$ is realized with the probability 1/3. If $|\eta_1\rangle\langle\eta_1|$ is realized, X is implemented in the correlation space.
- If the Pauli error is $I \otimes XZ$, $X \otimes Z$, $Z \otimes X$, or $XZ \otimes I$, $|\eta_1\rangle\langle\eta_1|$ is realized with the probability 1/3. If $|\eta_1\rangle\langle\eta_1|$ is realized, XZ is implemented in the correlation space.

If $|\eta_1\rangle\langle\eta_1|$ is realized, skip steps **(IV)**, **(V)** and **(VI)**. If $I - |\eta_1\rangle\langle\eta_1|$ is realized, Bob2 further applies the PEPS operation P on the two qubits. This PEPS operation is done deterministically, because the two qubits are already projected by $I - |\eta_1\rangle\langle\eta_1|$.

(IV) Alice sends the angle $\phi^Z_{(k-1)n+j,b}$ to Bob2. This angle is determined according to the following rule:

- If the Pauli error is $I \otimes I$, $I \otimes Z$, $Z \otimes I$, or $Z \otimes Z$,

$$\phi^Z_{(k-1)n+j,b} = \tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b} + r^Z_{(k-1)n+j,b}\pi \pmod{2\pi},$$

  where $\xi^Z_{(k-1)n+j,b} \in \mathcal{A}$ and $r^Z_{(k-1)n+j,b} \in \{0, 1\}$ are random numbers chosen by Alice, and signs of $\theta^Z_{k,b}$ and $\delta^Z_{k,b}$ should be changed if there is the byproduct X before this step.

- If the Pauli error is $X \otimes X$, $X \otimes XZ$, $XZ \otimes X$, or $XZ \otimes XZ$,

$$\phi^Z_{(k-1)n+j,b} = -\tau\theta^Z_{k,b} - \tau\delta^Z_{k,b} - \xi^Z_{(k-1)n+j,b} + r^Z_{(k-1)n+j,b}\pi \pmod{2\pi},$$

  where $\xi^Z_{(k-1)n+j,b} \in \mathcal{A}$ and $r^Z_{(k-1)n+j,b} \in \{0, 1\}$ are random numbers chosen by Alice, and signs of $\theta^Z_{k,b}$ and $\delta^Z_{k,b}$ should be changed if there is the byproduct X before this step.

- If the Pauli error is $I \otimes X$, $I \otimes XZ$, $X \otimes I$, $X \otimes Z$, $Z \otimes X$, $Z \otimes XZ$, $XZ \otimes I$, or $XZ \otimes Z$,

$$\phi^Z_{(k-1)n+j,b} = \xi^Z_{(k-1)n+j,b}$$

  where $\xi^Z_{(k-1)n+j,b} \in \mathcal{A}$ is a random number chosen by Alice.

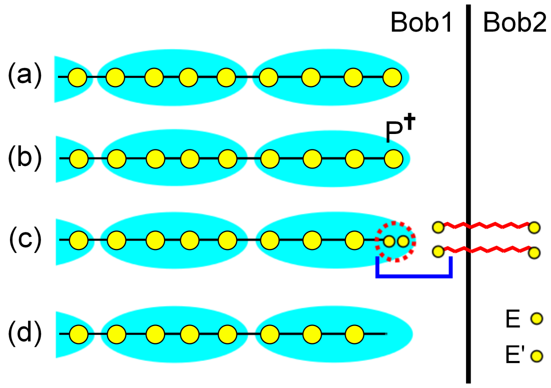

Fig. 5. (Color online.) (a): A chain $|AKLT^{N,L,R}\rangle$. Each AKLT subsystem is specified with a blue circle. In this example, $n = 4$. (b): Bob1 adiabatically turns off the interaction between a qutrit and others, and applies $P^\dagger$ to the qutrit in order to convert this qutrit into a pair of two qubits. (c): Bob1 teleports thus created two qubits to Bob2 by consuming two Bell pairs. (d): Because of the teleportation, Pauli errors E and E' occur.

Algorithm 5: Continued

(V) Bob2 does the measurement $\mathcal{M}(\phi^Z_{(k-1)n+j,b})$ (similar to Protocol 2), and sends the result to Alice. By this measurement, following operations are implemented in the correlation space (see also Appendix B):

- If the Pauli error is $I\otimes I$ or $Z\otimes Z$, $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$, $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability 1/3 respectively. If $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,

$$XZ^{r^Z_{(k-1)n+j,b}}\exp\Big[\frac{iZ}{2}\Big(\tau\theta^Z_{k,b}+\tau\delta^Z_{k,b}+\xi^Z_{(k-1)n+j,b}\Big)\Big]$$

is implemented. If $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,

$$XZ^{r^Z_{(k-1)n+j,b}+1}\exp\Big[\frac{iZ}{2}\Big(\tau\theta^Z_{k,b}+\tau\delta^Z_{k,b}+\xi^Z_{(k-1)+j,b}\Big)\Big]$$

is implemented. If $|\gamma\rangle$ is realized, Z is implemented.

Algorithm 5: — Continued

(V) —Continued

- If the Pauli error is $I \otimes Z$ or $Z \otimes I$, $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ occurs with the probability 1/2 respectively. If $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,
$$XZ^{r^Z_{(k-1)n+j,b}+1} \exp\left[\frac{iZ}{2}\left(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b}\right)\right]$$
is implemented. If $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,
$$XZ^{r^Z_{(k-1)n+j,b}} \exp\left[\frac{iZ}{2}\left(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b}\right)\right]$$
is implemented.
- If the Pauli error is $X \otimes X$ or $XZ \otimes XZ$, $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$, $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability 1/3 respectively. If $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,
$$XZ^{r^Z_{(k-1)n+j,b}} \exp\left[\frac{iZ}{2}\left(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b}\right)\right]$$
is implemented. If $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,
$$XZ^{r^Z_{(k-1)n+j,b}+1} \exp\left[\frac{iZ}{2}\left(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b}\right)\right]$$
is implemented. If $|\gamma\rangle$ is realized, Z is implemented.
- If the Pauli error is $X \otimes XZ$ or $XZ \otimes X$, $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ occurs with the probability 1/2 respectively. If $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,
$$XZ^{r^Z_{(k-1)n+j,b}+1} \exp\left[\frac{iZ}{2}\left(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b}\right)\right]$$
is implemented. If $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ is realized,
$$XZ^{r^Z_{(k-1)n+j,b}} \exp\left[\frac{iZ}{2}\left(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b}\right)\right]$$
is implemented.
- If the Pauli error is $I \otimes X$, $X \otimes I$, $Z \otimes XZ$, or $XZ \otimes Z$, $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$, $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability $\frac{1}{2}\sin^2[\frac{1}{2}\phi^Z_{(k-1)n+j,b}]$, $\frac{1}{2}\cos^2[\frac{1}{2}\phi^Z_{(k-1)n+j,b}]$, or 1/2, respectively. If $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ is realized, Z is implemented. If $|\gamma\rangle$ is realized, XZ is implemented.
- If the Pauli error is $I \otimes XZ$, $X \otimes Z$, $Z \otimes X$, or $XZ \otimes I$, $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$, $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability $\frac{1}{2}\cos^2[\frac{1}{2}\phi^Z_{(k-1)n+j,b}]$, $\frac{1}{2}\sin^2[\frac{1}{2}\phi^Z_{(k-1)n+j,b}]$, or 1/2, respectively. If $|\alpha(\phi^Z_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^Z_{(k-1)n+j,b})\rangle$ is realized, Z is implemented. If $|\gamma\rangle$ is realized, X is implemented.

(VI) If the z-rotation $\exp[\frac{iZ}{2}(\tau\theta^Z_{k,b} + \tau\delta^Z_{k,b} + \xi^Z_{(k-1)n+j,b})]$ is implemented in the previous step, Alice sets $\tau = 0$, and $\epsilon^Z_{k,b} = \epsilon^Z_{k,b} + \xi^Z_{(k-1)n+j,b}$ (mod 2π) (if there is no X byproduct before this rotation) or $\epsilon^Z_{k,b} = \epsilon^Z_{k,b} - \xi^Z_{(k-1)n+j,b}$ (mod 2π) (if there is the X byproduct before this rotation).

Algorithm 5: Continued

(VII) So far, the z-rotation

$$G_{k,b}^Z \exp\left[\frac{iZ}{2}(\epsilon_{k,b}^Z+\delta_{k,b}^Z)\right]\exp\left[\frac{iZ}{2}\theta_{k,b}^Z\right]$$

up to some Pauli byproduct $G_{k,b}^Z$ is implemented. The probability that they fail to perform this z-rotation is $(2/3)^{n/2}$, which is small for sufficiently large n. Alice asks Bob1 to correct the accumulated error. In order to do so she sends Bob1 the angle $\tilde{\epsilon}_{k,b}^Z=\epsilon_{k,b}^Z+\delta_{k,b}^Z \pmod{2\pi}$ if $G_{k,b}^Z$ contains no X byproduct, and $\tilde{\epsilon}_{k,b}^Z=-\epsilon_{k,b}^Z-\delta_{k,b}^Z$ $\pmod{2\pi}$ if $G_{k,b}^Z$ contains the X byproduct. Bob1 implements the rotation $\exp\left[-\frac{iZ}{2}\tilde{\epsilon}_{k,b}^Z\right]$ by using the rest of the qutrits in (k,b)th AKLT subsystem. The probability that Bob1 fails to perform this z-rotation is $(1/3)^{n/2}$, which is small for sufficiently large n.

6 Blindness of the double-server Protocol

In this section, we will show the blindness of the double-server protocol. Again, due to the independence of random numbers, combinations of gates are also secure.

Definition 2 *A double-sever protocol is blind if*

(D1) The conditional probability distribution of Alice's nontrivial computational angles, given all the classical information Bob1 can obtain during the protocol, and given the measurement results of any POVMs which Bob1 may perform on his system at any stage of the protocol, is uniform,

(D2) The conditional probability distribution of Alice's nontrivial computational angles, given all the classical information Bob2 can obtain during the protocol, and given the measurement results of any POVMs which Bob2 may perform on his system at any stage of the protocol, is uniform,

(D3) The register state in the correlation space is one-time padded to Bob1,

(D4) The register state in the correlation space is one-time padded to Bob2.

The proof is based on following lemmas.

Lemma 5 *Bob1 cannot send any information to Bob2.*

Proof: By the assumption, there is no channel between Bob1 and Bob2. Furthermore, Bob1 cannot send any information to Bob2 via Alice either. This is due to the following facts. First, what Bob1 sends to Alice are the "results of measurements in teleportations". Second, what Alice sends to Bob2 are $\{\phi_{(k-1)n+j,b}^{Z/X}\}$. Third, recall that Alice chooses the definition of each $\phi_{(k-1)n+j,b}^{Z/X}$ among

$$\begin{aligned}
\phi_{(k-1)n+j,b}^{Z/X} &= \tau\theta_{k,b}^{Z/X}+\tau\delta_{k,b}^{Z/X}+\xi_{(k-1)n+j,b}^{Z/X}+r_{(k-1)n+j,b}^{Z/X}\pi \pmod{2\pi},\\
\phi_{(k-1)n+j,b}^{Z/X} &= -\tau\theta_{k,b}^{Z/X}-\tau\delta_{k,b}^{Z/X}-\xi_{(k-1)n+j,b}^{Z/X}+r_{(k-1)n+j,b}^{Z/X}\pi \pmod{2\pi},
\end{aligned}$$

or

$$\phi^{Z/X}_{(k-1)n+j,b} = \xi^{Z/X}_{(k-1)n+j,b}$$

according to what Bob1 sends to Alice. However, the value of each $\phi^{Z/X}_{(k-1)n+j,b}$ is independent of what Bob1 sends to Alice, since $\xi^{Z/X}_{(k-1)n+j,b}$ is completely random and therefore $\phi^{Z/X}_{(k-1)n+j,b}$ takes any value in $\mathcal{A}$ with equal probability, whichever definition Alice chooses. Therefore,

$$\begin{aligned} P\Big(T=t\Big|\Phi=\{\phi^{Z/X}_{(k-1)n+j,b}\}\Big) &= \frac{P\Big(\Phi=\{\phi^{Z/X}_{(k-1)n+j,b}\}\Big|T=t\Big)P\Big(T=t\Big)}{P\Big(\Phi=\{\phi^{Z/X}_{(k-1)n+j,b}\}\Big)} \\ &= P\Big(T=t\Big), \end{aligned}$$

where T is the random variable which represents teleportation results.

Finally, Bell pairs shared between Bob1 and Bob2 cannot transmit any information from Bob1 to Bob2 without sending a classical message from Bob1 to Bob2, since if it is possible, information is transfered faster than light from Bob1 to Bob2. ■

Lemma 6 *Bob2 cannot send any information to Bob1.*

Proof: Similar to the previous lemma, Bob2 cannot send any information to Bob1 via Alice. This is due to the following facts. First, what Bob2 sends to Alice are the "results of filterings and measurements". Second, what Alice sends to Bob1 are $\{\tilde{\epsilon}^{Z/X}_{k,b}\}$. Third, although $\epsilon^{Z/X}_{k,b}$ depends on what Bob2 sends Alice, $\tilde{\epsilon}^{Z/X}_{k,b}$ is independent of what Bob2 sends Alice, since $\delta^{Z/X}_{k,b}$ is completely random. Therefore,

$$\begin{aligned} P\Big(F=f\Big|E=\{\tilde{\epsilon}^{Z/X}_{k,b}\}\Big) &= \frac{P\Big(E=\{\tilde{\epsilon}^{Z/X}_{k,b}\}\Big|F=f\Big)P\Big(F=f\Big)}{P\Big(E=\{\tilde{\epsilon}^{Z/X}_{k,b}\}\Big)} \\ &= P\Big(F=f\Big), \end{aligned}$$

where F is the random variable which represents the results of filterings and measurements. ■

Theorem 3 *The double-server protocol satisfies (D2).*

Proof: From Lemma 4, Bob1 cannot send any information to Bob2. Therefore, all quantum states which Bob2 receives are completely mixed states, and all classical information which Bob2 gains are only $\{\phi^{Z/X}_{(k-1)n+j,b}\}$. Since $\{\xi^{Z/X}_{(k-1)n+j,b}\}$ and $\{\delta^{Z/X}_{k,b}\}$ are completely random and independent from $\{\theta^{Z/X}_{k,b}\}$, Bob2 cannot have any information about $\{\theta^{Z/X}_{k,b}\}$ from $\{\phi^{Z/X}_{(k-1)n+j,b}\}$. ■

Theorem 4 *The double-server protocol satisfies (D4).*

Proof: It is easy to see that

- When the z-rotation $\exp\left[\frac{iZ}{2}\left(\theta^Z_{k,b}+\delta^Z_{k,b}+\xi^Z_{(k-1)n+j,b}\right)\right]$ is implemented, the byproduct $XZ^{r^Z_{(k-1)n+j,b}}$ or $XZ^{r^Z_{(k-1)n+j,b}+1}$ occurs.

- When the x-rotation $\exp\left[\frac{-iX}{2}\left(\theta_{k,b}^X+\delta_{k,b}^X+\xi_{(k-1)n+j,b}^X\right)\right]$ is implemented, the byproduct $X^{r_{(k-1)n+j,b}^X}Z$ or $X^{r_{(k-1)n+j,b}^X+1}Z$ occurs.

Bob2 cannot gain any information about $\{r_{(k-1)n+j,b}^{Z/X}\}$ from $\{\phi_{(k-1)n+j,b}^{Z/X}\}$, since $\{\xi_{(k-1)n+j,b}^{Z/X}\}$ and $\{\delta_{k,b}^{Z/X}\}$ are completely random and independent from $\{r_{(k-1)n+j,b}^{Z/X}\}$. ■

Theorem 5 *The double-server protocol satisfies (D3).*

Proof: First, since $\{\xi_{(k-1)n+j,b}^{Z/X}\}$ are completely random, hence $\{\epsilon_{k,b}^{Z/X}\}$ is independent from $\{r_{(k-1)n+j,b}^{Z/X}\}$. Second, although $\tilde{\epsilon}_{k,b}^{Z/X}$ is related to the parity of X or Z in $G_{k,b}^{Z/X}$, Bob1 cannot know these parities from $\{\tilde{\epsilon}_{k,b}^{Z/X}\}$ since Bob1 does not know $\{\delta_{k,b}^{Z/X}\}$. Therefore (D3) is satisfied. ■

Theorem 6 *The double-server protocol satisfies (D1).*

Proof: From Lemma 5, Bob2 cannot send any information to Bob1. Therefore, the classical information which Bob1 can gain are only $\{\tilde{\epsilon}_{k,b}^{Z/X}\}$. Obviously, $\{\tilde{\epsilon}_{k,b}^{Z/X}\}$ are independent from $\{\theta_{k,b}^{Z/X}\}$. Furthermore, from Theorem 5, Bob1's states are one-time padded to him, therefore, no POVM on Bob1's states gives information to Bob1. ■

7 Discussion

In this paper we have investigated possibilities of blind quantum computing on AKLT states, which are physically-motivated resource states for measurement-based quantum computation. We have shown that our blind quantum computation protocols can enjoy several advantages of AKLT states, such as the cooling preparation of the resource state, the energy-gap protection of the quantum computation, and the simple and efficient preparation of the resource state in linear optics with biphotons.

We have presented two protocols, namely the single-sever protocol and the double-server protocol. In the single-server protocol, we have shown that blind quantum computation is possible, if Alice is allowed to have weak quantum technology as in the case of Ref. [3]. Because AKLT resources states exhibit many different properties from those of the cluster state, several novel features have been introduced in our protocol compared with Ref. [3]. Furthermore, new techniques and formalism have been required for the proof of the blindness of our protocol.

We have also seen that in our single-server protocol, quantum computation cannot be performed in the ground space of a natural Hamiltonian, since if Bob does not know pre-rotated angles, he must prepare an unnatural Hamiltonian with exponentially-degenerated ground states. This no-go theorem is general (we do not assume the state to be the AKLT states), hence drastically new scheme of blind quantum computation must be required in order to perform blind quantum computation in the ground space of a natural Hamiltonian in the single-server setting. On the other hand, our double-server protocol is the first blind delegated quantum computing protocol in which Alice is completely classical and quantum computation is performed in the ground space of a physically-motivated Hamiltonian.

One might think that why we have not considered the direct generalization of the double-server protocol in Ref. [3]. Here, the direct generalization means following protocol: Alice sends hidden angles $\{\xi_{a,b}^Z\}$ to Bob1, and Bob1 creates rotated AKLT states. Bob1 then teleports his particles to Bob2, and Bob2 performs measurements. Let us briefly explain why such a direct generalization does not work for AKLT resource states. If Bob1 teleports a prerotated particle by $\xi_{a,b}^Z$, the operation implemented in the correlation space by Bob2's measurement can be unwanted Z rotation $e^{i\xi_{a,b}^Z Z/2}$ for certain teleportation error and Bob2's measurement result. In this case, Alice must compensate the accumulation of these unwanted rotations, and therefore she must send some number which is related to $\{\xi_{a,b}^Z\}$. Since Bob1 knows teleportation errors and $\{\xi_{a,b}^Z\}$, he can gain some information about Bob2's measurement results, and therefore Bob2 can send some classical message to Bob1.

The assumption in the double-server protocol that two Bobs share no communication channel is clearly strong. However, as mentioned before, the set up of entangled servers scheme has been an important setting in the context of computer science, cryptography, and, recently, verification of general quantum dynamics [40]. It would be an interesting research question to find scenarios, and also cryptographic tools, in which such a no-communicating requirement can be enforced.

To finalize, we note that at this stage, we do not know which quantum computation model (circuit, adiabatic, measurement-based model, etc.) is the most promising candidate for the realization of a scalable quantum computer. Therefore, it is valuable to explore possibilities of blind quantum computation in various models. It would be an interesting subject of future study.

Acknowledgements

The authors would like to acknowledge the support from Carnegie trust for the Universities of Scotland and the Quantum Information Scotland Network (QUISCO) for sponsoring TM visit which made this collaboration possible. TM acknowledges support by JSPS, Tenure Track system by MEXT Japan, and ANR (StatQuant JC07 07205763). VD was supported by EPSRC (grant EP/G009821/1) and EPSRC Doctoral Prize Fellowship. EK was supported by EPSRC (grant EP/E059600/1).

References

1. A. Childs, Quant. Inf. Compt. **5**, 456 (2005).
2. P. Arrighi and L. Salvail, Int. J. Quant. Inf. **4**, 883 (2006).
3. A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), pp.517.
4. D. Aharonov, M. Ben-Or, and E. Eban, Proceedings of Innovations in Computer Science 2010 (ICS 2010), pp. 453.
5. P. Shor, Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos, edited by Shafi Goldwasser (IEEE Computer Society Press), pp. 124.
6. J. Feigenbaum, Proceedings of Advances in Cryptology, CRYPTO 85, 1986, pp.477.
7. Non-deterministic polynomial-time hard function is a problem that is at least as hard as the hardest problems in the class **NP**, where **NP** is the class of all problems whose solutions are easy to verify, whereas finding a solution is considered intractable.
8. M. Abadi, J. Feigenbaum, and J. Kilian, Journal of Computer and System Sciences,1989, **39**, pp. 21.
9. Recently, the polynomial hierarchy collapses argument was found also in quantum information, such as [S. Aaronson and A. Arkhipov, arXiv:1011.3245]
10. C. Gentry, Proceedings of the 41st annual ACM Symposium on Theory of Computing (STOC 2009), pp. 169.
11. P. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).

12. R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
13. R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
14. F. Verstraete and J. I. Cirac, Phys. Rev. A **70**, 060302(R) (2004).
15. G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).
16. D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).
17. D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Phys. Rev. A **76**, 052315 (2007).
18. D. Gross and J. Eisert, Phys. Rev. A **82**, 040303(R) (2010).
19. A. Miyake, Phys. Rev. Lett. **105**, 040501 (2010).
20. A. Miyake, arXiv: 1009.3491.
21. T. C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).
22. J. Cai, A. Miyake, W. Dür, and H. J. Briegel, Phys. Rev. A **82**, 052309 (2010).
23. Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, arXiv: 1102.5153.
24. X. Chen, B. Zeng, Z. Gu, B. Yoshida, and I. L. Chuang, Phys. Rev. Lett. **102**, 220501 (2009).
25. X. Chen, R. Duan, Z. Ji, and B. Zeng, Phys. Rev. Lett. **105**, 020502 (2010).
26. I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Comm. Math. Phys. **115**, 477 (1988).
27. F. D. M. Haldane, Phys. Rev. Lett. **50**, 1153 (1983).
28. M. den Nijs and K. Rommelse, Phys. Rev. B **40**, 4709 (1989).
29. T. Kennedy, J. Phys. Condens. Matter **2**, 5737 (1990).
30. A. S. Darmawan and S. D. Bartlett, Phys. Rev. A **82**, 012328 (2010).
31. D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac, Quant. Inf. Comput. **7**, 401 (2007).
32. F. Verstraete, J. I. Cirac, and V. Murg, Adv. Phys. **57**, 143 (2008).
33. J. I. Cirac and F. Verstraete, J. Phys. A: Math. Theor. **42**, 504004 (2009).
34. F. Verstraete, M. Popp, and J. I. Cirac, Phys. Rev. Lett. **92**, 027901 (2004).
35. F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004).
36. Here we assume that Alice performs the projection $I - |\eta_1\rangle\langle\eta_1|$, since it makes our explanations simpler. Actually, this projection can be done by Bob.
37. P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, Proceedings of 40th Annual Symposium on Fondations of Computer Science (FOCS) (IEEE Press, Los Alamitos, CA, 1999), pp.486-494; arXiv:9906054.
38. T. Morimae, Phys. Rev. A **83**, 042337 (2011).
39. Physically, PEPS operation just means Bob encodes the three-dimensional subspace of the four-dimensional Hilbert space as a single qutrit.
40. B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).

Appendix A

The inverse $P^\dagger$ of the PEPS P can be implemented as follows. Bob1 first prepares the two-qubit state $|0\rangle\otimes|0\rangle$, and performs the filtering operation $\{F_{i,j}\}_{(i,j)=(0,0)}^{(1,1)}$ on the qutrit to which he wants to apply $P^\dagger$ and the two-qubit state, where

$$F_{i,j} \equiv |1\rangle\langle 1|\otimes|\eta_3\rangle\langle i,j| + |2\rangle\langle 2|\otimes|\eta_4\rangle\langle i,j| + |3\rangle\langle 3|\otimes|\eta_2\rangle\langle i,j|,$$

$|i,j\rangle \equiv |i\rangle\otimes|j\rangle$, and

$$\sum_{i=0}^{1}\sum_{j=0}^{1} F_{i,j}^\dagger F_{i,j} = I.$$

With probability 1, $F_{0,0}$ is realized. Next Bob1 measures the qutrit in the basis

$$\Big\{\frac{1}{\sqrt{3}}\Big(|1\rangle+|2\rangle+|3\rangle\Big), \frac{1}{\sqrt{3}}\Big(|1\rangle+e^{i2\pi/3}|2\rangle+e^{i4\pi/3}|3\rangle\Big), \frac{1}{\sqrt{3}}\Big(|1\rangle+e^{i4\pi/3}|2\rangle+e^{i8\pi/3}|3\rangle\Big)\Big\}$$

and corrects the phase error if the result is the second or the third one.

Appendix B

Let $E\otimes E'\in\{I,X,Z,XZ\}\otimes\{I,X,Z,XZ\}$ be the Pauli error on two qubits, and define the PEPS $\tilde{P}$ by

$$\tilde{P}\equiv P(E\otimes E')P^\dagger P.$$

Also define the matrices $\{\tilde{A}[1],\tilde{A}[2],\tilde{A}[3]\}$ by

$$\tilde{P}=\frac{1}{\sqrt{2}}\sum_{l=1}^{3}\sum_{a=0}^{1}\sum_{b=0}^{1}\tilde{A}_{a,b}[l]|l\rangle\langle a,b|,$$

where $\tilde{A}_{a,b}[l]$ depends on the Pauli error as summarized in the second, third, and fourth columns of the following table. The fifth, sixth, and seventh columns are the summary of the operations implemented in the correlation space by the measurement $\mathcal{M}(\phi)$ after the PEPS $\tilde{P}$ for each error. The eighth, nineth, and tenth columns are the summary of the operations implemented in the correlation space by the application of V and the measurement $\mathcal{M}(\phi)$ after the PEPS $\tilde{P}$ for each error.

$E \otimes E'$	$\tilde{A}[1]$	$\tilde{A}[2]$	$\tilde{A}[3]$	$\|\alpha(\phi)\rangle$	$\|\beta(\phi)\rangle$	$\|\gamma\rangle$	$\|\alpha(\phi)\rangle$	$\|\beta(\phi)\rangle$	$\|\gamma\rangle$
$I \otimes I$	X	XZ	Z	$Xe^{iZ\phi/2}$	$XZe^{iZ\phi/2}$	Z	$XZe^{-iX\phi/2}$	$Ze^{-iX\phi/2}$	X
$I \otimes X$	0	$-Z$	$-XZ$	$-Z$	$-Z$	$-XZ$	$-Ze^{-iX\phi/2}$	$-XZe^{-iX\phi/2}$	0
$I \otimes Z$	XZ	X	0	$XZe^{iZ\phi/2}$	$Xe^{iZ\phi/2}$	0	X	X	XZ
$I \otimes XZ$	Z	0	$-X$	Z	Z	$-X$	$-X$	$-X$	Z
$X \otimes I$	0	Z	XZ	Z	Z	XZ	$Ze^{-iX\phi/2}$	$XZe^{-iX\phi/2}$	0
$X \otimes X$	X	$-XZ$	$-Z$	$Xe^{-iZ\phi/2}$	$-XZe^{-iZ\phi/2}$	$-Z$	$-XZe^{-iX\phi/2}$	$-Ze^{-iX\phi/2}$	X
$X \otimes Z$	Z	0	X	Z	Z	X	X	X	Z
$X \otimes XZ$	XZ	$-X$	0	$XZe^{-iZ\phi/2}$	$-Xe^{-iZ\phi/2}$	0	$-X$	$-X$	XZ
$Z \otimes I$	$-XZ$	$-X$	0	$-XZe^{iZ\phi/2}$	$-Xe^{iZ\phi/2}$	0	$-X$	$-X$	$-XZ$
$Z \otimes X$	Z	0	X	Z	Z	X	X	X	Z
$Z \otimes Z$	$-X$	$-XZ$	Z	$-Xe^{iZ\phi/2}$	$-XZe^{iZ\phi/2}$	Z	$-XZe^{iX\phi/2}$	$Ze^{iX\phi/2}$	$-X$
$Z \otimes XZ$	0	$-Z$	XZ	$-Z$	$-Z$	XZ	$-Ze^{iX\phi/2}$	$XZe^{iX\phi/2}$	0
$XZ \otimes I$	Z	0	$-X$	Z	Z	$-X$	$-X$	$-X$	Z
$XZ \otimes X$	$-XZ$	X	0	$-XZe^{-iZ\phi/2}$	$Xe^{-iZ\phi/2}$	0	X	X	$-XZ$
$XZ \otimes Z$	0	Z	$-XZ$	Z	Z	$-XZ$	$Ze^{iX\phi/2}$	$-XZe^{iX\phi/2}$	0
$XZ \otimes XZ$	$-X$	XZ	$-Z$	$-Xe^{-iZ\phi/2}$	$XZe^{-iZ\phi/2}$	$-Z$	$XZe^{iX\phi/2}$	$-Ze^{iX\phi/2}$	$-X$

Appendix C

Protocol 6 describes how Alice performs the single-qubit x-rotation $\exp\left[\frac{-iX}{2}\theta^X_{k,b}\right]$ by $\theta^X_{k,b} \in \mathcal{A}$ in (k,b)th X-AKLT subsystem.

Algorithm 6: Double-server Blind X rotation

Initially the flag parameter (known to only Alice) is set $\tau = 1$. Alice sets her secret parameter $\epsilon^X_{k,b} = 0$ and also chooses random numbers $\delta^X_{k,b} \in \mathcal{A}$. Alice sends Bob1 parameter values N, M and $n < N$. Bob1 creates M AKLT chains $|AKLT^{N,L,R}_b\rangle$, where $b = 1, ..., M$ (see Equation 1) of N qutrits arranged in an array of N columns and M rows. For $j = 1, \cdots, n/2$, Alice, Bob1, and Bob2 repeat (I)-(VI), where the steps **(I)**,**(II)(III)** are the same as in Protocol 5.

(IV) Alice sends the angle $\phi^X_{(k-1)n+j,b}$ to Bob2. This angle is determined according to the following rule:

- If the Pauli error is $I \otimes I$, $I \otimes X$, $X \otimes I$, or $X \otimes X$,

$$\phi^X_{(k-1)n+j,b} = \tau\theta^X_{k,b} + \tau\delta^X_{k,b} + \xi^X_{(k-1)n+j,b} + r^X_{(k-1)n+j,b}\pi \pmod{2\pi},$$

  where $\xi^X_{(k-1)n+j,b} \in \mathcal{A}$ and $r^X_{(k-1)n+j,b} \in \{0,1\}$ are random numbers chosen by Alice, signs of $\theta^X_{k,b}$ and $\delta^X_{k,b}$ should be changed if there is the byproduct Z before this step.

- If the Pauli error is $Z \otimes Z$, $Z \otimes XZ$, $XZ \otimes Z$, or $XZ \otimes XZ$,

$$\phi^X_{(k-1)n+j,b} = -\tau\theta^X_{k,b} - \tau\delta^X_{k,b} - \xi^X_{(k-1)n+j,b} + r^X_{(k-1)n+j,b}\pi \pmod{2\pi},$$

  where $\xi^X_{(k-1)n+j,b} \in \mathcal{A}$ and $r^X_{(k-1)n+j,b} \in \{0,1\}$ are random numbers chosen by Alice. Signs of $\theta^X_{k,b}$ and $\delta^X_{k,b}$ should be changed if there is the byproduct Z before this step.

- If the Pauli error is $I \otimes Z$, $I \otimes XZ$, $X \otimes Z$, $X \otimes XZ$, $Z \otimes I$, $Z \otimes X$, $XZ \otimes I$, or $XZ \otimes X$,

$$\phi^X_{(k-1)n+j,b} = \xi^X_{(k-1)n+j,b}$$

  where $\xi^X_{(k-1)n+j,b} \in \mathcal{A}$ is a random number chosen by Alice.

Algorithm 6: Continued

(V) Bob2 applies V, does the measurement $\mathcal{M}(\phi^X_{(k-1)n+j,b})$, and sends the result to Alice. By this measurement, following operations are implemented in the correlation space (see also Appendix B):

- If the Pauli error is $I\otimes I$ or $X\otimes X$, $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$, $|\beta(\phi^X_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability 1/3, respectively. If $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}+1}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented. If $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented. If $|\gamma\rangle$ is realized, X is implemented.
- If the Pauli error is $I\otimes X$ or $X\otimes I$, $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ occurs with the probability 1/2, respectively. If $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented. If $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}+1}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented.
- If the Pauli error is $Z\otimes Z$ or $XZ\otimes XZ$, $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$, $|\beta(\phi^X_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability 1/3, respectively. If $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}+1}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented. If $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented. If $|\gamma\rangle$ is realized, X is implemented.
- If the Pauli error is $Z\otimes XZ$ or $XZ\otimes Z$, $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ occurs with the probability 1/2, respectively. If $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented. If $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ is realized, $X^{r^X_{(k-1)n+j,b}+1}Z\exp\left[\frac{-iX}{2}\left(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b}\right)\right]$ is implemented.
- If the Pauli error is $I\otimes Z$, $X\otimes XZ$, $Z\otimes I$, or $XZ\otimes X$, $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$, $|\beta(\phi^X_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability $\frac{1}{2}\cos^2[\frac{1}{2}\phi^X_{(k-1)n+j,b}]$, $\frac{1}{2}\sin^2[\frac{1}{2}\phi^X_{(k-1)n+j,b}]$, or 1/2, respectively. If $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ is realized, X is implemented. If $|\gamma\rangle$ is realized, XZ is implemented.
- If the Pauli error is $I\otimes XZ$, $X\otimes Z$, $Z\otimes X$, or $XZ\otimes I$, $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$, $|\beta(\phi^X_{(k-1)n+j,b})\rangle$, or $|\gamma\rangle$ occurs with the probability $\frac{1}{2}\sin^2[\frac{1}{2}\phi^X_{(k-1)n+j,b}]$, $\frac{1}{2}\cos^2[\frac{1}{2}\phi^X_{(k-1)n+j,b}]$, or 1/2, respectively. If $|\alpha(\phi^X_{(k-1)n+j,b})\rangle$ or $|\beta(\phi^X_{(k-1)n+j,b})\rangle$ is realized, X is implemented. If $|\gamma\rangle$ is realized, Z is implemented.

(VI) If the x-rotation $\exp[\frac{-iX}{2}(\tau\theta^X_{k,b}+\tau\delta^X_{k,b}+\xi^X_{(k-1)n+j,b})]$ is implemented in the previous step, Alice sets $\tau=0$, and $\epsilon^X_{k,b}=\epsilon^X_{k,b}+\xi^X_{(k-1)n+j,b}$ (mod 2π) (if there is no Z byproduct before this rotation) or $\epsilon^X_{k,b}=\epsilon^X_{k,b}-\xi^X_{(k-1)n+j,b}$ (mod 2π) (if there is the Z byproduct before this rotation).

Algorithm 6: Continued

(VII) So far, the x-rotation

$$G^X_{k,b} \exp\left[\frac{-iX}{2}(\epsilon^X_{k,b} + \delta^X_{k,b})\right] \exp\left[\frac{-iX}{2}\theta^X_{k,b}\right]$$

up to a Pauli byproduct $G^X_{k,b}$ is implemented. The probability that they fail to perform this rotation is $(2/3)^{n/2}$, which is small for sufficiently large n. Alice asks Bob1 to correct the accumulated error. In order to do so she sends Bob1 the angle $\tilde{\epsilon}^X_{k,b} = \epsilon^X_{k,b} + \delta^X_{k,b}$ (mod 2π) if $G^X_{k,b}$ contains no Z byproduct, and $\tilde{\epsilon}^X_{k,b} = -\epsilon^X_{k,b} - \delta^X_{k,b}$ (mod 2π) if $G^Z_{k,b}$ contains the Z byproduct. Bob1 implements the rotation $\exp\left[\frac{iX}{2}\tilde{\epsilon}^X_{k,b}\right]$ by using the rest of the qutrits in (k,b)th AKLT subsystem. The probability that Bob1 fails to perform this x-rotation is $(1/3)^{n/2}$, which is small for sufficiently large n.