Broadcasting single-qubit and multiqubit entangled states: Authentication, cryptography, and distributed quantum computation

Hiroki Sukeno,[1] Tzu-Chieh Wei,[1] Mark Hillery,[2,3] János A. Bergou,[2,3] Dov Fields,[4] and Vladimir S. Malinovsky[4]

[1]*C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy, Stony Brook University, Stony Brook, New York 11794-3840, USA*

[2]*Department of Physics and Astronomy, Hunter College of the City University of New York, 695 Park Avenue, New York, New York 10065, USA*

[3]*Graduate Center of the City University of New York, 365 Fifth Avenue, New York, New York 10016, USA*

[4]*DEVCOM Army Research Laboratory, Adelphi, Maryland 20783, USA*

(Received 31 March 2023; accepted 12 May 2023; published 5 June 2023)

Quantum entanglement assisted with measurements provides various pathways to communicate information to parties within a network. In this work, we generalize a previous broadcasting protocol and present schemes to broadcast product and multipartite entangled quantum states, where in the latter case the sender can remotely add phase gates or abort distributing the states. We first focus on the broadcasting of product quantum states in a network, and generalize the basic protocol to include an arbitrary basis rotation and allow for multiple receivers and senders. We show how to add and delete senders from the network. The generalization also includes the case where a phase to be applied to the broadcast states is not known in advance but is provided to a sender encoded in another quantum state. Applications of broadcasting product states include authentication and three-state quantum cryptography. In the second part, we study the distribution of a single multiqubit state shared among several receivers entangled with multiqubit phase gates, which includes the graph states as an example. We show that by coordinating with the sender, the receivers can assist in performing remote, distributed measurement-based quantum computation with the Pauli-X basis measurement alone. As another application of this, we discuss the distribution of the multiqubit Greenberger-Horne-Zeilinger state.

DOI: 10.1103/PhysRevA.107.062605

I. INTRODUCTION

In a quantum network, quantum information, encoded in the form of qubits or perhaps qudits, can be sent between users either by sending the qubits directly or making use of shared entanglement (such as in the teleportation protocol) [1–4]. If the same information is to be sent to a number of different users, the no-cloning theorem presents a constraint on one's ability to do so for general quantum states. Despite this, several schemes for broadcasting quantum information have been investigated, but they typically require one entanglement bit (ebit) per qubit for each receiving party [5–8].

An alternative, if one has knowledge of the state to be distributed, is a version of remote state preparation [9–13]. For sending states to a single receiver, remote state preparation has a smaller classical communication cost than teleportation. If one goes a step further and restricts the set of states to be sent, then it can be adapted for broadcasting quantum information [14,15]. The protocol in Ref. [14] made use of dark states, while that in Ref. [15] used entangled Dicke states.

In Ref. [15] we showed how qubit states of the form $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$, where α and β are fixed but θ can be varied by the sender, can be simultaneously sent to a number of different receivers. Let us briefly summarize how this works for two receivers, and refer to this as the basic broadcast protocol (BBP). Alice prepares a state consisting of one qutrit and two qubits in the form

$$|\Psi^{(1,2)}\rangle_{abc} = \alpha^2|0\rangle_a|00\rangle_{bc} + \beta^2|1\rangle_a|11\rangle_{bc} + \alpha\beta|2\rangle_a(|01\rangle_{bc} + |10\rangle_{bc}) \quad (1)$$

and transmits the two qubits to Bob and Charlie separately. One can regard this state as the starting point shared among Alice, Bob, and Charlie. Note that superscript (1,2) denotes that we have one sender and two receivers. Later we generalize this to $|\Psi^{(M,N)}\rangle$ when we consider the case with M senders and N receivers.

Alice then applies the operator $U_a(\theta)$ to her qutrit, where $U_a|0\rangle_a = e^{2i\theta}|0\rangle_a$, $U_a|1\rangle_a = e^{-2i\theta}|1\rangle_a$, and $U_a|2\rangle_a = |2\rangle_a$. She then measures her qutrit in the basis

$$\begin{aligned} |u_0\rangle_a &= \frac{1}{\sqrt{3}}(|0\rangle_a + |1\rangle_a + |2\rangle_a) \\ |u_1\rangle_a &= \frac{1}{\sqrt{3}}(e^{2\pi i/3}|0\rangle_a + e^{-2\pi i/3}|1\rangle_a + |2\rangle_a) \\ |u_2\rangle_a &= \frac{1}{\sqrt{3}}(e^{-2\pi i/3}|0\rangle_a + e^{2\pi i/3}|1\rangle_a + |2\rangle_a), \end{aligned} \quad (2)$$

and sends the result of her measurement m_a (which can be 0, 1, or 2) to Bob and Charlie. Each of them applies a correction operator, which depends on m_a, to their respective qubit. Specifically, for $m_a = 0$, there is no correction needed. For $m_a = 1$, Bob and Charlie each apply U_C, with $U_C|0\rangle_a = e^{-i\pi/3}|0\rangle_a$, $U_C|1\rangle_a = e^{-i\pi/3}|1\rangle_a$; for $m_a = 2$, they apply U_C^{-1} instead. The resulting state of Bob and Charlie is the same qubit state at stated in the beginning, i.e., $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$.

The procedure is both a restriction and an extension of remote state preparation. It is a restriction, because the set of transmitted states is not the entire qubit space, since α and

β are fixed. It is an extension because the states are sent to multiple receivers. In Ref. [15], we also showed how a value of θ unknown to the sender, but encoded in a quantum state, can be sent probabilistically to multiple receivers. Here, we would like to extend those results and generalize our BBP. First, we will show how Alice can apply a more general set of operations to the remote qubits. Rather than $e^{i\theta}|0\rangle\langle 0| + e^{-i\theta}|1\rangle\langle 1|$ she can apply $e^{i\theta}|s_0\rangle\langle s_0| + e^{-i\theta}|s_1\rangle\langle s_1|$, where $\langle s_0|s_1\rangle = 0$. Next, we will show how to incorporate multiple senders into the procedure, and how senders can be added or deleted from the network. We will then look further into the situation when Alice does not know θ, which is encoded into a quantum state she receives. There are both probabilistic and approximate procedures that allow her to transfer the general unknown θ into the qubits held by Bob and Charlie. Additionally, we will provide two more applications of these protocols: the first application enables the generation of sequences that can be used for the purpose of authentication, and the second is a three-state quantum key distribution (QKD) procedure.

Furthermore, as an extension of our BBP, we also consider distributing a single multiqubit state shared among several receivers, including the previous product broadcast qubit states extended by additional multiqubit entangling phase gates and general stabilizer states (such as graph states [16]). We explain how some of these multipartite entangled states can be distributed in two different ways. It turns out that in both methods, the sender can teleport phases chosen after the distribution to receivers. The latter method especially enables a remote, distributed measurement-based quantum computation (MBQC) [17,18], with the sender performing axis adaptation and receivers performing only X-basis measurement. Furthermore, we describe how the Greenberger-Horne-Zeilinger (GHZ) state [19] can be distributed.

The structure of the remaining paper is as follows. In Sec. II, we extend the protocol and show that Alice can apply more general operations to the remote qubits. We then explain the generalization to the protocol with multiple senders. In Sec. III, we discuss the application of protocol where Alice sends unknown phases to receivers. We then discuss applications to the authentication and the three-state QKD. In Sec. IV, we explain our method to broadcast a distributed stabilizer state. In Sec. V, we discuss applications of distributed stabilizer states. Section VI is devoted to conclusions.

II. EXTENSIONS OF BROADCASTING SCHEME FOR SINGLE-QUBIT STATES

In this section, we present a couple of generalizations of our BBP. First, we extend it to the case where the basis in the broadcast state can be arbitrary. Then, we generalize the BBP to multiple senders and multiple receivers.

A. Extension of BBP with general single-qubit unitaries

Consider the following scenario. Alice possesses two qubits, both of which are in the state $|\psi\rangle$, which she may or may not know. She wants to transmit qubits to Bob and Charlie in the rotated basis, $(e^{i\theta}|s_0\rangle\langle s_0| + e^{-i\theta}|s_1\rangle\langle s_1|)|\psi\rangle$,

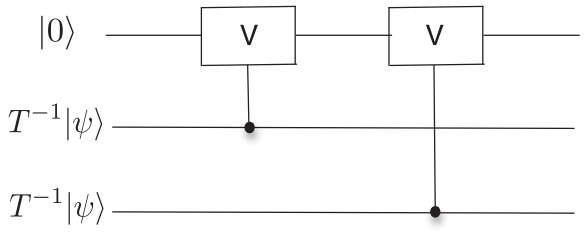

FIG. 1. Circuit for producing the state in Eq. (3). The top line is a qutrit, initially in the state $|0\rangle$, and the bottom two lines are qubits. The operation T is applied to the qubits at the output.

where she can vary the phase angle θ at a later time. Here, $\{|s_0\rangle, |s_1\rangle\}$ is an orthonormal qubit basis. Let T be the unitary operator that maps the $\{|0\rangle, |1\rangle\}$ basis to the $\{|s_0\rangle, |s_1\rangle\}$ basis, that is, $T|j\rangle = |s_j\rangle$ for $j = 0, 1$, and suppose that $|\psi\rangle = \mu|s_0\rangle + \nu|s_1\rangle$. Alice first applies T^{-1} to each of her qubits and subjects them to the circuit in Fig. 1. The top line is a qutrit, and the bottom two lines are the two qubits. The gates labeled V are controlled-shift gates, where V is the shift, in which the control is a qubit and the target a qutrit. If the control is in the state $|0\rangle$, nothing happens to the target, and if the control is in the state $|1\rangle$, then V is applied to the qutrit, where $V|j\rangle = |(j-1)\mathrm{mod}\,3\rangle$ for $j = 0, 1, 2$, and the subtraction is modulo 3. She then applies $T \otimes T$ to the qubits at the output of the circuit. The resulting state is

$$\mu^2|0\rangle_a|s_0, s_0\rangle_{bc} + \nu^2|1\rangle_a|s_1, s_1\rangle_{bc} + \mu\nu|2\rangle_a(|s_0, s_1\rangle_{bc} + |s_1, s_0\rangle_{bc}). \tag{3}$$

The qubits are then sent to Bob and Charlie, and at a later time $U_a(\theta)$ can be applied to the qutrit as in the original protocol. After that, the qutrit is then measured and Bob and Charlie perform any necessary correction procedures according to Alice's measurement outcome.

B. Extension to multiple senders

In this part, we are generalizing our BBP to the case of multiple senders and multiple receivers.

1. Example: Two senders and two receivers

To begin with, we now study the example of two senders and two receivers. We have two Alices, Alice 1 and Alice 2, who are the senders, and Bob and Charlie, who are the receivers. Alice 1 and Alice 2 have qutrits, and Bob and Charlie have qubits. We start with the entangled two-qutrit and two-qubit state

$$|\Psi^{(2,2)}\rangle = \alpha^2|0\rangle_{a1} \otimes |0\rangle_{a2} \otimes |00\rangle_{bc} + \alpha\beta|1\rangle_{a1} \otimes |1\rangle_{a2} \otimes (|01\rangle_{bc} + |10\rangle_{bc}) + \beta^2|2\rangle_{a1} \otimes |2\rangle_{a2} \otimes |11\rangle_{bc}, \tag{4}$$

which can be prepared locally, e.g., by Alice 1, and then distribute the corresponding qutrit and qubits to others. Alice 1 applies the operator $U_1(\theta_1)$ to her qutrit, where

$$U_1(\theta_1)|0\rangle_{a1} = e^{i\theta_1}|0\rangle_{a1}, \quad U_1(\theta_1)|1\rangle_{a1} = |1\rangle_{a1}, \quad U_1(\theta_1)|2\rangle_{a1} = e^{-i\theta_1}|2\rangle_{a1}. \tag{5}$$

Alice 2 applies $U_2(\theta_2)$ to her qutrit, and it has the same action as U_1 except with θ_1 replaced by θ_2. We find that

$$\begin{aligned}[I_{bc}\otimes U_1(\theta_1)\otimes U_2(\theta_2)]|\Psi^{(2,2)}\rangle &= \alpha^2 e^{i(\theta_1+\theta_2)}|0\rangle_{a1}\otimes|0\rangle_{a2}\otimes|00\rangle_{bc} \\ &\quad+\alpha\beta|1\rangle_{a1}\otimes|1\rangle_{a2}\otimes(|01\rangle_{bc}+|10\rangle_{bc}) \\ &\quad+\beta^2 e^{-i(\theta_1+\theta_2)}|2\rangle_{a1}\otimes|2\rangle_{a2}\otimes|11\rangle_{bc}. \end{aligned} \tag{6}$$

Both Alice 1 and Alice 2 now measure their qutrits in the $\{|u_j\rangle \mid j=0,1,2\}$ basis, where

$$|u_j\rangle = \frac{1}{\sqrt{3}}\sum_{l=0}^{2} e^{2\pi i l j/3}|l\rangle. \tag{7}$$

If Alice 1 gets j and Alice 2 gets k, then the resulting joint state of Bob and Charlie is

$$|\Psi^{(2,2)}\rangle \xrightarrow[\text{measure}]{U_1(\theta_1),U_2(\theta_2)} |\Phi_{(j,k)}\rangle, \tag{8}$$

where

$$\begin{aligned}|\Phi_{(j,k)}\rangle &= [\alpha e^{i(\theta_1+\theta_2)/2}|0\rangle_b + \beta e^{-2\pi i(j+k)/3}e^{-i(\theta_1+\theta_2)/2}|1\rangle_b] \\ &\quad\otimes[\alpha e^{i(\theta_1+\theta_2)/2}|0\rangle_c + \beta e^{-2\pi i(j+k)/3}e^{-i(\theta_1+\theta_2)/2}|1\rangle_c]. \end{aligned} \tag{9}$$

If Alice 1 and Alice 2 tell Bob and Charlie what their measurement results were, then Bob and Charlie can each apply a unitary operator to their qubits to remove the phase factor $e^{-2\pi i(j+k)/3}$. Thus, Bob and Charlie each receive a qubit that contains contributions from both Alice 1 and Alice 2. The procedure can be adapted so that only one Alice determines the sent qubits. For example, if Alice 2 does not apply $U_2(\theta_2)$, then $\theta_2 = 0$, and the sent qubits are determined only by Alice 1. However, to send these qubits to Bob and Charlie, the cooperation of Alice 2 is required; she has to measure her qutrit and send the result to Bob and Charlie.

2. General case: M senders and N receivers

This procedure can be extended to the case of M senders and N receivers. We start with a state consisting of M qudits with $N+1$ levels and N qubits

$$|\Psi^{(M,N)}\rangle = \sum_{k=0}^{N}\alpha^k\beta^{N-k}\binom{N}{k}^{1/2}\left(\prod_{j=1}^{M}|k\rangle_{aj}\right)|k;N-k\rangle. \tag{10}$$

Here $|k\rangle_{aj}$ is the state of the qudit of Alice j, and $|k;N-k\rangle$ is an N-qubit state, which is a normalized completely symmetric state in which k of the qubits are in the state $|0\rangle$ and $N-k$ are in the state $|1\rangle$,

$$|k;N-k\rangle \equiv \binom{N}{k}^{-1/2}\text{Symmetrize}\{\underbrace{|0\cdots0}_{k}\underbrace{1\cdots1\rangle}_{N-k}\}. \tag{11}$$

These N-qubit states are also known as Dicke states. Each Alice j has one of the qudits, and each of the receivers has one of the qubits. Alice j can now choose an angle θ_j by applying the operator U_{aj} to her qudit, where

$$U_{aj}(\theta_j)|k\rangle_{aj} = e^{i(2k-N)\theta_j}|k\rangle_{aj}. \tag{12}$$

The resulting state is

$$\begin{aligned}\prod_{j=1}^{M}U_{aj}|\Psi^{(M,N)}\rangle &= \sum_{k=0}^{N}\left(\alpha\prod_{j'=1}^{M}e^{i\theta_{j'}}\right)^k\left(\beta\prod_{j''=1}^{M}e^{-\theta_{j''}}\right)^{N-k} \\ &\quad\times\binom{N}{k}^{1/2}\prod_{j_3=1}^{M}|k\rangle_{aj_3}|k;N-k\rangle. \end{aligned} \tag{13}$$

Each Alice j now measures her qudit in the basis

$$|u_n\rangle = \frac{1}{\sqrt{N+1}}\sum_{k=0}^{N}e^{2\pi ink/(N+1)}|k\rangle, \tag{14}$$

where $n=0,1,\ldots N$. If Alice j obtains the result $|u_{n_j}\rangle$ the unnormalized N qubit state is

$$\begin{aligned}|\Psi^{(M,N)}\rangle &\xrightarrow[\text{measure}]{U_j(\theta_j)^{\otimes M}} |\Phi_{\bar n}\rangle, \\ |\Phi_{\bar n}\rangle &= \prod_{l=1}^{N}\left(\alpha e^{i\sum_{j=1}^{M}\theta_j}e^{-2\pi i(\sum_{j=1}^{M}n_j)/(N+1)}|0\rangle_l\right. \\ &\quad\left.+\beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle_l\right), \end{aligned} \tag{15}$$

where $\bar n = (n_1, n_2, \ldots, n_M)$. Each Alice then broadcasts the result of her measurement, and each of the parties applies the correction operator $U_{\bar n}$ to their qubit, where $U_{\bar n}|0\rangle = \exp[2\pi i(\sum_{j=1}^{M}n_j)/(N+1)]|0\rangle$ and $U_{\bar n}|1\rangle = |1\rangle$. This will result in each party possessing the state $\alpha e^{i\sum_{j=1}^{M}\theta_j}|0\rangle + \beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle$.

If only one sender is to send a message, that sender performs the corresponding unitary operation, and the others do nothing. However, all senders do have to measure their qudits and broadcast their results in order to complete the procedure.

3. Adding senders to the network: M → M + 1

It is possible to add senders if one of the original senders shares a fully entangled state with them. The purpose of this subsection is to present a procedure to generate $|\Psi^{(M+1,N)}\rangle$ from $|\Psi^{(M,N)}\rangle$ ($M \geqslant 1$). Suppose we start with the state

$$|\Psi^{(M,N)}\rangle\otimes\frac{1}{\sqrt{N+1}}\sum_{\ell=0}^{N}|\ell\rangle_{aM'}|\ell\rangle_{a(M+1)}. \tag{16}$$

Qudits aM and aM' are both held by Alice M, and $a(M+1)$ is held by the person we want to add as the additional sender, Alice $M+1$. Alice M sends them through a controlled-shift gate (written as $CX_{c,t}$), with aM as the control and aM' as the target. The controlled-shift gate acts as $|k\rangle_{aM}|\ell\rangle_{aM'}\to|k\rangle_{aM}|\ell+k\rangle_{aM'}$, where the addition is modulo $N+1$. Alice M now measures aM' in the computational basis. If she gets $|j\rangle_{aM'}$,

$$CX_{aM,aM'}\left(|\Psi^{(M,N)}\rangle\otimes\frac{1}{\sqrt{N+1}}\sum_{\ell=0}^{N}|\ell\rangle_{aM'}|\ell\rangle_{a(M+1)}\right)\xrightarrow{\text{measure}}\sum_{k=0}^{N}\alpha^k\beta^{N-k}\binom{N}{k}^{1/2}\prod_{j=1}^{M}|k\rangle_{aj}\otimes|j-k\rangle_{a(M+1)}\otimes|k;N-k\rangle. \tag{17}$$

Alice M sends the result of her measurement to Alice $M+1$, who can now apply a local unitary operator to map $|j-k\rangle_{a(M+1)} \to |k\rangle_{a(M+1)}$, then the resulting state is $|\Psi^{(M+1,N)}\rangle$.

A sender can delete herself by simply measuring her qutrit, and sending the result of the measurement to Bob_1, Bob_2, ...Bob_N, who can then each apply a unitary operator to remove the phase factor resulting from the measurement by the deleting party.

III. FURTHER GENERALIZATION AND APPLICATIONS OF BROADCASTING SINGLE-QUBIT STATES

Here, we give several applications of broadcasting single-qubit states. The first is an extension to send an unknown phase encoded in a quantum state. The second is an application of our broadcasting protocol to authentication. The last is an application to quantum key distribution using three states.

A. Sending unknown phases

Let us return to the case of one sender, Alice, who wants to send Bob and Charlie a state with an unknown phase. This was studied in Ref. [15]. There Alice had one qutrit, which is entangled with the qubits of Bob and Charlie. The phase θ was encoded in the qutrit state

$$|\Phi\rangle_d = \frac{1}{\sqrt{3}}(e^{2i\theta}|0\rangle_d + |1\rangle_d + e^{-2i\theta}|2\rangle_d). \tag{18}$$

A combination of a unitary operation and measurement allowed Alice to send the state $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$, where, as usual, α and β are fixed, to Bob and Charlie with a probability of $1/3$.

Here we would like to improve on that result using a different encoding of the angle to boost the probability of success. First, we will show that if θ is in the set $\{\pi k/K \mid k = 0, 1, \ldots, K-1\}$ and encoded in a K-level system, where K is fixed, we can send the state $e^{i\theta}\alpha|0\rangle + e^{-i\theta}\beta|1\rangle$ to Bob and Charlie with certainty at the expense of using an encoding state of higher dimension. In this case, the encoding states are orthogonal, so Alice could simply measure them in an appropriate basis (i.e., the Fourier basis) to determine the angle they encode, and then apply an appropriate unitary operator to her qutrit. Below, however, we will use a different strategy, which we can then extend to the case of a general angle. This in general succeeds with probability $(K-2)/K$, improving our previous protocol for $K > 3$, and it becomes deterministic for the above special values of θ.

1. Sending unknown restricted angle

Here we discuss the case with two receivers and demonstrate that Alice can send an angle unknown to her, but encoded in a state (with a label d). The case with N receivers will be given in Appendix A.

We start with the state

$$(\alpha^2|0\rangle_a|v_0\rangle_{bc} + \alpha\beta|1\rangle_a|v_1\rangle_{bc} + \beta^2|2\rangle_a|v_2\rangle_{bc}) \times \frac{1}{\sqrt{K}}\left(\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j\rangle_d\right). \tag{19}$$

Alice has a qutrit a, Bob and Charlie have qubits b and c, respectively, and the angle $2\pi k/K$ is encoded by a K-dimensional qudit d, which has been sent to Alice. Here $|v_0\rangle_{bc} = |00\rangle_{bc}$, $|v_1\rangle_{bc} = |01\rangle_{bc} + |10\rangle_{bc}$, and $|v_2\rangle_{bc} = |11\rangle$. Alice does not know what the angle is. She applies a controlled-shift operation to the ad system, with a as the control, which acts as $|j\rangle_a|k\rangle_d \to |j\rangle_a|k+j\rangle_d$, where the addition is modulo K. This results in the following state:

$$\frac{1}{\sqrt{K}}\left[\alpha^2|0\rangle_a|v_0\rangle_{bc}\left(\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j\rangle_d\right) + \alpha\beta|1\rangle_a|v_1\rangle_{bc}\left(\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j+1\rangle_d\right) + \beta^2|2\rangle_a|v_2\rangle_{bc}\left(\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j+2\rangle_d\right)\right]. \tag{20}$$

Using the identity

$$\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j+l\rangle_d = e^{-2\pi ikl/K}\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j\rangle_d, \tag{21}$$

the above state becomes

$$e^{-2\pi ik/K}[(\alpha e^{i\pi k/K})^2|0\rangle_a|v_0\rangle_{bc} + \alpha\beta|1\rangle_a|v_1\rangle_{bc} + (\beta e^{-i\pi k/K})^2|2\rangle_a|v_2\rangle_{bc}]\frac{1}{\sqrt{K}}\left(\sum_{j=0}^{K-1} e^{2\pi ikj/K}|j\rangle_d\right). \tag{22}$$

If Alice now performs the steps to send qubit states to Bob and Charlie, they will both receive $\alpha e^{i\pi k/K}|0\rangle + \beta e^{-i\pi k/K}|1\rangle$. Note that the state that encoded the angle is not affected by this procedure, and it can be sent to another Alice, who can use it to transmit the encoded angle to an additional Bob and Charlie.

2. Sending unknown general angle

Let us now consider a general angle θ. We begin with the state

$$(\alpha^2|0\rangle_a|v_0\rangle_{bc} + \alpha\beta|1\rangle_a|v_1\rangle_{bc} + \beta^2|2\rangle_a|v_2\rangle_{bc}) \times \frac{1}{\sqrt{K}}\left(\sum_{k=0}^{K-1} e^{ik\theta}|k\rangle_d\right). \tag{23}$$

Now Alice applies the controlled-shift operation as before. Suppose that she measures her qutrit in the $\{|u_j\rangle \mid j = 0, 1, 2\}$ basis [see Eq. (2)] and obtains $|u_0\rangle$ (if she obtains either of the other two basis elements, Bob and Charlie apply their correction operations to remove unwanted phase factors). The resulting bcd state is

$$|w_0\rangle_{bc}|0\rangle_d + |w_1\rangle_{bc}|1\rangle_d + |w_2\rangle_{bc} \times \frac{1}{\sqrt{K}}\left(\sum_{k=2}^{K-1} e^{ik\theta}|k\rangle_d\right). \tag{24}$$

Here, we have

$$|w_0\rangle_{bc} = \alpha^2|v_0\rangle_{bc} + \alpha\beta e^{i(K-1)\theta}|v_1\rangle_{bc} + \beta^2 e^{i(K-2)\theta}|v_2\rangle_{bc}, \tag{25}$$

$$|w_1\rangle_{bc} = \alpha^2 e^{i\theta}|v_0\rangle_{bc} + \alpha\beta|v_1\rangle_{bc} + \beta^2 e^{i(K-1)\theta}|v_2\rangle_{bc}, \tag{26}$$

$$\begin{aligned}|w_2\rangle_{bc} &= \alpha^2|v_0\rangle_{bc} + \alpha\beta e^{-i\theta}|v_1\rangle_{bc} + \beta^2 e^{-2i\theta}|v_2\rangle_{bc} \\ &= (\alpha|0\rangle_b + \beta e^{-i\theta}|1\rangle_b) \otimes (\alpha|0\rangle_c + \beta e^{-i\theta}|1\rangle_c).\end{aligned} \tag{27}$$

At this point, if Alice wants to adopt a probabilistic protocol, the most obvious thing for her to do is to measure the d system in the basis $\{|k\rangle_d \,|\, k = 0, 1, \ldots, K-1\}$. If she obtains $k = 0$ or 1, $|w_0\rangle$ and $|w_1\rangle$ are entangled between Bob and Charlie and cannot be corrected locally to the desired broadcast states. If, instead, she obtains anything except $k = 0, 1$, the protocol has succeeded, i.e., Bob and Charlie obtain the state $|w_2\rangle_{bc}$, and this happens with a probability of $(K-2)/K$, independent of θ. This procedure, however, destroys any information about the phase remaining in the d state. We discuss improvements that allow us to reuse the encoding state to some extent in Appendix A.

B. Authentication

Sequences of symbols that disagree in every place could find application in authentication protocols [20]. Alice can authenticate herself to Bob by providing elements of her sequence to him, and he can check that what Alice sent disagrees with his sequence in every place. The use of checking sequences for elements that were not sent, that is, the sequence of states sent and the sequence of measurement results disagree, has been used in digital signature schemes [21]. If there are more than two parties, then disagreeing sequences can be used to anonymously send messages or to authenticate votes. Suppose we have three parties, Alice, Bob, and Charlie, and they possess sequences of four symbols that disagree in all of their places. Bob wants to send a message to Alice but does not want her to know from whom it came. He attaches part of his sequence to the message and sends it to Alice. Alice can then verify that the message came from Bob or Charlie, but not which one. In a voting scenario, each voter will have a sequence, and the authority, who counts the votes, will as well. Each voter sends their vote accompanied by their sequence. The authority can check that each sequence disagrees with his in all places, which authenticates the votes, and he will not know which sequence came from which voter. One quantum method of generating such sequences was provided, for example, by Cabello [22], using a supersinglet quantum state.

Here we will show how three random sequences of three symbols can be generated. These sequences have the property that the sequences held by Bob and Charlie disagree in every place with the sequence held by Alice, but they do not necessarily disagree with each other. It is also the case that Bob does not know Charlie's sequence and vice versa. The basis of this procedure is provided by the trine and antitrine states of a qubit. Define the trine states for a qubit to be

$$\begin{aligned}|\psi_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}(e^{2\pi i/3}|0\rangle + e^{-2\pi i/3}|1\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(e^{-2\pi i/3}|0\rangle + e^{2\pi i/3}|1\rangle),\end{aligned} \tag{28}$$

and, similarly, the antitrine states to be

$$\begin{aligned}|\bar{\psi}_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ |\bar{\psi}_1\rangle &= \frac{1}{\sqrt{2}}(e^{2\pi i/3}|0\rangle - e^{-2\pi i/3}|1\rangle) \\ |\bar{\psi}_2\rangle &= \frac{1}{\sqrt{2}}(e^{-2\pi i/3}|0\rangle - e^{2\pi i/3}|1\rangle).\end{aligned} \tag{29}$$

This is a rotated version of the usual trine and antitrine states, but these are the ones that are most useful in the kind of procedure we have been discussing. Note that

$$\langle\psi_j|\psi_k\rangle = \langle\bar{\psi}_j|\bar{\psi}_k\rangle = -\tfrac{1}{2} \quad (j \neq k), \tag{30}$$

$$\langle\bar{\psi}_j|\psi_j\rangle = 0. \tag{31}$$

We now consider the positive-operator valued measure (POVM) based on the antitrine states with measurement operators given by

$$A_j = \sqrt{\frac{2}{3}}|\bar{\psi}_j\rangle\langle\bar{\psi}_j|, \quad \sum_{j=0}^{2} A_j^\dagger A_j = I, \tag{32}$$

and the probability of obtaining result j in the state ρ is $\mathrm{Tr}(\rho A_j^\dagger A_j)$. Bob and Charlie will measure their qubits using this POVM and use the results to generate their sequences.

To generate the sequences, Alice sends a qubit in one of the trine states to Bob and Charlie using the original broadcast procedure. Bob and Charlie measure their qubits using the antitrine POVM and use their measurement results as the elements of their sequences. Both Bob and Charlie will obtain results different from what Alice sent. For example, if Alice sent $|\psi_0\rangle$, then Bob can obtain 1 or 2, and Charlie can obtain 1 or 2. Bob does not know Charlie's result and Charlie does not know Bob's, and their results can be the same or different. (The probability of being the same decays exponentially with the size of the sequence.) However, their results will differ from what Alice sent. Thus, Bob and Charlie can separately establish a sequence that can be used for authentication with Alice. We provide one example in Table I. If there are two Alices, as in Sec. II B 1, the qubits received by Bob and

TABLE I. An example of how to generate keys for authentication from the broadcast states.

Slot	1	2	3	4	5	6
State Alice broadcasts	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_1\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$
Bob's outcome	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_1\rangle$	$\|\bar{\psi}_0\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_0\rangle$
Charlie's outcome	$\|\bar{\psi}_0\rangle$	$\|\bar{\psi}_1\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_0\rangle$	$\|\bar{\psi}_0\rangle$

TABLE II. An example of the PBC three-state QKD protocol. In the original design [23], Bob performs a randomly chosen two-outcome projective measurement and this can be replaced by a POVM defined by the antitrine states.

Time	1	2	3	4	5	6	7	8	9	10
State Alice broadcasts: $\|\psi_j\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_1\rangle$	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_0\rangle$	$\|\psi_0\rangle$	$\|\psi_2\rangle$	$\|\psi_1\rangle$
Bob's measurement $\{\|\psi_\ell\rangle, \|\bar{\psi}_\ell\rangle\}$	1	1	0	2	1	1	1	2	0	1
Outcome	$\|\psi_1\rangle$	$\|\bar{\psi}_1\rangle$	$\|\psi_0\rangle$	$\|\bar{\psi}_2\rangle$	$\|\psi_1\rangle$	$\|\bar{\psi}_1\rangle$	$\|\psi_1\rangle$	$\|\bar{\psi}_2\rangle$	$\|\bar{\psi}_0\rangle$	$\|\psi_1\rangle$
Alice announces not (k)		0		1		1		2	1	
Bob successfully infers $\|\psi_j\rangle$		✓		✓		No		No	✓	
$j \to k$		$2 \to 0$		$0 \to 1$					$2 \to 1$	
Shared bit		0		0					1	

Charlie will depend on the angles chosen by both of them. In particular, the angle will be the sum of the angles chosen by Alice 1 and Alice 2. In order to authenticate Bob or Charlie, the Alices would have to cooperate.

We note that in the case with two receivers and a single sender, Alice simply needs to set $\alpha = \beta = 1/\sqrt{2}$ and $\theta = 0$ in the BBP, then one of the trine states is generated by random phases that come from her measurement. One can also consider the direct broadcast of the trine states to N receivers, where Alice would make use of α, β, and $U(\theta)$, and communicate her measurement result to let receivers correct the unwanted phases.

C. Three-state QKD

Phoenix, Barnett, and Chefles (PBC) [23] proposed a three-state QKD protocol by using the three states in Eq. (28). The sender, Alice, will randomly choose one of the three states to send to the receiver, Bob, who then randomly chooses one of the three measurement bases

$$\{|\psi_j\rangle, |\bar{\psi}_j\rangle\} \quad (j = 0, 1, 2) \tag{33}$$

to measure the received qubit. We first describe their protocol (Alice and a single Bob), and it will then be obvious that our broadcasting protocol allows Alice to establish separate secret keys with two Bobs.

First, if Bob's measurement outcome corresponds to $|\psi_j\rangle$, then he announces the failure of this round. Otherwise, Alice announces one of the states in Eq. (28) that she did not send. Suppose Bob measures in the basis labeled by $j = 1$ and Alice announces that she did not send $j = 1$, then there is nothing Bob can infer, as his measurement outcome $|\bar{\psi}_1\rangle$ basically confirms this. The useful case is that the state Alice announces has a different label than Bob's measurement basis label. For example, if she announces that she did not send $j = 0$, then Bob can infer that she must have sent $|\psi_{j=2}\rangle$ and we can label this event as (sent label, state not sent) = (2,0). Then we use the rule that from the first index to the second index, if there is a $+1$ hop (mod 3), then it is assigned a 0. On the other hand, if Alice announces that she did not send $j = 2$, then Bob can infer the state Alice sent has the label $j = 0$, and the event is labeled as (0,2), which requires $+2$ to get from 0 to 2 modulo 3, and hence this corresponds to a 1. We illustrate the convention of assigning 0 or 1 in Fig. 2. In Table II, we provide an example of the PBC protocol. Doing the above for a long sequence k of repetitions, one can establish a secret key of an expected length $k/3$. Note that Bob can use a POVM defined by $\{\frac{2}{3}|\bar{\psi}_j\rangle\langle\bar{\psi}_j|, j = 0, 1, 2\}$, then one gains a factor of $3/2$ and the expected key length is $k/2$. In our protocol, *Alice can broadcast to two Bobs randomly but in the same state.* Namely, we use the broadcast state $|\Psi^{(1,2)}\rangle$ with $\alpha = \beta = \frac{1}{\sqrt{2}}$ and $\theta = 0$, then two Bobs have one of the trine states. However, the two Bobs may have different choices of projective measurement bases, or in the case of POVM they may have different POVM outcomes. From the PBC protocol, it is obvious that Alice and each Bob share a different secret key. (The two Bobs may also share a smaller subset of the key.)

Obviously, we can have more than two receivers, in which case we use $|\Psi^{(1,N)}\rangle$ to distribute the same state to N receivers. Instead of random phases arising from Alice's measurement, Alice can make use of either $U(\theta)$ or the preset parameters α, β to choose which trine state to be sent, and let receivers correct the unwanted phases from the measurement $e^{2\pi nj/(N+1)}$ $(n = 0, .., N)$.

IV. BROADCASTING A DISTRIBUTED STABILIZER STATE

In this section, we discuss different ways of broadcasting a distributed stabilizer state $|\psi\rangle$, where $S|\psi\rangle = |\psi\rangle$ for any S being a product of Pauli operators of a group G that does not contain $-I$. The sender(s) has the choice of distributing the state or aborting the mission. We will mostly focus on graph states as an illustration, to which cluster states are special

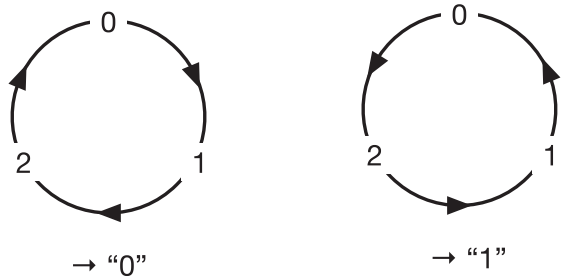

FIG. 2. Encoding of secret keys in PBC QKD. The numbers within each circle represent the label j of a trine state $|\psi_j\rangle$ [Eq. (28)]. One reads the pair of labels j: the label of the sent state (which either Alice knows herself or Bob infers from his measurement), k: the label of the state not sent (as announced by Alice), and see if the arrow "$j \to k$" flows counterclockwise or clockwise, which encodes "0" and "1," respectively.

cases. Moreover, all stabilizer states are locally equivalent to graph states [24]. A graph state is defined in terms of a graph that consists of a set of vertices V and a set of edges E such that the stabilizer is of the form $K_v = X_v \bigotimes_{\langle u,v\rangle\in E} Z_u$ with $v \in V$. (Note that we have used the symbol K for a graph-state stabilizer instead of S, as this is the convention in the literature.) Since $K_v = (\prod_{\langle u,v\rangle\in E} CZ_{v,u})^\dagger X_v (\prod_{\langle u,v\rangle\in E} CZ_{v,u})$, the graph state $|\psi_G\rangle$ is given by

$$|\psi_G\rangle = U_{CZ}|+\rangle^{\otimes|V|}, \quad U_{CZ} = \prod_{\langle u,v\rangle\in E} CZ_{u,v}. \tag{34}$$

One of the approaches we discuss can be used for states that are not stabilizer states.

A. Distribution of graph states (*I*)

The approach in this section works for graph states and other nonstabilizer states, such as hypergraph states and other states for which the key entangling part consists of only phases.

Let us first consider the simplest example of distributing a graph state, extending the setup in the Introduction. Namely, we have Alice (sender) and two Bobs (receivers), and in the end, the two receivers will share two qubits which comprise two-qubit graph state ($V = \{v_1, v_2\}$). We consider a state to be shared by the three players, which is proportional to

$$|0\rangle_a|0,0\rangle_{b_1,b_2} + |1\rangle_a(|0,1\rangle + |1,0\rangle)_{b_1,b_2} + |2\rangle_a|1,1\rangle_{b_1,b_2}. \tag{35}$$

This state is a special broadcast state with $\alpha = \beta = \frac{1}{\sqrt{2}}$ and can be created by Alice locally. For the graph state distribution, Alice applies a phase gate so that the state is now proportional to

$$|0\rangle_a|0,0\rangle_{b_1,b_2} + |1\rangle_a(|0,1\rangle + |1,0\rangle)_{b_1,b_2} - |2\rangle_a|1,1\rangle_{b_1,b_2}. \tag{36}$$

She distributes the corresponding qubits to the two Bobs, respectively. Then Alice measures her qutrits in the basis $\{|\tilde{j}\rangle\}$,

$$|\tilde{j}\rangle = \frac{1}{\sqrt{3}} \sum_{k=0,1,2} e^{2\pi ijk/3}|k\rangle \quad (j = 0, 1, 2). \tag{37}$$

The resulting state for two receivers is

$$\begin{aligned}&(|0,0\rangle + e^{-2\pi ij/3}(|0,1\rangle + |1,0\rangle) - e^{-4\pi ij/3}|1,1\rangle)_{b_1,b_2}\\ &\quad = CZ_{b_1,b_2}(|0\rangle + e^{-2\pi ij/3}|1\rangle)_{b_1}(|0\rangle + e^{-2\pi ij/3}|1\rangle)_{b_2}.\end{aligned} \tag{38}$$

We note that the extra phase $e^{-2\pi ij/3}$ commutes with the CZ operator, so it is locally correctable by each receiver if Alice informs them of the measured value of j, as in the previous broadcasting case.

If Alice decides to abort the protocol instead, she should change her measurement basis to $\{|0\rangle, |1\rangle, |2\rangle\}$. This may leave behind an entangled state shared among Bobs.

Generalization to graphs with N vertices is straightforward. In order to distribute a graph state with a general graph connectivity, the CZ gate should be applied locally by Alice before the distribution of physical qubits. In this scenario, we prepare

$$\left|\Psi_{CZ}^{(1,N)}\right\rangle = \sum_{k=0}^{N} \binom{N}{k}^{1/2} |k\rangle_a U_{CZ}|k; N-k\rangle, \tag{39}$$

where U_{CZ} is the product of CZ gates that generates the graph state with the desired connectivity. After the measurement by Alice (assuming the result is j), receiver Bobs obtain the state

$$\begin{aligned}\left|\Psi_{CZ}^{(1,N)}\right\rangle &\xrightarrow{\text{measure}} \sum_{k=0}^{N} \binom{N}{k}^{1/2} e^{-2\pi ijk/N} U_{CZ}|k; N-k\rangle\\ &= U_{CZ}(|0\rangle + e^{-2\pi ij/N}|1\rangle)^{\otimes N}.\end{aligned} \tag{40}$$

The resulting state is the graph state (34), up to a correctable phase $e^{-2\pi ij/N}$.

In general, any state that can be generated by applying a multiqubit phase gate (such as a product of CZ gates or CCZ gates) on product states can be distributed using this strategy. This class of quantum state includes graph states [16], hypergraph states [25], and other short-range entangled states, including symmetry-protected topological (SPT)-ordered states [26,27], where the phases in the last case come from the cocycles associated with the symmetric phase.

We can generalize the result in Eq. (15) so we have multiple senders who add phases after distribution. We write the multiqubit phase gate as U_{phase}, then using

$$\left|\Psi_{\text{phase}}^{(M,N)}\right\rangle = \sum_{k=0}^{N} \alpha^k \beta^{N-k} \binom{N}{k}^{1/2} \prod_{j=1}^{M} |k\rangle_{aj} U_{\text{phase}}|k; N-k\rangle \tag{41}$$

and letting Alices apply the additional phase gate, the following entangled state is distributed among receivers:

$$\left|\Psi_{\text{phase}}^{(M,N)}\right\rangle \xrightarrow[\text{measure}]{U_j(\theta_j)^{\otimes M}} U_{\text{phase}} \prod_{l=1}^{N} \left(\alpha e^{i\sum_{j=1}^{M}\theta_j} e^{-2\pi i(\sum_{j=1}^{M} n_j)/(N+1)}|0\rangle_l + \beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle_l\right) \tag{42}$$

$$\xrightarrow{\text{correct}} U_{\text{phase}} \prod_{l=1}^{N} \left(\alpha e^{i\sum_{j=1}^{M}\theta_j}|0\rangle_l + \beta e^{-i\sum_{j=1}^{M}\theta_j}|1\rangle_l\right). \tag{43}$$

B. Broadcasting a stabilizer state

Here we describe another protocol to "broadcast" a single stabilizer state distributed among multiple receivers. For simplicity, we consider an N-qubit stabilizer state, for which there are N independent stabilizer generators $\{S_k\}$. (One can consider fewer stabilizer generators to encode a distributed logical state.) In this case, Alice will need $2N$ qubits, where the first N qubits, all initialized in $|+\rangle$, serve as a control set

that involves the action of control S_k's to the corresponding qubits in the second group, whose qubits are conveniently initialized all in $|+\rangle$ as well. Given that each S_k is a product of single Pauli operators, the control-S_k gate is decomposed into a product of two-qubit control-Pauli gates. Then Alice sends the qubits in the second group to the desired receivers, Bobs.

The resultant state before any measurement by Alice can be rewritten as

$$|\psi\rangle = \prod_{k=1}^{N} \frac{1}{\sqrt{2}} (|0\rangle_k \otimes I + |1\rangle_k \otimes S_{k'}) \prod_{k'=1}^{N} |+\rangle_{k'}. \tag{44}$$

If Alice intends to distribute the stabilizer state, then she performs measurement on her remaining N qubits in the X basis. The outcomes represent the action $(I \pm S_k)/2$ that is performed or equivalently the value of the stabilizer operators $S_k = \pm 1$. She can find out the correcting Pauli product and inform the appropriate parties to make their correction operation.

On the other hand, if she intends to abort the mission, she simply measures all her qubits in the Z basis. The measurement outcomes represent whether the corresponding S_k operator was applied or not, and regardless of the outcomes, all Bobs then share a product state.

1. Distribution of graph states (II)

In the remainder of this section, we focus on graph states, as a special case of the general stabilizer states. We consider qubits initialized as the $2|V|$ product of $|+\rangle$, i.e., $\prod_{v\in V} |+\rangle_v \prod_{v'\in V} |+\rangle_{v'}$, where the qubit v will be associated with the stabilizer operator $K_{v'} = X_{v'} \prod_{\langle u',v'\rangle\in E} Z_{u'}$ and the symbol $'$ denotes qubits that will be distributed to Bobs. After applying all the control-$K_{v'}$ gates (which can be decomposed into a product of CX and CZ gates),

$$|\psi\rangle = \prod_{v\in V} \frac{1}{\sqrt{2}} \left(|0\rangle_v \otimes I + |1\rangle_v \otimes X_{v'} \prod_{\langle u',v'\rangle\in E} Z_{u'} \right) \prod_{w'\in V} |+\rangle_{w'}. \tag{45}$$

Denoting the outcome of the Pauli-X measurement for the v qubit of Alice being $s(v) \in \{0, 1\}$, the resulting state after the measurement is given by

$$\prod_{v\in V} \frac{1}{2} \left[1 + (-1)^{s(v)} X_{v'} \prod_{\langle u',v'\rangle\in E} Z_{u'} \right] \prod_{w'\in V} |+\rangle_{w'}, \tag{46}$$

and this state is a graph state shared by Bobs up to by-product operators,

$$\left(\prod_{v\in V} Z_v^{s(v)} \right) |\psi_G\rangle_B, \tag{47}$$

where $|\psi_G\rangle_B$ denotes the graph state with $s(v) = 0$. Note that the operator acting on the product state in Eq. (46) is a projector. If the measurement outcome is ideal [i.e., $s(v) = 0$ for all $v \in V$], Bobs obtain the state projected to the desired subspace with $K_v = 1$ for all $v \in V$, which is the graph state $|\psi_G\rangle$. If there appear outcomes $s(v) = 1$, then one can apply the Pauli-Z operator at corresponding v' to correct the eigenvalue of the stabilizer. In Fig. 3, we give an example of a graph state whose graph consists of three vertices.

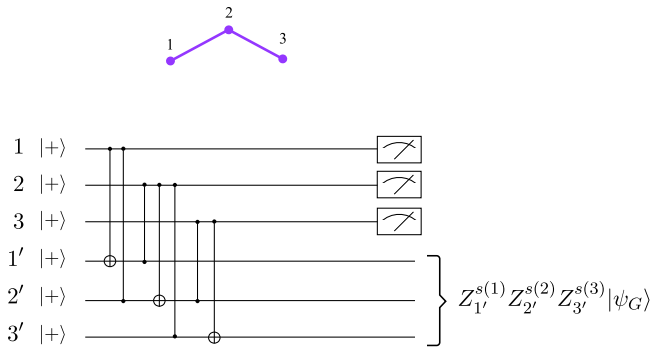

FIG. 3. An example of graph state distribution. The graph in this example consists of three vertices, $v \in \{1, 2, 3\}$, and the graph state is distributed. The graph state $|\psi_G\rangle$ is stabilized by X_1Z_2, $Z_1X_2Z_3$, and Z_2X_3.

2. Rotated graph states

The previous discussion on sending phases motivates us to devise a method to teleport phase gates in the setup with the graph states. If one wishes to encode a phase θ acting on a vertex v held by a Bob, we can, for example, add an additional gate teleportation to the graph state prepared with the procedure above. Let us say Alice wants to send a phase gate $e^{i\theta Z}$ to the vertex $u \in V$. Then Alice prepares another supplemental qubit in $|+\rangle_{u_A}$ and couples it with u_B via CZ_{u_A,u_B}. After distributing all Bobs' qubits, Alice measures her supplemental qubit with the basis

$$\mathcal{M}_\theta = \{e^{-i\theta X}|s\rangle | s = 0, 1\}. \tag{48}$$

Then by virtue of the gate teleportation, the unitary gate $(Z)^s e^{i\theta Z}$ is induced at u_B, which acts on the graph state. One can easily generalize this procedure with a different phase gate for each vertex. In the end, the following state is distributed:

$$\left(\prod_{v\in V} e^{i\theta_v Z_v} \right) |\psi_G\rangle, \tag{49}$$

up to Z by-product operators that depend on Alice's measurement outcomes. We elaborate on more details of our scheme in Appendix D.

V. APPLICATIONS OF DISTRIBUTED STABILIZER STATES

A. Distribution of GHZ state

A distributed GHZ state has applications such as quantum secret sharing [28]. The GHZ state can be obtained from a star-graph state and applying a Hadamard gate to every qubit but the one at the center of the star [16]. For example, one can assign Alice to the central qubit, and other qubits are possessed by Bobs. After that, all Bobs apply Hadamard, then Bobs and Alice share a GHZ state. In Appendix C, we present an alternative way to distribute a GHZ state.

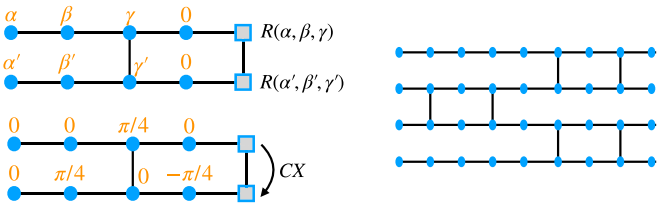

FIG. 4. (Left top) Measurement pattern to realize the single-qubit $SU(2)$ rotation gate. $R(\alpha, \beta, \gamma)$ represents the Euler rotation. (Left bottom) Measurement pattern to realize the controlled-NOT gate. The information flows from left to right as we sequentially measure qubits in order. The number above each ball represents the angle θ in the measurement basis $\{e^{i\theta Z}|+\rangle, e^{i\theta Z}|-\rangle\}$. (Right) The brickwork state. One tiles up the blocks depicted on the left to concatenate the unitaries sequentially. See Refs. [33,34] for details.

B. Distributed MBQC with X alone by receivers

Quantum network may allow for distributed quantum computation on physically separate devices [29–32], which is potentially useful when computational resources in each local quantum device are limited. Below, we describe how the phase rotation gate teleported from Alice can be used by Bob to perform MBQC [17,18]. With her ability to send phase rotation gates, Alice and Bob can work together to perform the universal MBQC, for which Alice controls the adaptation of the measurement axis (by the rotation) and Bob always performs measurement in the same basis, X. This allows a universal gate set to be implemented. We also point out in Appendix B that Alice can remove a vertex from the graph possessed by Bob by appropriately choosing her measurement basis.

The universal MBQC can be achieved on an appropriate graph state—the brickwork state—and measurements with the rotated basis, $B = \{e^{i\theta Z}|+\rangle, e^{i\theta Z}|-\rangle\}$ [18,33,34]. Namely, appropriately choosing the angle θ in the basis B, one can achieve single-qubit $SU(2)$ rotation gates and the controlled-NOT gate (see Fig. 4). As we discussed in Sec. IV, Alice can send a phase gate $e^{i\theta_v Z_v}$ to Bob's qubits, thus the universal MBQC can be performed on the Bob's graph state with the X basis measurement alone by Bob. Bob needs to inform his measurement outcomes to Alice so she knows the by-product operators from the former measurements acting on his graph state, and she can decide if she needs to teleport $e^{i\theta_v Z_v}$ or $e^{-i\theta_v Z_v}$ to perform the desired rotation (see Fig. 5). We delegate the technical details to Appendix D.

VI. CONCLUSION

We extended our results for the broadcasting of quantum states to multiple receivers to now include the possibility of multiple senders. It is possible to add and delete senders from the network, and procedures for doing so were discussed. We also provided further results on sending states with an unknown phase. In this case, the phase is provided to the sender encoded in a quantum state. We showed how the encoding state can be reused, and, for a general phase, how each use degrades the information contained in it. We went on to give two applications of our broadcasting protocol, including authentication and three-state quantum cryptography.

We have considered the distribution of graph states in two different ways. The first method generalizes the state that is originally used for broadcasting product states, by supplementing multiqubit phase gates that entangle the product states. This applies beyond graph states, including hypergraph states and nontrivial, fixed-point symmetry-protected topologically ordered states. Another way to broadcast a graph state is to implement projection controlled by the sender. The sender Alice can decide the structure of the graph by choosing her measurement basis appropriately, and she can also send additional phase gates that act on the graph state. We have also discussed applications of the distribution of the graph state; the distribution of the GHZ state and the remote, distributed universal quantum computation done by the distributed receivers with the X basis measurement alone and by the sender who controls the (adaptive) rotation. The latter is in the same the reverse of the blind quantum computation; here the server is outsourcing computational tasks to third parties, without them having the possibility of knowing the computation.

ACKNOWLEDGMENTS

The authors would like to thank Himanshu Gupta for useful comments. The research of M.H., J.A.B., H.S., and T.-C.W. was supported by NSF Grant No. FET-2106447. The research of M.H. and J.A.B. was also sponsored by the DEVCOM Army Research Laboratory and was accomplished under

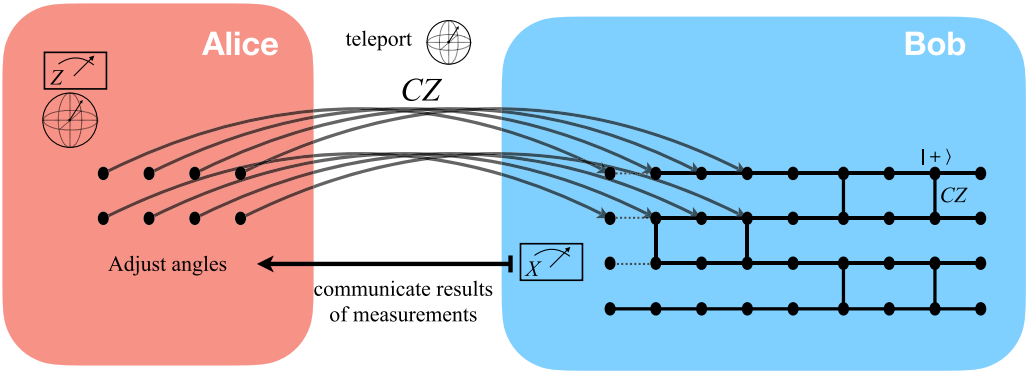

FIG. 5. After finishing the phase of distributing the brickwork state to the receiver(s), Alice and Bob can collaborate to perform a universal MBQC.

Cooperative Agreement No. W911NF-20-2-0097. Additionally, T.-C.W. and H.S. would like to acknowledge the support of a Provost's Venture Fund from the Provost's Office at Stony Brook University. We would like to thank Marcello Caleffi for informing us of useful references.

APPENDIX A: MORE ON SENDING UNKNOWN PHASES

1. Sending unknown restricted angle to N receivers

Let us start with the state

$$|\Psi^{(1,N)}\rangle \otimes \frac{1}{\sqrt{K}}\left(\sum_{j=0}^{K-1} e^{2\pi i k j/K}|j\rangle_d\right). \tag{A1}$$

As we did for the case with $N = 2$ (Bob, Charlie) in the main text, Alice applies the controlled-shift gate $CX_{a,d}$, which gives us

$$\sum_{\ell=0}^{N} \alpha^\ell \beta^{N-\ell}\binom{N}{\ell}^{1/2}|\ell\rangle_a|\ell; N-\ell\rangle \times \frac{1}{\sqrt{K}}\sum_{j=0}^{K-1} e^{2\pi i j k/K}|j+\ell\rangle_d. \tag{A2}$$

By shifting the summed index j by ℓ, we obtain

$$\sum_{\ell=0}^{N}(e^{-2\pi i k/K}\alpha)^\ell \beta^{N-\ell}\binom{N}{\ell}^{1/2}|\ell\rangle_a|\ell; N-\ell\rangle \otimes\left(\frac{1}{\sqrt{K}}\sum_{j=0}^{K-1} e^{2\pi i j k/K}|j\rangle_d\right). \tag{A3}$$

Alice measures her qudit in the Fourier basis, then each receiver obtains the following state after the correction of phases induced by Alice's measurement:

$$e^{-2\pi i k/K}\alpha|0\rangle + \beta|1\rangle. \tag{A4}$$

2. Reusing the encoding state with general angle

In the main text, we discussed methods to send unknown angle θ encoded in a state d to Bob and Charlie. In the case with a general angle, we showed that Alice can measure the encoding state d with the computational basis, and with a probability $(K-2)/K$ the procedure succeeds, but the encoding state will be destroyed. In this section, we discuss alternatives so we can reuse the encoding state.

A better procedure is the following. Define

$$Q_2 = \sum_{k=2}^{K-1}|k\rangle_d\langle k|. \tag{A5}$$

Alice measures Q_2, which has eigenvalues 0 and 1, on the d system, and if she obtains 1, which she does with probability $(K-2)/K$, the procedure has succeeded, and the resulting d state is $(1/\sqrt{K-2})\sum_{k=2}^{K-1} e^{ik\theta}|k\rangle_d$. This state does not contain as much information about the phase as the original state, but it still contains quite a bit. It could be passed on to a second Alice, who can then use it in the same protocol for a different Bob and Charlie. The subsequent success probability will be reduced to $(K-4)/(K-2)$ corresponding to eigenvalue 1 of

$$Q_4 = \sum_{k=4}^{K-1}|k\rangle_d\langle k|. \tag{A6}$$

An alternative is for Alice not to measure the d system, and this will leave Bob and Charlie with approximate versions of the desired state. In this case the d state can be reused, though it will have been altered somewhat by its first use. In order to see what Bob and Charlie have, we can form a density matrix from the state in Eq. (24) and trace out c and d to obtain Bob's state (Charlie's state is identical). The result is

$$\begin{aligned}\rho_b = {}& \frac{K-2}{K}(\alpha e^{i\theta/2}|0\rangle + \beta e^{-i\theta/2}|1\rangle)\\ &\times(\alpha^* e^{-i\theta/2}\langle 0| + \beta^* e^{i\theta/2}\langle 1|)\\ &+\frac{1}{K}[2|\alpha|^2|0\rangle\langle 0| + 2|\beta|^2|1\rangle\langle 1|\\ &+\alpha\beta^* e^{i\theta}(1+e^{-iK\theta})|0\rangle\langle 1|\\ &+\alpha^*\beta e^{-i\theta}(1+e^{iK\theta})|1\rangle\langle 0|].\end{aligned} \tag{A7}$$

Note that the size of the error is of order $1/K$.

As noted, the state encoding the phase can be reused. In order to see how much it has been changed by one use, we can calculate the fidelity of the reduced density matrix of the d system after one use, ρ_d, which can be found by tracing b and c out of Eq. (24), to the original encoding state, $|\Phi(\theta, K)\rangle = (1/\sqrt{K})\sum_{k=0}^{K-1} e^{ik\theta}|k\rangle_d$. We find that

$$\begin{aligned}F &= \langle\Phi(\theta,K)|\rho_d|\Phi(\theta,K)\rangle\\ &= 1 - 4|\beta|^2(1-\cos K\theta)\frac{1}{K^2}(K-2+|\alpha|^2),\end{aligned} \tag{A8}$$

so that the error induced by the first use is of order $1/K$. If the d state is now sent on to a new Alice, whom we shall call Alice$'$, who then uses it to send the angle to Bob$'$ and Charlie$'$, the resulting $bcb'c'$ density matrix is of the form

$$\rho_{bcb'c'} = \frac{K-4}{K}\rho_{\text{prod}} + \rho_{\text{noise}}, \tag{A9}$$

where ρ_{prod} is the density matrix corresponding to the product state $(e^{i\theta/2}\alpha|0\rangle_{bc} + e^{-i\theta/2}\beta|1\rangle_{bc})(e^{i\theta/2}\alpha|0\rangle_{b'c'} + e^{-i\theta/2}\beta|1\rangle_{b'c'})$, and ρ_{noise} is an incoherent superposition of four states and is of size (operator norm) of order $1/K$. If $\exp(iK\theta) = 1$, then $\rho_{\text{noise}} = (4/K)\rho_{\text{prod}}$. For large K, this procedure will provide both sets of Bob and Charlie with good approximations of the desired state. Further uses will degrade the encoding state further, and add more noise to the transmitted states. A more extensive analysis of the degradation of phase information stored in a quantum state with use is given in Ref. [35].

APPENDIX B: REDUCTION OF GRAPH BY Z MEASUREMENTS

Alice can decide to disconnect vertices from the graph, even after the distribution of qubits to Bob. (We assign $|+\rangle^{\otimes|V|}$ for Alice and $|0\rangle^{\otimes|V|}$ for Bob instead.) Suppose the original graph consists of vertices $v \in V$ and edges $e \in E$, but Alice wishes to reduce it to a graph that is made of vertices $V^R \subset V$

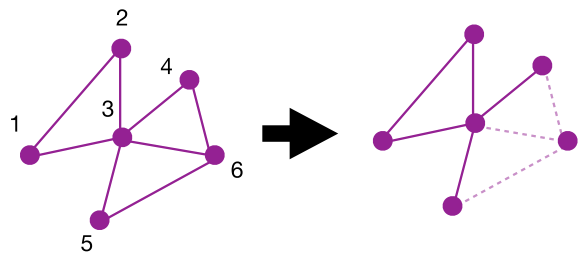

FIG. 6. An example of reduction of a graph. $V = \{1, 2, 3, 4, 5, 6\}$, $E = \{12, 13, 23, 34, 35, 36, 46, 56\}$, $V^R = \{1, 2, 3, 4, 5\}$, $E^R = \{12, 13, 23, 34, 35\}$, $\bar{V} = \{6\}$, $\bar{E} = \{36, 56, 46\}$.

and edges $E^R \subset E$. We denote $\bar{V} = V \backslash V^R$ and $\bar{E} = E \backslash E^R$ (see Fig. 6).

Alice measures her qubits that correspond to V^R with the X basis and those to $\bar{V}$ with the Z basis. Then Bob obtains

$$\left(\prod_{v\in V^R} \frac{1+(-1)^{s(v)}K_v}{2} \prod_{u\in\bar{V}} K_u^{s(u)}\right) \prod_{v\in V^R} |0\rangle_v \prod_{u\in\bar{V}} |0\rangle_u$$
$$= \left(\prod_{v\in V^R} \frac{1+(-1)^{s(v)}K_v}{2}\right) \prod_{v\in V^R} |0\rangle_v \prod_{u\in\bar{V}} |s(u)\rangle_u, \quad \text{(B1)}$$

with $K_v = X_v \prod_{\langle u,v\rangle} Z_u$, which is the graph-state stabilizer operator S_v. Now we write the stabilizers for the reduced graph as

$$K_v^R = X_v \prod_{\langle w,v\rangle\in E^R} Z_w \quad (v \in V^R). \quad \text{(B2)}$$

Then defining

$$\prod_{\langle u,v\rangle\in\bar{E}} (-1)^{s(u)} \equiv (-1)^{t(v)} \quad \text{(B3)}$$

with $t(v) = 0, 1$, the resultant state is given by

$$\left(\prod_{v\in V^R} \frac{1+(-1)^{s(v)+t(v)}K_v^R}{2}\right) \prod_{v\in V^R} |0\rangle_v \prod_{u\in\bar{V}} |s(u)\rangle_u. \quad \text{(B4)}$$

This is a graph state with the graph (V^R, E^R) and the product state for the rest of the qubits.

APPENDIX C: ALTERNATIVE WAY TO DISTRIBUTE GHZ

Here we consider the distribution of a N-qubit GHZ-like state. We consider a graph state given by vertices $V = \{1, 2, ..., 2N\}$ and edges $E = \{\langle 1, 2\rangle, \langle 2, 3\rangle, ..., \langle 2N-1, 2N\rangle, \langle 2N, 1\rangle\}$. Namely, this is a one-dimensional periodic chain labeled by integers. We use the quantum circuit described in Sec. IV B to generate the broadcasting state Eq. (45). However, this time the difference is that among the target qubits, the odd part $V_o = \{1, 3, ..., 2N-1\}$ is distributed among receivers, while the even part $V_e = \{2, 4, ..., 2N\}$ is kept by Alice. Note that Alice also keeps her qubits that control the stabilizer operators acting on Bobs' qubits, so that she has $|V| + |V_e| (= |V| + |V|/2)$ qubits. After Alice performs her measurement on her control qubits, due to the projection, Alice and Bobs share the graph state stabilized by

$$Z_{2n-1}X_{2n}Z_{2n+1}|\psi_G\rangle = |\psi_G\rangle \quad \text{(C1)}$$

$$Z_{2n}X_{2n+1}Z_{2n+2}|\psi_G\rangle = |\psi_G\rangle \quad \text{(C2)}$$

up to ± 1 signs. Now, Alice measures the even part V_e with the X basis. Because the new stabilizer conditions from Eq. (C1) become

$$Z_{2n-1}X_{2n}Z_{2n+1} = (-1)^{s_{2n}} Z_{2n-1}Z_{2n+1} = 1 \quad \text{(C3)}$$

and the global symmetry $X_1 ... X_{2n+1} ... X_{2N+1} = 1$ derived from the condition Eq. (C2) remains, the state shared by receivers is now a GHZ-type state [19] up to bit flips. This technique was given in, for example, Ref. [36].

APPENDIX D: SOME TECHNICAL DETAILS ON DISTRIBUTED REMOTE MBQC

The aim of this section is to give readers some details of distributed remote MBQC. We will focus on explanation of our method, and along the way we give basic ingredients commonly known in the field of MBQC. The original idea of using the brickwork state for the blind universal quantum computation was from Ref. [33]. Readers may find it helpful to look at Refs. [34,37] for pedagogical introduction to MBQC on the brickwork state.

1. Rotated graph state and measurement

Consider a graph state depicted in Fig. 4 (left). We label the ten qubits using an ordered set $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ from top left, top right, bottom left, to bottom right. The pairs (1, 2) (2, 3) (3, 4) (4, 5) (6, 7) (7, 8) (8, 9) (9, 10) are entangled with the CZ gate in the horizontal direction. The pairs (3,8) and (5,10) are entangled with the CZ gate in the vertical direction as well. We denote the set of these edges as E_{bw}. The initial information is encoded at (1,6) qubits (the leftmost pair) as $|\psi\rangle_{1,6}$. The brickwork state in this setup is written as

$$|\psi_{bw}\rangle := \prod_{\langle u,v\rangle\in E_{bw}} CZ_{u,v}(|\psi\rangle_{1,6} \otimes |+\rangle^{\otimes V\backslash\{1,6\}}). \quad \text{(D1)}$$

Alice possesses a copy of ten qubits to teleport XY-plane rotations. We label them by the subscript A, while the qubits of the brickwork state possessed by Bob will be labeled by the subscript B. Consider a state (which is the state after the projection with the stabilizers and corrections by Bob in our broadcast protocol)

$$|\Psi\rangle_{AB} = \prod_{v\in V} CZ_{v_A,v_B}\left(|\psi_{bw}\rangle_B \otimes |+\rangle_A^{\otimes V}\right). \quad \text{(D2)}$$

Now consider measurements by Alice with the basis $\{e^{-i\theta X}|0\rangle, e^{-i\theta X}|1\rangle\}$. Writing the measurement outcome at v as $s_v \in \{0, 1\}$ and the angle as θ_v, the postmeasurement

state is

$$\left(\bigotimes_{v\in V}\langle s_v|e^{i\theta_v X_v}\right)_A|\Psi\rangle_{AB} \propto \left(\prod_{v\in V} Z_v^{s_v} e^{i\theta_v Z_v}\right)|\psi_{bw}\rangle_B =: |\psi_{bw}(\theta;s)\rangle \tag{D3}$$

up to a normalization constant.

Now we move on to consider Bob's measurements with the basis $\{|\tilde{t}\rangle|t=0,1\}$ with $|\tilde{0}\rangle=|+\rangle$ and $|\tilde{1}\rangle=|-\rangle$. As the building block of MBQC, we note that for a pair of states entangled with CZ,

$${}_1\langle\widetilde{t}|Z_1^s e^{i\theta Z_1} CZ_{1,2}|\psi\rangle_1\otimes|+\rangle_2 = \frac{1}{\sqrt{2}}(He^{i\theta Z}Z^{t+s})_2|\psi\rangle_2. \tag{D4}$$

This involves a teleportation and a rotation gate. The Pauli Z^{t+s} depends on the measurement outcomes and is an example of by-product operators. The set of unitary gates for MBQC is obtained by sequentially applying this formula to the rotated brickwork state $|\psi_{bw}(\theta;s)\rangle$. It is convenient to define $w_v = t_v \oplus s_v \in \{0,1\}$ ($\oplus$: $\mathbb{Z}_2$ sum) for $v\in V$.

2. CNOT gate

We look at the measurement pattern for the controlled-NOT (CNOT) gate. We measure qubits in V except 5 and 10, where the output state will be defined. (The expression $|\psi_{bw}(\theta;s)\rangle$ contains teleported phase gates acting on 5 and 10. They are used in subsequent steps in MBQC, where the output state induced at 5 and 10 is seen as a new input state. In the present analysis, we simply ignore them when we look at derived unitaries.) We set

$$\theta_i = 0 \quad (i=1,2,4,6,8),$$
$$\theta_9=\alpha,\ \theta_3=\beta,\ \theta_7=\gamma. \tag{D5}$$

Using the formula, we get the following unitary acting on $|\psi\rangle_{5,10}$:

$$CZ\,(HZ^{w_4}\otimes He^{i\alpha Z}Z^{w_9})(He^{i\beta Z}Z^{w_3}\otimes HZ^{w_8})$$
$$CZ\,(HZ^{w_2}\otimes He^{i\gamma Z}Z^{w_7})(HZ^{w_1}\otimes HZ^{w_6}). \tag{D6}$$

Here, in $(\mathcal{P}\otimes\mathcal{Q})$, $\mathcal{P}$ acts on qubit 5, $\mathcal{Q}$ on qubit 10. It is equal to

$$\pm(X^{w_2+w_4}Z^{w_1+w_3+w_9}\otimes X^{w_7+w_9}Z^{w_4+w_6+w_8}) \times\exp[i(-1)^{w_2}\beta Z\otimes I]\exp[i(-1)^{w_2+w_6+w_8}\alpha Z\otimes X] \times\exp[i(-1)^{w_6}\gamma I\otimes X]. \tag{D7}$$

The set of Pauli operators in front of rotation gates is an example of by-product operators in MBQC. It is always propagated to the front of unitaries we wish to simulate, and the set of parameters such as (α,β,γ) are chosen based on the preceding measurement outcomes.

To be more precise, if we regard the ten-qubit brickwork state as a block in the middle of MBQC, the "initial" state $|\psi\rangle_{1,6}$ also carries by-product operators from former MBQC steps. Thus, we write the state defined at 1,6 as $|\psi\rangle_{1,6} = (X^{x_1}Z^{z_1}\otimes X^{x_6}Z^{z_6})|\psi'\rangle_{1,6}$. Then the state after the set of measurements will be

$$\pm(X^{w_2+w_4+x_1}Z^{w_1+w_3+w_9+z_1} \otimes X^{w_7+w_9+x_6}Z^{w_4+w_6+w_8+z_6}) \times\exp[i(-1)^{w_2+x_1}\beta Z\otimes I] \times\exp[i(-1)^{w_2+w_6+w_8+x_1+z_6}\alpha Z\otimes X] \times\exp[i(-1)^{w_6+z_6}\gamma I\otimes X]|\psi'\rangle_{5,10}. \tag{D8}$$

Now, let us choose the parameters as follows:

$$\alpha=(-1)^{w_2+w_6+w_8+x_1+z_6}\times\frac{-\pi}{4},$$
$$\beta=(-1)^{w_2+x_1}\times\frac{\pi}{4},$$
$$\gamma=(-1)^{w_6+z_6}\times\frac{\pi}{4}. \tag{D9}$$

Then we obtain the unitary

$$\exp\left[-\frac{\pi i}{4}(I-Z_5)(I-X_{10})\right] = CX_{5,10} \tag{D10}$$

with the by-product operators and a constant phase in front.

We note that the parameters can be always set as in (D9) because all the measurement outcomes w_i (as well as x_i, z_i) are obtained before the step to implement the parametric rotation. For example, we have results of measurements t_v, s_v (as well as x_i, z_i) at $\{1,2,3,6,7,8\}$ before the measurement with α at 9. It is clear that in order for Alice to properly choose θ_i to be sent, she needs to know the preceding measurement outcomes by Bobs, which we denoted t_v, so she can construct $w_v = s_v \oplus t_v$ combined with her s_v.

3. Single-qubit rotation gate

With the measurement pattern with $\theta_4=\theta_9=0$, we find the following unitary:

$$\pm(X^{w_2+w_4+x_1}Z^{w_1+w_3+w_9+z_1}\otimes X^{w_7+w_9+x_6}Z^{w_4+w_6+w_8+z_6}) \times(\exp[i(-1)^{x_1}\theta_3 Z]\exp[i(-1)^{w_1+z_1}\theta_2 X]\exp[i(-1)^{x_1}\theta_1 Z] \otimes\exp[i(-1)^{x_6}\theta_8 Z]\exp[i(-1)^{w_6+z_6}\theta_7 X]\exp[i(-1)^{x_6}\theta_6 Z]). \tag{D11}$$

Choosing the parameters as

$$\theta_1=(-1)^{x_1}\alpha,\quad \theta_2=(-1)^{w_1+z_1}\beta,\quad \theta_3=(-1)^{x_1}\gamma \tag{D12}$$

$$\theta_6=(-1)^{x_6}\gamma',\quad \theta_7=(-1)^{w_6+z_6}\beta',\quad \theta_8=(-1)^{x_6}\alpha', \tag{D13}$$

we obtain the single-qubit ration gate

$$R(\alpha,\beta,\gamma)=e^{i\gamma Z}e^{i\beta X}e^{i\alpha Z} \tag{D14}$$

acting on 5 and 10 as $R(\alpha,\beta,\gamma)\otimes R(\alpha',\beta',\gamma')$.

[1] H. J. Kimble, The quantum internet, Nature (London) **453**, 1023 (2008).

[2] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, eaam9288 (2018).

[3] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, Quantum internet: Networking challenges in distributed quantum computing, IEEE Network **34**, 137 (2020).

[4] P. P. Rohde, *The Quantum Internet: The Second Quantum Revolution* (Cambridge University Press, Cambridge, 2021).

[5] Y. Yu, X. W. Zha, and W. Li, Quantum broadcast scheme and multi-output quantum teleportation via four-qubit cluster state, Quant. Info. Proc. **16**, 41 (2017).

[6] Y. Yu and N. Zhao, General quantum broadcast and multicast communications based on entanglement, Opt. Express **26**, 29296 (2018).

[7] Y.-J. Zhou and Y.-H. Tao, Probabilistic broadcast-based multiparty remote state preparation scheme via four-qubit cluster state, Int. J. Theor. Phys. **57**, 549 (2018).

[8] N. Zhao, W. Li, and Y. Yu, Quantum broadcast and multicast schemes based on partially entangled channel, IEEE Access **8**, 29658 (2020).

[9] H.-K. Lo, Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity, Phys. Rev. A **62**, 012313 (2000).

[10] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, Remote State Preparation, Phys. Rev. Lett. **87**, 077902 (2001).

[11] D. W. Leung and P. W. Shor, Oblivious Remote State Preparation, Phys. Rev. Lett. **90**, 127905 (2003).

[12] C. Bennett, P. Hayden, D. Leung, P. Shor, and A. Winter, Remote preparation of quantum states, IEEE Trans. Inf. Theory **51**, 56 (2005).

[13] M. Rådmark, M. Wieśniak, M. Żukowski, and M. Bourennane, Experimental multilocation remote state preparation, Phys. Rev. A **88**, 032304 (2013).

[14] P. Agrawal, P. Parashar, and A. K. Pati, Exact remote state preparation for multiparties using dark states, Int. J. Quantum. Inform. **01**, 301 (2003).

[15] M. Hillery, J. A. Bergou, T.-C. Wei, S. Santra, and V. Malinovsky, Broadcast of a restricted set of qubit and qutrit states, Phys. Rev. A **105**, 042611 (2022).

[16] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, Entanglement in graph states and its applications, in *Proceedings of the International School of Physics Enrico Fermi*, edited by G. Casati *et al.*, Vol. 162 (IOS Press, 2006), pp. 115–218.

[17] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states, Phys. Rev. A **68**, 022312 (2003).

[18] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).

[19] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Springer Netherlands, Dordrecht, 1989), pp. 69–72.

[20] A. Dutta and A. Pathak, A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice? Quant. Info. Proc. **21**, 369 (2022).

[21] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Quantum digital signatures with quantum-key-distribution components, Phys. Rev. A **91**, 042304 (2015).

[22] A. Cabello, Supersinglets, J. Mod. Opt. **50**, 1049 (2003).

[23] S. J. D. Phoenix, S. M. Barnett, and A. Chefles, Three-state quantum cryptography, J. Mod. Opt. **47**, 507 (2000).

[24] M. Van den Nest, J. Dehaene, and B. de Moor, Local unitary versus local Clifford equivalence of stabilizer states, Phys. Rev. A **71**, 062323 (2005).

[25] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, Quantum hypergraph states, New J. Phys. **15**, 113022 (2013).

[26] X. Chen, Z.-C. Gu, Z.-X. Liu, and X.-G. Wen, Symmetry-protected topological orders in interacting bosonic systems, Science **338**, 1604 (2012).

[27] B. Yoshida, Topological phases with generalized global symmetries, Phys. Rev. B **93**, 155131 (2016).

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

[29] R. Beals, S. Brierley, O. Gray, A. W. Harrow, S. Kutin, N. Linden, D. Shepherd, and M. Stather, Efficient distributed quantum computing, Philos. Trans. R. Soc. London, Ser. A **469**, 20120686 (2013).

[30] H. Buhrman and H. Röhrig, Distributed quantum computing, in *Mathematical Foundations of Computer Science 2003: 28th International Symposium, MFCS 2003, Bratislava, Slovakia, August 25-29, 2003* (Springer, New York, 2003), pp. 1–20.

[31] V. S. Denchev and G. Pandurangan, Distributed quantum computing: A new frontier in distributed systems or science fiction? ACM SIGACT News **39**, 77 (2008).

[32] M. Caleffi, M. Amoretti, D. Ferrari, D. Cuomo, J. Illiano, A. Manzalini, and A. S. Cacciapuoti, Distributed quantum computing: A survey, arXiv:2212.10609 [quant-ph].

[33] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2009), pp. 517–526.

[34] J. F. Fitzsimons, Private quantum computation: An introduction to blind quantum computing and related protocols, npj Quantum Inf. **3**, 23 (2017).

[35] J. A. Vaccaro, S. Croke, and S. M. Barnett, Is coherence catalytic? J. Phys. A: Math. Theor. **51**, 414008 (2018).

[36] N. Tantivasadakarn, R. Thorngren, A. Vishwanath, and R. Verresen, Long-range entanglement from measuring symmetry-protected topological phases, arXiv:2112.01519 [cond-mat.str-el].

[37] T.-C. Wei, Quantum spin models for measurement-based quantum computation, Adv. Phys.: X **3**, 1461026 (2018).