Quantum secret sharing with qudit graph states

Adrian Keet,[1] Ben Fortescue,[1] Damian Markham,[2] and Barry C. Sanders[1]

[1]*Institute for Quantum Information Science, University of Calgary, Alberta, T2N 1N4, Canada*
[2]*LTCI-CNRS, Telecom ParisTech, 37/39 rue Dareau, F-75014 Paris, France*

We present a unified formalism for threshold quantum secret sharing using graph states of systems with prime dimension. We construct protocols for three varieties of secret sharing: with classical and quantum secrets shared between parties over both classical and quantum channels.

I. INTRODUCTION

"Secret sharing" refers to an important family of multiparty cryptographic protocols in both the classical [1,2] and the quantum [3–6] contexts. A secret-sharing protocol comprises a dealer and n players who are interconnected by some set of classical or quantum channels. The "secret" to be shared is a classical string or quantum state and is distributed among the players by the dealer in such a way that it can be recovered only by certain subsets of players acting collaboratively. The *access structure* is the set of all subsets of players who can recover the secret, and the *adversary structure* corresponds to those subsets who obtain no knowledge of the secret. There may, in addition, be external eavesdroppers who should also gain no knowledge of the secret. Secret-sharing protocols have practical applications in, for example, money transfer [4] and voting [7] schemes. Recently, a unified formalism for a range of protocols for sharing both classical and quantum secrets using qubit graph states [8] has been proposed [6]. The formalism allows for both classical and quantum channels between the dealer and players and covers three common varieties of secret sharing within a single framework. In this article we develop an analogous formalism for the case of systems of prime-dimensional quantum states.

Although qubit systems are generally the most straightforward to describe and the theory of qubit graph states is well developed, there are good reasons to consider higher-dimensional systems as well. If players' shares consist of such systems, it may be more efficient to make direct use of the larger Hilbert space than to work with encoded qubits. Additionally, certain access structures are known not to be possible using the existing secret-sharing schemes on qubit graph states [6,9] or, in some cases, using any scheme with qubit shares. An example of the latter (which can, however, be implemented using qutrits) was given by Cleve, Gottesman, and Lo [4]. A more broad justification is that one often needs to consider higher-dimensional states in order to derive rigorous general results in quantum information theory, such as in certain *no-go theorems* [10–12].

Our aim is therefore to find a unified formalism for secret sharing that is not restricted to the qubit case. As discussed recently [8,13,14], graph and stabilizer states can be extended to the qudit case for prime dimensions. Following this approach, we find direct extensions of the existing qubit protocols [6] in d dimensions, where d is prime, i.e., we find protocols for sharing classical secrets with d possible values and secret quantum states within a d-dimensional Hilbert

space, using graph states shared by a dealer and players, each with a d-dimensional subsystem. Our work therefore achieves, in higher-dimensional systems, the goals previously achieved for qubits [6], namely providing a general graph-state unification for sharing classical and quantum secrets using both classical and quantum channels and in this way extends the protocols to more general access structures. Note that we are primarily demonstrating how a subset of existing secret-sharing protocols, already known to be achievable, can be unified within our formalism; we are not attempting to address via the formalism any existing limitations in quantum and classical secret sharing. Additionally, however, we have demonstrated protocols within our formalism which have not been previously shown: the case of three parties sharing classical secrets distributed over quantum channels (secure or insecure), in which a minimum of two parties are required to recover the secret.

In general, there are many different possible access structures for secret-sharing schemes. In our work we consider the specific case of *threshold* secret sharing. In such a scheme the secret can be recovered if and only if any k of the n players collaborate to do so (and any set of fewer than k players are denied any knowledge of the secret). All that is required is that enough players collaborate; i.e., it does not matter which k players do so. Thus the access structure comprises any set of at least k players, with the remainder forming the adversary structure. This is denoted as a (k,n) threshold secret-sharing scheme. Note that one can construct arbitrary access structures for both classical [15] and quantum [5] secret sharing by concatenating threshold protocols; thus it is sufficient to consider only threshold secret sharing to address general secret sharing.

Here we consider three specific varieties of such schemes previously demonstrated in qubit graph states [6]. We note that all existing forms of secret sharing that have been proposed fall into one of these categories.

 (i) CC schemes: The secret is classical, the dealer is connected to the players via private quantum channels, and all players are connected by private classical channels.

 (ii) CQ schemes: The secret is classical, the dealer shares public quantum channels with each player, and the players are connected to each other by private classical channels.

 (iii) QQ schemes: The secret is quantum, the dealer shares either private or public quantum channels with each player, and the players are connected to each other by private quantum or classical channels.

In Sec. II, we formally define the structure and graphical representation of graph states for qudits and explain how classical information can be encoded on to such states and later accessed. In Sec. II D we show the effect of local (d-dimensional) Pauli measurements on qudit graphs and derive rules (partially shown previously [14]) for the form of the consequent-reduced graph states, analogous to "local complementation" in the qubit case. In Sec. III we demonstrate specific CC, CQ, and QQ protocols which may be implemented in qudit graphs given the properties previously derived [though we note that in the case of the (n,n) QQ scheme, the secret is not perfectly denied to the adversary structure]. We present, as an example of the power of higher dimensions, the $(2,3)$ case, which is not possible with qubit graph state schemes [6], as well as higher-dimensional analogs to those presented in Ref. [6].

II. GRAPH STATES FOR QUDITS

Graph states [16] are a class of entangled multipartite states (including the well-known n-qubit GHZ state) of wide interest in quantum information. Their useful properties include a convenient graphical representation and characterization within the stabilizer formalism [17], as well as their practical application within information processing, in particular for computation [18] and error correction [14,19,20], and their amenability for the representation of information flow [9,21]. Such states have been created and applied in this way for up to six qubits [22,23], and recent work [14] has considered the case of higher-dimensional graph states. We employ the same framework in Secs. II B and II A as that in previous work [8,13,14] although we use different notation more suited to secret sharing.

A. Graph states

We now introduce qudit graph states and their graphical representation. Consider a finite field $\mathbb{F}_d$ of order d, where d is a prime number >2, and a weighted undirected graph, i.e., a set of n vertices $\mathsf{V} = \{\mathsf{v}_i\}$ joined by a set of edges $\mathsf{E} = \{\mathsf{e}_{ij} = \{\mathsf{v}_i, \mathsf{v}_j\}\}$.

Each edge e_{ij} has an assigned "weight" $A_{ij} \in \mathbb{F}_d$. E only contains edges with nonzero weights: A weight of zero corresponds to two vertices not being joined by an edge. No vertex is joined to itself. We can summarize this information in an $n \times n$ "adjacency matrix" A with elements A_{ij}. We therefore have $A_{ij} = A_{ji}$ for all $\mathsf{v}_i, \mathsf{v}_j \in \mathsf{V}$ and $A_{ii} = 0$ for all $\mathsf{v}_i \in \mathsf{V}$.

We define the computational basis $\{|j\rangle \mid j \in \mathbb{F}_d\}$. Then the graph state represented by the above graphical construction is

$$|G\rangle := \prod_{\mathsf{e}_{ij} \in \mathsf{E}} C_{ij}^{A_{ij}} |\bar{0}\rangle^{\otimes n}, \tag{1}$$

where we define the two-qudit controlled-Z operator

$$C_{ab}|j\rangle_a |k\rangle_b := \omega^{jk} |j\rangle_a |k\rangle_b, \tag{2}$$

the operator

$$U|i\rangle := \sum_{j \in \mathbb{F}_d} \omega^{ij} |j\rangle \tag{3}$$

and the basis

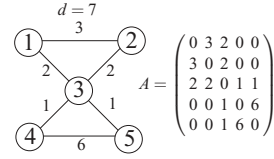$$|\bar{i}\rangle := U^{-1}|i\rangle \mid i \in \mathbb{F}_d. \tag{4}$$

FIG. 1. A five-qudit graph in $d = 7$ and associated adjacency matrix A.

An example graph and associated adjacency matrix are depicted in Fig. 1.

B. Local operators and labeling

Here, in an analogous way to the qubit case [6], we describe the encoding of classical information onto the graph state by applying local operators to the individual qudits that are graphically represented by the vertices of the graph. Here and later we make use of the *generalized Pauli operators* [24–26]

$$Z|j\rangle := \omega^j |j\rangle, \tag{5}$$

$$X|j\rangle := |j + 1\rangle, \tag{6}$$

where $\omega = e^{2\pi i/d}$. These operators satisfy $X^d = Z^d = I$. (It follows that $ZX = \omega XZ$ and that the eigenstates of the operators $Z, X, XZ, XZ^2 \cdots XZ^{d-1}$ form a set of mutually unbiased bases [27]. We consider only this subset of the general operators $X^m Z^n$ as they are sufficient for defining the graph-state stabilizers and for our secret-sharing protocols.) We further define the operator

$$S|j\rangle := \omega^{j(j-1)/2} |j\rangle, \tag{7}$$

which satisfies $SZ = ZS$ and $SXS^{-1} = XZ$.

In a labeled graph state each vertex v_i is assigned a label $\ell_i := (z_i, x_i, m_i)$, where $z_i, x_i, m_i \in \mathbb{F}_d$. Denoting an operator O acting on a vertex v_i as O_i, the graph state is labeled by applying the operators $S_i^{m_i} X_i^{x_i} Z_i^{z_i}$ to the state $|G\rangle$. We describe the combined labels for all vertices by $\boldsymbol{\ell} := (\boldsymbol{z}, \boldsymbol{x}, \boldsymbol{m})$, where $\boldsymbol{z} := (z_1, z_2 \ldots, z_n)$, and similarly for $\boldsymbol{x}$ and $\boldsymbol{m}$. We use the notation

$$Z^{\boldsymbol{z}} := Z_1^{z_1} \otimes Z_2^{z_2} \otimes \cdots \otimes Z_n^{z_n} \tag{8}$$

and similarly for X and S. Thus the labeled graph state is

$$|G_{\boldsymbol{\ell}}\rangle := S^{\boldsymbol{m}} X^{\boldsymbol{x}} Z^{\boldsymbol{z}} |G\rangle. \tag{9}$$

Note that our definition differs from that used previously for qubits [6] in that we apply the S operators after the X operators rather than before.

Finally, we define an *encoded graph state* as a labeled graph state with $\boldsymbol{x} = \boldsymbol{0}$.

C. Stabilizers

Higher-dimensional graph states can be represented within the stabilizer formalism [8,13,14]. The encoded graph state with labels $\boldsymbol{\ell}$ satisfies, for each vertex v_i [14],

$$K_i |G_{\boldsymbol{\ell}}\rangle = \omega^{-z_i} |G_{\boldsymbol{\ell}}\rangle, \tag{10}$$

where

$$K_i := (XZ^{m_i})_i Z^{A_i}, \tag{11}$$

and we define, for a qudit operator O and scalar multiple k,

$$O^{kA_i} := \prod_{\mathsf{v}_j \in \mathsf{V}} O_j^{kA_{ij}}. \tag{12}$$

The $\{K_i\}$ is thus a set of stabilizers for the encoded graph state, and $|G_\ell\rangle$ is the unique state (up to a global phase) satisfying (10) for all vertices v_i. Note that the $\{K_i\}$ are tensor products of local operators; thus, even in the absence of any quantum communication, the value of K_i may be measured through local operations and classical communication (LOCC) by the appropriate subset of parties combining their local measurement results. Note also that we need only consider exponents of these local operators modulo d.

It follows from (11) and (9) and the commutation relations of Sec. II B that applying the stabilizer K_i to a labeled graph state $|G_\ell\rangle$ is equivalent (up to a global phase) to implementing the label change $x_i \to x_i + 1$, $z_j \to z_j + A_{ij}$ (mod d) for all $e_{ij} \in E$; i.e.,

$$|G_\ell\rangle = S^m X^x Z^z |G\rangle \propto S^m X^x X_i Z^z Z^{A_i} |G\rangle. \tag{13}$$

Thus the two different labelings correspond to the same physical state. As in the qubit case [6], we can exploit this property to determine the state's dependence on particular qudit labels.

D. Local measurements

Our CQ and QQ protocols involve one of the parties as a designated "dealer," whose local measurement on her own qudit produces a reduced graph state shared by the other parties with some access structure and labeling determined by the dealer's measurement outcome. We therefore consider the effect of local measurements on qudit graph states. This has previously been determined in the qubit case.

We will closely follow the derivation for the effect of measurements on qubit graphs in Ref. [8], the results of which were used in Ref. [6]. The results below for the effect of local measurement on the adjacency matrix were previously derived [14] in the context of local complementation [8,28], although here we also explicitly derive the effect of local measurement on the graph labels. We find the following:

Proposition 1. Given an encoded graph state $|G_\ell\rangle$, suppose a measurement of $(X^m Z)_i$ yields the value ω^s. Then the resultant labeled graph state is obtained by the following procedure:

(M1) For each pair j,k of distinct neighbors of i, change $A_{jk} \mapsto A_{jk} + mA_{ij}A_{ik}$.

(M2) Relabel each vertex j by $z_j \mapsto z_j + A_{ij}s + mA_{ij}z_i + mA_{ij}(A_{ij} + 1)/2$ and $m_j \mapsto mA_{ij}^2$.

(M3) Remove vertex i and corresponding edges.

Proof. We first introduce the operators U and R, defined as

$$U|k\rangle := \sum_{j \in \mathbb{F}_d} \omega^{jk} |j\rangle \tag{14}$$

$$R := U^{-1} S^{-1} U. \tag{15}$$

It follows that $UXU^{-1} = Z$ and $UZU^{-1} = X^{-1}$. We also have $[R,X] = [S,Z] = 0$ and $RZR^{-1} = SXS^{-1} = XZ$; i.e., the R operator performs a $Z \leftrightarrow XZ$ basis transformation just as S performs $X \leftrightarrow XZ$.

For each local Pauli operator $O = X^n Z^m$, we define the operator $P_{O,j}$, which is the projection onto the ω^j eigenspace of O:

$$P_{O,j} := \frac{1}{d} \sum_{k \in F_d} \omega^{-jk} O^k. \tag{16}$$

We first consider the case $m = 0$ where the projective measurement is of Z_i. We have

$$|G_\ell\rangle = \prod_{\mathsf{v}_j \in \mathsf{V}} C_{ij}^{A_{ij}} |\bar{0}\rangle_i |G_\ell \setminus \mathsf{v}_i\rangle_{\mathsf{V} \setminus \mathsf{v}_i}, \tag{17}$$

where $|G_\ell \setminus \mathsf{v}_i\rangle$ denotes the graph state with vertex v_i and all its edges removed and $\mathsf{V} \setminus \mathsf{v}_i$ denotes the set all of players excluding player i. Next, noting that

$$\prod_{\mathsf{v}_j \in \mathsf{V}} C_{ij}^{A_{ij}} = \prod_{\mathsf{v}_j \in \mathsf{V}} \sum_{k \in \mathbb{F}_d} (P_{Z,k})_i Z_j^{kA_{ij}} = \sum_{k \in \mathbb{F}_d} (P_{Z,k})_i Z^{kA_i}, \tag{18}$$

we have

$$(P_{Z,s})_i |G_\ell\rangle = (P_{Z,s})_i \prod_{\mathsf{v}_j \in \mathsf{V}} C_{ij}^{A_{ij}} |\bar{0}\rangle_i |G_\ell \setminus \mathsf{v}_i\rangle_{\mathsf{V} \setminus \mathsf{v}_i}$$

$$= (P_{Z,s})_i \left(\sum_{k \in \mathbb{F}_d} (P_{Z,k})_i Z^{kA_i} \right) |\bar{0}\rangle_i |G_\ell \setminus \mathsf{v}_i\rangle_{\mathsf{V} \setminus \mathsf{v}_i}$$

$$= \frac{1}{\sqrt{d}} |s\rangle_i Z^{sA_i} |G_\ell \setminus \mathsf{v}_i\rangle_{\mathsf{V} \setminus \mathsf{v}_i}. \tag{19}$$

Now we consider the case $m \neq 0$. Let

$$L_i := R_i^{-1} S^{-A_i^2}. \tag{20}$$

where we define

$$O^{kA_i^2} := \prod_{\mathsf{v}_j \in \mathsf{V}} O_j^{kA_{ij}^2}. \tag{21}$$

Then, for each $\mathsf{v}_j \in \mathsf{V}$,

$$L_i^m K_j L_i^{-m} = R_i^{-m} S^{-mA_i^2} X_j Z^{A_j} S^{mA_i^2} R_i^m$$

$$= \omega^{mA_{ij}(A_{ij}+1)/2} K_i^{-mA_{ij}} K_j', \tag{22}$$

where $K_j' = X_j Z^{A_j + mA_{ij}(A_i)} Z_j^{-mA_{ij}^2}$. Equation (22) follows from the relation

$$(X^{-1}Z)^{A_{ij}} = \omega^{A_{ij}(A_{ij}-1)/2} X^{-A_{ij}} Z^{A_{ij}}. \tag{23}$$

Thus, noting that K_i commutes with L_i, we have

$$K_j' = \omega^{-mA_{ij}(A_{ij}+1)/2} L_i^m K_i^{mA_{ij}} K_j L_i^{-m}, \tag{24}$$

so

$$K_j' L_i^m |G_\ell\rangle = \omega^{-mA_{ij}(A_{ij}+1)/2} L_i^m K_i^{mA_{ij}} K_j |G_\ell\rangle$$

$$= \omega^{-mA_{ij}(A_{ij}+1)/2 - mA_{ij}z_i - z_j} L_i^m |G_\ell\rangle. \tag{25}$$

The state $L_i^m |G_\ell\rangle$, which we will denote $|\tau_i^m(G_\ell)\rangle$, is therefore an encoded graph state $|\tau_i^m(G_\ell)\rangle$, stabilized by the K_j' operators. The structure (i.e., the adjacency matrix) of the graph $\tau_a^m(G_\ell)$ is given by equating the A_j' for each vertex to the A_i given in the standard form for graph-state stabilizers in (11), and we similarly find the labels

$$z_j' = z_j + mA_{ij}z_i + mA_{ij}(A_{ij} + 1)/2. \tag{26}$$

We also have

$$L_i^{-m}(P_{Z,s})_i L_i^m = \frac{1}{d} \sum_{k \in \mathbb{F}_d} \omega^{-sk} R_i^m S^{m A_i^2} Z_i^k S^{-m A_i^2} R_i^{-m}$$

$$= \frac{1}{d} \sum_{k \in \mathbb{F}_d} \omega^{-sk} (X^m Z)_i^k$$

$$= (P_{X^m Z,s})_i. \qquad (27)$$

Thus we compute

$$(P_{X^m Z,s})_i |G_\ell\rangle = L_i^{-m}(P_{Z,s})_i L_i^m |G_\ell\rangle$$

$$= \frac{1}{\sqrt{d}}(R^m |s\rangle)_i \left(S^{m A_i^2} Z^{s A_i} \left| \tau_i^m(G_\ell) \setminus \mathsf{v}_i \right\rangle \right)_{\mathsf{V} \setminus \mathsf{v}_i}. \qquad (28)$$

Hence a local measurement of XZ^m on the vertex v_i gives the graph $|\tau_i^m(G_\ell)\rangle$ with the v_i vertex removed and additional labeling operators $S^{m A_i^2} Z^{s A_i}$ applied. ∎

The reduced-state graph transformation given in M1 can be regarded as an analog of local complementation for qubit graphs; note, however, that we have not shown (as is true for the qubit case) that all graphs equivalent under local Clifford group operations are similarly equivalent under such transformations. This has been proven elsewhere [14].

An example of the effect of local measurement is given in Fig. 2 for a four-party square state with $d = 5$, all edges of weight 2 and each vertex having the labels $(z,x,m) = (1,0,1)$. If player 1 performs a measurement of XZ^2 and gets a result of ω^2, the state is transformed as shown.

E. Dependence and access

We now consider conditions such that a subset of players can independently recover a secret encoded into the labels of a labeled qudit graph state, using the terminology previously employed for the qubit case [6]. For a state $|G_\ell\rangle\langle G_\ell|$, consider a subset of players $\mathsf{V}' \subseteq \mathsf{V}$. Without any assistance from any other players the subset V' only has access to the reduced state $\rho_{\mathsf{V}'} = \mathrm{Tr}_{\mathsf{V} \setminus \mathsf{V}'} |G_\ell\rangle\langle G_\ell|$ and must recover the secret from this state.

Considering then some secret $s \in \mathbb{F}_d$, which is a function of the labels ℓ, it follows that the set of players V' are clearly unable to recover s if the state $\rho_{\mathsf{V}'}$ is invariant under changes in
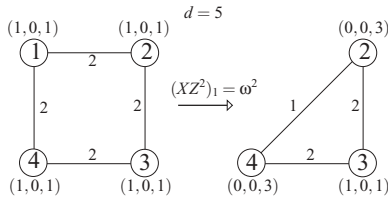

FIG. 2. Effect of a local XZ^2 measurement (with result ω^2) on vertex 1 of an encoded-square qudit graph with weight-2 edges in $d = 5$. Labels are denoted (z,x,m). Following the measurement, vertex 1 and all its edges are removed. Vertices 2 and 3 gain an edge of weight $N_{23} = 0 + 6 = 1$ (modulo $d = 5$) and vertex labels $z = 1 + 4 + 4 + 6 = 0$, $m = 8 = 3$.

k. If this is not the case, we say the reduced state is *dependent* on the value s.

However, dependency is generally insufficient for the players to be able to recover s. We say that a set of players V' can *access* s if there is a measurement protocol the players in V' can perform on $\rho_{\mathsf{V}'}$ such that the value of s is revealed to them with certainty.

We find the following:

Proposition 2. Given an encoded graph state, if for a set of vertices $\mathsf{V}' \subseteq \mathsf{V}$, we have some corresponding set of values $\{w_i\} \in \mathbb{F}_d$ (with $w_i = 0$ for all $\mathsf{v}_i \notin \mathsf{V}'$), then $\sum_i w_i z_i$ is accessible to the parties in V' via LOCC if $\sum_{\mathsf{v}_j \in \mathsf{V}} w_i A_{ij} = 0$ for all $\mathsf{v}_i \in \mathsf{V} \setminus \mathsf{V}'$.

Proof. Each party $\mathsf{v}_i \in \mathsf{V}'$ measures $K_i^{w_i}$ for an overall stabilizer $K = \prod_{\mathsf{v}_i \in \mathsf{V}'} K_i^{w_i}$. The graph state is thus an eigenstate of K with eigenvalue $\omega^{-\sum_i w_i z_i}$; thus the parties in V' can jointly retrieve $\sum_i w_i z_i$. ∎

Corollary 3. In an encoded graph state, the label z_k is accessible via LOCC by V' if V' contains v_k and all of its neighbors.

Proof. Apply Proposition 2 with $w_k = 1$ and all $w_{i \neq k} = 0$ so $\sum_i w_i z_i = z_k$. For any $\mathsf{v}_j \in \mathsf{V} \setminus \mathsf{V}'$, we have that $\sum_{\mathsf{e}_{ij} \in \mathsf{e}} w_i A_{ij} = A_{kj} = 0$ since v_j is outside V' and thus not a neighbor of v_i. The stabilizer K in the proof of Proposition 2 is just K_i in this case; hence measuring K_i gives the value z_i. ∎

Note that, because labels are applied to a given vertex via *local* Pauli operations on that vertex, the reduced graph state obtainable by tracing out a given vertex (i.e., a given player) must be independent of that vertex's labels. Hence those labels are inaccessible to the remaining players. We exploit this property to determine the minimum number of players required to recover a secret in threshold secret-sharing protocols.

1. Label "shuffling"

As for the qubit case, we demonstrate that a given subset of parties is independent of a particular qudit label by "shuffling" the label onto qudits not in the subset. That is, we demonstrate that the transfer of the label onto a different qudit (such that the original qudit no longer has any dependence on the label) results in a physically equivalent state. Thus the label shuffling procedure does not represent any physical operation or change in the state: It merely generates an equally valid relabeling of the same physical state.

Proposition 4. Let $|G_\ell\rangle$ be an encoded graph state, and let players i and j be neighbors. Then $|G_\ell\rangle$ is equivalent to the labeled graph state $|G_{\ell'}\rangle$ where vertex i is relabeled $z_i' = 0$, vertex j is relabeled $(z_j', x_j') = (z_j, -A_{ij}^{-1} z_i)$, and each neighbor k of j is relabeled $z_k' = z_k - A_{ij}^{-1} A_{jk} z_i)$.

Proof. Noting that K_j stabilizes $|G_\ell\rangle$, it follows that $K_j^{-A_{ij}^{-1} z_i} |G_\ell\rangle \propto |G_{\ell'}\rangle$, which, from (11), corresponds to the above relabeling.

We demonstrate the above concept in Fig. 3 using a four-qudit square graph with weight-2 edges in $d = 5$, with a label of $z = 3$ on vertex 1 and all other labels equal to zero, and shuffling player 1's label to player 2.
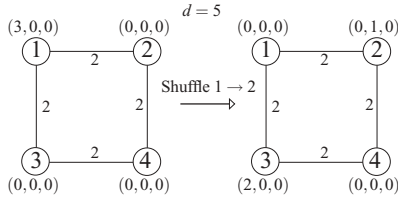
FIG. 3. Effect of label shuffling from vertex 1 to 2 on an encoded square qudit graph with weight-2 edges in $d = 5$. Labels are denoted (z, x, m). Vertex 1's z label is set to 0. Vertex 2's x label is set to $-3/2 = 1 \pmod{d = 5}$, and vertex 3's z label is set to $-6/2 = 2$.

III. SECRET-SHARING PROTOCOLS

A. CC scheme

In a (k, n) CC threshold scheme, the players' shared quantum state is privately transferred to them by the dealer, after which a classical secret can be reconstructed by any k of n players (but no fewer) using classical channels between the players. We demonstrate the feasibility of such schemes using labeled graph states by encoding a secret "dit" s on to the z labels of certain vertices of the graph. We then show that a subset of m parties may measure s by jointly measuring one of the graph state's stabilizers K_i. Finally, to demonstrate that fewer than m parties cannot obtain s, it is sufficient to show that we can shuffle the vertices' z values such that any given set of fewer than k parties has no dependence on s (for which it is clearly sufficient to demonstrate the above for $k - 1$ parties only).

Note that secret sharing is known to be information-theoretically secure in the classical case; in our analysis we are showing that such protocols may be unified within the graph state formalism. CC protocols within our formalism also provide a useful basis for the CQ and QQ cases, as shown later.

We find that such schemes may be implemented for d-dimensional analogs of all the qubit states for which it was previously demonstrated [6], using essentially the same reasoning.

1. (n,n) CC protocol in the tree state

We can implement an (n, n) protocol using a tree state, consisting of a single vertex connected by weight-1 edges to $n - 1$ additional vertices, as illustrated in Fig. 4. (In the three-party qubit case with all labels set to zero this is the well-known Greenberger-Horne-Zeilinger-Mermin state). We set $z_1 = s$ and $z_i = 0$ for all $i \neq 1$.
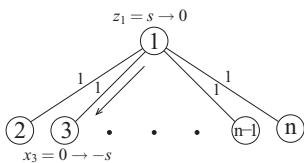

FIG. 4. Shuffling of a classical secret s from player 1 to player 3 in a CC protocol for an encoded tree state. As this label can be shuffled to any player (or remain with player 1), any subset of the parties has no dependence on s.
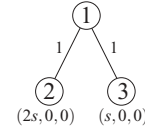

FIG. 5. Encoding of a classical secret $s \in \mathbb{F}_d$ onto a three-party state to enable a (2,3) CC protocol. It can be seen that the secret can be shuffled away from any single qubit. At the same time any two players can access the secret as explained in the text.

For this state, the stabilizer $K_1 = (XZ^{m_1})_1 \otimes Z_2 \otimes \cdots \otimes Z_n$ has the eigenvalue ω^{-s}, and the value of s may thus be accessed through local measurements by all n parties. We see that s is inaccessible to any smaller number of parties as follows: The set of $n - 1$ parties excluding player 1 has no dependence on s. However, we can also shuffle the s dependence from player 1 to any other party i as described in Proposition 4. This leaves us with $z_1 = 0$, $x_i = -z_1 = -s$, and all other labels unchanged, in which case the labels for all players other than i have no dependence on s. Hence all n players are necessary to recover s.

2. (2,3) CC protocol

We can implement a (2,3) protocol using the labeled graph state in Fig. 5. We encode the classical secret $s \in \mathbb{F}_d$ by setting $z_1 = 0$, $z_2 = 2s$, and $z_3 = s$ and set all other labels to zero as illustrated.

To see that no single player can access the secret we apply the shuffling as described in Proposition 3. Player 1 cannot access the secret, as he has no label dependence on the secret. The label $z_2 = 2s$ can be removed by shuffling it to player 1 and player 3 as per Proposition 3 (explicitly by multiplication of stabilizer K_1^{-2s}); hence player 2 cannot access the secret. The label $z_3 = s$ can be removed by shuffling it to player 1 and player 3 as per Proposition 3 (explicitly by multiplication of stabilizer K_1^{-s}), hence player 3 also cannot access the secret.

To see that any pair can access the secret, we take each pair separately. Players 1 and 2 can measure $K_2 = Z_1 X_2$, giving outcome ω^{-2s}. Players 1 and 3 can measure $K_3 = Z_1 X_3$, giving outcome ω^{-s}. Players 2 and 3 can measure $K_2^{d-1} K_3 = X_2^{d-1} X_3$, giving outcome ω^s.

3. (3,4) CC protocol in the ring state

We can implement a (3,4) protocol using a square encoded graph state with weight-1 edges and $m_i = 0$ for all i, by setting $z_i = s$ for all i.

Thus we have $K_i = \omega^s$ for all i and, e.g., $K_2 = Z_1 X_2 Z_3$, so players 1, 2, and 3 can collaborate to measure s. By the symmetry of the state, this is similarly the case for any set of three players.

As depicted in Fig. 6, we can shuffle the s dependence of player 1 to player 2. This sets $z_1 = 0$, $x_2 = -s$, and $z_3 = s - s = 0$. This leaves the labels of 1 and 3 independent of s; hence neither they, nor (by symmetry) any two nonadjacent parties, can obtain s.

If they subsequently perform a $4 \to 3$ shuffle, this leaves player 1's labels unaltered and sets player 4's z label to 0; hence 1 and 4 (and thus any two adjacent players) cannot obtain Z, thereby completing the proof.
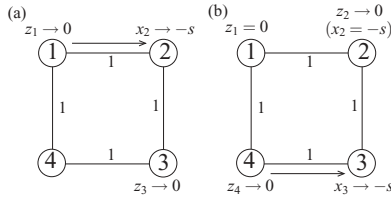
FIG. 6. CC protocol in an encoded (3,4) ring state. All players start with $z = s$. Dependence on the label s can be shuffled such that any two (a) nonadjacent or (b) adjacent parties are independent of the label. Note that the the shuffling in (b) occurs after first performing that in (a).

4. (3,5) CC protocol in the ring state

We can implement a (3,5) protocol using a five-vertex ring-shaped encoded graph state with weight-1 edges, as shown in Figs. 7 and 8, setting $m_i = 0$ for all i and $z_i = s$ for all i, so again a K_i measurement yields ω^{-s} for all i and, for example, $K_2 = Z_1 X_2 Z_3$ so players 1, 2, and 3 (hence any three adjacent parties) can measure s.

The other possibility is where only two of three players are adjacent, e.g., 1, 2, and 4. For the ring state we have

$$K_i = X_i Z_{i+1} Z_{i-1} \tag{29}$$

so

$$K_1 K_2 K_4^{-1} = X_1 Z_2 X_2 Z_4 X_4^{-1}, \tag{30}$$

which can be measured by players 1, 2, and 4, giving ω^{-s}. Hence any three parties can recover s.

In the five-qudit ring state we can always renumber the parties such that for two parties i and j, $i + 1 \leqslant j \leqslant i + 2$. In this case i and j can shuffle their s dependence to the parties $i - 1$ and $j + 1$; hence two players are not sufficient to recover s.

B. The CQ scheme

As in Ref. [6], we implement CQ schemes by performing a quantum key distribution (QKD) protocol, wherein the dealer and a subset of the players end up securely sharing a *random* secret dit s. This shared random classical information can then be used by these parties to securely share any *specified* secret of the same length via standard classical cryptography protocols.

We implement such QKD protocols in graph states by having the dealer distribute the players' qudits to them over public channels, after which the dealer and the players
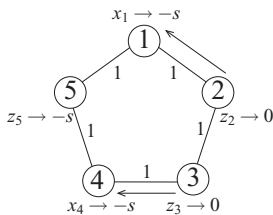

FIG. 7. CC protocol for an encoded (3,5) ring state. All players start with $z = s$. Dependence on the label s can be shuffled such that any two adjacent parties are independent of s (see Fig. 8 for nonadjacent parties).
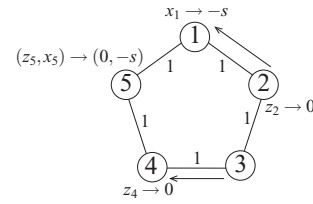
measure their own qudits using bases chosen at random. After measurement the dealer and players publicly announce their bases and retain their measurement results only for certain combinations of chosen bases, such that m of the players may collaborate to obtain a classical secret shared with the dealer.

The CQ protocols we have found follow a pattern whereby the result of the dealer's measurement is a projection of the resultant reduced graph into a labeled state whose labels are correlated with the dealer's measurement and for which the players can perform a CC protocol. As in Ref. [6], our protocol is based on that of Hillery, Bužek, and Berthiaume [3] and has the same limitation of being secure against certain classes of attack such as intercept-resend attacks by an eavesdropper or certain classes of attack by dishonest participants [3] but not against all attacks by dishonest participants [29]. Additionally, we do not consider the case of noisy channels, although existing protocols which do [30] could potentially be adapted to our model.

1. (n,n) CQ protocol in the extended tree state

We can construct an (n,n) CQ protocol using an "extended" tree state, consisting of an n-party tree state (as in the CC protocol) with the dealer's qudit connected to player 1's qudit by a weight-1 edge and all labels set to 0, as illustrated in Fig. 9. This graph state therefore has stabilizers

$$K_D = X_D Z_1 \tag{31}$$

$$K_1 = Z_D X_1 \prod_{i \neq 1} Z_i \tag{32}$$

$$K_i = X_i Z_1 \quad (i \neq 1). \tag{33}$$

In our protocol, the dealer and the players $1, \ldots, n$ each independently randomly choose a value $t_D, t_1, \ldots t_n \in \mathbb{F}_d$. The dealer then measures her qudit in the basis $X^{t_D} Z$ and player 1 measures $X Z^{t_1}$, whereas the remaining players i each measure $X^{t_i} Z$.
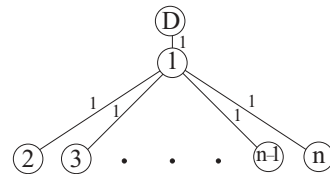

FIG. 9. The "extended" tree state used for the CQ protocol. Local measurement on the dealer's qudit produces a reduced state of the form of that in Fig. 4 (although with an additional $m = t_D$ label on vertex 1).

If the dealer's measurement result is ω^s then, from Proposition 1, the reduced state of the remaining n parties is the nGHZM state (without the additional dealer's vertex), still with weight-1 edges. The only relabeled vertex is that of player 1, with $z_1 = s$, $m_1 = t_D$. All other labels remain zero. The reduced graph therefore has stabilizers

$$k_1 = (XZ^{t_D})_1 Z_2 \cdots Z_n \tag{34}$$

$$k_i = Z_1 X_i, \quad i \neq 1 \tag{35}$$

(here and henceforth we use k_i to denote reduced-state stabilizers and K_i for the full state including the dealer). Furthermore, the labeling is such that the reduced state has eigenvalue 1 for all the stabilizers with $i \neq 1$. Thus any product of stabilizers $k_1 k_2^{l_2} \cdots k_n^{l_n}$ will have eigenvalue ω^{-s}. As

$$\left(XZ_1^t\right)_1 \prod_{i \neq 1} (X^{t_i} Z)_i = k_1 k_2^{t_2} \cdots k_n^{t_n} Z_1^{(t_D - t_1 + \sum_{i \neq 1})} \tag{36}$$

the players measure such a product (and hence are able to recover s) if $t_1 = t_D + t_2 + \cdots + t_n$, which occurs with probability $1/d$.

Security against an eavesdropper having tampered with the qudits (e.g., an intercept-resend attack) is established by noting that the combination of the player and dealer's measurements satisfies

$$(X_{t_D} Z)_D \left(XZ_1^t\right)_1 \prod_{i \neq 1} (X^{t_i} Z)_i = K_D^{t_D} K_1 K_2^{t_2} \cdots K_n^{t_n}, \tag{37}$$

i.e., the players and dealer can also combine their measurement statistics for the various values of t_i to measure the stabilizers of, and hence verify, the original state.

2. (2,3) CQ protocol

We can construct a (2,3) CQ protocol through extending the CC case by attaching the dealer's qudit to those of players 2 and 3 with weights of 2 and 1 respectively and setting all labels to zero, as illustrated in Fig. 10. The stabilizers for this state are

$$K_D = X_D Z_2^2 Z_3, \tag{38}$$

$$K_1 = X_1 Z_2 Z_3, \tag{39}$$

$$K_2 = Z_D^2 Z_1 X_2, \tag{40}$$

$$K_3 = Z_D Z_1^2 X_3. \tag{41}$$

The dealer randomly selects a variable $t_D \in \mathbb{F}_d$ and measures $X^{t_D} Z$ and obtains result ω^s. The resultant graph states are given by Proposition 5, as shown in Fig. 10(b), with stabilizers
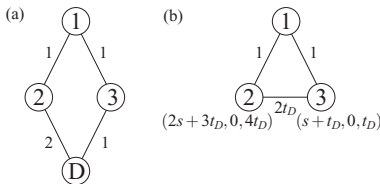
$$k_{1,t_D} = X_1 Z_2 Z_3, \tag{42}$$

FIG. 10. (a) The "extended" (2,3) state used for the CQ protocol. Local measurement on the dealer's qudit produces a reduced state of the type in (b).

$$k_{2,t_D} = Z_1 X_2 Z_2^{4t_D} Z_3^{2t_D}, \tag{43}$$

$$k_{3,t_D} = Z_1 Z_2^{2t_D} X_3 Z_3^{t_D}. \tag{44}$$

We now need to see how sets of players can or cannot access the random value s of the dealer's measurement result. First, for any choice of t_D, no single player can access s by application of Proposition 3 to Fig. 10(b). To see how any pair can access the dealer's result, we must address each measurement parameter t_D and resultant graph separately and see which measurement the players would ideally make. In the protocol, any given authorized set of players then choose randomly one of these possible measurements, which sometimes match that of the dealer and enable this set of players to access the secret and in addition provide security by effectively measuring a stabilizer of the total state Fig. 10(a).

We now go through how each pair can access s if the dealer measures as above. Players 1 and 2 can access the dealer's result by measuring

$$k_{1,t_D}^{-2t_D} k_{2,t_D},$$

allowing them to obtain $\omega^{-(2s+3t_D)}$. Players 1 and 3 would measure

$$k_{1,t_D}^{-2t_D} k_{3,t_D},$$

allowing them to obtain $\omega^{-(s+t_D)}$. Players 2 and 3 would measure

$$k_{2,t_D} k_{3,t_D}^{-1},$$

allowing them to obtain $\omega^{-(s+2t_D)}$.

In this protocol, each authorized set will measure randomly from one of the three possible measurements corresponding to t_D. For example, if players 1 and 2 decide to work together to obtain the secret, they will randomly measure

$$k_{1,t_D'}^{-2t_D'} k_{2,t_D'}$$

by choosing their random variable t_D' (agreed between players 1 and 2). By definition of the stabilizers these do not commute, hence cannot be measured simultaneously. Their measurements will coincide with the dealer's when $t_D' = t_D$, which happens with probability $1/d$. After announcing the bases they can then throw away all results that do not coincide.

Security can be proven by noting that including the dealer's measurement results allows the dealer plus an authorized set to simulate measurement of stabilizers of the original graph Fig. 10(a). An additional subtlety of simulating measurements locally in the qudit case, as apposed to the qubit case, is that there is more than one possible commuting Pauli. Any local extended Pauli on a qudit i, O_i, commutes with all powers of this Pauli operator O_i^m, which means they share common eigenbases. Further, as there are no degeneracies, the eigenvalues are just a reordering. Thus, if measuring O_i yields result ω^s, we know that, even without doing any further measurement, O_i^m would give result ω^{ms}. In this way, we can simulate any power of a Pauli O_i^m just by measuring O_i.

In the protocol, some of the sifted key would be sacrificed now to check the security by announcing some randomly chosen results. If we again look at players 1 and 2, for example, by combining their results with those of the dealer,

they can simulate measuring stabilizers K_i of the original state [Fig. 10(a)], Eqs. (42)–(44), since

$$K_D^{2t_D} K_1^{-2t_D} K_2 = \omega^{3t_D} \left(X_D^{t_D} Z_D \right)^2 k_{1,t_D}^{-2t_D} k_{2,t_D}. \tag{45}$$

If there has been no interference from an eavesdropper, they will all measure outcome 1 for, with high probability given a large number of announced results, every value of t_D. Although this outcome is not enough to guarantee that the state before measurement was the state of Fig. 10(a), it restricts the allowed space to that which guarantees security as follows: If g is the subgraph got by removing player 3 and all its edges from Fig. 10(a), having eigenvalue 1 for all these stabilizers implies that the state of the dealer plus players 1 and 2 is in the subspace spanned by $\{g_{z=(i,i,0)}\}$, i.e., where players 1 and 2 have $z_1 = z_2$ and players 3 has $z_3 = 0$. Thus, the most general state including an eavesdropper E can be written

$$\sum_i \alpha_i |i\rangle_E |g_{z=(i,i,0)}\rangle_{D,1,2}. \tag{46}$$

It can then be checked that the reduced density matrix of the dealer and the eavesdropper is

$$\rho_{ED} = \rho_E \otimes \mathbb{1}_D/d, \tag{47}$$

which implies that the eavesdropper cannot share any information about the dealer's results. It can similarly be checked for pairs of players 2 and 3 and then 1 and 3.

3. (3,5) CQ protocol

We can construct a (3,5) CQ protocol by extending the CC case by attaching the dealer's qudit to each player with weight one edges, and all labels set to zero, as illustrated in Fig. 11. The stabilizers for this state are

$$K_D = X_D Z_1 Z_2 Z_3 Z_4 Z_5 \tag{48}$$

$$K_1 = Z_D X_1 Z_2 Z_5 \tag{49}$$

$$K_2 = Z_D Z_1 X_2 Z_3 \tag{50}$$

$$K_3 = Z_D Z_2 X_3 Z_4 \tag{51}$$

$$K_4 = Z_D Z_3 X_4 Z_5 \tag{52}$$

$$K_5 = Z_D Z_1 Z_4 X_5 \tag{53}$$

The dealer randomly selects a variable $t_D \in \mathbb{F}_d$ and measures $X^{t_D} Z$ and obtains result ω^s. The resultant graph states are shown in Fig. 12. The associated stabilizers of player i are denoted k_{i,t_D}.

First we check that each pair of players cannot access s without collaborating with the others. From Proposition 3, players 1 and 2 cannot access the dealer's result (the secret) as
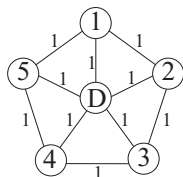

FIG. 11. The "extended" (3,5) state used for the CQ protocol. Local measurement on the dealer's qudit produces a reduced state of the type in Fig. 12.
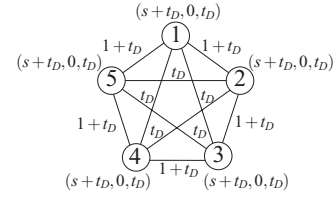

FIG. 12. Resultant state from the dealer's local measurement on Fig. 11.

explicitly by application of the stabilizers

$$k_{4,t_D}^{-(1+st_D^{-1})}$$

(shuffling from player 1 to 4) if $t_D \neq 0$ or

$$k_{3,t_D}^{-s} k_{5,t_D}^{-s}$$

(shuffling from 1 to 5 and 2 to 3) if $t_D = 0$. We can see that players 1 and 3 cannot access s since the dependence can be removed by application of

$$k_{2,t_D}^{-(s+t_D)(1+t_D)^{-1}}$$

(shuffling from 1 to 2) if $t_D + 1 \neq 0$ or

$$k_{4,t_D}^{-(1+st_D^{-1})} k_{5,t_D}^{-(1+st_D^{-1})}$$

(shuffling from 3 to 4 and 1 to 5) if $t_D + 1 = 0$. By symmetry no pair alone can access s.

We now see how any three players can access the secret for a given t_D. Players 1, 2, and 3 can do so by measuring

$$k_{1,t_D}^{-t_D} k_{2,t_D}^{1+2t_D} k_3^{-t_D},$$

yielding result $\omega^{-(s+t_D)}$. Players 1, 3, and 4 can do so by measuring

$$k_{1,t_D}^{-(1+2t_D)} k_{3,t_D}^{1+t_D} k_{4,t_D}^{1+t_D},$$

yielding result $\omega^{-(s+t_D)}$. By symmetry any three players can therefore find s.

In this protocol, any set of authorized players measures randomly in accordance with these procedures. For example players 1, 2, and 3 will randomly measure stabilizers

$$k_{1,t_D'}^{-t_D'} k_{2,t_D'}^{1+2t_D'} k_3^{-t_D'},$$

by choosing a shared random variable t_D'. Security is then checked by verifying that the eigenequations are satisfied by the dealer and the player by communicating results to simulate measurement of a subset of stabilizers. For example, the dealer plus players 1, 2, and 3 can, by comparing results, calculate what would have been the measured value for the stabilizers [of the original graph, Fig. 11, Eqs. (48)–(53)], because

$$K_D^{t_D'} K_1^{-t_D'} K_2^{1+2t_D'} K_3^{-t_D'} = \omega^{t_D'} X_D^{t_D'} Z_D k_{1,t_D'}^{-t_D'} k_{2,t_D'}^{1+2t_D'} k_3^{-t_D'}. \tag{54}$$

If the eigenvalue is 1 for all of these (as should be the case; if not the protocol restarts), this implies the joint state of the dealer plus players 1, 2, and 3 is in the subspace spanned by $\{|g_{z=(i+j,i,0,j)}\rangle_{D,1,2,3}\}$. As for the (2,3) case, this implies that, for the most general state of an eavesdropper E and dealer, their reduced density matrix is of the form

$$\rho_{E,D} = \rho_E \otimes \mathbb{1}_D/d; \tag{55}$$

hence the eavesdropper's state is completely uncorrelated with the dealer's measurement result and therefore uncorrelated with the secret. Security can similarly be checked for all sets of three or more players.

C. The QQ scheme

The QQ scheme proposed in Ref. [6] is readily generalizable to qudits. This protocol is similar to the CQ scheme, but the secret to be shared is now a quantum state $|s\rangle$ in a d-dimensional Hilbert space, initially possessed by the dealer, who distributes it to the other parties via a joint operation on the secret state and the parties' shared graph state, in a manner analogous to quantum teleportation. We describe the general protocol explicitly below.

Denoting the dealer's secret qudit as

$$|s\rangle_D = \sum_{i=0}^{d-1} \alpha_i |i\rangle_D, \qquad (56)$$

the dealer prepares the state

$$|s\rangle_D |G\rangle_{D,V} \qquad (57)$$

corresponding to some graph state G for the dealer's qudit D and all the players' qudits V. The dealer distributes the players' qudits to them (over perfect quantum channels, which we can assume to be public). The dealer then measures her two qudits in the generalized Bell basis [31] $\{|\psi_{mn}\rangle\}$, where

$$|\psi_{mn}\rangle := \frac{1}{\sqrt{d}} \sum_j \omega^{jn} |j\rangle |j+m\rangle. \qquad (58)$$

If the dealer's measurement result is (m,n), corresponding to the state $|\psi_{mn}\rangle$, then it follows from our rules for projective measurement that the resultant state for all parties is

$$|\psi_{mn}\rangle_D \langle \psi_{mn}||s\rangle_D |G\rangle_{D,V}$$
$$\propto |\psi_{mn}\rangle_D \sum_j \alpha_j \omega^{-jn} \big| g_{z=(j+m)(A_{D1}, A_{D2}..., A_{DN})} \big\rangle_V, \qquad (59)$$

where $|g_z\rangle$ is the encoded reduced graph state on the players $1, \ldots, n$ with labels z.

If the dealer informs the players of their measurement result (m,n), then a set of players $\in V$ (including some player a with $N_{Da} \neq 0$) can apply a correction operator

$$U_{mn} := K_a^{-nN_{Da}^{-1}} Z^{-mA_D} \qquad (60)$$

to obtain the state

$$|s_g\rangle^V = \sum_j \alpha_j \big| g_{z=j(A_{D1}, ... A_{DN})} \big\rangle_V. \qquad (61)$$

The access properties of this final state depend on the graph state used. Qualitatively, for certain initial graph states, the state $|s_g\rangle^V$ can be regarded as a superposition (with coefficients corresponding to those of the encoded secret) of orthogonal labeled graph states whose labels have the same access structure as CC protocols. Thus, the ability to recover the quantum secret corresponds to the ability to recover these classical labels, providing a natural extension of the classical protocols to the quantum case.

However, the above reasoning does not guarantee that such a QQ protocol will have the same adversary structure as the corresponding CC protocol, as seen below, where we achieve "perfect" threshold schemes in the (2,3) and (5,3) cases, but fewer than n players can still obtain some secret information in the (n,n) case.

1. (n,n) QQ protocol using the nGHZM state

If the joint graph state of the dealer and players $|G\rangle$ is the same as for the CQ scheme (i.e., an nGHZM state with an additional dealer's vertex, connected to player 1, and all labels set to zero), then the final players' state is

$$|s_g\rangle_V = \sum_j \alpha_j |g_{z=(j,0,...,0)}\rangle_V, \qquad (62)$$

where V is the set of all players. The $|g\rangle$ states, in the form of nGHZM states with a label on player 1's vertex, are the same as those used in the (n,n) CC protocol, to which the access properties described in Sec. III A 1 apply, and fewer than n players cannot perfectly reconstruct the secret.

However, we note that the reduced states of fewer than n players are not independent of the α_j. For example, in the analogous qubit protocol [6] we can, in some basis (depending on the player), express the reduced state of a single player as diag($|\alpha_0 + \alpha_1|^2, |\alpha_0 - \alpha_1|^2$). Thus this (n,n) protocol is not a "perfect" threshold scheme; it allows some incomplete information to be accessed by fewer than n players. However, the secret qudit is clearly encoded within the state of the n players and so may be accessed by all players by performing joint quantum operations. Furthermore, the secret can be isolated to any individual player through LOCC as follows.

For any player i other than player 1, the secret can be isolated by player 1 measuring X and the rest of the players other than i measuring Z, which is evident by rewriting the state as

$$|s_g\rangle_V = \sum_j |g_{z=(j,0,...,0)}\rangle_{V \setminus v_i} \left(\sum_k \alpha_k |j-k\rangle_i \right). \qquad (63)$$

The secret can be isolated to player 1 by every player other than 1 measuring Z, thereby producing the state

$$|s'_g\rangle_V = \sum_{k_2} \cdots \sum_{k_n} \sum_j \alpha_j \overline{|-(j+k_2+\cdots+k_n)\rangle_1}$$
$$\times |k_2\rangle_2 \cdots |k_n\rangle_n. \qquad (64)$$

Thus the quantum secret requires collaboration by all n players (and no fewer) to recover but the players may collaboratively make the secret locally accessible to a single player if they so wish.

2. (2,3) QQ protocol

We can construct a (2,3) QQ protocol by teleporting the secret qudit (56) into the extended graph state of Fig. 10. The encoded state is

$$|s_g\rangle_V = \sum_{j=0}^{d-1} \alpha_j |g_{z=j(0,2,1)}\rangle \qquad (65)$$

for g the (unlabeled) graph in Fig. 5. The state (65) can be rewritten as

$$|s_g\rangle_V = \frac{1}{\sqrt{d}} \sum_{j,k=0}^{d-1} \alpha_j |k\rangle_1 |\overline{2j+k}\rangle_2 |\overline{j+k}\rangle_3$$

$$= \frac{1}{\sqrt{d}} \sum_{j,M=0}^{d-1} \alpha_j |M-j\rangle_1 |\overline{M+j}\rangle_2 |\overline{M}\rangle_3, \quad (66)$$

where $M = j + k$.

For $d = 3$ this state corresponds exactly to the (2,3) qutrit code presented in Ref. [4]. Any pair of players can thus access the secret, and any single player cannot. For example, players 1 and 2 perform control operations that add the value of the first register (without an overbar) to the second register (with an overbar) and then $-\frac{1}{2}$ times the value of the second to the first (again, keeping the first register nonbarred and the second always barred). This leaves the resultant state as

$$\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \alpha_j |-j\rangle_1 \sum_{M=0}^{d-1} |\overline{2M}\rangle_2 |\overline{M}\rangle_3. \quad (67)$$

Any pair can similarly obtain the secret. Since single players form complementary sets to pairs of players, it follows from information gain implying disturbance [4] (and can be shown explicitly) that no single player can obtain any information about the secret, so this is a perfect threshold scheme.

3. (3, 5) QQ protocol

We can construct a (3,5) QQ protocol by teleporting the secret qudit into the extended graph state of Fig. 11. The encoded state is then

$$|s_g\rangle_V = \sum_{j=0}^{d-1} \alpha_j |g_{z=(j,j,\ldots j)}\rangle \quad (68)$$

where g is the (unlabeled) graph of Fig. 7. The state can be rewritten as

$$|s_g\rangle_V = \frac{1}{d} \sum_{x,y=0}^{d-1} |x\rangle_1 |y\rangle_2$$

$$\times \left(\sum_{j=0}^{d-1} \alpha_j \omega^{j(x+y)+xy} |h_{z=(j+x,j,j+y)}\rangle_{3,4,5} \right), \quad (69)$$

where h is the subgraph corresponding to players 3, 4, and 5 taken by removing all other vertices and their edges. The fact that each vector z occurs only once means that players 3, 4, and 5 can always measure in such a way to project them only onto the a subspace corresponding to some $|xy\rangle_{1,2}$. Each would occur with equal probability of $1/d^2$.

If, for example, their measurements put them onto the $|h_{z=(j,j,j)}\rangle_{3,4,5}$ subspace (corresponding to $x = y = 0$), they know from the above that they would obtain the state

$$\sum_{j=0}^{d-1} \alpha_j |h_{z=(j,j,j)}\rangle_{3,4,5}, \quad (70)$$

hence would have the secret encoded into the graph state $|h\rangle$. Suitable global operations could then be used to map the

state onto any subsystem they liked. For example, performing $(C_{ab})^{-1}$ between players 3 and 4, as well as between players 4 and 5, gives the state

$$\sum_{j=0}^{d-1} \alpha_j |\bar{j}\rangle_3 |\bar{j}\rangle_4 |\bar{j}\rangle_5. \quad (71)$$

Players 3 and 4 can measure in their respective Z bases to shuffle the information to player 5. Similarly it can be shuffled to any player.

To see how players 2, 4, and 5 can access the secret qutrit, we rewrite the state as

$$|s_g\rangle_V = \frac{1}{d} \sum_{x,y=0}^{d-1} |x\rangle_1 |y\rangle_2$$

$$\times \left(\sum_{j=0}^{d-1} \alpha_j \omega^{j(x+y)} |h_{z=(j+x+y,j+x,j+y)}\rangle_{2,4,5} \right), \quad (72)$$

where h is the subgraph of players 2, 4, and 5 found by removing all other vertices and their edges. Each possible vector z occurs only once in this expansion. By the same tactics players 2, 4, and 5 can access the secret. By symmetry, any three can access the secret. As with the (2,3) case, perfect secret recovery by three players requires that the complementary sets of two players cannot obtain any information about the secret (as can also be shown explicitly), so this is a perfect threshold scheme.

We note that the existence of a (3,5) QQ protocol in graph states of arbitrary dimension has been implied by the work of Gheorghiu, Looi, and Griffiths [32], who showed that encoded information can be isolated to three of the five qudits in a graph state.

IV. CONCLUSION

We have developed a unified framework for the three types of secret sharing in prime-dimensional Hilbert space. Our formalism uses prime-dimensional graph states, analogous to those in the qubit case, and our protocols allow sharing of classical "dits" and prime-dimensional quantum states as secrets. Our protocols include the case of (2,3) sharing, which was not achievable in the qubit formalism in addition to higher-dimensional analogs of qubit protocols. Our work provides a useful step toward describing schemes sharing classical and quantum secrets of any size within a graph-state formalism for general physical systems.

Our work suggests several areas for further research. Still open are the questions of whether any achievable threshold secret-sharing scheme can be constructed within our formalism, and, if so, what the associated graph states and protocols would be. If prime-dimensional systems are not sufficient to construct any scheme, it is possible that an analogous formalism involving states of any dimension might allow for a richer array of protocols, as we have shown occurs when moving beyond the qubit case. Generalizing to the case of arbitrary d is thus another promising area for further work, and some of the methods described in Ref. [32] (which considers such general graph states) may be useful here.

With regard to achieving arbitrary threshold schemes, we additionally note that the graph state formalism can in principle

be used for sharing of quantum secrets for arbitrary access structures. This property of the formalism stems from the fact that schemes exist for arbitrary access structures using high-dimensional stabilizer states [4,5] and that it can be shown that all stabilizer states are locally equivalent to qudit graph states [14,33]. However, there is no explicit procedure for converting these schemes to graphs, and further, it is not immediately clear that they can also be used for sharing classical secrets (though it seems very likely). Developing such a procedure would provide a graph state formalism for arbitrary access structures in quantum secret sharing, although it may not be equivalent to that in our current work.

There are also several possible extensions to the analysis of CQ protocols within our formalism: considering more general attacks involving dishonest participants, the presence of channel noise, and the overall efficiency of the protocol; i.e., the need to discard states when the participants' bases do not match. It is an open question which graph states would produce the highest key rates (and hence secret-sharing rates) per state within our formalism.

Further generalization may allow a wide range of secret-sharing schemes to be described in this intuitively appealing way.

ACKNOWLEDGMENTS

[1] A. Shamir, Commun. ACM **22**, 621 (1979).

[2] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. (Wiley, New York, 1996).

[3] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[4] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[5] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[6] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[7] B. Schoenmakers, in *Advances in Cryptology - CRYPTO '99 Proceedings*, Lecture Notes in Computer Science, Vol. 1666, edited by M. Wiener (Springer, New York, 1999), p. 148.

[8] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, in *Quantum Computers, Algorithms and Chaos, Proceedings of the International School of Physics Enrico Fermi Vol. 162*, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS Press, Amsterdam, 2006).

[9] E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix, Elec. Proc. Theor. Comp. Sci. **9**, 87 (2009).

[10] J. S. Shaari, M. R. B. Wahiddin, and S. Mancini, Phys. Lett. A **372**, 1963 (2008).

[11] X. Chen, H. Chung, A. W. Cross, B. Zeng, and I. L. Chuang, Phys. Rev. A **78**, 012353 (2008).

[12] J. Niset, J. Fiurášek, and N. J. Cerf, Phys. Rev. Lett. **102**, 120501 (2009).

[13] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, IEEE Trans. Inf. Theory **52**, 4892 (2005).

[14] M. Bahramgiri and S. Beigi, e-print arXiv:quant-ph/0610267 (2006).

[15] J. Benaloh and J. Leichter, in *Advances in Cryptology - CRYPTO '88 Proceedings*, Lecture Notes in Computer Science, Vol. 403, edited by S. Goldwasser (Springer, Berlin, 1990), p. 27.

[16] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[17] D. Gottesman, Ph.D. thesis, Caltech, 1997, e-print arXiv:quant-ph/9705052.

[18] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[19] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **78**, 042303 (2008).

[20] S. Beigi, I. Chuang, M. Grassl, P. Shor, and B. Zeng, e-print arXiv:0910.4129.

[21] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **78**, 042303 (2008).

[22] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature **434**, 169 (2005).

[23] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, Nat. Phys. **3**, 91 (2007).

[24] J. Patera and H. Zassenhaus, J. Math. Phys. **29**, 665 (1988).

[25] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).

[26] S. D. Bartlett, H. de Guise, and B. C. Sanders, Phys. Rev. A **65**, 052316 (2002).

[27] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[28] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).

[29] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[30] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).

[31] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[32] V. Gheorghiu, S. Y. Looi, and R. B. Griffiths, Phys. Rev. A **81**, 032326 (2010).

[33] D. Schlingemann, Quantum Inf. Comput. **2**, 307 (2002).