


Communication efficient quantum secret sharing

Kaushik Senthoo and Pradeep Kiran Sarvepalli

Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai 600 036, India

 (Received 16 May 2019; published 11 November 2019)

A quantum secret sharing scheme is a cryptographic protocol by which a dealer can share a secret among a group of n players so that only certain subsets of players can recover the secret by collaboration. In this paper we propose communication efficient quantum threshold secret sharing schemes. They minimize the amount of quantum communication required to reconstruct the secret when more than the necessary number of players collaborate. They are based on a class of staircase codes proposed by Bitar and El Rouayheb. In a standard $((k, n))$ quantum threshold scheme, any subset of k or more players can recover the secret. The quantum communication cost for reconstruction in such schemes is k qudits for each secret qudit. Using the proposed construction, any subset of $d \geq k$ players can also collaborate to recover the secret with a communication cost of d qudits for $d - k + 1$ secret qudits. In other words, for the proposed schemes the quantum communication cost is only $\frac{d}{d-k+1}$ qudits for every secret qudit. For $d > k$, proposed schemes are communication efficient with respect to standard schemes; and when $d = 2k - 1$, the quantum communication cost is reduced by a factor $O(k)$. Further, when $n = 2k - 1$, the proposed schemes have optimal communication cost for secret reconstruction.

DOI: [10.1103/PhysRevA.100.052313](https://doi.org/10.1103/PhysRevA.100.052313)

I. INTRODUCTION

Quantum information enables cryptographic protocols that are much more secure than their classical counterparts. The most prominent example is that of quantum key distribution [1–3]. In recent years there has been significant research in other cryptographic protocols such as quantum secure direct communication [4,5], quantum private query [6,7], quantum secret sharing [8–15], and many more. See the survey articles [16–18] and references therein for more details.

A quantum secret sharing (QSS) scheme is a protocol by which a dealer can distribute an arbitrary secret state (in an encoded form) among n participants so that only authorized subsets of participants can reconstruct the secret. The secret can be a classical state as in [8] or quantum state as in [9,10]. The states distributed to the participants are called shares. Following the distribution of the secret by the dealer, certain subsets of the participants can, at a later time, recover the secret.

A subset of parties that can reconstruct the secret is called an authorized set. Any subset of parties that has no information about the secret is called an unauthorized set. In this paper we are only interested in perfect secret sharing schemes where a subset is either authorized or unauthorized. In the reconstruction phase, the participants of an authorized set pool their shares together and recover the secret. Alternatively, the participants could communicate their shares to a third party or user, called the combiner, whose job is to recover the secret from the data communicated to the combiner. In this model, a metric of interest is the amount of communication between the participants and the combiner. The amount of communication from the participants to the combiner is called the communication cost. In this paper we focus on reducing the quantum communication cost during recovery.

In this paper we initiate the study of communication efficient quantum secret sharing schemes for quantum secrets, opening a new avenue for further research in quantum secret sharing. We propose schemes which aim to minimize the communication cost of QSS schemes. While the problem of communication cost in classical secret sharing schemes was studied previously, see [19–24], the corresponding problem for quantum secret sharing schemes has not been studied thus far. Quantum secret sharing has become experimentally viable and there are many demonstrations; see, for instance, [25–32]. However, quantum information is still an expensive resource, and clearly, we would like to reduce the cost of storing and transmitting it. Our results should be of interest to experimentalists as well.

The collection of authorized sets is called the access structure (denoted as Γ) of the secret sharing scheme. We focus on an important class of QSS schemes, namely, the $((k, n))$ quantum threshold schemes (QTSs) where $n \leq 2k - 1$ and any subset of t participants with $k \leq t \leq n$ can reconstruct the secret.

Contributions. Based on the staircase codes proposed by Bitar and El Rouayheb [19], we propose a class of quantum threshold secret sharing schemes that are also communication efficient. In the standard model of quantum secret sharing, sharing a secret of one qudit using a $((k, 2k - 1))$ threshold scheme requires k qudits to be communicated to reconstruct the secret. In the proposed schemes, we can recover the secret of $m = d - k + 1$ qudits by communicating d qudits where $k \leq d \leq 2k - 1$, in average $\frac{d}{d-k+1}$ qudits for every qudit in secret. Note that d is fixed and m is dependent on the choice of d . Further, we show that these schemes are optimal with respect to communication cost in the given model of quantum secret sharing. When $d = k$, the proposed schemes reduce to the standard quantum threshold schemes.

Previous work. The closest work related to ours appears to be that of [33] who also aimed at reducing the communication cost in quantum secret sharing schemes. However, there are important differences: their work uses a combination of nonperfect secret sharing schemes along with a hybrid QSS scheme. A hybrid QSS scheme is one in which participants have (partly or wholly) classical shares. Our schemes in contrast are purely quantum in that no share is classical. The work in [33] is concerned with the communication cost of the secret sharing schemes during distribution of the (encoded) secret more than the cost during reconstruction, which is our focus here.

Our results have a bearing on hybrid schemes also. The schemes we propose here can be adapted to improve the quantum communication cost of hybrid schemes. Since a hybrid scheme consists of both classical and quantum components, we might expect that in general that a fully quantum version of the scheme would be much more secure than the hybrid version. For instance, one of the components of the hybrid secret sharing scheme in [33] is a classical secret sharing scheme. We can replace this classical component by quantum secret sharing giving us a much more secure protocol.

Scope of the work. In this paper we focus on reducing the quantum communication cost for the recovery of the secret. Other metrics such as the cost of distributing the shares, classical communication, and computational costs due to encoding and reconstruction of the secret are not considered in this paper. We also do not consider eavesdropping detection.

The quantum communication cost during the share distribution stage of the proposed schemes is the same as that of standard QSS schemes such as [9,10]. Since the proposed schemes do not involve any classical shares, they do not incur any classical communication cost. The encoding complexity of our schemes is comparable to that of the standard schemes in [9]. The decoding complexity is also comparable to that of the scheme in [9] when we use minimal authorized sets for recovery. However, while using nonminimal authorized sets, we expect the decoding complexity to be lower than that of standard threshold schemes.

Our paper is organized as follows. In Sec. II, we provide the intuition behind our protocol by considering a simple example that illustrates how standard QSS schemes can be improved with respect to their communication cost. Then in Sec. III, we give the proposed schemes. In Sec. IV, we prove the optimality of the proposed schemes and conclude in Sec. V.

II. MOTIVATING EXAMPLE

The intuition behind the communication efficient secret sharing schemes lies in using a nonminimal authorized set to recover the secret. (An authorized set is said to be a minimal authorized set if every proper subset of the authorized set is unauthorized.)

Let \mathbb{F}_q denote the finite field with q elements. Consider the ternary ((2,3)) quantum threshold scheme proposed by Cleve *et al.* [9]. In this scheme, the secret state $s \in \mathbb{F}_3$ is encoded into three qudits as

$$|s\rangle \mapsto \frac{1}{\sqrt{3}} \sum_{r=0}^2 |r\rangle_A |s+r\rangle_B |2s+r\rangle_C, \tag{1}$$

where one qudit each is given to parties A , B , and C . (The notation $|i\rangle |j\rangle$ stands for the tensor product $|i\rangle \otimes |j\rangle$.) In order to reconstruct the secret we need to communicate two qudits to the combiner.

We propose an alternate ((2,3)) quantum threshold scheme where we can obtain better communication costs. In this scheme, the secret is an arbitrary state from a Hilbert space of dimension nine. For each basis state $|s_1, s_2\rangle$ where $(s_1, s_2) \in \mathbb{F}_3^2$, the encoding is as follows:

$$|s_1, s_2\rangle \mapsto \sum_{r_1, r_2 \in \mathbb{F}_3} |s_1 + r_1, r_2\rangle_A |s_2 + r_1, r_1 + r_2\rangle_B |s_1 + s_2 + r_1, r_1 + 2r_2\rangle_C, \tag{2}$$

where we have ignored the normalizing factors and the tensor product $|i\rangle \otimes |j\rangle$ is also written as $|i, j\rangle$ or one above the other as $\begin{smallmatrix} |i\rangle \\ |j\rangle \end{smallmatrix}$. In this scheme, the secret of two qudits is encoded into six qudits, equivalently each secret qudit is encoded into three qudits as in the scheme of [9], see Eq. (1).

Let us look at the reconstruction of the secret from the four qudits of the first two participants A and B from the state as given in Eq. (2). The reconstruction steps are similar for other choices of two participants as well. (Values of qudits which have changed after each operation are indicated in bold.)

In the secret recovery, we need the generalized CNOT gate, namely, the ADD gate, see [34], defined as follows:

$$\text{ADD } |i\rangle_c |j\rangle_t \rightarrow |i\rangle_c |i+j\rangle_t. \tag{3}$$

The inverse of this gate is denoted ADD^\dagger and it acts as follows:

$$\text{ADD}^\dagger |i\rangle_c |j\rangle_t \rightarrow |i\rangle_c |j-i\rangle_t, \tag{4}$$

If we apply ADD^\dagger on the second qudits of A and B , i.e., $\text{ADD}^\dagger |r_2\rangle_A |r_1+r_2\rangle_B$ we obtain the following state:

$$\sum_{r_1, r_2 \in \mathbb{F}_3} |s_1 + r_1, r_2\rangle_A |s_2 + r_1, \mathbf{r}_1\rangle_B |s_1 + s_2 + r_1, r_1 + 2r_2\rangle_C.$$

Next we apply ADD^\dagger on the second qudit of B and first qudit of A , i.e., $\text{ADD}^\dagger |r_1\rangle_B |s_1+r_1\rangle_A$. This gives us the following state:

$$\sum_{r_1, r_2 \in \mathbb{F}_3} |s_1, r_2\rangle_A |s_2 + r_1, \mathbf{r}_1\rangle_B |s_1 + s_2 + r_1, r_1 + 2r_2\rangle_C.$$

Then we apply ADD^\dagger on the second qudit and first qudit of B , i.e., $\text{ADD}^\dagger |r_1\rangle_B |s_2+r_1\rangle$. This gives the following state:

$$\sum_{r_1, r_2 \in \mathbb{F}_3} |s_1, r_2\rangle_A |s_2, \mathbf{r}_1\rangle_B |s_1 + s_2 + r_1, r_1 + 2r_2\rangle_C.$$

Rearranging the qudits, we obtain

$$|s_1\rangle_A |s_2\rangle_B \sum_{r_1, r_2 \in \mathbb{F}_3} |r_2\rangle_A |r_1\rangle_B |s_1 + s_2 + r_1\rangle_C |r_1 + 2r_2\rangle_C.$$

This does not end the reconstruction process because the information about the secret could still be entangled with the rest of the qudits and we may not be able to recover an arbitrary superposition. Further steps are required to recover an arbitrary secret completely. Let us now apply ADD^\dagger on the

second qudits of A and B , i.e., $|r_2\rangle_A |r_1\rangle_B$. We obtain

$$|s_1\rangle_A |s_2\rangle_B \sum_{r_1, r_2 \in \mathbb{F}_3} |r_2\rangle_A |r_1 + 2r_2\rangle_B |s_1 + s_2 + r_1\rangle_C |r_1 + 2r_2\rangle_C.$$

Next we transform the second qudits of B and A as $\text{ADD } |r_1 + 2r_2\rangle_B |r_2\rangle_A$,

$$|s_1\rangle_A |s_2\rangle_B \sum_{r_1, r_2 \in \mathbb{F}_3} |r_1\rangle_A |r_1 + 2r_2\rangle_B |s_1 + s_2 + r_1\rangle_C |r_1 + 2r_2\rangle_C.$$

Next we transform as $\text{ADD } |s_2\rangle_B |r_1\rangle_A$ followed by $\text{ADD } |s_1\rangle_A |s_2 + r_1\rangle_A$,

$$|s_1\rangle_A |s_2\rangle_B \sum_{r_1, r_2 \in \mathbb{F}_3} |s_1 + s_2 + r_1\rangle_A |r_1 + 2r_2\rangle_B |s_1 + s_2 + r_1\rangle_C |r_1 + 2r_2\rangle_C.$$

Setting $t_1 = s_1 + s_2 + r_1$, we obtain the following state

$$|s_1\rangle_A |s_2\rangle_B \sum_{t_1, r_2 \in \mathbb{F}_3} |t_1\rangle_A |t_1 + 2s_1 + 2s_2 + 2r_2\rangle_B |t_1\rangle_C |t_1 + 2s_1 + 2s_2 + 2r_2\rangle_C.$$

Setting $t_2 = t_1 + 2s_1 + 2s_2 + 2r_2$, we obtain

$$|s_1\rangle_A |s_2\rangle_B \sum_{t_1, t_2 \in \mathbb{F}_3} |t_1\rangle_A |t_2\rangle_B |t_1\rangle_C |t_2\rangle_C.$$

At this point the secret is completely disentangled with the rest of the qudits and the state of the remaining qudits is independent of the secret, thereby ensuring we can recover an arbitrary linear combination of basis states.

Let us recover the secret when we have access to all three participants (they constitute a nonminimal authorized set). We do not need to have access to all six qudits of the participants. We need only the first qudit from each of three participants, see Eq. (2).

First, we apply ADD^\dagger to $|s_2 + r_1\rangle_B |s_1 + s_2 + r_1\rangle_C$ obtaining $|s_2 + r_1\rangle_B |s_1\rangle_C$. Next, we have $\text{ADD}^\dagger |s_1\rangle_C |s_1 + r_1\rangle_A = |s_1\rangle_C |r_1\rangle_A$. Then we transform as $\text{ADD}^\dagger |r_1\rangle_A |s_2 + r_1\rangle_B$, we obtain the following state.

$$\sum_{r_1, r_2 \in \mathbb{F}_3} |r_1, r_2\rangle_A |s_2, r_1 + r_2\rangle_B |s_1, r_1 + 2r_2\rangle_C.$$

Reordering the qudits, we have

$$|s_1\rangle_C |s_2\rangle_B \sum_{r_1, r_2 \in \mathbb{F}_3} |r_1, r_2\rangle_A |r_1 + r_2\rangle_B |r_1 + 2r_2\rangle_C.$$

Once again the secret is completely disentangled from the rest of the system and we are able to recover the secret using only three qudits. However, note that in this case we are able to recover a secret of two qudits. Had we used the ((2,3)) threshold scheme of [9], we would have needed four qudits even when we allow access to all three participants. This example demonstrates we can reduce the number of qudits to be communicated when reconstructing the secret.

III. COMMUNICATION EFFICIENT QSS SCHEMES

A. Preliminaries

To specify a quantum secret sharing concretely, we give the encoding for the basis states of the secret. Linearity can be invoked to encode an arbitrary superposition of basis states.

An encoding \mathcal{E} realizes a perfect quantum secret sharing scheme with access structure Γ if it satisfies the following constraints [26]:

- (i) (Recoverability) Any set in Γ can recover the secret.
- (ii) (Secrecy) Any set not in Γ has no information about the secret.

To show recoverability, we explicitly show that the set can recover the secret. To show secrecy, we show that the complement of the set contains an authorized set. A quantum secret sharing scheme is said to be a pure state scheme if it encodes pure state secrets to global pure states.

Notation. We denote by $((k, n, d))_q$ a q -ary quantum threshold scheme with n participants, where any k participants can recover the secret and d is chosen to be a fixed integer such that $k \leq d \leq n$. If $d = k$, then it is a standard $((k, n))$ scheme. If $d > k$, then the scheme is communication efficient if d participants can recover the secret with lower communication cost. We suppress the subscript for convenience and write it as $((k, n, d))$.

B. Encoding

We assume that the number of participants is $n = 2k - 1$ and fewer than k cannot recover the secret. Fix an integer $k \leq d \leq n$, and a prime $q > n$. The secret contains m qudits where each qudit is q -dimensional and

$$m = d - k + 1. \tag{5}$$

Consider the vectors $\underline{s} = (s_1, s_2, \dots, s_m)$ in \mathbb{F}_q^m and $\underline{r} = (r_1, r_2, \dots, r_{m(k-1)})$ in $\mathbb{F}_q^{m(k-1)}$. The vector \underline{r} is further split into m vectors $\underline{r}_1 = (r_1, r_2, \dots, r_{k-1})$, $\underline{r}_2 = (r_k, r_{k+1}, \dots, r_{2(k-1)})$, \dots $\underline{r}_m = (r_{(m-1)(k-1)+1}, r_{(m-1)(k-1)+1}, \dots, r_{m(k-1)})$. The vector \underline{r}_1 alone is further split into two vectors with its first $(k - m)$ values in \underline{u} and the remaining $(m - 1)$ values in \underline{v} .

Let x_1, x_2, \dots, x_n be distinct nonzero elements from \mathbb{F}_q . Denote by $V_{n,d}$ a Vandermonde matrix (over \mathbb{F}_q) given as

$$V_{n,d} = \begin{bmatrix} 1 & x_1 & \dots & x_1^{d-1} \\ 1 & x_2 & \dots & x_2^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{d-1} \end{bmatrix}, \tag{6}$$

where x_1, x_2, \dots, x_n are distinct nonzero elements from \mathbb{F}_q , known to all the parties involved. Let $s_i, r_j \in \mathbb{F}_q$, where $1 \leq i \leq m$ and $1 \leq j \leq m(k - 1)$. We define the following matrix Y .

$$Y = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_m \\ \hline r_1 & r_k & r_{2(k-1)+1} & \dots & r_{(m-1)(k-1)+1} \\ r_2 & r_{k+1} & r_{2(k-1)+2} & \dots & r_{(m-1)(k-1)+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{k-1} & r_{2(k-1)} & r_{3(k-1)} & \dots & r_{m(k-1)} \end{bmatrix}. \tag{7}$$

We also represent Y in a slightly compact form as follows:

$$Y = \begin{bmatrix} \underline{s} & & & & & & 0 \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ \underline{r}_1 & \underline{r}_2 & \underline{r}_3 & \cdots & \underline{r}_m & & \end{bmatrix}. \quad (8)$$

Consider the matrix $C = V_{n,d}Y$ where Y is defined as in Eq. (7). Each entry in matrix C , c_{ij} is a function of \underline{s} and \underline{r} . The encoding for the basis states $(s_1, \dots, s_m) \in \mathbb{F}_q^m$ is given by \mathcal{E} , where

$$\mathcal{E} : |s_1 s_2 \dots s_m\rangle \mapsto \sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} \bigotimes_{i=1}^{2k-1} |c_{i1} c_{i2} \dots c_{im}\rangle, \quad (9)$$

where we have omitted the normalizing factor. The qudits in the share of the i th participant are indexed by i . The first share contains the first m qudits, the second share contains the next set of m qudits, and so on till the $(2k - 1)$ th share.

C. Secret reconstruction and secrecy

Lemma 1. (Recoverability for nonminimal authorized sets).

For the encoding scheme given in Eq. (9), we can recover the secret from any d shares by accessing only the first qudit in each share.

Proof. We shall prove this by giving the sequence of operations to be performed so that the d shares can recover the secret with *only* d qudits. Each of the d participants sends their first qudit to the combiner for reconstructing the secret. Let $D = \{i_1, i_2, \dots, i_d\} \subseteq \{1, 2, \dots, 2k - 1\}$ be the set of d shares chosen and $E = \{i_{d+1}, i_{d+2}, \dots, i_{2k-1}\}$ be the complement of D . Let V_D and V_E be the matrices containing the rows of $V_{n,d}$ corresponding to D and E respectively. Then, Eq. (9) can be rearranged as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |\mathbf{c}_{i_1,1} \mathbf{c}_{i_2,1} \dots \mathbf{c}_{i_d,1}\rangle |c_{i_{d+1},1} c_{i_{d+2},1} \dots c_{i_{2k-1},1}\rangle \\ |(c_{i_1,2} c_{i_2,2} \dots c_{i_{2k-1},2}) \dots (c_{i_1,m} c_{i_2,m} \dots c_{i_{2k-1},m})\rangle,$$

where we have highlighted (in bold) the qudits accessed by the combiner. Now using the fact that c_{ij} is the product of the i th row of $V_{n,q}$ and j th column of Y and $\underline{r} = (r_1, \dots, r_m)$, we can rewrite this as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_D(\underline{s}, \underline{r}_1)\rangle |V_E(\underline{s}, \underline{r}_1)\rangle |V(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots \\ \cdots |V(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Since V_D is a $d \times d$ Vandermonde matrix of full rank, we can apply V_D^{-1} to the d qudits with the combiner to transform the state as follows:

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |\underline{s}, \underline{r}_1\rangle |V_E(\underline{s}, \underline{r}_1)\rangle |V(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots \\ \cdots |V(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Then from Eq. (7) we have $\underline{r}_1 = (\underline{u}, \underline{v})$, and $r_{k-m+j} = v_j$ for $1 \leq j \leq m - 1$, we can write

$$|\underline{s}\rangle \sum_{\substack{(\underline{v}, r_2, r_3, \dots, r_m) \\ \in \mathbb{F}_q^{k(m-1)}}} \sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |\underline{u}\rangle |\underline{v}\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |V(\underline{0}, v_1, \underline{r}_2)\rangle \cdots \\ \cdots |V(\underline{0}, v_{m-1}, \underline{r}_m)\rangle.$$

Since the combiner has access to $|\underline{s}\rangle$, $|\underline{u}\rangle$, and $|\underline{v}\rangle$, we can use the matrix V_E , of rank $k - m$ equal to the size of \underline{u} , to transform $|\underline{u}\rangle$ to $|V_E(\underline{s}, \underline{u}, \underline{v})\rangle$.

$$|\underline{s}\rangle \sum_{\substack{(\underline{v}, r_2, r_3, \dots, r_m) \\ \in \mathbb{F}_q^{k(m-1)}}} \sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |\underline{v}\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle \\ |V(\underline{0}, v_1, \underline{r}_2)\rangle \cdots |V(\underline{0}, v_{m-1}, \underline{r}_m)\rangle.$$

Rearranging qudits $|\underline{v}\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle$ to $|V_E(\underline{s}, \underline{u}, \underline{v})\rangle |\underline{v}\rangle$,

$$|\underline{s}\rangle \sum_{\substack{(\underline{v}, r_2, r_3, \dots, r_m) \\ \in \mathbb{F}_q^{k(m-1)}}} \left(\sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle \right) |\underline{v}\rangle \\ |V(\underline{0}, v_1, \underline{r}_2)\rangle \cdots |V(\underline{0}, v_{m-1}, \underline{r}_m)\rangle.$$

Since E is of size $(2k - 1 - d)$, with Eq. (5), we see that V_E is a Vandermonde matrix of size $(k - m) \times d$ and rank $k - m < d$. Therefore, the image of V_E spans \mathbb{F}_q^{k-m} and $\sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle$ is independent of \underline{s} . The state can be written as

$$|\underline{s}\rangle \sum_{\underline{f} \in \mathbb{F}_q^{k-m}} |\underline{f}\rangle |\underline{f}\rangle \sum_{\substack{(\underline{v}, r_2, r_3, \dots, r_m) \\ \in \mathbb{F}_q^{k(m-1)}}} |\underline{v}\rangle |V(\underline{0}, v_1, \underline{r}_2)\rangle \\ \cdots |V(\underline{0}, v_{m-1}, \underline{r}_m)\rangle.$$

The secret is now completely disentangled from the rest of the system, therefore even when the secret is an arbitrary superposition we can recover the secret from d shares as claimed. ■

Lemma 2. (Recoverability for minimal authorized sets). For the encoding scheme given in Eq. (9), we can recover the secret by accessing (all) the qudits of any k shares.

Proof. For secret recovery from k shares, all the qudits from each chosen share are sent to the user. Let $K = \{j_1, j_2, \dots, j_k\} \subset \{1, 2, \dots, 2k - 1\}$ be the set of k shares chosen and $L = \{j_{k+1}, j_{k+2}, \dots, j_{2k-1}\}$ be the complement of K . Let V_K and V_L be the matrices containing the rows of $V_{n,d}$ corresponding to K and L respectively. Then, grouping the (i)th qudits of K and L , the encoded state in Eq. (9) can be written as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |\mathbf{c}_{j_1,1} \mathbf{c}_{j_2,1} \dots \mathbf{c}_{j_k,1}\rangle \cdots |\mathbf{c}_{j_1,m} \mathbf{c}_{j_2,m} \dots \mathbf{c}_{j_k,m}\rangle \\ |c_{j_{k+1},1} c_{j_{k+2},1} \dots c_{j_{2k-1},1}\rangle \\ \cdots |c_{j_{k+1},m} c_{j_{k+2},m} \dots c_{j_{2k-1},m}\rangle.$$

This can be written in terms of V_K and V_L as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_K(\underline{s}, \underline{r}_1)\rangle |V_K(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots \\ |V_K(\underline{0}, r_{k-1}, \underline{r}_m)\rangle \\ |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots \\ |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Letting $V_{K,\ell}$ be the submatrix of V_K consisting of the last k columns. Then we can simplify the state as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_K(\underline{s}, \underline{r}_1)\rangle |V_{K,\ell}(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_{K,\ell}(\underline{0}, r_{k-1}, \underline{r}_m)\rangle \\ |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Since $V_{K,\ell}$ is a $k \times k$ Vandermonde matrix of full rank, we can apply $V_{K,\ell}^{-1}$ to further transform the state as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_K(\underline{s}, \underline{r}_1)\rangle |r_{k-m+1}, \underline{r}_2\rangle \cdots |r_{k-1}, \underline{r}_m\rangle |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Then from Eq. (7) we have $\underline{r}_1 = (\underline{u}, \underline{v})$, and $r_{k-m+j} = v_j$ is the j th entry in \underline{v} for $1 \leq j \leq m-1$, and rearranging the qudits, we can write the state as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_K(\underline{s}, \underline{u}, \underline{v})\rangle |\underline{v}\rangle |r_2, r_3, \dots, r_m\rangle |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Let $V_{K,f}$ be the first k columns of V_K and $V_{K,\bar{f}}$ be the submatrix of remaining columns. Note that $V_{K,\bar{f}}$ has $m-1$ columns. Then $V_K(\underline{s}, \underline{u}, \underline{v}) = V_{K,f}(\underline{s}, \underline{u}) + V_{K,\bar{f}}(\underline{v})$. Thus, the above state can be written as

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_{K,f}(\underline{s}, \underline{u}) + V_{K,\bar{f}}(\underline{v})\rangle |\underline{v}\rangle |r_2, r_3, \dots, r_m\rangle |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

At this point the combiner has access to $|\underline{v}\rangle$ and can subtract $V_{K,\bar{f}}(\underline{v})$ from $|V_{K,f}(\underline{s}, \underline{u}) + V_{K,\bar{f}}(\underline{v})\rangle$ to obtain

$$\sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_{K,f}(\underline{s}, \underline{u})\rangle |\underline{v}\rangle |r_2, r_3, \dots, r_m\rangle |V_L(\underline{s}, \underline{u}, \underline{v})\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

Since $V_{K,f}$ is a $k \times k$ Vandermonde matrix of full rank, we can apply $V_{K,f}^{-1}$ to extract $|\underline{s}\rangle$ as shown below.

$$\begin{aligned} & \sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |\underline{s}\rangle |\underline{u}\rangle |\underline{v}\rangle |r_2, r_3, \dots, r_m\rangle |V_L(\underline{s}, \underline{u}, \underline{v})\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle \\ &= |\underline{s}\rangle \sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |r_1\rangle |r_2, r_3, \dots, r_m\rangle |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle. \end{aligned}$$

Since V_L is a $(k-1) \times d$ matrix of rank $k-1$, we can now modify each of the registers $|r_i\rangle$ of size $(k-1)$ qudits, $|r_1\rangle$ to $|V_L(\underline{s}, \underline{r}_1)\rangle$ and $|r_i\rangle$ for $2 \leq i \leq m$, to $|V_L(\underline{0}, r_{k-m+i-1}, \underline{r}_i)\rangle$.

$$|\underline{s}\rangle \sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

On rearranging the qudits, we obtain

$$|\underline{s}\rangle \sum_{\underline{r}_1 \in \mathbb{F}_q^{k-1}} |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{s}, \underline{r}_1)\rangle \sum_{\underline{r}_2 \in \mathbb{F}_q^{k-1}} |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle |V_L(\underline{0}, r_{k-m+1}, \underline{r}_2)\rangle \cdots \sum_{\underline{r}_m \in \mathbb{F}_q^{k-1}} |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle |V_L(\underline{0}, r_{k-1}, \underline{r}_m)\rangle.$$

V_L is a Vandermonde matrix of size $(k-1) \times d$ with $d > k-1$. So the image of V_L is of dimension $k-1$. Therefore $\sum_{\underline{r}_i \in \mathbb{F}_q^{k-1}} |V_L(\underline{0}, r_{k-m+i-1}, \underline{r}_i)\rangle |V_L(\underline{0}, r_{k-m+i-1}, \underline{r}_i)\rangle$ is a uniform superposition independent of $r_{k-m+i-1}$, for $2 \leq i \leq m$.

$$|\underline{s}\rangle \sum_{\underline{r}_1 \in \mathbb{F}_q^{k-1}} |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{s}, \underline{r}_1)\rangle \sum_{\underline{f}_2 \in \mathbb{F}_q^{k-1}} |\underline{f}_2\rangle |\underline{f}_2\rangle \cdots \sum_{\underline{f}_m \in \mathbb{F}_q^{k-1}} |\underline{f}_m\rangle |\underline{f}_m\rangle.$$

Now we can show that $\sum_{\underline{r}_1 \in \mathbb{F}_q^{k-1}} |V_L(\underline{s}, \underline{r}_1)\rangle |V_L(\underline{s}, \underline{r}_1)\rangle$ is a uniform superposition independent of \underline{s} , since V_L has rank $k-1$.

$$|\underline{s}\rangle \sum_{\underline{f}_1 \in \mathbb{F}_q^{k-1}} |\underline{f}_1\rangle |\underline{f}_1\rangle \cdots \sum_{\underline{f}_m \in \mathbb{F}_q^{k-1}} |\underline{f}_m\rangle |\underline{f}_m\rangle.$$

At this point the state is given by the above expression with the secret completely disentangled from the rest of the system and we can recover any arbitrary superposition. This completes the proof that k shares can recover the secret. ■

Lemma 3. (Secrecy). In the encoding scheme defined in Eq. (9), any $k-1$ or lesser number of shares do not give any information about the secret $|\underline{s}\rangle$.

Proof. The encoding scheme is a pure state encoding scheme with the total number of shares $n = 2k-1$. If some set of $k-1$ or lesser number of shares give any information about the secret, then the secret cannot be recovered from the remaining k or more number of shares, because of the no-cloning theorem. However, from Lemma 2, any k shares are enough to recover the secret completely. Hence, no set of $k-1$ (or lesser number of) shares gives any information about the secret. ■

D. Proposed scheme

From the results in previous subsections we obtain our central result.

Theorem 1. (Communication efficient QSS). The encoding given in Eq. (9) gives rise to a $((k, 2k-1, d))$ quantum secret sharing scheme where d is a fixed integer satisfying $k \leq d \leq 2k-1$. The scheme shares a secret of $m = d - k + 1$ qudits. The communication cost for any k participants to recover the secret is mk qudits, while the communication cost for any d participants is d qudits.

A standard $((k, 2k-1))$ QTS will incur a communication cost of km qudits to share m qudits, while the proposed schemes will require only d qudits. The gains over the standard threshold schemes will depend on the number of parties contacted; equivalently, it depends on the size of the secret. If the secret is of size $m = k$, then the standard method will lead to a communication cost of k^2 qudits. For the proposed scheme, the number of parties contacted is $d = 2k-1$, therefore, the communication complexity is only $2k-1$ qudits. The complexity is lower by a factor of $O(k)$. If the secret is of size $m = 1$, then in effect only k parties are contacted and the scheme reduces to a standard threshold scheme. A subtle point to be noted is that the communication efficient scheme requires the dealer to share a larger secret for obtaining the gains in communication complexity.

An $((k, 2k - 1))$ QTS can be converted to $((k, n))$ QTS for $k \leq n \leq 2k - 1$ by throwing away or ignoring $2k - 1 - n$ shares of the $((k, 2k - 1))$ scheme (Theorem 1 in [9]). If $n < 2k - 1$, then the scheme is a mixed state scheme. Therefore, Theorem 1 implies the existence of $((k, n, d))$ QSS schemes, where $k \leq d \leq n \leq 2k - 1$. Note that a $((k, n))$ QTS cannot exist for $n \geq 2k$ by Theorem 2 in [9].

IV. BOUNDS ON COMMUNICATION COMPLEXITY

In this section we study the optimality of the proposed schemes. We focus on the $((k, 2k - 1, d))$ schemes. We show that the proposed $((k, 2k - 1, d))$ secret sharing schemes are optimal with respect to the communication cost. We need the following lemma given by Gottesman (Theorem 5 in [10]).

Lemma 4. Even in the presence of preexisting entanglement, sending an arbitrary state from a Hilbert space of dimension h requires a channel of dimension h .

Lemma 5. (Secret replacement with authorized set). A party having access to an authorized set of shares in a quantum secret sharing scheme can replace the secret encoded with any arbitrary state (of the same dimension as the secret) without disturbing the remaining shares. After this replacement, secret recovery from any of the authorized sets will give only the new state.

Proof. Let $A \subseteq [1, n]$ be an arbitrary authorized set in the given QSS scheme and B be its complement. Let $\mathcal{E} : \mathcal{S} \rightarrow \mathcal{A} \otimes \mathcal{B}$ denote the operation for encoding the secret and $\mathcal{R}_A : \mathcal{A} \rightarrow \mathcal{S}$ be the operation required for recovering the secret from the authorized set A .

If $|\phi\rangle$ is the secret encoded, then the encoding can be given as $\mathcal{E}|\phi\rangle|0\rangle$ where $|0\rangle$ represents the ancilla qudits. To replace the secret $|\phi\rangle$ with the arbitrary state $|\psi\rangle$ of the same dimension, perform the following steps on the set A : (i) Recover the secret $|\phi\rangle$ using \mathcal{R}_A by acting only on A . The joint state with A and B becomes $|\phi\rangle\langle\phi| \otimes \rho$ where $|\phi\rangle$ is with A and ρ is jointly with A and B and independent of $|\phi\rangle$. (ii) Swap the secret $|\phi\rangle$ with the arbitrary state $|\psi\rangle$. (iii) Encode $|\psi\rangle$ but using $\mathcal{R}_A^\dagger \otimes \mathcal{I}_B$ by acting on the state $|\psi\rangle\langle\psi| \otimes \rho$. Note that all these steps do not involve any operations on the shares in B . After these steps, the final state of qudits with A and B is the same as $\mathcal{E}|\psi\rangle|0\rangle$. The recovery operation by any authorized set from the n shares remains the same as before but the state recovered is $|\psi\rangle$. ■

Application of Lemma 5 in the proof of our next lemma is similar to Theorem 6 in [10]. However, Lemma 5 is convenient and sufficient for our work. In the next theorem, we prove a lower bound on the communication cost for a $((k, n, d))$ quantum secret sharing scheme. We build on the ideas of Gottesman [10] and Huang *et al.* [20].

Lemma 6. In any $((k, 2k - 1, d))$ QSS scheme, which recovers a secret of dimension M from any set of d shares, the total communication to the combiner from any $d - k + 1$ shares among the d shares is of dimension at least M .

Proof. We prove this by means of a communication protocol between Alice and Bob based on the QSS scheme. Alice needs to send an arbitrary state $|\psi\rangle$ of dimension M to Bob.

First, encode the pure state $|0\rangle$ using the given QSS scheme. Consider any set of d participants D such that each participant in D can send a part of its share to the combiner to

recover the secret. Consider any subset $L \subseteq D$ with $d - k + 1$ shares.

A third party, say Carol, is given the $k - 1$ shares from the set $D \setminus L$. Alice is given the $d - k + 1$ shares from L and all the remaining $2k - 1 - d$ shares in the scheme. If Bob wants to reconstruct the secret by accessing some qudits from each of the d shares in D , both Alice and Carol have to communicate some qudits from each share in L and $D \setminus L$ respectively. Next, Carol sends the qudits needed for this reconstruction from each share in $D \setminus L$ to Bob.

Clearly, Bob has no prior information on $|\psi\rangle$ even though he may share some entanglement with Alice due to qudits he received earlier from Carol. Now, instead of directly transmitting $|\psi\rangle$ to Bob, Alice can exploit the secret sharing scheme for the communication. Using the authorized set of k shares she already has, Alice replaces the secret $|0\rangle$ in the scheme with $|\psi\rangle$ (by Lemma 5). Then, she transmits the qudits from the shares in L which Bob needs to reconstruct the encoded secret. Now, Bob uses the qudits received from shares in both L and $D \setminus L$ to reconstruct the secret $|\psi\rangle$. By Lemma 4, the communication from the shares in L has to be at least M . ■

Theorem 2. (Lower bound on communication cost). In any $((k, 2k - 1, d))$ quantum secret sharing scheme, recovery of a secret of dimension M from d shares requires communication of a state from a Hilbert space of dimension at least $M^{d/(d-k+1)}$ to the combiner.

Proof. Consider any set of d participants D such that each participant in D can send a part of its share to the combiner to recover the secret. Label the part of i th share in D communicated to the combiner as H_i such that

$$\dim(H_1) \geq \dim(H_2) \geq \dots \geq \dim(H_d). \tag{10}$$

Applying Lemma 6 for the set $\{H_k, H_{k+1}, \dots, H_d\}$ which is the overall communication from a set of $d - k + 1$ shares,

$$\prod_{i=k}^d \dim(H_i) \geq M. \tag{11}$$

Then by Eq. (10), we have

$$\dim(H_k) \geq M^{1/(d-k+1)} \text{ and } \dim(H_i) \geq M^{1/(d-k+1)} \tag{12}$$

for $1 \leq i \leq k$. From Eqs. (11) and (12), the communication to the combiner from the d shares in D can be lower bounded as

$$\prod_{i=1}^d \dim(H_i) = \prod_{i=1}^{k-1} \dim(H_i) \prod_{i=k}^d \dim(H_i) \tag{13}$$

$$\geq \left(\prod_{i=1}^{k-1} M^{1/(d-k+1)} \right) M = M^{d/(d-k+1)}. \tag{14}$$

This shows that the set of d participants in D must communicate a state that is in a Hilbert space of dimension at least $M^{d/(d-k+1)}$. This completes the proof. ■

If we let $M = q^\ell$, then we obtain the following corollary which immediately implies the optimality of the proposed schemes.

Corollary 1. (Optimality of proposed schemes). Any $((k, 2k - 1, d))$ QSS scheme sharing ℓ qudits incurs a communication cost of $\geq \frac{d\ell}{d-k+1}$ qudits. The $((k, 2k - 1, d))$ QSS

scheme of Theorem 1 has optimal communication cost (for fixed d).

V. CONCLUSION

In this paper we have proposed communication efficient quantum secret sharing schemes and demonstrated their

optimality with respect to communication cost. There are many further directions for research, some of which generalize the classical analogues [19–24] to the quantum setting. For instance, it is natural to study secret sharing schemes that are efficient with variable d as studied classically in [19]. Another direction for research is that of general access structures.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984) pp. 175–179.
- [2] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [4] K. Böstroem and T. Felbinger, *Phys. Rev. Lett.* **89**, 187902 (2002).
- [5] F. G. Deng, G. L. Long, and X. S. Liu, *Phys. Rev. A* **68**, 042317 (2003).
- [6] V. Giovannetti, S. Lloyd, and L. Maccone, *Phys. Rev. Lett.* **100**, 230502 (2008).
- [7] M. Jakobi, C. Simon, N. Gisin, J. D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, *Phys. Rev. A* **83**, 022301 (2011).
- [8] M. Hillery, V. Buzek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
- [9] R. Cleve, D. Gottesman, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999).
- [10] D. Gottesman, *Phys. Rev. A* **61**, 042311 (2000).
- [11] A. Karlsson, M. Koashi, and N. Imoto, *Phys. Rev. A* **59**, 162 (1999).
- [12] A. D. Smith, [arXiv:quant-ph/0001087](https://arxiv.org/abs/quant-ph/0001087).
- [13] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, *Phys. Rev. A* **72**, 032318 (2005).
- [14] D. Markham and B. C. Sanders, *Phys. Rev. A* **78**, 042309 (2008).
- [15] P. Zhang and R. Matsumoto, *Quant. Info. Proc.* **14**, 715 (2015).
- [16] A. Broadbent and C. Schaffner, *Designs Codes Cryptogr.* **78**, 351 (2016).
- [17] J. Müller-Quade, *Inform. Forsch. Entwickl.* **21**, 39 (2006).
- [18] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, *ACM Comput. Surv.* **39**, 6 (2007).
- [19] R. Bitar and S. El Rouayheb, in *Proceedings 2016 IEEE International Symposium on Information Theory, Barcelona, Spain* (IEEE, New York, 2016) pp. 1396–1400, extended version, [arXiv:1512.02990](https://arxiv.org/abs/1512.02990).
- [20] W. Huang, M. Langberg, J. Kliewet, and J. Bruck, *IEEE Trans. Inform. Theory* **62**, 7195 (2016).
- [21] W. Huang and J. Bruck, in *Proceedings 2017 IEEE International Symposium on Information Theory, Aachen, Germany* (IEEE, New York, 2017) pp. 1813–1817.
- [22] H. Wang and D. S. Wong, *IEEE Trans. Inform. Theory* **54**, 473 (2008).
- [23] U. Martínez-Peñas, *IEEE Trans. Inform. Theory* **64**, 4191 (2018).
- [24] X. Yan, C. Lin, R. Lu, and C. Tang, *IEEE Commun. Lett.* **22**, 1556 (2018).
- [25] W. Tittel, H. Zbinden, and N. Gisin, *Phys. Rev. A* **63**, 042301 (2001).
- [26] H. Imai, J. Müller-Quade, A. C. A. Nascimento, P. Tuijls, and A. Winter, *Quantum Info. Comput.* **5**, 69 (2005).
- [27] K. J. Wei, H. Q. Ma, and J. H. Yang, *Opt. Express* **21**, 16663 (2013).
- [28] L. Hao, C. Wang, and G. L. Long, *Opt. Commun.* **284**, 3639 (2011).
- [29] J. Bogdanski, N. Rafiei, and M. Bourennane, *Phys. Rev. A* **78**, 062307 (2008).
- [30] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, *Nat. Commun.* **5**, 5480 (2014).
- [31] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 230505 (2005).
- [32] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, *Phys. Rev. Lett.* **98**, 020503 (2007).
- [33] B. Fortescue and G. Gour, *IEEE Trans. Inform. Theory* **58**, 6659 (2012).
- [34] M. Grassl, M. Rötteler, and T. Beth, *Int. J. Found. Comput. Sci.* **14**, 757 (2003).