

# Communication Efficient Quantum Secret Sharing

Kaushik Senthoo and Pradeep Kiran Sarvepalli

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

(Dated: May 16, 2019)

In the standard model of quantum secret sharing, typically, one is interested in minimal authorized sets for the reconstruction of the secret. In such a setting, reconstruction requires the communication of all the shares of the corresponding authorized set. If we allow for non-minimal authorized sets, then we can trade off the size of the authorized sets with the amount of communication required for reconstruction. Based on the staircase codes, proposed by Bitar and El Rouayheb, we propose a class of quantum threshold secret sharing schemes that are also communication efficient. We call them  $((k, 2k - 1, d))$  communication efficient quantum secret sharing schemes where  $k \leq d \leq 2k - 1$ . Using the proposed construction, we can recover a secret of  $d - k + 1$  qudits by communicating  $d$  qudits whereas using the standard  $((k, 2k - 1))$  quantum secret sharing requires  $k(d - k + 1)$  qudits to be communicated. In other words, to share a secret of one qudit, the standard quantum secret sharing requires  $k$  qudits whereas the proposed schemes communicate only  $\frac{d}{d-k+1}$  qudits per qudit in the communication complexity. Proposed schemes can reduce communication overheads by a factor  $O(k)$  with respect to standard schemes, when  $d$  equals  $2k - 1$ . Further, we show that our schemes have optimal communication cost for secret reconstruction.

*Introduction.* 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 [1–8]. The secret can be a classical or quantum state. 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 have 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 reconstruction phase, the participants constituting an authorized set pool their shares together and then 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 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 quantum secret sharing schemes. While the problem of communication cost in classical secret sharing schemes was studied previously, [9–14], 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 [15–22]. 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 struc-

ture (denoted as  $\Gamma$ ) of the secret sharing scheme. We focus on an important class of secret sharing schemes, namely, the  $((k, n))$  quantum threshold schemes (QTS) where any subset of  $t$  participants with  $k \leq t \leq n$  can reconstruct the secret.

*Contributions.* Based on the staircase codes proposed by Bitar *et al.* [9], 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  $k < d \leq 2k - 1$ , in average  $\frac{d}{d-k+1}$  qudits for every qudit in secret. Further, we show that these schemes are optimal with respect to communication cost in the given model of quantum secret sharing.

*Previous Work.* The closest work related to ours appears to be that of [23] who also aimed at reducing the communication cost in quantum secret sharing schemes. However, there are important differences, their work uses a combination of non-perfect secret sharing schemes along with a hybrid quantum secret sharing scheme. A hybrid QSS scheme is one which participants have (partly or wholly) classical shares. Our schemes in contrast are purely quantum in that no share is classical. Furthermore, the work in [23] 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.

*A Motivating Example.* The intuition behind the communication efficient secret sharing schemes lies in using a non-minimal 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 unable to recover the secret.) Let  $\mathbb{F}_q$  denote the finite field with  $q$  elements. Consider the ternary  $((2, 3))$  quantum threshold scheme proposed by Cleve *et al* [3]. In this scheme, the secret state  $s \in \mathbb{F}_3$  is encoded into three qudits as  $|s\rangle \mapsto \frac{1}{\sqrt{3}} \sum_{r=0}^2 |r\rangle_A |s+r\rangle_B |2s+r\rangle_C$



We also represent  $Y$  in a slightly compact form as follows.

$$Y = \begin{bmatrix} \underline{s} & & & & 0 \\ \vdots & \ddots & & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \underline{r}_1 & \underline{r}_2 & \underline{r}_3 & \cdots & \underline{r}_m \end{bmatrix} \quad (4)$$

Consider the matrix  $C = V_{n,d}Y$  where  $Y$  is defined as in Eq. (3). 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

$$\mathcal{E} : |s_1 s_2 \dots s_m\rangle \mapsto \sum_{\underline{r} \in \mathbb{F}_q^{m(k-1)}} \bigotimes_{i=1}^{2k-1} |c_{i1} c_{i2} \dots c_{im}\rangle, \quad (5)$$

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.

**Lemma 1** (Recoverability for non-minimal authorized sets). *For the encoding scheme given in Eq. (5), 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  $D = \{i_1, i_2, \dots, i_d\} \subset \{1, 2, \dots, 2k-1\}$  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. (5) can be rearranged as

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

where we have highlighted (in color) the qudits accessed by the combiner. Now using the fact that  $c_{ij}$  is the product of  $i$ 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

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

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

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

Then from Eq. (3) 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

$$|\underline{s}\rangle \sum_{\substack{(\underline{u}, \underline{r}_2, \underline{r}_3, \dots, \underline{r}_m) \\ \in \mathbb{F}_q^{k(m-1)}}} \sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |\underline{u}\rangle |\underline{v}\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |V(\underline{Q}, v_1, \underline{r}_2)\rangle \dots \dots |V(\underline{Q}, v_{m-1}, \underline{r}_m)\rangle$$

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  $|V_E(\underline{s}, \underline{u}, \underline{v})\rangle$ .

$$|\underline{s}\rangle \sum_{\substack{(\underline{u}, \underline{r}_2, \underline{r}_3, \dots, \underline{r}_m) \\ \in \mathbb{F}_q^{k(m-1)}}} \sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |\underline{v}\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |V(\underline{Q}, v_1, \underline{r}_2)\rangle \dots |V(\underline{Q}, v_{m-1}, \underline{r}_m)\rangle$$

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

$$|\underline{s}\rangle \sum_{\substack{(\underline{u}, \underline{r}_2, \underline{r}_3, \dots, \underline{r}_m) \\ \in \mathbb{F}_q^{k(m-1)}}} \left( \sum_{\underline{u} \in \mathbb{F}_q^{k-m}} |V_E(\underline{s}, \underline{u}, \underline{v})\rangle |V_E(\underline{s}, \underline{u}, \underline{v})\rangle \right) |\underline{v}\rangle |V(\underline{Q}, v_1, \underline{r}_2)\rangle \dots |V(\underline{Q}, v_{m-1}, \underline{r}_m)\rangle$$

Since  $E$  is of size  $(2k-1-d)$ , with Eq. (2), 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

$$|\underline{s}\rangle \sum_{\underline{f} \in \mathbb{F}_q^{k-m}} |\underline{f}\rangle |\underline{f}\rangle \sum_{\substack{(\underline{u}, \underline{r}_2, \underline{r}_3, \dots, \underline{r}_m) \\ \in \mathbb{F}_q^{k(m-1)}}} |\underline{v}\rangle |V(\underline{Q}, v_1, \underline{r}_2)\rangle \dots |V(\underline{Q}, v_{m-1}, \underline{r}_m)\rangle$$

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.  $\square$

**Lemma 2** (Recoverability for minimal authorized sets). *For the encoding scheme given in Eq. (5), 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. (5) can be written as

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

This can be written in terms of  $V_K$  and  $V_L$  as

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

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

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

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

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

Then from Eq. (3) 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

$$\sum_{\underline{x} \in \mathbb{F}_q^{m(k-1)}} |V_K(\underline{s}, \underline{u}, \underline{v})\rangle |\underline{v}\rangle |\underline{\mathcal{L}}_2, \underline{\mathcal{L}}_3, \dots, \underline{\mathcal{L}}_m\rangle |V_L(\underline{s}, \underline{\mathcal{L}}_1)\rangle \\ |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle \cdots |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle$$

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,

$$\sum_{\underline{x} \in \mathbb{F}_q^{m(k-1)}} |V_{K,f}(\underline{s}, \underline{u}) + V_{K,\bar{f}}(\underline{v})\rangle |\underline{v}\rangle |\underline{\mathcal{L}}_2, \underline{\mathcal{L}}_3, \dots, \underline{\mathcal{L}}_m\rangle \\ |V_L(\underline{s}, \underline{\mathcal{L}}_1)\rangle \\ |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle \cdots |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle$$

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

$$\sum_{\underline{x} \in \mathbb{F}_q^{m(k-1)}} |V_{K,f}(\underline{s}, \underline{u})\rangle |\underline{v}\rangle |\underline{\mathcal{L}}_2, \underline{\mathcal{L}}_3, \dots, \underline{\mathcal{L}}_m\rangle |V_L(\underline{s}, \underline{u}, \underline{v})\rangle \\ |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle \cdots |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle$$

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

$$\sum_{\underline{x} \in \mathbb{F}_q^{m(k-1)}} |s\rangle |\underline{u}\rangle |\underline{v}\rangle |\underline{\mathcal{L}}_2, \underline{\mathcal{L}}_3, \dots, \underline{\mathcal{L}}_m\rangle |V_L(\underline{s}, \underline{u}, \underline{v})\rangle \\ |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle \cdots |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle \\ = |s\rangle \sum_{\underline{x} \in \mathbb{F}_q^{m(k-1)}} |\underline{r}_1\rangle |\underline{\mathcal{L}}_2, \underline{\mathcal{L}}_3, \dots, \underline{\mathcal{L}}_m\rangle |V_L(\underline{s}, \underline{\mathcal{L}}_1)\rangle \\ |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle \cdots |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle$$

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

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

On rearranging the qudits, we obtain

$$|s\rangle \sum_{\underline{\mathcal{L}}_1 \in \mathbb{F}_q^{k-1}} |V_L(\underline{s}, \underline{\mathcal{L}}_1)\rangle |V_L(\underline{s}, \underline{\mathcal{L}}_1)\rangle \\ \sum_{\underline{\mathcal{L}}_2 \in \mathbb{F}_q^{k-1}} |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle |V_L(\underline{Q}, r_{k-m+1}, \underline{\mathcal{L}}_2)\rangle \\ \vdots \\ \sum_{\underline{\mathcal{L}}_m \in \mathbb{F}_q^{k-1}} |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle |V_L(\underline{Q}, r_{k-1}, \underline{\mathcal{L}}_m)\rangle$$

$V_L$  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  $\sum_{\underline{r}_i \in \mathbb{F}_q^{k-1}} |V_L(\underline{Q}, r_{k-m+i-1}, \underline{\mathcal{L}}_i)\rangle |V_L(\underline{Q}, r_{k-m+i-1}, \underline{\mathcal{L}}_i)\rangle$  is a uniform superposition independent of  $r_{k-m+i-1}$ , for  $2 \leq i \leq m$ .

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

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

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

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.  $\square$

**Lemma 3 (Secrecy).** *In the encoding scheme defined in Eq. (5), any  $k-1$  or lesser number of shares do not give any information about the secret  $|s\rangle$ .*

*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 give any information about the secret.  $\square$

With these results in place we have our central result.

**Theorem 1 (Communication efficient QSS).** *The encoding given in Eq. (5) 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. A subtle point to be noted is that the communication efficient scheme requires the dealer to share a larger secret.

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, [3, Theorem 1]. If  $n < 2k-1$ , then the scheme is a mixed state scheme. Therefore, Theorem 1 implies the existence of  $((k, n, d))$  quantum secret sharing schemes where  $k \leq d \leq n \leq 2k-1$ . Note that a  $((k, n))$  QTS cannot exist for  $n \geq 2k$  by [3, Theorem 2].

Next we show that the proposed secret sharing schemes are optimal with respect to the communication cost. We need the following lemma due to Gottesman [4, Theorem 5].

**Lemma 4.** *Even in the presence of pre-existing 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 quantum secret sharing 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  $\rho$  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  $|\psi\rangle$ .  $\square$

Application of Lemma 5 in the proof of our next lemma is similar to [4, Theorem 6]. 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 [4] and Huang et al [10].

**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  $M$ .  $\square$

**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

$$\dim(H_1) \geq \dim(H_2) \geq \dots \geq \dim(H_d) \quad (6)$$

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,

$$\prod_{i=k}^d \dim(H_i) \geq M \quad (7)$$

Then by Eq. (6), we have

$$\dim(H_k) \geq M^{1/(d-k+1)} \text{ and } \dim(H_i) \geq M^{1/(d-k+1)} \quad (8)$$

for  $1 \leq i \leq k$ . From Eq. (7) and (8), the communication to the combiner from the  $d$  shares in  $D$  can be lower bounded as

$$\begin{aligned} \prod_{i=1}^d \dim(H_i) &= \prod_{i=1}^{k-1} \dim(H_i) \prod_{i=k}^d \dim(H_i) \\ &\geq \left( \prod_{i=1}^{k-1} M^{1/(d-k+1)} \right) M = M^{d/d-k+1} \end{aligned} \quad (9)$$

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

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  $\ell$  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  $d$ ).*

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 which generalize the classical analogues [9–14] to the quantum setting. For instance, it is natural to study secret sharing schemes that are efficient with variable  $d$  as studied classically in [9]. Another direction for research is that of general access structures.

- 
- [1] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
- [2] A. Karlsson, M. Koashi, and N. Imoto, *Phys. Rev. A* **59**, 162 (1999).
- [3] R. Cleve, D. Gottesman, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999).
- [4] D. Gottesman, *Phys. Rev. A* **61**, 042311 (2000).
- [5] A. D. Smith, e-print quant-ph/0001087 (2000).
- [6] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, *Phys. Rev. A* **72**, 032318 (2005).
- [7] D. Markham and B. C. Sanders, *Phys. Rev. A* **78**, 042309 (2008).
- [8] P. Zhang and R. Matsumoto, *Quantum Information Processing* **14**, 715 (2015).
- [9] R. Bitar and S. El Rouayheb, in *Proc. 2016 IEEE Intl. Symposium on Information Theory, Barcelona, Spain* (2016) pp. 1396–1400, extended version, arXiv:1512.02990.
- [10] W. Huang, M. Langberg, J. Kliewet, and J. Bruck, *IEEE Trans. Inform. Theory* **62**, 7195 (2016).
- [11] W. Huang and J. Bruck, in *Proc. 2017 IEEE Intl. Symposium on Information Theory, Aachen, Germany* (2017) pp. 1813–1817.
- [12] H. Wang and D. S. Wong, *IEEE Trans. Inform. Theory* **54**, 473 (2008).
- [13] U. Martínez-Peñas, *IEEE Trans. Inform. Theory* **64**, 4191 (2018).
- [14] X. Yan, C. Lin, R. Lu, and C. Tang, *IEEE Communications Letters* **22**, 1556 (2018).
- [15] W. Tittel, H. Zbinden, and N. Gisin, *Phys. Rev. A* **63**, 042301 (2001).
- [16] H. Imai, J. Miller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, e-print quant-ph/0311136 (2003).
- [17] K. J. Wei, H. Q. Ma, and J. H. Yang, *Optics express* **21**, 16663 (2013).
- [18] L. Hao, C. Wang, and G. L. Long, *Optics Communications* **284**, 3639 (2011).
- [19] J. Bogdanski, N. Rafiei, and M. Bourennane, *Phys. Rev. A* **78**, 062307 (2008).
- [20] B. A. Bell, D. Markham, D. A. Herrera-Mart, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, *Nature communications* **5**, 5480 (2014).
- [21] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, *Phys. Rev. Lett.* **95**, 230505 (2005).
- [22] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, *Phys. Rev. Lett.* **98**, 020503 (2007).
- [23] B. Fortescue and G. Gour, *IEEE Trans. Inform. Theory* **58**, 6659 (2012).