Communication Efficient Quantum Secret Sharing via Extended CSS Codes

Senthoor, Kaushik; Sarvepalli, Pradeep Kiran

DOI
10.1109/JSAC.2024.3380082

Publication date
2024

Document Version
Final published version

Published in
IEEE Journal on Selected Areas in Communications

Citation (APA)
Senthoor, K., & Sarvepalli, P. K. (2024). Communication Efficient Quantum Secret Sharing via Extended CSS Codes. *IEEE Journal on Selected Areas in Communications*, *42*(7), 1818-1829. https://doi.org/10.1109/JSAC.2024.3380082

Communication Efficient Quantum Secret Sharing via Extended CSS Codes

Kaushik Senthoor and Pradeep Kiran Sarvepalli

***Abstract*— Recently, a class of quantum secret sharing schemes called communication efficient quantum threshold secret sharing schemes (CE-QTS) was introduced. These schemes reduced the communication cost during secret recovery. In this paper, we introduce a general class of communication efficient quantum secret sharing schemes (CE-QSS) which include both threshold and non-threshold schemes. We propose a framework for constructing CE-QSS schemes to generalize the earlier construction of CE-QTS schemes which was based on the staircase codes. The main component in this framework is a class of quantum codes which we call the extended Calderbank-Shor-Steane codes. These extended CSS codes could have other applications. We derive a bound on communication cost for CE-QSS schemes. Finally, we provide a construction of CE-QSS schemes meeting this bound using the proposed framework.**

***Index Terms*— Quantum secret sharing, communication complexity, quantum cryptography, staircase codes, extended CSS codes.**

I. Introduction

A QUANTUM secret sharing (QSS) scheme is a quantum cryptographic protocol for securely distributing a secret among multiple parties with quantum information. In these schemes, the authorized sets of parties are allowed to recover the secret while unauthorized sets of parties are not allowed to have any information about the secret. QSS schemes were first proposed by Hillery et al. for sharing a classical secret [1]. QSS schemes with multiple parties sharing a quantum secret were discussed by Cleve et al. [2]. The connections of QSS with quantum error correction codes were studied in [2], [3], [4], [5], [6], [7], and [8]. Quantum secret sharing continues to be extensively studied [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20] and experimentally implemented [21], [22], [23], [24].

In this paper, we focus on quantum secret sharing schemes which share a *quantum* secret. An important class of such QSS schemes is the $((t, n))$ quantum threshold schemes (QTS). In these schemes any set of t or more parties is authorized and any set of less than t parties is unauthorized. Cleve et al. [2] first gave a general construction for QTS schemes. Motivated with a view to improve the storage cost of the schemes, Ogawa et al. [16] proposed ramp QSS schemes. These schemes include non-threshold QSS schemes in which any set of size t is authorized, but sets of size z or less are unauthorized. Furthermore any set of size $z + 1$ to $t - 1$ have only partial information about the secret. Allowing for such sets they were able to improve the storage cost of the QSS schemes.

The part of the encoded state given to a party is called the *share* of that party. For recovering the secret, the parties in an authorized set send their shares to a new party called the *combiner*. The combiner then recovers the secret with suitable operations. The amount of quantum information sent to the combiner by the parties during secret recovery is called the *quantum communication cost*. Alternatively, the parties in an authorized set can collaborate among themselves to recover the secret. The communication cost for secret recovery will be slightly different in this case.

In the standard $((t, n))$ QTS schemes, when the combiner accesses t or more parties, some t parties have to send their complete shares. It was shown by Gottesman [3] that the size of each share in a QTS scheme has to be at least the size of the secret. Here, the size of the secret (resp. share) is given by the number of qudits in the secret state (resp. share). This implies that the communication cost is at least t times the secret size. Recently, [25] proposed a class of QTS schemes, called communication efficient quantum threshold secret sharing (CE-QTS) schemes, which reduced the communication cost for secret recovery. In CE-QTS schemes, each party can also send just a part of its share instead of the full share. In these schemes, the combiner can access any t parties to recover the secret as in the QTS schemes. Additionally, the combiner can also access any d $(> t)$ parties downloading only a part of the share from each party. The communication cost while accessing t parties is t for each qudit of the secret. This reduces to $\frac{d}{d-t+1}$ while accessing d parties. For the maximum value of $d = 2t - 1$, this reduced communication cost is much less than the communication cost for t parties. The construction of CE-QTS schemes was motivated by the constructions for classical communication efficient secret sharing schemes in [26] and [27]. The theory of CE-QTS was further developed in [28] and [29].

Manuscript received 4 June 2023; revised 3 December 2023; accepted 20 December 2023. Date of publication 29 March 2024; date of current version 19 June 2024. This work was supported in part by the Department of Science and Technology, Government of India, under Grant DST/ICPS/QuST/Theme-3/2019/Q59; and in part by the Mphasis Center for Quantum Information, Communication, and Computing (CQuICC), Indian Institute of Technology Madras. *(Corresponding author: Kaushik Senthoor.)*

Kaushik Senthoor is with QuTech, Delft University of Technology, 2628 CJ Delft, The Netherlands (e-mail: r.k.senthoor@tudelft.nl).

Pradeep Kiran Sarvepalli is with the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai 600036, India (e-mail: pradeep@ee.iitm.ac.in).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSAC.2024.3380082.

Digital Object Identifier 10.1109/JSAC.2024.3380082

TABLE I

PARAMETERS OF VARIOUS $((t, n))_q$ QTS SCHEMES AND $((t, n; z))_q$ QSS SCHEMES WHERE $z < t \leq n$. NOTICE THAT QSS SCHEMES WITH $z = t - 1$ REDUCE TO QTS SCHEMES.A QSS SCHEME IS COMMUNICATION EFFICIENT IF THE COMMUNICATION COST REDUCES WHILE GOING FROM t PARTIES TO $d (> t)$ PARTIES *i.e.* $\mathrm{CC}_n(d) < \mathrm{CC}_n(t)$

	Type of scheme	Secret size m (in qudits)	Qudit dimension q	Storage cost $(\sum_{i=1}^{n} w_i)/m$	Communication cost $\mathrm{CC}_n(t)/m$	Communication cost $\mathrm{CC}_n(d)/m$	Communication efficient
Cleve et al [2]	QTS	1	$\geq 2t-1$	n	t	t	No
Senthoor et al [25]	QTS	$d-t+1$	$> 2t-1$	n	t	$\frac{d}{d-t+1}$	Yes
Ogawa et al [16]	QSS	$t-z$	$> t+z$	$\frac{n}{t-z}$	$\frac{t}{t-z}$	$\frac{t}{t-z}$	No
Corollary 4	QSS	$\mathrm{lcm}\{d-z, t-z\}$	$> t+z$	$\frac{n}{t-z}$	$\frac{t}{t-z}$	$\frac{d}{d-z}$	Yes

As mentioned earlier, the size of each share in a QTS scheme is at least the size of the secret. However, Ogawa et al. [16] proved that in the non-threshold ramp QSS schemes, the size of each share can be just $\frac{1}{t-z}$ times the secret size. In general, non-threshold QSS schemes have less storage overhead compared to threshold schemes. This motivates us to look for communication efficient non-threshold QSS schemes as well. The trade-off between threshold and non-threshold schemes is the presence of intermediate sets to whom (partial) information could be leaked. Smaller the value of z, more is the number of such intermediate sets. The contributions in this paper are listed below.

(i) In this paper, we construct communication efficient quantum secret sharing schemes which include both threshold and non-threshold schemes. This work generalizes the construction in [25] for communication efficient QTS schemes. We refer to the proposed class of communication efficient quantum secret sharing schemes as CE-QSS schemes.

(ii) As the main result of this paper, we propose a general framework for constructing CE-QSS schemes. This framework constructs CE-QSS schemes by concatenating a CSS code with another CSS code. We analyze the parameters of the CE-QSS scheme thus obtained in terms of the classical linear codes used in the two CSS codes. Our work is inspired from the framework for constructing classical communication efficient secret sharing schemes by Martínez-Peñas [30].

(iii) For the outer code used in the concatenation, we propose a class of CSS codes called *extended CSS codes*. The encoding in the extended CSS code is by extending an underlying CSS code with extra ancilla qudits. We then characterize the extended CSS code as a QSS scheme. This characterization builds upon Matsumoto [8] which showed how CSS codes can be characterized as QSS schemes. The extended CSS codes described in this paper may be of independent interest.

(iv) The framework can provide many different constructions for CE-QSS schemes based on the family of classical linear codes being used in the CSS codes. We use the family of generalized Reed-Solomon codes to obtain the construction for CE-QSS schemes similar to the construction for CE-QTS schemes in [25]. We also derive the bound on communication cost for secret recovery in CE-QSS schemes. We see that the CE-QSS schemes from this construction are optimal in both the storage overhead and the communication cost. We have provided a comparison of our proposed CE-QSS schemes with QSS schemes from existing literature in Table I.

The paper is organized as follows. In Section II, the necessary background on quantum secret sharing and CSS codes is given. This section includes the definition of CE-QSS schemes. In Section III, we describe the extended CSS codes and then propose the framework to construct CE-QSS schemes from these codes. In Section IV, we use this framework to provide a construction of optimal CE-QSS schemes based on generalized Reed-Solomon codes. For an extended version of the paper, see [31]. Some results in this work have been presented in the *International Symposium on Topics in Coding 2023*.

II. BACKGROUND

A. Notation

If q is a prime power, then $\mathbb{F}_q$ denotes a finite field with q elements. For any natural number n, we use the notation $[n] := \{1, 2, \ldots, n\}$. For any $P \subseteq [n]$, its complement $[n] \setminus P$ is denoted as $\overline{P}$. The collection of all subsets of $[n]$ given by $\{P : P \subseteq [n]\}$ is denoted as $2^{[n]}$.

If M is an $\ell \times n$ matrix and $P \subseteq [n]$, then $M^{(P)}$ denotes the $\ell \times |P|$ submatrix of M formed by taking the columns indexed by entries in P. The $\ell \times \ell$ identity matrix is denoted as I_ℓ. For any linear code $C \subseteq \mathbb{F}_q^n$, we denote its generator matrix by G_C. For linear codes C_0 and C_1 such that $C_1 \subseteq C_0$, the term G_{C_0/C_1} indicates the generator matrix of a complement of C_1 in C_0.

We denote $|x_1 x_2 \cdots x_\ell\rangle$ by $|\underline{x}\rangle$ where $\underline{x}$ is the vector with entries from $(x_1, x_2, \ldots, x_\ell)$. For a matrix $M \in \mathbb{F}_q^{a\times b}$, the notation $|M\rangle$ indicates the state $|m_{11}m_{21}\ldots m_{a1}\rangle$ $|m_{12}m_{22}\ldots m_{a2}\rangle \ldots |m_{1b}m_{2b}\ldots m_{ab}\rangle$ where $m_{ij} = [M]_{ij}$.

Definition 1 (Minimum distance of a code): For a linear code C, the minimum distance of the code is defined as $\mathrm{wt}(C) = \min\{\mathrm{wt}(\underline{c}) \mid \underline{c} \in C,\ \underline{c} \neq \underline{0}\}$.

Definition 2 (Minimum distance of a nested code pair): For linear codes C_0 and C_1 such that $C_1 \subsetneq C_0$, the minimum distance of the nested code pair (C_0, C_1) is defined as $\mathrm{wt}(C_0 \setminus C_1) = \min\{\mathrm{wt}(\underline{c}) \mid \underline{c} \in C_0,\ \underline{c} \notin C_1\}$.

B. Quantum Secret Sharing (QSS)

In this subsection, we review QSS schemes and some of their properties. A quantum secret sharing (QSS) scheme is a quantum cryptographic protocol where a secret is encoded and distributed among multiple parties such that only certain subsets of parties can recover the secret. Subsets of parties which can recover the secret are called *authorized* sets (or *qualified* sets) while subsets which have no information about the secret are called *unauthorized* sets (or *forbidden* sets). We refer to the collection of all authorized sets as the *access structure*, denoted by Γ. The collection of all unauthorized sets is referred to as the *adversary structure*, denoted by $\mathcal{A}$. The access structure satisfies a monotonicity property in that if a set A can recover the secret, then any set $A' \supseteq A$ can also recover the secret. A QSS scheme is formally defined as follows.

Definition 3 (QSS scheme): Consider two disjoint sets $\Gamma \subseteq 2^{[n]}$ and $\mathcal{A} \subseteq 2^{[n]}$. An encoding of a quantum secret distributed among n parties is defined as a QSS scheme for an access structure Γ and an adversary structure $\mathcal{A}$ when the following conditions hold.

1) *(Recovery) For any $A \in \Gamma$, the secret can be recovered from parties in A.*
2) *(Secrecy) For any $B \in \mathcal{A}$, the set of parties B has no information about the secret.*

A QSS scheme over n parties is said to be *perfect* if every subset $P \subseteq [n]$ is either authorized or unauthorized *i.e.* if $\Gamma \cup \mathcal{A} = 2^{[n]}$. In a *non-perfect* QSS scheme, there are sets of parties which are neither authorized nor unauthorized. Such sets are called *intermediate sets*. Though an intermediate set of parties cannot recover the secret completely, it can retrieve partial information about the secret. In this case, $\Gamma \cup \mathcal{A} \subsetneq 2^{[n]}$ and the collection of intermediate sets is given by $2^{[n]} \backslash (\Gamma \cup \mathcal{A})$.

In a classical secret sharing scheme, there may be two authorized sets which are disjoint. This implies that there can be two copies of the secret which can be recovered independently. However, the no-cloning theorem prohibits making copies of the quantum secret. Hence any QSS scheme cannot have an access structure with two disjoint authorized sets.

Lemma 1: [2, Corollary 8] In a QSS scheme, the complement of an authorized set is an unauthorized set i.e. if $A \in \Gamma$ then $\overline{A} \in \mathcal{A}$.

A QSS scheme is called a *pure state QSS scheme* when any pure state secret is encoded into a pure state (shared among the n parties). The corresponding encoding is called a *pure state encoding*. A QSS scheme in which some pure state is encoded into a mixed state is called a *mixed state QSS scheme*.

Lemma 2: [2, Corollary 8] In a pure state QSS scheme, the complement of a set is an unauthorized set if and only if the set is an authorized set i.e. $A \in \Gamma \Leftrightarrow \overline{A} \in \mathcal{A}$.

Although the above two lemmas were shown by Cleve et al in the context of perfect schemes [2, Corollary 8], the proof therein follows for non-perfect schemes as well.

Ramp QSS schemes are a class of QSS schemes first defined by Ogawa et al [16].

Definition 4 (Ramp QSS scheme): [16, Definition 1] For $0 \leq z < t \leq n$, a $((t, n; z))$ ramp QSS scheme is a QSS scheme with n parties where

1) *Any $P \subseteq [n]$ is authorized if $|P| \geq t$.*
2) *Any $P \subseteq [n]$ is unauthorized if $|P| \leq z$.*
3) *Any $P \subseteq [n]$ is intermediate (i.e. neither authorized nor unauthorized) if $z < |P| < t$.*

The parameter t is the threshold of the scheme and z is said to be the secrecy parameter. We can also define these parameters for any QSS scheme with a non-empty access structure. For such a QSS scheme with n parties, we can find some $0 < t \leq n$ such that any set of t or more parties is authorized. Similarly, some $0 \leq z < t$ can be found such that any subset of z or less parties is unauthorized.

Definition 5 ($((t, n; z))$ QSS scheme): For $0 \leq z < t \leq n$, a QSS scheme is called a $((t, n; z))$ QSS scheme when the following conditions hold.

1) Any $P \subseteq [n]$ is authorized if $|P| \geq t$.
2) Any $P \subseteq [n]$ is unauthorized if $|P| \leq z$.

The above definition of $((t, n; z))$ QSS schemes follow the definition given in [7] and [8]. This definition differs from the preceding definition of ramp QSS schemes in [16]. Whereas Definition 5 allows the possibility that some sets of size between $z+1$ to $t-1$ are authorized or unauthorized, these sets have to be intermediate (neither authorized nor unauthorized) for the $(t, t-z, n)$ ramp QSS scheme in [16, Definition 1]. To denote this difference, we call the schemes in Definition 5 simply as $((t, n; z))$ QSS schemes instead of referring to them as ramp QSS schemes. Henceforth, in the paper, we refer to only the general class of $((t, n; z))$ QSS schemes.

If $z = t - 1$, then there are no intermediate sets in a $((t, n; z))$ QSS scheme and the scheme becomes a $((t, n))$ quantum threshold secret sharing (QTS) scheme.

For a QSS scheme with non-empty Γ, let $t_{\min}$ be the minimum value of t such that any set of t or more parties is authorized. Let $z_{\max}$ be the maximum value of z such that any set of z or less parties is unauthorized. The following lemma gives the relation between n, $t_{\min}$ and $z_{\max}$.

Lemma 3 (Bound on number of parties): For any QSS scheme with non-empty Γ, the number of parties $n \leq t_{\min} + z_{\max}$. If the QSS scheme is a pure state scheme, then equality holds.

Proof: By Lemma 1, any set of size $n - t_{\min}$ is unauthorized which implies $z_{\max} \geq n - t_{\min}$. Hence $n \leq t_{\min} + z_{\max}$. Additionally, for a pure state QSS scheme, by Lemma 2, any set of $n - z_{\max}$ is authorized which implies $t_{\min} \leq n - z_{\max}$. Hence $n \geq t_{\min} + z_{\max}$ as well. □

The above lemma says that for any pure state QSS scheme, $n = t_{\min} + z_{\max}$. However, the converse need not be true. There can be mixed state schemes with $n = t_{\min} + z_{\max}$. In $((t, n))$ QTS schemes, we can see that $t_{\min} = t$ and $z_{\max} = t - 1$ which leads to the following lemma.

Lemma 4: [2, Theorem 2] For any $((t, n))$ QTS scheme, the number of parties $n \leq 2t - 1$. If the QTS scheme is a pure state scheme, then equality holds.

A QSS scheme with the secret and all the shares having qudits of the same dimension q is indicated by a subscript. We refer to such a $((t, n; z))$ QSS scheme as $((t, n; z))_q$ QSS scheme. The number of qudits (each of dimension q) in the secret is denoted by m. The number of qudits in the jth share is denoted by w_j. Notice that $m = \log_q \dim \mathcal{M}$ and $w_j = \log_q \dim \mathcal{W}_j$ where $\mathcal{M}$ and $\mathcal{W}_j$ are the quantum states corresponding to the secret and the jth share respectively. We refer to m as the size of the secret and w_j as the share size. The lemma below gives the storage cost in distributing a secret in terms of number of the qudits.

Definition 6 (Storage cost): The storage cost for secret distribution in a $((t, n; z))_q$ QSS scheme equals $w_1 + w_2 + \cdots + w_n$.

C. Communication Efficient QSS (CE-QSS)

In this paper we are interested in designing QSS schemes which require a reduced communication overhead while reconstructing the secret. First we define the communication complexity of secret recovery for a given authorized set.

Definition 7 (Communication cost for an authorized set): The communication cost for an authorized set $A \subseteq [n]$ in a $((t, n; z))_q$ QSS scheme is defined as

$$CC_n(A) = \sum_{j \in A} h_{j,A} \tag{1}$$

where $h_{j,A}$ indicates the number of qudits sent to the combiner by the jth party during secret recovery from parties in A.

Here we assume that for a given authorized set, the portion of an accessed share which needs to be sent to the combiner is fixed a priori. This assumption is necessary because there could be different ways to partition the shares from an authorized set for a successful secret recovery.

Definition 8 (Communication cost for d-sets): The communication cost for a threshold d such that $t \le d \le n$ in a $((t, n; z))_q$ QSS scheme is defined as

$$\mathrm{CC}_n(d) = \max_{A \subseteq [n],\, |A| = d} \mathrm{CC}_n(A). \tag{2}$$

Based on the communication cost in $((t, n; z))_q$ QSS schemes as described above, we define a communication efficient QSS scheme as follows. Here d is a fixed value between $t + 1$ and n.

Definition 9 (CE-QSS): Let $0 \le z < t < d \le n$. A $((t, n, d; z))_q$ communication efficient QSS scheme is a $((t, n; z))_q$ QSS scheme where $CC_n(d) < CC_n(t)$.

Our previous work in [25], [28], and [29] has focused on communication efficient QSS schemes which are threshold schemes (with $z = t - 1$), referred to as CE-QTS schemes. However, the schemes in Definition 9 include communication efficient QSS schemes which are non-threshold as well. We refer to the schemes introduced here as CE-QSS schemes.

D. CSS Codes as QSS Schemes

We briefly review the basics of CSS codes and the relevant results on QSS schemes based on CSS codes. The CSS construction (for qubits) was independently proposed in [32] and [33]. For the generalization to qudits of prime power dimension, see [34, Theorem 3] and [35, Lemma 20].

Definition 10 (CSS code): Let $C_1 \subsetneq C_0 \subseteq \mathbb{F}_q^n$ where C_i is an $[n, k_i]_q$ linear code for $i \in \{0, 1\}$. The CSS code of C_0 over C_1 is defined as the vector space spanned by the states

$$|\underline{x} + C_1\rangle \;\equiv\; \frac{1}{\sqrt{|C_1|}} \sum_{\underline{y} \in C_1} |\underline{x} + \underline{y}\rangle \tag{3}$$

where $\underline{x} \in C_0$. This code is denoted as CSS(C_0, C_1). It is an $[[n, k_0 - k_1, \delta]]_q$ quantum code with distance $\delta = \min\{\mathrm{wt}(C_0 \setminus C_1), \mathrm{wt}(C_1^\perp \setminus C_0^\perp)\}$.

Since $C_1 \subsetneq C_0$, their generator matrices can be written as

$$G_{C_0} = \begin{bmatrix} G_{C_0/C_1} \\ G_{C_1} \end{bmatrix}. \tag{4}$$

Given $\underline{s} \in \mathbb{F}_q^{k_0 - k_1}$, CSS$(C_0, C_1)$ encodes the state $|\underline{s}\rangle$ as

$$|\underline{s}\rangle \;\mapsto\; \sum_{\underline{r} \in \mathbb{F}_q^{k_1}} \left| \left[\, G_{C_0/C_1}^T \;\; G_{C_1}^T \,\right] \begin{bmatrix} \underline{s} \\ \underline{r} \end{bmatrix} \right\rangle \;=\; \sum_{\underline{r} \in \mathbb{F}_q^{k_1}} \left| G_{C_0}^T \begin{bmatrix} \underline{s} \\ \underline{r} \end{bmatrix} \right\rangle \tag{5}$$

where we dropped the normalization constant for convenience.

Lemma 5 (QSS and QECC): [3, Theorem 1] A pure state encoding of a quantum secret is a QSS scheme if and only if the encoded space corrects erasure errors on unauthorized sets and it corrects erasure errors on the complements of authorized sets.

Lemma 5 is due to [3, Theorem 1] which discusses about the connection between quantum codes and QSS schemes. Though [3] discusses only about perfect QSS schemes, this lemma holds for non-perfect QSS schemes as well. Using this lemma, we can obtain a QSS scheme from a CSS code.

Theorem 1 (QSS schemes from a CSS code): For any $0 \le z < t \le n$ satisfying

$$t \ge n - \min\{\mathrm{wt}(C_0 \setminus C_1), \mathrm{wt}(C_1^\perp \setminus C_0^\perp)\} + 1 \tag{6a}$$

$$z \le \min\{\mathrm{wt}(C_0 \setminus C_1), \mathrm{wt}(C_1^\perp \setminus C_0^\perp)\} - 1 \tag{6b}$$

the encoding in Eq. (5) gives a $((t, n; z))_q$ QSS scheme with

$$m = k_0 - k_1, \tag{7a}$$

$$w_j = 1 \;\text{ for all } j \in [n], \tag{7b}$$

$$CC_n(t) = t. \tag{7c}$$

Proof: Let each of the n parties be given one encoded qudit. An $[[n, k, \delta]]_q$ quantum code can correct erasures up to $\delta - 1$ qudits. Therefore, any set of $n - (\delta - 1)$ or more parties is an authorized set. By Lemma 1, any set of size up to $\delta - 1$ is unauthorized as well. Thus the CSS code gives a $((t, n; z))_q$ QSS scheme. Clearly, the share size $w_j = 1$. The communication cost is t times the share size *i.e.* $\mathrm{CC}_n(t) = t$. Since the code encodes $k_0 - k_1$ qudits, the QSS scheme shares $m = k_0 - k_1$ qudits. □

The CSS(C_0, C_1) is a quantum code with distance $\delta = \min\{\mathrm{wt}(C_0 \setminus C_1), \mathrm{wt}(C_1^\perp \setminus C_0^\perp)\}$. We know that a quantum code with distance δ can correct any $\delta - 1$ erasures. The corresponding QSS scheme derived from this code should be able to do secret recovery from any $n - \delta + 1$ parties. Likewise, this also implies any $\delta - 1$ or fewer parties have no information the secret. This is the intuition behind the conditions in Eq. (6a) and Eq. (6b).

Theorem 1 discusses only about sets with t or more parties and sets with z or less parties. It does not characterize whether a set of parties of size between $z + 1$ to $t - 1$ is authorized, unauthorized or intermediate. Matsumoto [8] studies the QSS scheme from CSS code in more detail. The following theorem from Matsumoto completely characterizes the access structure and the adversary structure.

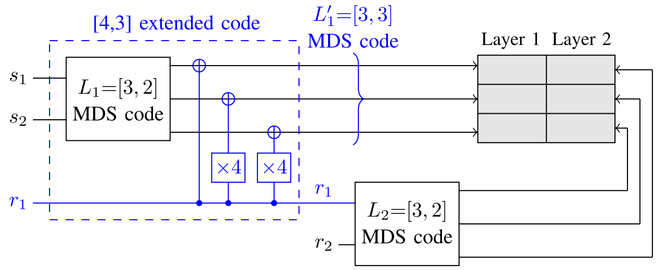

Fig. 1. Encoding circuit for the CE-SS scheme. The extension of the [3,2] code to [4,3] extended code is shown in blue.

Theorem 2 (Authorized sets of QSS from CSS code): The $CSS(C_0, C_1)$ code gives a QSS scheme where $J \subseteq [n]$ is an authorized set if and only if both the conditions below hold.

$$\operatorname{rank} G_{C_0}^{(J)} - \operatorname{rank} G_{C_1}^{(J)} = \dim C_0 - \dim C_1 \tag{8a}$$

$$\operatorname{rank} G_{C_0}^{(\overline{J})} - \operatorname{rank} G_{C_1}^{(\overline{J})} = 0 \tag{8b}$$

The theorem above gives the necessary and sufficient set of conditions for a given set J to be authorized. Note that the encoding for the CSS code is a pure state encoding. Therefore, by Lemma 2, the conditions (8a) and (8b) give the set of necessary and sufficient conditions for $\overline{J}$ to be an unauthorized set as well. Now we can characterize Γ and $\mathcal{A}$ as follows.

$$\Gamma = \{X \subseteq [n] : \text{Eq. (8a) and (8b) hold true for } J = X\} \tag{9a}$$

$$\mathcal{A} = \{Y \subseteq [n] : \text{Eq. (8a) and (8b) hold true for } J = \overline{Y}\} \tag{9b}$$

III. CE-QSS From Extended CSS Codes

In this section, we give a classical communication efficient secret sharing (CE-SS) scheme based on the staircase structure and illustrate the idea behind the proposed framework for constructing CE-QSS schemes. Then we describe the extended CSS codes and study its properties. Finally we give the core result of this paper which is a framework to construct CE-QSS schemes by concatenating extended CSS code with CSS code.

Consider the following CE-SS scheme over $n = 3$ parties with $t = 2$ and $d = 3$. A secret $(s_1, s_2) \in \mathbb{F}_5^2$ is encoded and each party is given two symbols from $\mathbb{F}_5$.

	Layer 1	Layer 2
Share 1	$s_1 + s_2 + r_1$	$r_1 + r_2$
Share 2	$s_1 + 2s_2 + 4r_1$	$r_1 + 2r_2$
Share 3	$s_1 + 3s_2 + 4r_1$	$r_1 + 3r_2$

The symbols r_1 and r_2 are chosen randomly from a uniform probability distribution over $\mathbb{F}_5$. The set of first symbols with the three parties is called the first layer and the set of second symbols is called the second layer.

While accessing any two parties, each accessed party sends both its layers to the combiner thereby giving communication cost of 4 symbols. However, while accessing all three parties, the combiner downloads symbols only from the first layer thereby giving a reduced communication cost of 3 symbols.

The encoding in this scheme can be visualized as given in Fig. 1. Whenever the combiner has access to any two parties, with the two symbols from the second layer, the code L_2 is first decoded to obtain r_1. Now, the extension in the accessed two symbols in the first layer are inverted using r_1. This gives the combiner two code symbols of the inner code L_1 which are then decoded to obtain the secret (s_1, s_2). The steps below explain the secret recovery when the first two parties are accessed. The cells in blue highlight the symbols whose values are modified during the recovery at that step.

	Layer 1		Layer 2	
	$s_1 + s_2 + r_1$	$s_1 + 2s_2 + 4r_1$	$r_1 + r_2$	$r_1 + 2r_2$
$\rightarrow$	$s_1 + s_2 + r_1$	$s_1 + 2s_2 + 4r_1$	r_1	r_2
$\rightarrow$	$s_1 + s_2$	$s_1 + 2s_2$	r_1	r_2
$\rightarrow$	s_1	s_2	r_1	r_2

When the combiner accesses all three parties, the punctured code L_1' from the extended code is decoded to obtain s_1, s_2.

	Layer 1		
	$s_1 + s_2 + r_1$	$s_1 + 2s_2 + 4r_1$	$s_1 + 3s_2 + 4r_1$
$\rightarrow$	s_1	s_2	r_1

A. Extended CSS Codes

We will now describe the extended CSS code motivated from the classical extended code in the illustration above. To construct a CE-QSS scheme encoding m qudits, we take an $[[n, m]]_q$ CSS code and suitably extend it to an $[[n+e, m]]_q$ CSS code. The encoding for this extended CSS code is done by suitably entangling some e ancilla qudits with the n encoded qudits from the $[[n, m]]_q$ CSS code.

Consider linear codes F_0 and F_1 of length n over $\mathbb{F}_q$ with dimensions f_0 and f_1 respectively. Also, consider the matrix $G_E \in \mathbb{F}_q^{e \times n}$, whose row space is denoted by E. Note that E is a linear code. Let F_0, F_1 and G_E satisfy the following conditions.

N1. $F_1 \subsetneq F_0$
N2. $F_0 \cap E = \{\underline{0}\}$

We can describe N1–N2 in terms of generator matrices as

$$\begin{bmatrix} G_{F_0} \\ \hline G_E \end{bmatrix} = \begin{bmatrix} G_{F_0/F_1} \\ G_{F_1} \\ \hline G_E \end{bmatrix}. \tag{10}$$

With this choice of F_0, F_1 and G_E, we define the extended CSS code as follows.

Definition 11 (Extended CSS code): The extended CSS code ECSS(F_0, F_1, G_E) is defined as the CSS(C_0, C_1) code where

$$G_{C_0} = \begin{bmatrix} G_{F_0} & 0 \\ G_E & I_e \end{bmatrix}, \quad G_{C_1} = \begin{bmatrix} G_{F_1} & 0 \\ G_E & I_e \end{bmatrix}. \tag{11}$$

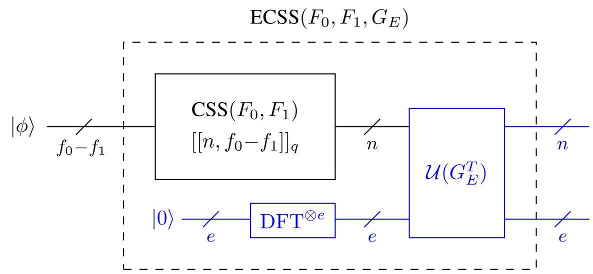

Fig. 2. Encoding circuit for $\mathrm{ECSS}(F_0, F_1, G_E)$. The extension of $\mathrm{CSS}(F_0, F_1)$ to $\mathrm{ECSS}(F_0, F_1, G_E)$ is shown in blue. Note that the ECSS code takes $f_0 - f_1$ logical qudits as input and outputs $n+e$ physical qudits as output. For an encoding circuit for $\mathrm{CSS}(F_0, F_1)$ and the definition of DFT, see [36].

Note that the matrix G_E here need not be of full rank for the above definition of extended CSS code. From Theorem 1, it is clear that this code gives a QSS scheme with $n+e$ qudits.

The encoding in $\mathrm{ECSS}(F_0, F_1, G_E)$ can be written as

$$\begin{aligned} |\underline{s}\rangle \mapsto & \sum_{\substack{\underline{r}_1\in\mathbb{F}_q^{f_1}\\ \underline{r}_2\in\mathbb{F}_q^{e}}} \left| \begin{bmatrix} G_{F_0/F_1}^T & G_{F_1}^T & G_E^T \\ 0 & 0 & I_e \end{bmatrix} \begin{bmatrix} \underline{s} \\ \underline{r}_1 \\ \underline{r}_2 \end{bmatrix} \right\rangle \\ = & \sum_{\substack{\underline{r}_1\in\mathbb{F}_q^{f_1}\\ \underline{r}_2\in\mathbb{F}_q^{e}}} \left| \left[G_{F_0/F_1}^T \; G_{F_1}^T \; G_E^T \right] \begin{bmatrix} \underline{s} \\ \underline{r}_1 \\ \underline{r}_2 \end{bmatrix} \right\rangle |\,\underline{r}_2\,\rangle \end{aligned} \tag{12}$$

for any $\underline{s} \in \mathbb{F}_q^{f_0-f_1}$. We refer to the first n qudits in the encoded state as the *original qudits* and the last e qudits as the *extension qudits*. The block diagram for the encoding is given in Fig. 2 where $\mathcal{U}(M)$ is the unitary operator such that, for any $\underline{x} \in \mathbb{F}_q^n$, $\underline{y} \in \mathbb{F}_q^e$ and $M \in \mathbb{F}_q^{n\times e}$,

$$|\underline{x}\rangle\,|\underline{y}\rangle \xrightarrow{\mathcal{U}(M)} |\underline{x}+M\underline{y}\rangle\,|\underline{y}\rangle\,. \tag{13}$$

In the example CE-SS scheme discussed earlier, access to the extra parity (r_1) from the extended code depends on the number of parties accessed. This extra parity encoded in the layer 2 is accessible to the combiner when any two parties are accessed. However, it is inaccessible when only layer 1 of all the three parties are accessed. Similarly, in the extended CSS code, we will consider the case when some of the extension qudits are known to be accessible or inaccessible to the combiner.

We will assume that the combiner has prior access to some u of the extension qudits and does not have access to the remaining $v = e - u$ extension qudits. In other words, in a QSS scheme from the extended CSS code, among the parties in $\{n+1, n+2, \ldots, n+e\}$, the combiner has prior access to some u parties and no access to the remaining $v = e - u$ parties. Under this assumption, we ask how many among the first n parties is needed to recover the secret.

Without loss of generality, we take the already accessible parties as $\{n+1, n+2, \ldots n+u\}$ and the inaccessible parties as $\{n+u+1, n+u+2, \ldots n+e\}$. Now, we can partition the rows in G_E corresponding to these two sets as $G_E = \begin{bmatrix} G_U \\ G_V \end{bmatrix}$ where G_U is of size $u \times n$ and G_V is of size $v \times n$. The row spaces of G_U and G_V are indicated as U and V respectively.

The encoding in Eq. (12) can be rewritten as

$$|\underline{s}\rangle \mapsto \sum_{\substack{\underline{r}_1\in\mathbb{F}_q^{f_1}\\ \underline{r}_2'\in\mathbb{F}_q^{u}\\ \underline{r}_2''\in\mathbb{F}_q^{v}}} \left| \begin{bmatrix} G_{F_0/F_1}^T & G_{F_1}^T & G_U^T & G_V^T \\ 0 & 0 & I_u & 0 \\ 0 & 0 & 0 & I_v \end{bmatrix} \begin{bmatrix} \underline{s} \\ \underline{r}_1 \\ \underline{r}_2' \\ \underline{r}_2'' \end{bmatrix} \right\rangle . \tag{14}$$

Now we analyze the access structure in the QSS scheme from extended CSS code when the extension qudits are either accessible or inaccessible to the combiner. The set of authorized sets which include the accessed u parties and exclude the inaccessible v parties is given by

$$\Omega_u = \left\{ J \subseteq [n] \;\middle|\; \begin{array}{l} J \cup \{n+1, n+2, \ldots n+u\} \text{ is an} \\ \text{authorized set} \end{array} \right\}. \tag{15}$$

Specifically, we are interested in finding the threshold number τ_u of parties required out of the first n parties to recover the secret with prior access to parties $n+1$, $n+2$, $\ldots$ $n+u$.

$$\tau_u = \min\{\,\tau \,|\, \text{For all } J \subseteq [n] \text{ s.t. } |J| = \tau,\; J \in \Omega_u\} \tag{16}$$

We will use the conditions for a set to be authorized given in Theorem 2 to characterize τ_u. We also need the following two lemmas. (Refer Appendix A for their proofs.) These lemmas were used in Martínez-Peñas [30] to find the threshold number of parties needed for secret recovery in classical CE-SS schemes based on nested linear codes.

Lemma 6: [30] Let $1 \le \rho \le n$. For linear codes C_0 and C_1 such that $C_1 \subsetneq C_0 \subseteq \mathbb{F}_q^n$,

$$\operatorname{rank} G_{C_0}^{(P)} - \operatorname{rank} G_{C_1}^{(P)} = \dim C_0 - \dim C_1 \tag{17}$$

for all $P \subseteq [n]$ such that $|P| = \rho$ if and only if $\rho \ge n - \mathrm{wt}(C_0 \setminus C_1) + 1$.

Lemma 7: [30] Let $1 \le \rho \le n$. For linear codes C_0 and C_1 such that $C_1 \subsetneq C_0 \subseteq \mathbb{F}_q^n$,

$$\operatorname{rank} G_{C_0}^{(\overline{P})} - \operatorname{rank} G_{C_1}^{(\overline{P})} = 0 \tag{18}$$

for all $P \subseteq [n]$ such that $|P| = \rho$ if and only if $\rho \ge n - \mathrm{wt}(C_1^\perp \setminus C_0^\perp) + 1$.

The following theorem studies the size of the sets in Ω_u using these two lemmas.

Theorem 3 (Threshold With Prior Access to Extension Gudits): For every set $J \subseteq [n]$ such that $|J| = \tau$, the set $J \cup \{n+1, n+2, \ldots n+u\}$ is an authorized set in the QSS scheme from the $\mathrm{ECSS}(F_0, F_1, G_E)$ code if and only if $\tau \ge \tau_u$ where

$$\begin{aligned} \tau_u = n - \min\{&\mathrm{wt}((F_0+V) \setminus (F_1+V)), \\ &\mathrm{wt}((F_1+U)^\perp \setminus (F_0+U)^\perp)\} + 1. \end{aligned} \tag{19}$$

Proof: Applying Theorem 2 to the encoding for the QSS scheme as given in Eq. (14), the set $J \cup \{n+1, n+2, \ldots n+u\}$ is authorized if and only if

$$\operatorname{rank} \begin{bmatrix} G_{F_0}^{(J)} & \mathbf{0} \\ G_U^{(J)} & I_u \\ G_V^{(J)} & \mathbf{0} \end{bmatrix} - \operatorname{rank} \begin{bmatrix} G_{F_1}^{(J)} & \mathbf{0} \\ G_U^{(J)} & I_u \\ G_V^{(J)} & \mathbf{0} \end{bmatrix} = f_0 - f_1, \tag{20a}$$

$$\text{rank}\begin{bmatrix} G_{F_0}^{(\overline{J})} & \mathbf{0} \\ G_U^{(\overline{J})} & \mathbf{0} \\ G_V^{(\overline{J})} & I_v \end{bmatrix} - \text{rank}\begin{bmatrix} G_{F_1}^{(\overline{J})} & \mathbf{0} \\ G_U^{(\overline{J})} & \mathbf{0} \\ G_V^{(\overline{J})} & I_v \end{bmatrix} = 0 \tag{20b}$$

where $\overline{J} = [n] \setminus J$. This set of conditions can be simplified to

$$\text{rank}\begin{bmatrix} G_{F_0}^{(J)} \\ G_V^{(J)} \end{bmatrix} - \text{rank}\begin{bmatrix} G_{F_1}^{(J)} \\ G_V^{(J)} \end{bmatrix} = f_0 - f_1, \tag{21a}$$

$$\text{rank}\begin{bmatrix} G_{F_0}^{(\overline{J})} \\ G_U^{(\overline{J})} \end{bmatrix} - \text{rank}\begin{bmatrix} G_{F_1}^{(\overline{J})} \\ G_U^{(\overline{J})} \end{bmatrix} = 0. \tag{21b}$$

The condition in Eq. (21a) is same as Eq. (8a) with $P = J$, $C_0 = F_0 + V$ and $C_1 = F_1 + V$. By Lemma 6, Eq. (21a) holds true for all J such that $|J| = \tau$ if and only if

$$\tau \geq n - \text{wt}((F_0 + V) \setminus (F_1 + V)) + 1. \tag{22}$$

Similarly, the condition in Eq. (21b) is same as Eq. (8b) with $P = J$, $C_0 = F_0 + U$ and $C_1 = F_1 + U$. By Lemma 7, Eq. (21b) holds true for all J such that $|J| = \tau$ if and only if

$$\tau \geq n - \text{wt}((F_1 + U)^\perp \setminus (F_0 + U)^\perp) + 1. \tag{23}$$

Combining the two bounds above, we prove the theorem. □

So far we studied the extended CSS code under the assumption that some of the extension qudits are already accessible and others are inaccessible. Now we evaluate the threshold τ_u in two specific cases, where the extension qudits are all accessible ($u = e$) or all inaccessible ($u = 0$) to the combiner.

Corollary 1 (Threshold with full access to extension qudits): When the combiner has prior access to all the extension qudits in ECSS(F_0, F_1, G_E)*, the secret can be recovered from any* τ *qudits out of the* n *original qudits if and only if* $\tau \geq \tau_e$ *where*

$$\tau_e = n - \min\{\text{wt}(F_0 \setminus F_1), \text{wt}((F_1 + E)^\perp \setminus (F_0 + E)^\perp)\} + 1. \tag{24}$$

Corollary 2 (Threshold with no access to extension qudits): When the combiner has access to none of the extension qudits in ECSS(F_0, F_1, G_E)*, the secret can be recovered from any* τ *qudits out of the* n *original qudits if and only if* $\tau \geq \tau_0$ *where*

$$\tau_0 = n - \min\{\text{wt}((F_0 + E) \setminus (F_1 + E)), \text{wt}(F_1^\perp \setminus F_0^\perp)\} + 1. \tag{25}$$

B. Concatenating Extended CSS Codes for CE-QSS

In this subsection, we give the main result of this paper. We construct the CE-QSS scheme by concatenating an extended CSS code with another CSS code. In the proposed CE-QSS scheme, the secret is first encoded using an extended CSS code. The original qudits are stored in layer 1 and the extension qudits encoded using another CSS code are stored in layer 2. We first give the conditions on the linear codes used to construct the extended CSS code and the CSS code used in layer 2.

Consider an $[n, b_0]$ linear code B_0 over $\mathbb{F}_q$. Let B_1, B_2, A_1, A_2 and E be linear codes of dimensions b_1, b_2, a_1, a_2 and e respectively satisfying the following conditions.

M1. $B_2 \subsetneq B_1 \subsetneq B_0$

M2. $A_2 \subseteq A_1 \subsetneq B_0$ such that $B_0 = B_1 + A_1$ and $B_1 \cap A_1 = \{\underline{0}\}$ with $\dim A_2 > 0$

M3. $E \subseteq B_1$ such that $B_1 = B_2 + E$ and $B_2 \cap E = \{\underline{0}\}$

Clearly $e = b_1 - b_2$ and $a_1 = b_0 - b_1$. We can describe the conditions M1–M3 in terms of generator matrices as

$$G_{B_0} = \begin{bmatrix} G_{A_1} \\ \hline G_{B_1} \end{bmatrix} = \begin{bmatrix} G_{A_1/A_2} \\ G_{A_2} \\ \hline G_{B_2} \\ G_E \end{bmatrix}. \tag{26}$$

Encoding. The encoding for the proposed CE-QSS scheme is illustrated in Fig. 3. The $m = a_1 v_1$ qudits in the secret is partitioned into v_1 blocks of a_1 qudits each where each block is encoded by an ECSS($A_1 + B_2, B_2, G_E$). This encoding gives v_1 blocks each with $n + e$ qudits. The n original qudits from each of this block is stored in layer 1 of the n parties. The remaining $v_1 e$ extension qudits are rearranged into v_2 blocks of a_2 qudits each. Then each of these blocks is encoded using a CSS($A_2 + B_1, B_1$) code. This encoding gives v_2 blocks each with n encoded qudits which are stored in layer 2 of the n parties.

Extended CSS code provides the flexibility for the combiner to recover the secret from two different numbers of parties. The secret can be recovered using the original qudits from layer 1 in one of the two following ways.

(i) from any $d \geq \tau_0$ parties in layer 1

(ii) from any $t \geq \tau_e$ parties in layer 1 by also accessing the extension qudits stored in layer 2.

The encoding of the extension qudits in layer 2 by a CSS code of distance more than z is necessary to avoid eavesdropping by any z parties. If some z parties were to get access to some information about the extension qudits from their layer 2, it is possible that this information can be used to recover some partial information about the secret from layer 1 of those z parties.

We could have taken the original qudits of just a single extended CSS code for layer 1 and encoded its extension qudits with another CSS code for layer 2 to design the QSS scheme. Instead we take v_1 instances of the extended CSS code and encode their extension qudits using v_2 instances of the CSS code. This is because by varying v_1 and v_2, we get different (normalized) storage and communication costs in the CE-QSS scheme. Then we can choose v_1 and v_2 to get the best possible storage and communication costs.

The encoding for the proposed CE-QSS scheme is defined using a message matrix with the staircase structure. Using linear codes satisfying the conditions M1–M3, consider the encoding

$$|S\rangle \mapsto \sum_{\substack{R_{1,1} \in \mathbb{F}_q^{b_2 \times v_1} \\ R_{1,2} \in \mathbb{F}_q^{(b_1 - b_2) \times v_1} \\ R_2 \in \mathbb{F}_q^{b_1 \times v_2}}} \left| G_{B_0}^T \begin{bmatrix} S & \mathbf{0} \\ & D_1 \\ R_{1,1} & \\ R_{1,2} & R_2 \end{bmatrix} \right\rangle. \tag{27}$$

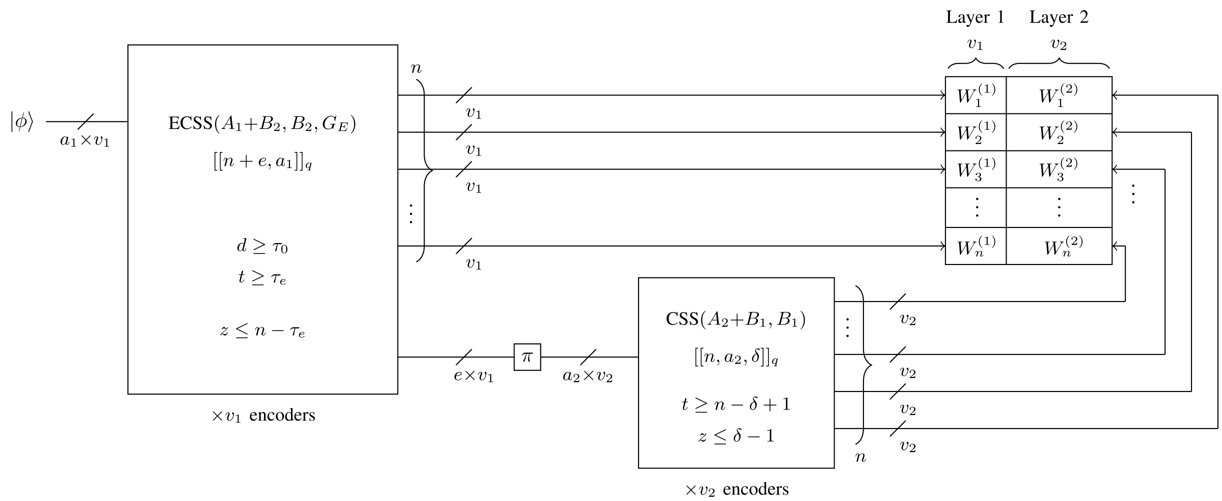

Fig. 3. Encoding for a $((t, n, d; z))_q$ CE-QSS scheme by concatenating extended CSS codes with CSS codes. The secret $|\phi\rangle$ of size $m = a_1 v_1$ qudits is partitioned into v_1 blocks of a_1 qudits and each block is encoded by an ECSS$(A_1 + B_2, B_2, G_E)$. The original qudits from every extended CSS code are stored in Layer 1 of each of the n parties. All the extension qudits from the v_1 extended CSS codes are rearranged into v_2 blocks of a_2 qudits. Each block of these a_2 qudits is encoded using a CSS$(A_2 + B_1, B_1)$. The encoded qudits from every CSS code are then stored in Layer 2 of each of the n parties.

Here $S \in \mathbb{F}_q^{a_1\times v_1}$ indicates the basis state of the secret being encoded and $D_1 \in \mathbb{F}_q^{a_2\times v_2}$ is the matrix formed by any rearrangement of the entries in $R_{1,2}$ where $a_2 v_2 = (b_1-b_2)v_1$. The message matrix M used in the encoding in Eq. (27) and the sizes of its submatrices are given below.

$$M_{b_0\times(v_1+v_2)} = \begin{matrix} a_1\{ \\ b_2\{ \\ e\{ \end{matrix} \overbrace{\left[\begin{array}{c|c} S & \begin{matrix} 0 \\ D_1 \end{matrix} \\ \hline R_{1,1} & \multirow{2}{*}{R_2} \\ R_{1,2} & \end{array}\right]}^{v_1 \quad v_2} \begin{matrix} \}\, a_2 \\ \}\, b_1 \end{matrix} \tag{28}$$

This encoding gives an $[[n(v_1 + v_2), a_1 v_1]]$ quantum code. For $1 \leq j \leq n$, the jth party is given $v_1 + v_2$ qudits corresponding to the jth row of the $n\times(v_1+v_2)$ matrix $G_{B_0}^T M$. We refer to the first v_1 qudits in each party as layer 1 and the next v_2 qudits as layer 2. We choose the smallest possible positive integers v_1 and v_2 such that $a_2 v_2 = (b_1-b_2)v_1$ given by

$$v_1 = \frac{a_2}{\gcd\{a_2, b_1-b_2\}}, \quad v_2 = \frac{b_1-b_2}{\gcd\{a_2, b_1-b_2\}}. \tag{29}$$

Secret recovery. During secret recovery from d parties, the combiner is given access to only layer 1 of the d accessed parties. The combiner then recovers the secret from the d original qudits of the extended CSS code. However, when the combiner has access to only $t < d$ parties, it downloads both the layers from these t parties. The combiner now first recovers the extension qudits by decoding the CSS code. Then the combiner recovers the secret from t original qudits from layer 1 and the extension qudits recovered from the second layer. The following theorem gives the conditions when the encoding in Eq. (27) gives a CE-QSS scheme.

Theorem 4 (CE-QSS using extended CSS codes): For any $0 \leq z < t < d \leq n$ satisfying

$$t \geq n - \min\{\mathrm{wt}(A_2 + B_1 \setminus B_1), \mathrm{wt}(A_1 + B_2 \setminus B_2), \mathrm{wt}(B_1^\perp \setminus B_0^\perp)\} + 1 \tag{30a}$$

$$d \geq n - \min\{\mathrm{wt}(B_0 \setminus B_1), \mathrm{wt}(B_2^\perp \setminus (A_1+B_2)^\perp)\} + 1 \tag{30b}$$

$$z \leq \min\{\mathrm{wt}(A_2 + B_1 \setminus B_1), \mathrm{wt}(A_1 + B_2 \setminus B_2), \mathrm{wt}(B_1^\perp \setminus B_0^\perp)\} - 1 \tag{30c}$$

$$\frac{d}{t} < \frac{a_2 + b_1 - b_2}{a_2}, \tag{30d}$$

the encoding in Eq. (27) gives a $((t, n, d; z))_q$ CE-QSS scheme with the following parameters.

$$m = \frac{a_1 a_2}{\gcd\{a_2, b_1-b_2\}} \tag{31a}$$

$$w_j = \frac{a_2 + b_1 - b_2}{\gcd\{a_2, b_1-b_2\}} \quad \text{for all } j \in [n] \tag{31b}$$

$$\mathrm{CC}_n(t) = \frac{t(a_2 + b_1 - b_2)}{\gcd\{a_2, b_1-b_2\}} \tag{31c}$$

$$\mathrm{CC}_n(d) = \frac{d a_2}{\gcd\{a_2, b_1-b_2\}} \tag{31d}$$

Proof: (i) Recovery from d shares: When the combiner accesses any d parties, each of these parties send the v_1 qudits from layer 1 to the combiner.

Let $D \subseteq [n]$ with $|D| = d$ give the set of accessed parties. Layer 1 contains all the original qudits of the extended CSS code ECSS$(A_1 + B_2, B_2, G_E)$ encoding the secret. By Corollary 2, this implies that the secret state $|S\rangle$ can be recovered from layer 1 of parties in D if

$$d \geq n - \min\{\mathrm{wt}(B_0 \setminus B_1), \mathrm{wt}(B_2^\perp \setminus (A_1+B_2)^\perp)\} + 1. \tag{32}$$

From Eq. (30b), it is clear that d satisfies this condition and hence secret recovery is possible. This implies that $\mathrm{CC}_n(D) = dv_1$. Since this is true for any D such that $|D| = d$, from Definition 8, we obtain $\mathrm{CC}_n(d) = dv_1$.

(ii) Recovery from t shares: When the combiner accesses any t parties, each of these t parties sends all its $v_1 + v_2$ qudits. The encoded state in Eq. (27) can also be

written as

$$\sum_{R_{1,1},\,R_{1,2},\,R_2} |G_{A_1}^T S + G_{B_2}^T R_{1,1} + G_E^T R_{1,2}\rangle_{[n],1} \left|G_{A_2}^T D_1 + G_{B_1}^T R_2\right\rangle_{[n],2} \quad (33)$$

where the subscript to each ket indicates the set of parties and the layer containing the corresponding qudits.

Let $J \subseteq [n]$ with $|J| = t$ be the set of accessed parties. Rearranging the qudits in the encoded state we obtain

$$\sum_{R_{1,1},\,R_{1,2},\,R_2} \left|G_{A_1}^{(J)^T} S + G_{B_2}^{(J)^T} R_{1,1} + G_E^{(J)^T} R_{1,2}\right\rangle_{J,1} \left|G_{A_2}^{(J)^T} D_1 + G_{B_1}^{(J)^T} R_2\right\rangle_{J,2} \left|G_{A_1}^{(\bar{J})^T} S + G_{B_2}^{(\bar{J})^T} R_{1,1} + G_E^{(\bar{J})^T} R_{1,2}\right\rangle_{\bar{J},1} \left|G_{A_2}^{(\bar{J})^T} D_1 + G_{B_1}^{(\bar{J})^T} R_2\right\rangle_{\bar{J},2}. \quad (34)$$

Layer 2 gives the encoded state from the CSS$(A_2 + B_1, B_1)$ code encoding the extension qudits from the extended CSS code. From Theorem 1, these extension qudits can be recovered from layer 2 of parties in J if

$$t \geq n - \min\{\mathrm{wt}(A_2 + B_1 \setminus B_1), \mathrm{wt}(B_1^\perp \setminus (A_2 + B_1)^\perp)\} + 1. \quad (35)$$

Since $A_2 + B_1 \subseteq B_0$, we know that $\mathrm{wt}(B_1^\perp \setminus (A_2 + B_1)^\perp) \geq \mathrm{wt}(B_1^\perp \setminus B_0^\perp)$. Hence, from Eq. (30a), t satisfies the condition in Eq. (35) and therefore the extension qudits can be recovered.

Recovering the extension qudits and discarding the remaining qudits from layer 2, we obtain

$$\sum_{R_{1,1},\,R_{1,2},\,R_2} \left|G_{A_1}^{(J)^T} S + G_{B_2}^{(J)^T} R_{1,1} + G_E^{(J)^T} R_{1,2}\right\rangle_{J,1} |D_1\rangle_{J,2} \left|G_{A_1}^{(\bar{J})^T} S + G_{B_2}^{(\bar{J})^T} R_{1,1} + G_E^{(\bar{J})^T} R_{1,2}\right\rangle_{\bar{J},1} \quad (36)$$

Since the matrix D_1 contains exactly the entries of $R_{1,2}$, the qudits can be rearranged to obtain

$$\sum_{R_{1,1},\,R_{1,2},\,R_2} \left|G_{A_1}^{(J)^T} S + G_{B_2}^{(J)^T} R_{1,1} + G_E^{(J)^T} R_{1,2}\right\rangle_{J,1} |R_{1,2}\rangle_{J,2} \left|G_{A_1}^{(\bar{J})^T} S + G_{B_2}^{(\bar{J})^T} R_{1,1} + G_E^{(\bar{J})^T} R_{1,2}\right\rangle_{\bar{J},1} \quad (37)$$

Layer 1 of the n parties contains exactly the n original qudits of the ECSS$(A_1 + B_2, B_2, G_E)$ codes encoding the secret. The combiner already has access to the extension qudits (indicated by $|R_{1,2}\rangle_{J,2}$) recovered from layer 2. By Corollary 1, the secret can be recovered from layer 1 of parties in J if

$$t \geq n - \min\{\mathrm{wt}(A_1 + B_2 \setminus B_2), \mathrm{wt}(B_1^\perp \setminus B_0^\perp)\} + 1. \quad (38)$$

Clearly t from Eq. (30a) satisfies this condition and hence secret recovery is possible from layers 1 and 2 of any t parties. This implies that the communication cost for secret recovery is $\mathrm{CC}_n(J) = t(v_1 + v_2)$. Since this is true for any J such that $|J| = t$, from Definition 8, we obtain $\mathrm{CC}_n(t) = t(v_1 + v_2)$.

(iii) Secrecy: We proved above that the secret can be recovered from any set of

$$n - \min\{\mathrm{wt}(A_2 + B_1 \setminus B_1), \mathrm{wt}(A_1 + B_2 \setminus B_2), \mathrm{wt}(B_1^\perp \setminus B_0^\perp)\} + 1 \quad (39)$$

or more parties. By Lemma 1, this implies that any set of z parties is an unauthorized set for $z \leq \min\{\mathrm{wt}(A_2 + B_1 \setminus B_1), \mathrm{wt}(A_1 + B_2 \setminus B_2), \mathrm{wt}(B_1^\perp \setminus B_0^\perp)\} - 1$.

(iv) Communication efficiency: Since $a_2 v_2 = (b_1 - b_2) v_1$,

$$\mathrm{CC}_n(t) = t(v_1 + v_2) = t\left(\frac{a_2 + b_1 - b_2}{a_2}\right) v_1 > d v_1 = \mathrm{CC}_n(d). \quad (40)$$

The inequality in the above expression is due to Eq. (30d). □

The n original qudits from the extended CSS (or the n encoded qudits from the CSS code) can be stored in the first layer (or the second layer) of the n parties in any order. The CE-QSS scheme thus obtained will have the same parameters as the original CE-QSS scheme.

IV. CE-QSS Construction From the Extended CSS Framework

So far we have provided the framework for constructing CE-QSS schemes using extended CSS codes. For getting a specific construction of CE-QSS schemes based on this framework, we need to choose a family of classical linear codes to be used in the extended CSS codes. Different choices of code families will give us different CE-QSS schemes.

For instance, in this section, we use a family of classical MDS codes called generalized Reed-Solomon (GRS) codes [37, Section 5.3] to provide optimal CE-QSS schemes. To show the optimality, we need the following bounds on storage and communication costs for CE-QSS schemes.

Lemma 8 (Bound on storage cost): For a $((t, n; z))_q$ QSS scheme encoding a secret of m qudits,

$$\sum_{j=1}^{n} w_j \geq \frac{nm}{t - z}. \quad (41)$$

Proof: The proof follows from [16, Theorem 4]. □

In the $(t, t-z, n)$ ramp QSS schemes defined in [16, Defintion 1], any set of size between $z+1$ to $t-1$ should have neither full information nor zero information about the secret. In contrast, the $((t, n; z))$ QSS schemes from Definition 5 may have some sets of size between $z + 1$ to $t - 1$ as authorized or unauthorized. However, [16, Theorem 4] and its proof for $(t, t-z, n)$ ramp QSS schemes hold true for $((t, n; z))_q$ QSS schemes as well.

For secret recovery from a given set of parties in a QSS scheme, we can design a truncated QSS scheme containing only these parties and storing only the parts of their shares sent to the combiner. The communication cost for this set of parties in the original QSS scheme is then same as the storage cost of the truncated QSS scheme. The following lemma uses this idea to derive a bound on the communication cost from an authorized set.

Theorem 5 (Bound on communication cost): For a secret of size m qudits, in a $((t,n;z))_q$ QSS scheme, the communication cost for secret recovery from an authorized set A is bounded as

$$\mathrm{CC}_n(A) \geq \frac{|A|m}{|A|-z}. \tag{42}$$

Proof: Construct a new QSS scheme from the given $((t,n;z))_q$ QSS scheme by discarding the parties in $\overline{A}$ and the qudits not downloaded by the combiner from the parties in A. Clearly, this is a $((|A|,|A|;z))_q$ QSS scheme encoding the same secret of m qudits. Let ℓ be the number of parties with no qudits in this truncated QSS scheme. By dropping these ℓ parties, we obtain a $((|A|-\ell,|A|-\ell;z))_q$ QSS scheme.

The storage cost in the $((|A|-\ell,|A|-\ell;z))_q$ QSS scheme obtained is same as the communication cost $\mathrm{CC}_n(A)$ in the given $((t,n;z))_q$ QSS scheme. Then, by Lemma 8,

$$\mathrm{CC}_n(A) \geq \frac{(|A|-\ell)m}{|A|-\ell-z} \geq \frac{|A|m}{|A|-z}. \tag{43}$$

□

Corollary 3 (Bound on Communication Cost for d-sets): For $t \leq d \leq n$, in a $((t,n;z))_q$ QSS scheme,

$$\mathrm{CC}_n(d) \geq \frac{dm}{d-z}. \tag{44}$$

Proof: The proof follows from Theorem 5. □

Now we discuss a construction for CE-QSS schemes using the framework from Theorem 4. The construction is realised by choosing the linear codes in conditions from Eq. (30) to be generalized Reed-Solomon codes.

Lemma 9: (Choosing GRS codes for CE-QSS) Let B_0, B_1, B_2, A_1, A_2 and E be codes satisfying conditions M1–M3 with generator matrices given by

$$\begin{bmatrix} G_{A_1/A_2} \\ G_{A_2} \\ G_{B_2} \\ G_E \end{bmatrix} = \left[\begin{array}{cccc} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{a_1-a_2-1} & x_2^{a_1-a_2-1} & \dots & x_n^{a_1-a_2-1} \\ \hdashline \vdots & \vdots & \ddots & \vdots \\ x_1^{a_1-1} & x_2^{a_1-1} & \dots & x_n^{a_1-1} \\ \hdashline \vdots & \vdots & \ddots & \vdots \\ x_1^{a_1+b_2-1} & x_2^{a_1+b_2-1} & \dots & x_n^{a_1+b_2-1} \\ \hdashline \vdots & \vdots & \ddots & \vdots \\ x_1^{b_0-1} & x_2^{b_0-1} & \dots & x_n^{b_0-1} \end{array}\right]. \tag{45}$$

Here $x_1, x_2, \dots x_n$ are distinct non-zero constants from $\mathbb{F}_q$ where $q \geq n+1$ is a prime power. Then the codes B_0, B_1, B_2, A_1+B_2, A_2+B_1 are generalized Reed-Solomon codes.

With the choice of linear codes as described above, we now discuss the CE-QSS construction based on Theorem 4. The staircase codes based construction for $((t,n=2t-1,d))_q$ CE-QTS schemes given in [25, Section III] is a special case of the construction given below with $z=t-1$.

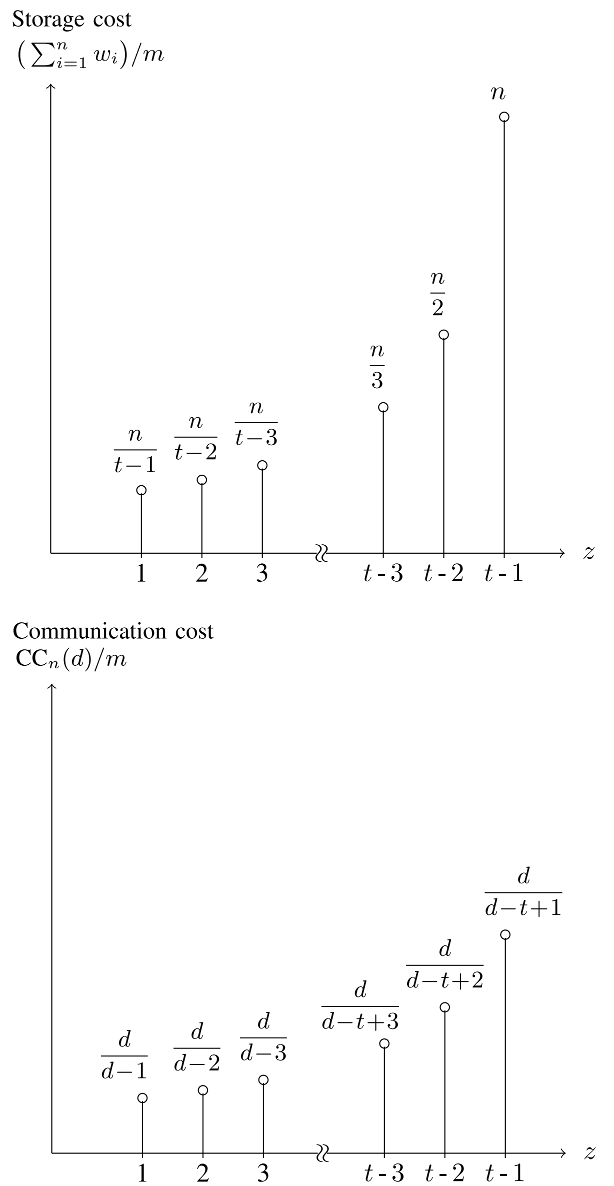

Fig. 4. Variation of normalized storage and communication costs for the $((t,n,d;z))$ CE-QSS schemes from the construction in Section IV for $z \in [t-1]$. Refer to Eq. (47) for the expressions of storage cost and communication cost. Note $z=t-1$ case corresponds to the CE-QTS scheme from [25]. Observe that, for $z<t-1$, the storage and communication costs are lower than the CE-QTS scheme. (Both storage cost and communication cost are normalized over the number of qudits m in the secret).

Corollary 4 (Construction for CE-QSS from GRS codes): Let $q \geq n+1$ be a prime power. For any $0<z<t<d \leq n=t+z$, choosing B_0, B_1, B_2, A_1, A_2 and E as generalized Reed-Solomon codes as given in Lemma 9 for the encoding in Eq. (27) with

$$b_0 = d\,,\quad b_1 = z\,,\quad b_2 = z-d+t\,,\quad e = d-t\,, \tag{46a}$$
$$a_1 = d-z\,,\quad a_2 = t-z \tag{46b}$$

gives a $((t,n=t+z,d;z))_q$ QSS scheme with following parameters having optimal storage and communication costs.

$$m = \mathrm{lcm}\{d-z, t-z\} \tag{47a}$$
$$w_j = \frac{d-z}{\gcd\{d-z,t-z\}} \quad \text{for all } j \in [n] \tag{47b}$$

$$\mathrm{CC}_n(t) = \frac{t(d-z)}{\gcd\{d-z, t-z\}} \tag{47c}$$

$$\mathrm{CC}_n(d) = \frac{d(t-z)}{\gcd\{d-z, t-z\}} \tag{47d}$$

Proof: By Lemma 9, we know that the codes B_0, B_1, B_2, $A_1 + B_2$ and $A_2 + B_1$ are generalized Reed-Solomon codes. Due to the Singleton bound, for any linear MDS code L_0 with another linear code $L_1 \subsetneq L_0$, we know that $\mathrm{wt}(L_0 \setminus L_1) \geq \mathrm{wt}(L_0) = n - \dim L_0 + 1$. Now applying this bound, we see that conditions in Eq. (30) from Theorem 4 hold true for the chosen classical codes. The parameters m, w_j, $\mathrm{CC}_n(t)$ and $\mathrm{CC}_n(d)$ follow from Eq. (31).

The CE-QSS scheme has optimal storage cost since the bound in Lemma 8 is satisfied with equality. The scheme has optimal communication costs as the values of $\mathrm{CC}_n(t)$ and $\mathrm{CC}_n(d)$ satisfy the bound in Corollary 3 with equality. □

Compared to the $((t, n; z))$ ramp QSS schemes by Ogawa et al [16], the communication cost is reduced by a factor of $\frac{t(d-z)}{d(t-z)}$. For instance, when $d = t + z$ and $z = t - 2$, the reduction in communication cost is by a factor of $O(t)$. See Fig. 4 to observe the reduction in storage and communication costs for lesser values of z in our CE-QSS schemes.

In [25] and [29], the communication cost for secret recovery from d parties in a $((t, n))$ QTS scheme is shown to be lower bounded by $\frac{dm}{d-t+1}$. The Staircase construction in [25] provided a communication efficient QTS scheme achieving this lower bound. Hence it has optimal communication cost for a $((t, n))$ QTS scheme.

While considering the more general case of $((t, n; z))$ QSS schemes, the lower bound on communication cost is $\frac{dm}{d-z}$ (see Corollary 3). This generalizes the lower bound given in [25] and [29]. (When $z = t - 1$ it reduces to the lower bound therein.) The construction in Section IV of this paper for communication efficient QSS schemes achieves this lower bound. Hence it has optimal communication cost for a $((t, n; z))$ QSS scheme. Refer to Table I in the introduction to compare the parameters of the various schemes.

V. Conclusion

In this paper, we introduced the class of communication efficient QSS schemes called CE-QSS which generalized CE-QTS schemes to include non-threshold schemes. We proposed a framework based on extended CSS codes to construct CE-QSS schemes. A specific construction using this framework has been provided to obtain CE-QSS schemes with optimal storage and communication costs. As future work, we can look at constructions using this framework with families of linear codes other than GRS codes. This work could be also extended to study CE-QSS schemes which generalize universal CE-QTS schemes from [28]. Another fruitful direction would be to consider CE-QSS schemes under noisy setting. If there is noise during encoding or secret recovery operations, it needs to be addressed using fault tolerance techniques. Noise occurring in the shares after the encoding can be corrected by taking ECSS codes and CSS codes with larger distances. However, such addressing of noise in the shares will come with an increase in storage and/or communication cost.

Appendix A
Proofs for Lemmas 6 and 7

We first define punctured codes and shortened codes and describe some of their properties. For a general introduction to punctured codes and shortened codes, see [37, Section 1.5].

Definition 12 (Punctured code): For any $[n, k]$ code C and $A \subseteq [n]$, the punctured code C^A is defined as

$$C^A = \{(c_i)_{i \in A} : (c_1, c_2, \dots c_n) \in C\}.$$

Definition 13 (Shortened code): For any $[n, k]$ code C and $A \subseteq [n]$, the shortened code C_A is defined as

$$C_A = \{(c_i)_{i \in A} : c_j = 0 \ \forall j \in \overline{A},\ (c_1, c_2, \dots c_n) \in C\}.$$

Lemma 10 (Properties of punctured codes & shortened codes):

(i) *[38, Lemma 1]* $\dim C^A + \dim C_{\overline{A}} = \dim C$

(ii) *[38, Lemma 2]* $\dim C^A + \dim (C^\perp)_A = |A|$

(iii) *[37, Section 1.5.1]* $\dim C^A = \operatorname{rank} G_C^{(A)}$

Lemma 11: Consider linear codes C_0 and C_1 such that $C_1 \subsetneq C_0 \subseteq \mathbb{F}_q^n$. For any $W \subseteq [n]$,

$$(C_0)_W \supsetneq (C_1)_W \quad \Leftrightarrow \quad \exists \underline{c} \in C_0 \setminus C_1 \textit{ with } \operatorname{supp}(\underline{c}) \subseteq W. \tag{48}$$

Proof: Assume $\exists \underline{c} = (c_1, c_2, \dots c_n) \in C_0 \setminus C_1$ with $\operatorname{supp}(\underline{c}) \subseteq W$. This implies $(c_i)_{i \in W} \in (C_0)_W \setminus (C_1)_W$ and hence $(C_0)_W \supsetneq (C_1)_W$.

To prove the converse, since $(C_0)_W \supsetneq (C_1)_W$, take some $\underline{c}' \in (C_0)_W \setminus (C_1)_W$. Consider the vector $\underline{c} \in \mathbb{F}_q^n$ with entries in W from those in $\underline{c}'$ and remaining entries zero. Clearly, $\underline{c} \in C_0 \setminus C_1$ and $\operatorname{supp}(\underline{c}) \subseteq W$. □

Lemma 12: Consider linear codes C_0 and C_1 such that $C_1 \subsetneq C_0 \subseteq \mathbb{F}_q^n$. Let $1 \leq w \leq n$. Then

$$(C_0)_W = (C_1)_W \quad \forall W \in [n] \textit{ such that } |W| = w \\ \Leftrightarrow \ \mathrm{wt}(C_0 \setminus C_1) > w. \tag{49}$$

Proof: By contraposition of Lemma 11, for any $W \subseteq [n]$,

$$(C_0)_W = (C_1)_W \ \Leftrightarrow \ \nexists \underline{c} \in C_0 \setminus C_1 \text{ with } \operatorname{supp}(\underline{c}) \subseteq W.$$

Considering only sets of size w, this implies $(C_0)_W = (C_1)_W$ for all $W \subseteq [n]$ such that $|W| = w$ if and only if

$$\nexists \underline{c} \in C_0 \setminus C_1 \text{ with } \operatorname{supp}(\underline{c}) \subseteq W, \\ \forall W \in [n] \text{ such that } |W| = w. \tag{50}$$

This is same as the condition $\mathrm{wt}(C_0 \setminus C_1) > w$. □

Proof for Lemma 6: By Lemma 12, the condition $\rho \geq n - \mathrm{wt}(C_0 \setminus C_1) + 1$ holds if and only if for all $W \subseteq [n]$ such that $|W| = n - \rho$, $(C_0)_W = (C_1)_W$. By taking $P = \overline{W}$, this is equivalent to the condition that for all P such that $|P| = \rho$, $(C_0)_{\overline{P}} = (C_1)_{\overline{P}}$ *i.e.*

$$\dim (C_0)_{\overline{P}} = \dim (C_1)_{\overline{P}} \tag{51}$$

$$\dim C_0 - \dim C_0^P = dim C_1 - \dim C_1^P \tag{52}$$

$$\dim C_0^P - \dim C_1^P = \dim C_0 - \dim C_1 \tag{53}$$

$$\operatorname{rank} G_{C_0}^{(P)} - \operatorname{rank} G_{C_0}^{(P)} = \dim C_0 - \dim C_1. \tag{54}$$

The equivalences in Eq. (52) and (54) follow from (i) and (iii) in Lemma 10 respectively.

Proof for Lemma 7: By Lemma 12, the condition $\rho \geq n - \mathrm{wt}(C_1^{\perp} \setminus C_0^{\perp}) + 1$ holds if and only if for all $W \subseteq [n]$ such that $|W| = n - \rho$, $(C_1^{\perp})_W = (C_0^{\perp})_W$. By taking $P = \overline{W}$, this is equivalent to the condition that for all P such that $|P| = \rho$, $(C_1^{\perp})_{\overline{P}} = (C_0^{\perp})_{\overline{P}}$ *i.e.*

$$\dim(C_1^{\perp})_{\overline{P}} = \dim(C_0^{\perp})_{\overline{P}} \tag{55}$$

$$\dim C_1^{\overline{P}} = \dim C_0^{\overline{P}} \tag{56}$$

$$\mathrm{rank}\, G_{C_0}^{(\overline{P})} = \mathrm{rank}\, G_{C_1}^{(\overline{P})}. \tag{57}$$

The equivalences in Eq. (56) and (57) follow from (ii) and (iii) in Lemma 10 respectively.

REFERENCES

[1] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 59, pp. 1829–1834, Mar. 1999.

[2] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, pp. 648–651, Nov. 1999.

[3] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 61, no. 4, Mar. 2000, Art. no. 042311.

[4] K. Rietjens, B. Schoenmakers, and P. Tuyls, "Quantum information theoretical analysis of various constructions for quantum secret sharing," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Aug. 2005, pp. 1598–1602.

[5] P. Sarvepalli, "Nonthreshold quantum secret-sharing schemes in the graph-state formalism," *Phys. Rev. A, Gen. Phys.*, vol. 86, no. 4, Oct. 2012, Art. no. 042303.

[6] V. Gheorghiu, "Generalized semiquantum secret-sharing schemes," *Phys. Rev. A, Gen. Phys.*, vol. 85, no. 5, May 2012, Art. no. 052309.

[7] A. Marin and D. Markham, "Equivalence between sharing quantum and classical secrets and error correction," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 4, Oct. 2013, Art. no. 042332.

[8] R. Matsumoto, "Coding theoretic construction of quantum ramp secret sharing," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. E101.A, no. 8, pp. 1215–1222, Aug. 2018.

[9] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 1, pp. 162–168, Jan. 1999.

[10] A. D. Smith, "Quantum secret sharing for general access structures," 2000, *arXiv:quant-ph/0001087*.

[11] S. Bandyopadhyay, "Teleportation and secret sharing with pure entangled states," *Phys. Rev. A, Gen. Phys.*, vol. 62, no. 1, Jun. 2000, Art. no. 012308.

[12] A. Nascimento, J. Mueller-Quade, and H. Imai, "Improving quantum secret-sharing schemes," *Phys. Rev. A, Gen. Phys.*, vol. 64, no. 4, Sep. 2001, Art. no. 042311.

[13] T. Tyc and B. C. Sanders, "How to share a continuous-variable quantum secret by optical interferometry," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 4, Apr. 2002, Art. no. 042310.

[14] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, "An information theoretical model for quantum secret sharing schemes," *Quantum Inf. Comput.*, vol. 5, no. 1, pp. 68–79, Jan. 2005.

[15] S. K. Singh and R. Srikanth, "Generalized quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 71, no. 1, Jan. 2005, Art. no. 012328.

[16] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 3, Sep. 2005, Art. no. 032318.

[17] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 4, Oct. 2008, Art. no. 042309.

[18] P. Sarvepalli and R. Raussendorf, "Matroids and quantum-secret-sharing schemes," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 5, May 2010, Art. no. 052333.

[19] B. Fortescue and G. Gour, "Reducing the quantum communication cost of quantum secret sharing," *IEEE Trans. Inf. Theory*, vol. 58, no. 10, pp. 6659–6666, Oct. 2012.

[20] H. Qin, W. K. S. Tang, and R. Tso, "Hierarchical quantum secret sharing based on special high-dimensional entangled state," *IEEE J. Sel. Topics Quantum Electron.*, vol. 26, no. 3, pp. 1–6, May 2020.

[21] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 63, no. 4, Mar. 2001, Art. no. 042301.

[22] K.-J. Wei, H.-Q. Ma, and J.-H. Yang, "Experimental circular quantum secret sharing over telecom fiber network," *Opt. Exp.*, vol. 21, no. 14, p. 16663, 2013.

[23] J. Pinnell, I. Nape, M. de Oliveira, N. TabeBordbar, and A. Forbes, "Experimental demonstration of 11-dimensional 10-party quantum secret sharing," *Laser Photon. Rev.*, vol. 14, Sep. 2020, Art. no. 2000012.

[24] J. Ding, Y. Li, Y. Mao, and Y. Guo, "Discrete modulation continuous variable quantum secret sharing," *Int. J. Theor. Phys.*, vol. 61, no. 4, pp. 1–14, Apr. 2022.

[25] K. Senthoor and P. K. Sarvepalli, "Communication efficient quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 100, no. 5, Nov. 2019, Art. no. 052313.

[26] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7195–7206, Dec. 2016.

[27] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 933–943, Feb. 2018.

[28] K. Senthoor and P. K. Sarvepalli, "Universal communication efficient quantum threshold secret sharing schemes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Riva del Garda, Italy, Apr. 2021, pp. 1–5.

[29] K. Senthoor and P. K. Sarvepalli, "Theory of communication efficient quantum secret sharing," *IEEE Trans. Inf. Theory*, vol. 68, no. 5, pp. 3164–3186, May 2022.

[30] U. Martínez-Peñas, "Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4191–4206, Jun. 2018.

[31] K. Senthoor and P. K. Sarvepalli, "Concatenating extended CSS codes for communication efficient quantum secret sharing," 2022, *arXiv:2211.06910*.

[32] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.

[33] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Royal Soc. London A, Math., Phys. Eng. Sci.*, vol. 452, pp. 2551–2577, 1996.

[34] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 55–64, Mar. 2004.

[35] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

[36] M. Grassl, M. Rötteler, and T. Beth, "Efficient quantum circuits for non-qubit quantum error-correcting codes," *Int. J. Found. Comput. Sci.*, vol. 14, no. 5, pp. 757–775, Oct. 2003.

[37] W. C. Huffman and V. Pless, *Fundamentals Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[38] G. D. Forney Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 1741–1752, Nov. 1994.

Kaushik Senthoor received the bachelor's degree in electronics and communication engineering from the Amrita School of Engineering, Coimbatore, the master's degree in telecommunication engineering from Indian Institute of Science, Bengaluru, and the Ph.D. degree in electrical engineering from Indian Institute of Technology Madras, India. He is currently a Post-Doctoral Researcher with Delft University of Technology, The Netherlands. After finishing the master's degree, he was an Engineer with Ittiam Systems, Bengaluru. His research interests include classical and quantum error control codes, information theory, distributed storage, and signal processing.

Pradeep Kiran Sarvepalli received the B.Tech. degree in electrical engineering from Indian Institute of Technology Madras and the master's degree in electrical engineering and the Ph.D. degree in computer science from Texas A&M University. He is currently an Associate Professor with Indian Institute of Technology Madras. He was a Post-Doctoral Fellow with the University of British Columbia and Georgia Institute of Technology. He was also an IC Design Engineer with Texas Instruments, Bengaluru, India. His research interests are quantum and classical error correcting codes, quantum cryptography, quantum computation, and distributed storage.