Concatenating Extended CSS Codes for Communication Efficient Quantum Secret Sharing

Kaushik Senthoor† and Pradeep Kiran Sarvepalli†
†Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai 600 036, India

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 quantum communication cost during secret recovery in quantum threshold secret sharing schemes. However, non-threshold schemes are known to have less storage cost compared to threshold schemes. This motivates us to extend the idea of communication efficiency to non-threshold schemes as well. 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. Specifically, we provide a framework for constructing CE-QSS schemes by concatenating a pair of CSS codes. The main component in this framework is a new class of Calderbank-Shor-Steane (CSS) codes called the 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 able to recover the secret while unauthorized sets of parties are not able to recover the secret and have no information about the secret. QSS schemes were first proposed by Hillery et al. for sharing a classical secret [1]. A general construction for QSS schemes sharing quantum secrets was given by Cleve et al. [2] who also elucidated the connections with quantum erasure correcting codes. Following these seminal works, there has been extensive research into quantum secret sharing.

In this paper, we focus on quantum secret sharing schemes which share a quantum secret. An important type of QSS scheme is the quantum threshold scheme (QTS), first proposed by Cleve et al. [2]. In a $(t,n)$ QTS, any set of $t$ or more parties is authorized, while any set of $t-1$ or fewer parties is unauthorized. Later Ogawa et al [3] introduced ramp QSS schemes which are non-threshold QSS schemes and gave a construction. In these schemes, any set of size $t$ is authorized but only sets of size $z$ or less have to be unauthorized. Sets of sizes $z+1$ to $t-1$ have partial information about the secret.

The part of the encoded state given to a party is called its share. For secret recovery, the parties in an authorized set can send their shares to a new party called the combiner. The combiner will then recover the secret with suitable operations.

The amount of quantum information sent to the combiner by the parties during secret recovery is called the communication cost. Alternatively, the parties in an authorized set can collaborate among themselves to recover the secret. The communication cost 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. Gottesman [4] showed that the size of each share in a QTS scheme has to be at least the size of the secret. Therefore the communication cost is at least $t$ times the secret size. Recently, [5] proposed communication efficient quantum threshold secret sharing (CE-QTS) schemes, which reduced the communication cost for secret recovery. 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 $\frac{d}{t+1}$ while accessing $d$ parties. For the maximum value of $d = 2t - 1$, this reduced communication cost is less than half the communication cost for $t$ parties. CE-QTS was motivated by [6], [7] which studied communication efficient classical secret sharing. The theory of CE-QTS was further developed in [8].

As mentioned earlier, the size of each share in a QTS scheme is at least the size of the secret. However, Ogawa et al [3] proved that in the non-threshold ramp QSS schemes, the size of each share can be just $\frac{1}{t}$ times the secret size. In general, non-threshold QSS schemes have less storage cost compared to threshold schemes. This motivates us to look for communication efficient non-threshold QSS schemes as well.

In this paper, we introduce a class of communication efficient quantum secret sharing (CE-QSS) schemes which include both threshold and non-threshold schemes. These schemes generalize the CE-QTS schemes.

Our main result is a general framework for constructing CE-QSS schemes. The proposed CE-QSS schemes are obtained by concatenating a pair of CSS codes. Our work is inspired from the classical communication efficient secret sharing schemes by Martínez-Peñas [9]. Along the way, we propose a class of CSS codes called extended CSS codes which may be of independent interest. We then characterize the extended CSS code as a QSS scheme. This characterization builds upon Matsumoto [10] which characterized CSS as QSS schemes.

Due to space constraint, we skip the proofs here. See the extended version [11] of the paper for proofs and more details.
II. BACKGROUND

Let \( q \) be a prime power and \( \mathbb{F}_q \) 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 \( \mathcal{P} \). The collection of all subsets of \([n]\) given by \( \{P : P \subseteq [n]\} \) is denoted as \( 2^n \).

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 \( C_0 \). The rows of \( G_{C_0/ C_1} \) and \( G_{C_1} \) form a basis for \( C_0 \). The \( \ell \times \ell \) identity matrix is denoted as \( I_\ell \). The minimum distance of the nested code pair \((C_0, C_1)\) is defined as \( \text{wt}(C_0 \setminus C_1) = \min \{\text{wt} (\zeta) : \zeta \in C_0, \zeta \notin C_1\} \).

We denote \( |x_1 x_2 \cdots x_\ell\rangle \) by \( |\bar{x}\rangle \) where \( \bar{x} \) is the vector with entries \( x_1, x_2, \ldots, x_\ell \) from \( \mathbb{F}_q \). For a matrix \( M \in \mathbb{F}_q^{m \times b} \), the notation \( |M| \) indicates the state \(|m_1 m_2 \cdots m_a\rangle |m_1 m_2 \cdots m_b\rangle \cdots |m_1 m_2 \cdots m_b\rangle \) where \( m_{ij} = |M|_{ij} \).

A. Quantum secret sharing (QSS)

We refer to the collection of all authorized sets of a secret sharing scheme as the access structure; it is denoted by \( \Gamma \). The collection of all unauthorized sets is referred to as the adversary structure and denoted by \( A \). A QSS scheme is formally defined as follows.

**Definition 1 (QSS scheme).** Consider two disjoint sets \( \Gamma \subseteq 2^{[n]} \) and \( A \subseteq 2^{[n]} \). An encoding of a quantum secret distributed among \( n \) parties is defined as a QSS scheme for an access structure \( \Gamma \) and an adversary structure \( A \) when the following conditions hold.

1) (Recovery) For any \( \Gamma \in \Gamma \), the secret can be recovered from parties in \( A \).

2) (Secrecy) For any \( B \in A \), the set of parties \( B \) has no information about the secret.

In any QSS scheme with \( n \) parties and non-empty \( \Gamma \), 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 2.** 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 \( |P| \leq z \).

This definition of \(((t, n; z))\) QSS schemes follow the definition of the ramp QSS schemes given in \([10, 12]\). This definition differs from the stricter definition of ramp QSS schemes in \([3]\). Whereas Definition 2 allows the possibility that some sets of size between \( z + 1 \) to \( t - 1 \) are authorized or unauthorized, these sets have to be authorized or unauthorized for the \((t, t - z, n)\) ramp QSS scheme in \([3, \text{Definition 1}]\). In view of this difference, we denote the schemes in Definition 2 simply as \(((t, n; z))\) QSS schemes instead of referring to them as ramp QSS schemes. If \( z = t - 1 \), then a \(((t, n; z))\) QSS scheme is a \(((t, n))\) QTS scheme.

We refer to a \(((t, n; z))\) QSS scheme with the secret and all the shares having qudits of the same dimension \( q \) 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 \( j \)th share is denoted by \( w_j \). We define the storage cost for distributing a secret in terms of number of the qudits.

**Definition 3 (Storage cost).** The storage cost for secret distribution in a \(((t, n; z))_q\) QSS scheme equals \( w_1 + w_2 + \cdots + w_n \).

Similarly we define the communication complexity of secret recovery for a given authorized set in as follows.

**Definition 4 (Communication cost for an authorized set).** The quantum communication cost for an authorized set \( A \subseteq [n] \) in a \(((t, n; z))_q\) QSS scheme is defined as \( CC_n(A) = \sum_{j \in A} h_{j, A} \) where \( h_{j, A} \) indicates the number of qudits sent to the \( j \)th party during secret recovery.

The quantum communication cost for \( d \)-sets where \( t \leq d \leq n \) in a \(((t, n; z))_q\) QSS scheme is defined as

\[
CC_n(d) = \max_{A \subseteq [n], |A| = d} CC_n(A).
\]

Here we assume that for a given authorized set, which portion of an accessed share 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.

B. CSS codes as QSS schemes

The CSS construction (for qubits) was independently proposed in \([13, 14]\). For the generalization to qudits of prime power dimension, see \([15, \text{Theorem 3}] \) and \([16, \text{Lemma 20}] \).

**Definition 5 (CSS code).** Let \( C_1 \subseteq C_0 \subseteq \mathbb{F}_q^n \) where \( C_i \) is an \([n, k_i, q]\) linear code for \( i \in \{0, 1\} \). The CSS code \( C_0 \) over \( C_1 \) is defined as the vector space spanned by the states

\[
|x + C_1\rangle = \frac{1}{\sqrt{|C_1|}} \sum_{y \in C_1} |x + y\rangle
\]

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

Since \( C_1 \subseteq C_0 \), the generator matrix of \( C_0 \) can be written as

\[
G_{C_0} = \begin{bmatrix} G_{C_0/C_1} & G_{C_0/C_1} \end{bmatrix}.
\]

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

\[
|s\rangle \mapsto \sum_{r \in \mathbb{F}_q^{k_1}} |G_{C_0/C_1}^T G_{C_1}^T |s\rangle = \sum_{r \in \mathbb{F}_q^{k_1}} |G_{C_0}^T |s\rangle
\]

where we dropped the normalization constant for convenience.

Any CSS code can be used to construct a QSS scheme. Consider the \( n \)-party QSS scheme where each party is given one qudit from the encoded state in Eq. (4). Matsumoto \([10]\) studied the access structure of such a QSS scheme.

**Theorem 1 (Authorized sets of QSS scheme from CSS code).** \([10, \text{Theorem 1}]\) 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.

\[
\begin{align*}
\text{rank } G_{C_0}^{(J)} - \text{rank } G_{C_1}^{(J)} &= \dim C_0 - \dim C_1 \quad (5a) \\
\text{rank } G_{C_0}^{(J)} - \text{rank } G_{C_1}^{(J)} &= 0 \quad (5b)
\end{align*}
\]

### III. Extended CSS Codes

In this section, we introduce a new class of codes called the extended CSS codes and study some of their properties. The encoding in an extended CSS code is by extending an underlying CSS code with extra ancilla qudits.

#### A. Construction of extended CSS codes

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 $G_E \in \mathbb{F}_q^{n \times n}$ whose row space is denoted by $E$. Let $F_0$, $F_1$ and $G_E$ satisfy the following conditions.

\begin{enumerate}[N1.]
\item $F_1 \subseteq F_0$
\item $F_0 \cap \Gamma = \{\emptyset\}$
\end{enumerate}

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

\[
\begin{bmatrix} G_{F_0}^T \\ G_E \end{bmatrix} = \begin{bmatrix} G_{F_0/F_1}^T \\ G_{F_1/F_1}^T \\ G_{E/F_1}^T \end{bmatrix}.
\]

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

**Definition 6** (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

\[
G_{C_0} = \begin{bmatrix} G_{F_0}^T \\ G_E \end{bmatrix}, \quad G_{C_1} = \begin{bmatrix} G_{F_1}^T \\ G_E \end{bmatrix}.
\]

Clearly, the code $ECSS(F_0, F_1, G_E)$ is an $[[n+e, f_0-f_1]]_q$ code. Note that the matrix $G_E$ need not be of full rank in the above definition of extended CSS code.

The encoding in $ECSS(F_0, F_1, G_E)$ can be written as

\[
|\mathbf{s}\rangle \mapsto \sum_{\mathbf{f}_1 \in \mathbb{F}_q^{f_1}} \sum_{\mathbf{f}_2 \in \mathbb{F}_q^{f_1}} \begin{bmatrix} G_{F_0/F_1}^T \\ G_{F_1/F_1}^T \\ G_{E/F_1}^T \end{bmatrix} \begin{bmatrix} \mathbf{f}_1 \\ \mathbf{f}_2 \\ \mathbf{e}_2 \end{bmatrix}
\]

for any $\mathbf{s} \in \mathbb{F}_q^{f_0-f_1}$. We refer to the first $n$ qudits in the encoded state as the original qudits and the last $e$ qudits as the extension qudits.

#### B. Erasure correction with CSS codes

Consider the $(n+e)$-party QSS scheme where each party is given one qudit from the encoded state of $ECSS(F_0, F_1, G_E)$. Assume that the combiner has access to the first $u$ of the extension qudits and does not have access to the remaining $v = e-u$ extension qudits. In other words, in the QSS scheme, among the parties in $\{n+1, n+2, \ldots, n+e\}$, the combiner has access to the parties in $\{n+1, n+2, \ldots, n+u\}$ and no access to the parties in $\{n+u+1, n+u+2, \ldots, n+e\}$. Under this assumption, we ask how many of the first $n$ parties i.e. how many original qudits is needed to recover the secret.

First we partition the rows in $G_E$ corresponding to the two sets of extension qudits 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. Then the encoding in Eq. (9) can be rewritten as

\[
|\mathbf{s}\rangle \mapsto \sum_{\mathbf{f}_1 \in \mathbb{F}_q^{f_1}} \sum_{\mathbf{f}_2 \in \mathbb{F}_q^{f_1}} \begin{bmatrix} G_{F_0/F_1}^T \\ G_{F_1/F_1}^T \\ G_{E/F_1}^T \end{bmatrix} \begin{bmatrix} \mathbf{f}_1 \\ \mathbf{f}_2 \\ \mathbf{e}_2 \end{bmatrix}.
\]

Now we analyze the access structure in the QSS scheme. The set of authorized sets which include the accessed $u$ parties and exclude the inaccessible $v$ parties is given by

\[
\Omega_u = \left\{ J \subseteq [n] \mid J \cup \{n+1, n+2, \ldots, n+u\} \text{ is an authorized set} \right\}.
\]

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

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

We will use the conditions for a set to be authorized given in Theorem 1 to characterize $\tau_u$.

**Theorem 2** (Minimal number of original qudits needed). 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 $ECSS(F_0, F_1, G_E)$ code if and only if $\tau \geq \tau_u$ where

\[
\tau_u = n - \min\{\text{wt}((F_0 + V) \setminus (F_1 + V)), \text{wt}((F_1 + U) \setminus (F_0 + U))\} + 1.
\]

**Proof.** The proof is by using $G_{C_0}$ and $G_{C_1}$ from Eq. (7) in Theorem 1. Refer to [11, Theorem 3] for the full proof. \qed

We evaluate $\tau_u$ in two specific cases where the extension qudits are all accessible or all inaccessible. When the combiner has access to all the extension qudits, we get $u = e$ which implies $U = E$ and $V = \{\emptyset\}$.

\[
\tau_u = n - \min\{\text{wt}(F_0 \setminus F_1), \text{wt}((F_1 + E) \setminus (F_0 + E))\} + 1
\]

When the combiner has no access to any of the extension qudits, we get $u = 0$ which implies $U = \{\emptyset\}$ and $V = E$.

\[
\tau_0 = n - \min\{\text{wt}((F_0 + E) \setminus (F_1 + E)), \text{wt}(F_1 \setminus F_0)\} + 1
\]

### IV. Concatenating ECSS codes for CE-QSS

In this section, we formally define the CE-QSS schemes. Then we give a framework for constructing CE-QSS schemes using extended CSS codes.
Definition 7 (CE-QSS). Let \( 0 \leq z < t < d \leq n \). A \((t, n; d; z)_q\) communication efficient QSS (CE-QSS) scheme is a \((t, n; z)_q\) QSS scheme where \( CC_n(d) < CC_n(t) \).

Taking \( z = t - 1 \) in this definition gives us the \((t, n; d)_q\) CE-QTS schemes.

Now we give a general framework to construct CE-QSS schemes. We construct a CE-QSS scheme by concatenating an extended CSS code with another CSS code. We first give the conditions on the linear codes used to construct the extended CSS code and the CSS code.

Consider an \([n, b_0]_q\) 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. \( B_2 \subseteq B_1 \subseteq B_0 \)

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

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

We have \( a_1 = b_0 - b_1 \) by M2 and \( e = b_1 - b_2 \) by M3. We can describe \( M_1-M_3 \) in terms of generator matrices as

\[
G_{B_0} = \begin{bmatrix} G_{A_1} \\ G_{A_2} \\ G_{B_2} \\ G_{E} \end{bmatrix} = \begin{bmatrix} G_{A_1/A_2} \\ G_{A_2} \\ G_{B_2} \\ G_{E} \end{bmatrix}.
\]

Encoding. The encoding for the proposed \((t, n; d; z)_q\) CE-QSS scheme is illustrated in Fig. 1. 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 are 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 layer 2 of the \( n \) parties.

The encoding of the extension qudits in layer 2 by a CSS code of distance more than \( z \) is necessary to avoid leakage of information to sets of size \( z \) or smaller. 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 obtain some partial information about the secret from layer 1 of those \( z \) parties.

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

\[
|S| \mapsto \sum_{R_1,1 \in \mathbb{F}_q^{a_1 \times v_1}} \cdots \sum_{R_2 \in \mathbb{F}_q^{e \times v_2}} \begin{bmatrix} G^{T}_{B_0} \\ \vdots \\ G^{T}_{B_2} \end{bmatrix} \begin{bmatrix} S \\ \vdots \\ R_2 \end{bmatrix}.
\]

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. (17) and the sizes of its submatrices are given below.

\[
M_{b_0 \times (v_1 + v_2)} = a_1 \begin{bmatrix} S & 0 \\ \vdots & D_1 \end{bmatrix} a_2 \begin{bmatrix} \vdots & \vdots \\ R_{1,1} & \vdots \\ R_{1,2} & R_2 \end{bmatrix} b_1
\]

The encoding in Eq. (17) gives an \([n(v_1 + v_2), a_1 v_1]_q\) quantum code. For \( 1 \leq j \leq n \), the \( j \)th party is given \( v_1 + v_2 \) qudits corresponding to the \( j \)th row of the \( n \times (v_1 + v_2) \) matrix \( G^{T}_{B_0} M \). 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 \( v_1 \) and \( v_2 \) such that \( a_2 v_2 = (b_1 - b_2) v_1 \) given by
\[
v_1 = \frac{a_2}{\gcd(a_2, b_1 - b_2)}, \quad v_2 = \frac{b_1 - b_2}{\gcd(a_2, b_1 - b_2)}.
\]
(19)
The encoding for the CE-QTS schemes in [5] can be seen as a special case of the encoding in Eq. (17) where \( G_{B_0} \) is a Vandermonde matrix.

**Secret recovery.** During secret recovery from \( d \) parties, the combiner accesses only layer 1 of the shares of the \( d \) parties. The combiner then recovers the secret from the \( d \) original qudits from each of the \( v_1 \) ECSS codes. For such a secret recovery from \( d \) original qudits without accessing the extension qudits (encoded in the layer 2), we need \( d \geq \tau_0 \). Here \( \tau_0 \) is defined as in Eq. (15) for the ECSS \((A_1 + B_2, B_2, G_E)\) code.

To recover the secret from \( t \) parties, the combiner downloads both the layers from the shares of the \( t \) parties. The combiner first decodes each of the \( v_2 \) CSS codes in layer 2. This decoding requires \( t \geq n - \delta + 1 \) where \( \delta \) is the distance of the CSS \((A_2 + B_1, B_1)\) code. On decoding, the combiner obtains \( e \) extension qudits of each of the \( v_1 \) ECSS codes. For each ECSS code, the combiner now has access to \( t \) original qudits obtained from layer 1 and the \( e \) extension qudits recovered from layer 2. By Eq. (14), if \( t \geq \tau_e \), the combiner can now recover \( a_1 \) qudits of the secret from each of the \( v_1 \) ECSS codes. Here we assume that \( t < \tau_0 \) so that for secret recovery from \( t \) parties, the combiner needs to download the qudits from both the layers.

If any \( n - z \) shares can recover the secret, then by no-cloning theorem, any set of \( z \) shares has no information about the secret. Similar to the secret recovery from \( t \) shares, the secret can be recovered from any \( n - z \) shares if \( n - z \geq \tau_e \) and \( n - z \geq n - \delta + 1 \).

For communication efficiency, the communication cost for secret recovery from \( d \) parties should be less than that from \( t \) parties i.e. \( CC_n(d) = d v_1 < t (v_1 + v_2) = CC_n(t) \) where \( v_1 \) and \( v_2 \) are as in Eq. (19). The linear codes should be chosen such that this inequality is satisfied.

Summarizing the above discussion, the following theorem describes how to obtain CE-QSS schemes from ECSS codes. For a detailed proof of the theorem, see [11, Theorem 4].

**Theorem 3 (CE-QSS using extended CSS Codes).** For any \( 0 \leq z < t < d \leq n \) satisfying
\[
t \geq n - \min\{\gcd(A_2 + B_1, B_1), \gcd(A_1 + B_2, B_2), (B_1^+ \setminus B_0^+)\} + 1 \quad (20a)
d \geq n - \min\{\gcd(B_0 \setminus B_1), (B_2^+ \setminus (A_1 + B_2^+))\} + 1 \quad (20b)
z \leq \min\{\gcd(A_2 + B_1, B_1), (A_1 + B_2^+)\} - 1 \quad (20c)
\]
\[
d < \frac{a_2 b_1 - b_2}{a_2}, \quad \frac{a_2}{a_2} \quad (20d)
\]
\[
t < n - \min\{\gcd(B_0 \setminus B_1), (B_2^+ \setminus (A_1 + B_2^+))\} + 1 \quad (20e)
\]
the encoding in Eq. (17) gives a \((t, n, d; z)_{q^1}\) CE-QSS scheme with the following parameters.

\[
m = \frac{a_1 a_2}{\gcd(a_2, b_1 - b_2)} \quad (21a)
w_j = \frac{a_2 + b_1 - b_2}{\gcd(a_2, b_1 - b_2)} \quad \text{for all } j \in [n] \quad (21b)
\]
\[
CC_n(t) = t (a_2 + b_1 - b_2) \quad (21c)
\]
\[
CC_n(d) = \frac{a_2}{\gcd(a_2, b_1 - b_2)} \quad (21d)
\]

The above theorem provides a general framework for constructing CE-QSS schemes. Using different families of linear codes, we can obtain different constructions. For a construction using generalized Reed-Solomon codes, which gives optimal storage and communication costs, see [11, Section IV].

**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. This work could be also extended to study QSS schemes generalizing the universal CE-QTS schemes from [8].

**REFERENCES**

[1] M. Hillery, V. Buˇzek, and A. Berthone, “Quantum secret sharing,” Phys. Rev. A, vol. 59, no. 3, pp. 1829–1834, 1999.
[2] R. Cleve, D. Gottesman, and H. K. Lo, “How to share a quantum secret,” Phys. Rev. Lett., vol. 83, no. 3, pp. 648–651, 1999.
[3] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, “Quantum secret sharing schemes and reversibility of quantum operations,” Phys. Rev. A, vol. 72, no. 3, p. 032318, 2005.
[4] D. Gottesman, “Theory of quantum secret sharing,” Phys. Rev. A, vol. 61, no. 4, pp. 042311, 2000.
[5] K. Senthoo and P. K. Sarvepalli, “Communication efficient quantum secret sharing,” Phys. Rev. A, vol. 100, no. 5, p. 052313, 2019.
[6] W. Huang, M. Langberg, J. Kliewet, and J. Bruck, “Communication efficient secret sharing,” IEEE Trans. Inform. Theory, vol. 62, no. 12, pp. 7195 – 7206, 2016.
[7] R. Bitar and S. E. Rouayheb, “Staircase codes for secret sharing with optimal communication and read overheads,” IEEE Trans. Inform. Theory, vol. 64, no. 2, pp. 933–943, 2018.
[8] K. Senthoo and P. K. Sarvepalli, “Theory of communication efficient quantum secret sharing,” IEEE Trans. Inform. Theory, vol. 68, no. 5, pp. 3164–3186, 2022.
[9] U. Martínez-Peñas, “Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes,” IEEE Trans. Inform. Theory, vol. 64, no. 6, pp. 4191 – 4206, 2018.
[10] R. Matsumoto, “Coding theoretic construction of quantum ramp secret sharing,” e-print arXiv:1405.0149, 2014.
[11] K. Senthoo and P. K. Sarvepalli, “Concatenating extended CSS codes for communication efficient quantum secret sharing,” e-print quant-ph/2002.09229, 2022.
[12] A. Marin and D. Markham, “Equivalence between sharing quantum and classical secrets and error correction,” Phys. Rev. A, vol. 88, p. 042332, 2013.
[13] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A, vol. 54, no. 2, pp. 1098–1105, 1996.
[14] A. Steane, “Multiple-particle interference and quantum error correction,” Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 452, no. 1954, pp. 2551–2577, 1996.
[15] M. Grässl, T. Beth, and M. Roetteler, “On optimal quantum codes,” International Journal of Quantum Information, vol. 2, no. 01, pp. 55–64, 2004.
[16] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” IEEE Trans. Inform. Theory, vol. 52, no. 11, pp. 4892–4914, 2006.