Advance Sharing of Quantum Shares for Quantum Secrets

Mamoru SHIBATA, Nonmember and Ryutaroh MATSUMOTO, Senior Member

SUMMARY Secret sharing is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that only qualified sets of participants can restore the original secret from their shares. When we encode a secret by a secret sharing scheme and distribute shares, sometimes not all participants are accessible, and it is desirable to distribute shares to those participants before a secret information is determined. Secret sharing schemes for classical secrets have been known to be able to distribute some shares before a given secret. However, it is unknown whether distributing some shares before a given secret is possible with other access structures of secret sharing for quantum secrets. We propose a quantum secret sharing scheme for quantum secrets that can distribute some shares before a given secret with other access structures.

key words: quantum secret sharing, advance sharing, stabilizer code, EAQECC

1. Introduction

To protect important information from destruction or loss, we should not store it in one place, but we should store copies of it across multiple places and media. However, if the important information is secret, this strategy clearly increases the risk of information leakage. A revolutionary method to solve this problem is the secret sharing (SS), which was invented independently by Shamir [1] and Blakley [2] in 1979. SS is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that certain sufficiently large sets of participants can restore the secret from their shares. In quantum information theory, Hillery et al. [3] and Cleve et al. [4] simultaneously presented the quantum secret sharing (QSS) scheme in 1999. Cleve et al. clarified the relationships between QSS and quantum error-correcting codes. In that relations, a share of QSS is each qubit of a codeword in a quantum error-correcting code [4]. Quantum mechanics extends the capabilities of secret sharing beyond those of classical secret sharing [5]. QSS is actively studied recently [6], [7]. A set of participants that can restore a secret is called a qualified set, and a set of participants that can gain no information about a secret is called a forbidden set. The set of qualified sets and that of forbidden sets are called an access structure. A set of participants that are not qualified set is called an unqualified set.

SS for quantum secrets can be classified into two categories. One is perfect QSS and the other is non-perfect or ramp QSS [8]. In a perfect QSS, every unqualified set is a forbidden set. A major disadvantage of perfect SS is that the size of each share must be larger than or equal to that of the secret [5]. By tolerating partial information leakage to unqualified sets, the size of shares can be smaller than that of secret. Such QSS is called ramp QSS or non-perfect QSS. The ramp QSS was proposed by Ogawa et al. [8]. In an \((a, k, n)\)-ramp QSS, a dealer encodes \(k\) qudits of a quantum secret into \(n\) shares in such a way that any \(a\) or more shares can restore the secret while any \((a - k)\) or fewer shares have no information about the secret. A perfect \((a, 2a - 1)\)-threshold quantum secret sharing is a \((a, 1, 2a - 1)\)-ramp QSS.

Sometimes some participants are inaccessible after the dealer obtains a secret. The following situation was considered in [9]. In a country, the president suffers from a serious disease and is anxious about his sudden death. He is afraid that his death makes a national secret inaccessible to anyone if he alone knows about a national secret. For this reason, the president wishes to share a national secret to the dignitaries by a secret sharing scheme. A national secret is sensitive information and the president needs to hand encoded information of a national secret to the dignitaries. The president will obtain a national secret three days later but some dignitaries will make an extended business trip to foreign country from tomorrow. How can the president share the secret? In this situation, it is desirable for the dealer to distribute shares to some participants while the dealer can communicate with them. To realize this distribution, the dealer needs to be capable of distributing shares to some participants before a given secret.

We call a distribution of shares to some participants before a given secret “advance sharing” and a set of shares that can be distributed in advance is called “advance shareable” [9]. A pure state QSS is a QSS such that both secret and whole shares are pure states [4]. Lie et al. [10] found that perfect \((2, 3)\)-threshold quantum secret sharing can distribute a share before a given secret. The approach by Lie et al. utilizes a quantum masker to construct a QSS. Let \(|\psi\rangle\) be a quantum secret of a quantum system \(A\), and \(\sigma_B\) be an ancilla quantum mixed state of a quantum system \(B\). A quantum masker applies a unitary matrix to \(|\psi\rangle\) and \(\sigma_B\) in order to distribute \(|\psi\rangle\) to two parties \(A\) and \(B\) so that each party has no access to any information about the quantum secrets \(|\psi\rangle\).

© 2024 The Institute of Electronics, Information and Communication Engineers
Let $K$ be a purification of $\sigma_B$ meaning that there exists a bipartite pure state $|\Sigma\rangle_{BK}$ such that $\text{Tr}_K |\Sigma\rangle_{BK} = \sigma_B$. By applying the quantum masker for a quantum secret, each of the three quantum systems $A, B, K$ becomes a share of perfect $((2,3))$-threshold QSS. This means that any two groups of parties, $AB, AK$ or $BK$, can restore the quantum secret without help of the other party. This is because that if the quantum information is hidden from one party then it should be isometrically transferred to the remaining parties [8]. The quantum masker applies a unitary matrix to the quantum systems $A$ and $B$ without interacting the quantum system $K$. So, this perfect $((2,3))$-threshold QSS is capable of advance sharing of $K$. However, it is unknown whether advance sharing is possible without threshold or ramp QSS. We propose a scheme of advance sharing of quantum shares for stabilizer-based QSS by using EAQECC [11]. Our proposal is capable of constructing a ramp QSS and non-threshold QSS.

Brun et al. [11] proposed entanglement-assisted quantum error-correcting codes (EAQECCs). An EAQECC encodes $k$ information qubits with the help of $c$ maximally entangled pairs. An $[[n, k; c]]_p$ EAQECC works as follows:

1. Before the quantum communication begins, a sender and a receiver share some maximally entangled pairs. An $[[n, k; c]]_p$ EAQECC construction of EAQECC from a stabilizer, which later enables us to analyze the access structure of resulting QSS. Then, we propose a scheme of advance sharing for QSS by EAQECCs, and we clarify necessary and sufficient conditions of advance shareable sets in our proposal. We propose a sufficient condition of advance shareable set that can be verified without computing dimensions of linear spaces. The conclusions follow in Sect. 4.

2. Preliminaries

In this section, we review stabilizer codes and EAQECCs. Throughout this paper, we suppose that $p$ is a prime number.

2.1 Stabilizer Codes

Let $\{|i\rangle \; | i = 0, \ldots, p-1\}$ be an orthonormal basis for $p$-dimensional Hilbert space $\mathbb{C}^p$. Let $\omega$ be a complex number such that $\omega^p = 1$ and $\omega^1, \omega^2, \ldots, \omega^{p-1}$ are different. We define two unitary matrices $X_p, Z_p$ that change $|i\rangle$ as $X_p |i\rangle = |i+1 \mod p\rangle$ and $Z_p |i\rangle = |\omega^i \rangle |i\rangle$ for $i = 0, \ldots, p-1$. Consider the set $E_n = \{\omega^i X_p^{a_1} Z_p^{b_1} \cdots \cdots \cdots X_p^{a_n} Z_p^{b_n} | \{a_1, b_1, \ldots, a_i, b_i\} \in \{0, \ldots, p-1\} \}$. $E_n$ is a non-commutative finite group with matrix multiplication as its group operation. Denote by $\mathbb{F}_p$ the finite field with $p$ elements. For two vectors $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{b} = (b_1, \ldots, b_n)$, we define $X_p^{a_i} Z_p^{b_i} = Z_p^{b_i} X_p^{a_i}$ and $Z_p^{a_i} Z_p^{b_i} = Z_p^{b_i} Z_p^{a_i}$. For two vectors $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{b} = (b_1, \ldots, b_n)$, we define $X_p^{a_i} Z_p^{b_i} = Z_p^{b_i} X_p^{a_i}$ and $Z_p^{a_i} Z_p^{b_i} = Z_p^{b_i} Z_p^{a_i}$. For two vectors $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{b} = (b_1, \ldots, b_n)$, we define $X_p^{a_i} Z_p^{b_i} = Z_p^{b_i} X_p^{a_i}$ and $Z_p^{a_i} Z_p^{b_i} = Z_p^{b_i} Z_p^{a_i}$. For two vectors $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{b} = (b_1, \ldots, b_n)$, we define $X_p^{a_i} Z_p^{b_i} = Z_p^{b_i} X_p^{a_i}$ and $Z_p^{a_i} Z_p^{b_i} = Z_p^{b_i} Z_p^{a_i}$.

An error whose position is known is called an erasure. EAQECCs are also capable of correcting erasures.

We can construct a QSS capable of advance sharing by distributing $c$ halves of maximally entangled pairs to some participants before a given secret, then distributing each qudit of $\rho_n$ to the remaining participants after a given secret. A set of participants can restore the secret by an erasure correction procedure of EAQECC. In practical use, the access structure of QSS should be clear. However, since erasures of receiver’s $c$ halves of maximally entangled pairs in EAQECC are not considered, it is difficult to clarify the access structures of the QSS considered in this paragraph. So, we give a construction of EAQECC from a stabilizer, which enables us to analyze the access structure of QSS capable of advance sharing. By using our proposed construction of an EAQECC, we propose a QSS for quantum secrets that is capable of distributing some shares before a given secret. Then, we clarify a necessary and sufficient condition on advance-shareable sets in our proposal.

Our proposed QSS can have an access structure that cannot be constructed by the schemes of Lie et al. [10]. The schemes of Ogawa et al. cannot construct an $((a, k, n))$-ramp QSS whose share has dimension $n$ or less [8]. We will give an example of advanced sharing for a $((3,2,4))$-ramp QSS with 1-qubit shares. For an $[[n, k; c]]_p$ EAQECC, we usually desire a small value of $c$, and the advantage of a large $c$ was little known. Our proposed scheme shows the significance of constructing an EAQECC with a large $c$ because the size of the advance shareable set increases by larger $c$.

This paper is organized as follows. In Sect. 2, we review stabilizer codes and EAQECCs. In Sect. 3, we give a construction of EAQECC from a stabilizer, which later enables us to analyze the access structure of resulting QSS. Then, we propose a scheme of advance sharing for QSS by EAQECCs, and we clarify necessary and sufficient conditions of advance shareable sets in our proposal. We propose a sufficient condition of advance shareable set that can be verified without computing dimensions of linear spaces. The conclusions follow in Sect. 4.
We define a stabilizer generator \( X_p(\alpha)Z_\omega(b) \). The projective measurement corresponding to the simultaneous eigenspaces gives an error syndrome \( \hat{e} = (e_1, \ldots, e_{n-k}) \).

Then, it is possible to find an unitary matrix \( M_E = X_p(\alpha E)Z_\omega(b E) \) such that \( \langle \langle \alpha E | \hat{b} | E \rangle, \langle \alpha E | \hat{b} | E \rangle \rangle = e_i \) for every \( i = 1, \ldots, n - k \). If the erasures are less than \( d \), these can be corrected by applying \( M_E^{-1} \).

Now, we explain a way to describe a stabilizer set of generators for an arbitrary non-abelian subgroup \( B_n \). The projective measurement corresponding to the simultaneous eigenspaces is 4 and the minimum distance of this \( m \)-ary EAQECC [11], [12]. Suppose that a sender \( B'_n \), is a commutative subgroup of \( B_n \). For an arbitrary \( k \) qudits \( \{|\psi_k\rangle\} \), the codeword \( |\Psi\rangle \) of a stabilizer code \( Q(B'_n) \) can be written as follows:

\[
|\Psi\rangle = \sum_{(i_1, \ldots, i_c) \in \mathbb{Z}_p^c} \frac{1}{\sqrt{\mathbf{p}}} |i_1 \rangle \ldots |i_c \rangle |0\rangle^\otimes |\psi_k\rangle |i_1 \rangle \ldots |i_c \rangle.
\]

(8)

where the pairs of \( j \) and \( (n + j) \) qudits \((j = 1, 2, \ldots, c)\) of \( |\Psi\rangle \) form maximally entangled pairs. The \( (n + 1) \) th through \((n+c)\) th qudits of \( |\Psi\rangle \) are the receiver’s \( c \) halves of maximally entangled pairs. We define \( \bar{X}_j, \bar{X}'_j \) as

\[
\bar{X}_j = \bar{X}_j I^{\otimes j-1} \otimes X_p^{\mu_j} \otimes I^{\otimes c-j}, \quad 1 \leq j \leq c, \\
\bar{X}'_j = \bar{X}'_j I^{\otimes j-1} \otimes X_\omega^{\nu_j} \otimes I^{\otimes c-j}, \quad 1 \leq j \leq c, \\
\bar{Z}_j = \bar{Z}_j I^{\otimes c}, \quad c < j \leq c + \ell.
\]

(9)

Let \( B'_n \) be a group generated by \( \{Z'_1(1), \ldots, Z'_c(1), X'_1(1), \ldots, X'_c(1)\} \). Then, \( B'_n \) is a stabilizer contained in \( B_n \). Because \( B'_n \) is a commutative subgroup of \( B_n \). For an arbitrary \( k \) qudits \( \{|\psi_k\rangle\} \), the codeword \( |\Psi\rangle \) of a stabilizer code \( Q(B'_n) \) can be written as follows:

\[
|\Psi\rangle = \sum_{(i_1, \ldots, i_c) \in \mathbb{Z}_p^c} \frac{1}{\sqrt{\mathbf{p}}} |i_1 \rangle \ldots |i_c \rangle |0\rangle^\otimes |\psi_k\rangle |i_1 \rangle \ldots |i_c \rangle.
\]

(10)
Example 2. We define a non-abelian subgroup $G \subset E_3$ generator $(\overline{X}_1, \overline{Z}_1)$ as follows:

$$
\overline{X}_1 = X_2 \otimes X_2 \otimes X_2,
\overline{Z}_1 = Z_1 \otimes Z_1 \otimes Z_1.
$$  \hfill (11)

Then, generators of $B_G$ can be written as follows:

$$
X_{(1)} = X_2 \otimes I_2 \otimes I_2,
Z_{(1)} = Z_1 \otimes I_2 \otimes I_2.
$$  \hfill (12)

From Lemma 1, we can find a unitary matrix $U$ as follows:

$$
U = \langle 000 \rangle + \langle 001 \rangle \langle 111 \rangle + \langle 010 \rangle \langle 110 \rangle + \langle 011 \rangle \langle 010 \rangle + \langle 100 \rangle \langle 011 \rangle + \langle 101 \rangle \langle 100 \rangle + \langle 110 \rangle \langle 110 \rangle + \langle 111 \rangle \langle 001 \rangle.
$$

Generators $\{X'_{(1)}, Z'_{(1)}\}$ of $B_G'$ can be written as follows:

$$
X'_{(1)} = X_2 \otimes I_2 \otimes I_2 \otimes X_2,
Z'_{(1)} = Z_1 \otimes I_2 \otimes I_2 \otimes Z_1.
$$  \hfill (13)

$B_G'$ is a stabilizer contained in $E_{3+1}$. For an arbitrary 2 qubits $|\psi_2\rangle$, the codeword $\langle \Psi \rangle$ of a stabilizer code $Q(B_{G'})$ can be written as follows:

$$
\langle \Psi \rangle = \frac{1}{\sqrt{2}} \langle | 0 \rangle \otimes | \psi_2 \rangle \otimes | 0 \rangle + | 1 \rangle \otimes | \psi_2 \rangle \otimes | 1 \rangle \rangle. \hfill (14)
$$

Then, generators $\{\overline{X}'_{1}, \overline{Z}'_{1}\}$ of $G'$ can be written as follows:

$$
\overline{X}'_{1} = X_2 \otimes X_2 \otimes X_2 \otimes X_2,
\overline{Z}'_{1} = Z_1 \otimes Z_1 \otimes Z_1 \otimes Z_1.
$$  \hfill (15)

$G'$ is a stabilizer contained in $E_{3+1}$. The code space $Q(G')$ is given by

$$
Q(G') = \{ (U \otimes I_2) \langle \Psi \rangle \mid \langle \Psi \rangle \in Q(B_{G'}) \}.
$$  \hfill (16)

Then $Q(G, G', U)$ is an $[3, 2, 2, 1]_p$ EAQECC that employs 1 maximally entangled pairs and 0 ancilla qudits to encode 2 information qudits.

2.3 Stabilizer-Based QSS

We review a stabilizer-based QSS [4]. It is accomplished by the following steps:

**Algorithm 1 Stabilizer-based QSS**

1. A dealer encodes a quantum secret by a stabilizer code.
2. The dealer distributes each qudit of that codeword to a participant.

There are some procedures to restore the secret for stabilizer-based QSS [13]. One of the simplest procedures is to use erasure correction of the stabilizer code [4]. The access structure of a stabilizer-based QSS depends on the used stabilizer code. Stabilizer-based QSS can construct a ramp QSS from $[n, k]_p$ stabilizer codes with $k \geq 2$.

We review necessary and sufficient conditions for an index set $J \subset \{1, \ldots, n\}$ to be a qualified set in QSS based on a stabilizer $S$ [13]. We define $\overline{p}_p^J$ for $J$ as

$$
\overline{p}_p^J = \{ (a_1, \ldots, a_n) | b_1, \ldots, b_n | \in \overline{p}_p^J \}
$$

Then, an index set $J$ is a qualified set if and only if the equation

$$
f(S)^+ \cap \overline{p}_p^J = f(S) \cap \overline{p}_p^J \hfill (17)
$$

holds. In addition, an index set $J$ is a forbidden set if and only if the complement of a qualified set becomes a forbidden set [8].

3. QSS Constructed from EAQECC

In this section, we propose a scheme of advance sharing for QSS by EAQECC. First, we construct an EAQECC from a stabilizer to clarify the access structure of our proposal. Second, we propose a construction of QSS from EAQECC. Third, we clarify necessary and sufficient conditions for an index set $J \subset \{1, 2, \ldots, n\}$ to be an advance shareable set. Finally, we present a sufficient condition to be advance shareable set for an index set $J \subset \{1, 2, \ldots, n\}$.

3.1 EAQECC Constructed from a Stabilizer

For a stabilizer $S$, we introduce a construction of an EAQECC that has the same erasure correcting ability, including the receiver’s halves of maximally entangled pairs, as its stabilizer code $Q(S)$. Lai et al. presented a method of this construction in the binary case [15]. Here, we extend that method to the $p$-ary case.

Let $J \subset \{1, 2, \ldots, n\}$ be an index set. For a check matrix $H_S$ of a stabilizer and an index set $J$, we define conditions C1 and C2 as follows:

**C1** For $j \in J$, $j$th column of $H_S$ has 1 at only $j$th row and its other rows are 0.

**C2** For $j \in J$, $(n+j)$th column of $H_S$ has 1 at only $(n+j)$th row and its other rows are 0.

**Lemma 2.** If a check matrix $H_S$ of a stabilizer $S$ satisfies the conditions C1 and C2, there exists a check matrix $H'_S$ of $S$ that is written as follows:

$$
H'_S = \begin{bmatrix}
   h_{1,1} & \cdots & 0 & \cdots & 0 & \cdots & h_{1,2^n} \\
   \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
   h_{i,1} & \cdots & \mu_i & \cdots & 0 & \cdots & h_{i,2^n} \\
   \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
   h_{i+[j-1],1} & \cdots & 0 & \cdots & -1 & \cdots & h_{i+[j-1],2^n} \\
   \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\
   h_{n-k,1} & \cdots & 0 & \cdots & 0 & \cdots & h_{n-k,2^n}
\end{bmatrix}
$$

where $\mu_i = \sum_{j=1, j \neq i}^{n} h_{i,j} h_{i+[j-1],n+j} - \sum_{j=1, j \neq i}^{n} h_{i+[j-1],j} h_{i,n+j}$.

Since $S$ is an abelian subgroup of $E_n$, we have $\mu_i \neq 0$. 

We define the $j$-th column of $H_S$ as $h_{S,j}$. Here $h_{S,j}^* = (0, \ldots ,0, \mu_j, 0, \ldots ,0)^\dagger$ and $h_{S_n,j}^* = (0, \ldots ,0, -1, 0, \ldots ,0)^\dagger$ for $j \in J$. 

Proof of Lemma 2 is straightforward. So, we omit the proof. Let $S$ be a stabilizer contained in $E_n$. Let $\mathcal{T} = \{1, \ldots , n\}$. J

**Lemma 3.** There exist a unitary matrix $U_j$ and non-abelian subgroup $S'$ of $E_n-|J|$ such that $Q(S', S, U_j)$ is an $[[n-|J|, k, d; |J|]_p]_{EAQecc}$ that has the same erasure correcting ability as its stabilizer code $Q(S)$ if $J$ and a check matrix $H_S$ of $S$ satisfies the conditions C1 and C2.

**Proof.** From Lemma 2, if a check matrix $H_S$ of $S$ satisfies the conditions C1 and C2, there exists a check matrix $H_S'$ of $S$ that is written as follows:

$$H_S' = \begin{pmatrix} h_{1,1} & \cdots & 0 & \cdots & \cdots & 0 & \cdots & h_{1,2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{l,1} & \cdots & \mu_l & \cdots & 0 & \cdots & h_{l,2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{l+|J|,1} & \cdots & 0 & \cdots & \cdots & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{n-k,1} & \cdots & 0 & \cdots & \cdots & \cdots & 0 & \cdots \end{pmatrix}$$

where $h_{S,j}^* = (0, \ldots ,0, \mu_j, 0, \ldots ,0)^\dagger$ and $h_{S_n,j}^* = (0, \ldots ,0, -1, 0, \ldots ,0)^\dagger$ for $j \in J$. Then, we can define generators $\{G_1, \ldots , G_{n-k}\}$ of $S$ as follows:

$$G_i = \bigotimes_{j=1}^{n} X_{h_{i,j}^p} Z_{h_{i,n-j}^p}, \quad i = 1, \ldots , n-k$$

where $h_{i,j}$ is the $(i,j)$ component of $H_S'$. We define $\{G_1', \ldots , G_{n-k}'\}$ as follows:

$$G_i' = \bigotimes_{j=1}^{n} X_{h_{i,j}^p} Z_{h_{i,n-j}^p}, \quad i = 1, \ldots , n-k.$$
restore the secret while any single share has no information about the secret. So, this is a ((3, 2, 4))-ramp QSS. This ramp QSS cannot be constructed by the scheme of Lie et al. [10]. In addition, since the dimension of a share is 2 and the number of participants is 4, this ramp QSS cannot be constructed by the scheme of Ogawa et al. [8].

Let S be a stabilizer contained in $E_n$. Let $J$ be an index set that satisfies the conditions C1 and C2 with a check matrix $H_S$ of $S$. From Lemma 3, we can define $S^j$ and $U^j$ such that $(S^j, S, U^j)$ is an $[[n - |J|, k, d; |J||]]_p$ EAQECC that has the same erasure correcting ability as the stabilizer code $Q(S)$. We propose a QSS for quantum secrets with an index set $J$ being advance shareable as following algorithm:

**Algorithm 2 Our proposal**

1. A dealer prepares $|J|$ pairs of maximally entangled states and distributes $|J|$ halves of the maximally entangled states to participants in $J$.
2. The dealer encodes a $k$-qubit quantum secret $|\psi_k\rangle$ into $n - |J|$ qubits of a codeword of $Q(S^j, S, U^j)$.
3. The dealer distributes each qubit of the encoded state to the remaining participants.

A qualified set of participants can obtain a codeword of $Q(S)$ with erasures by attaching arbitrary qudits as the missing shares to available shares. Then, they can restore the secret by the erasure correction of the stabilizer code $Q(S)$. So, the access structure of our proposal with a stabilizer $S$ is the same as that of the QSS based on $S$. In our proposed QSS, shares of an index set $J$ can be distributed to some participants before a given secret. Our proposed QSS from $S$ and $J$ has the same access structure of the stabilizer-based QSS constructed from $S$. Since $[[n, k, d]]_p$ stabilizer codes can correct less than $d$ erasure, a set of $n + 1 - d$ more shares is a qualified set of our proposal. From [8, Proposition 3], a set of less than $d$ shares is a forbidden set of our proposal.

**Remark 1.** Our proposed QSS is constructed by using an $[[n - |J|, k, d; |J||]]_p$ EAQECC. So, the size of advance shareable set $|J|$ is the number of maximally entangled pairs of EAQECC. Therefore, our proposal shows the significance of constructing an EAQECC with a large number of maximally entangled pairs.

**Remark 2.** In our proposal, a set of shares distributed after a given secret is generated by applying unitary matrix $U_J$. So, the secret can be restored by applying $U_J$ to the set of shares distributed after a given secret. Hence, the complement of an advance shareable set is a qualified set. Since the complement of a qualified set is a forbidden set [8], any advance shareable sets are forbidden sets. Therefore, it is impossible to restore the secret in advance sharing phase.

3.3 Necessary and Sufficient Condition of Advance Shareable Sets

Shortening in this paper refers to making a new linear code $C' \subset \mathbb{F}_p^{22n-2}$ from a linear code $C \subset \mathbb{F}_p^{22n}$ by selecting vectors in $C$ where the $i$th and the $(n + i)$th components $(1 \leq i \leq n)$ are both zero and then eliminating the $i$th and the $(n + i)$th components of the selected vectors. Let $C_{[S]}^{(j)}$ be the code obtained by shortening the linear code $C$ for the element corresponding to the index set $J \subset \{1, \ldots, n\}$.

We clarify a necessary and sufficient condition that a set of shares $J$ is an advance shareable in our proposal.

**Theorem 1.** Let $S$ be a stabilizer contained in $E_n$. An index set $J \subset \{1, \ldots, n\}$ and a check matrix $H_S$ satisfy the conditions C1 and C2 if and only if the equation

$$\dim f(S)_J = \dim (f(S) - 2|J|)$$

holds.

**Proof.** For ease of presentation, without loss of generality we may assume $J = \{1, \ldots, |J|\}$ and $J = \{|J| + 1, \ldots, n\}$, by reordering indices. First, we prove $\dim f(S)_J = \dim (f(S) - 2|J|)$ if $J$ and $H_S$ satisfy the conditions C1 and C2. From Lemma 2, the check matrix of stabilizer $S$ is written as follows:

$$H_S = \begin{bmatrix} D_{|J|} & A & 0 & B' \\ 0 & A' & -I_{|J|} & B \\ 0 & E & 0 & F \end{bmatrix}.$$  

where $A, B, A', B'$ are $|J| \times (n - |J|)$ matrices, $E, F$ are $(n - k - 2|J|) \times (n - |J|)$ matrices and $D_{|J|}$ is a diagonal matrix whose $i$th diagonal components are $\mu_i$ that is defined in Lemma 2. Since the row space of $H_S$ is $f(S)$, we obtain $\dim f(S)_J = \dim (f(S) - 2|J|)$.

Second, we prove that there exist $H_S$ satisfy the conditions C1 and C2 if $\dim f(S)_J = \dim (f(S) - 2|J|)$. When the dimension of $f(S)$ is reduced by $2$ by shortening for $j$th and $(n + j)$th columns, there is a check matrix $H_S$ that can be written as follows [14]:

$$H_S = \begin{bmatrix} h_{1,1} & \cdots & 0 & \cdots & 0 & \cdots & h_{1,2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{j,1} & \cdots & 1 & \cdots & 0 & \cdots & h_{j,2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{j+|J|,1} & \cdots & 0 & \cdots & 1 & \cdots & h_{j+|J|,2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{n-k,1} & \cdots & 0 & \cdots & 0 & \cdots & h_{n-k,2n} \end{bmatrix}.$$  

(28)

For all of $j \in J$, the dimension of $f(S)$ is reduced by $2$ by shortening for $j$th and $(n + j)$th columns. Therefore, there exist $H_S$ satisfy the conditions C1 and C2.

**Remark 3.** A check matrix $H_S$ is not uniquely determined for a stabilizer $S$. However, if there exists $H_S$ satisfying C1 and C2 for $J$, then it is possible to construct a QSS where $J$ is an advance shareable set. So, whether a set $J$ is an
advance shareable set or not depends on the stabilizer $S$ and is independent of the choice of check matrix $H_S$.

**Example 5.** Let $S$ be the stabilizer defined in Example 1. Let $H_S$ be the check matrix of $S$ defined in Example 1. Here, $H_S$ satisfies the conditions C1 and C2. Let $J = \{\}$ be an index set. Since we have $f(S)_{(s)} = \emptyset$, we have $\dim f(S)^J_{(s)} = 0$. Therefore, we have $\dim f(S)_{(s)} = \dim f(S) - 2|J|$.

3.4 Sufficient Condition of Advance Shareable Sets

We present a sufficient condition for a set of shares $J$ to be advance shareable in our proposal. Let $J$ be an index set. Puncturing in this paper refers to making a new linear code $C' \subset \mathbb{F}_p^{2n+2}$ from a linear code $C \subset \mathbb{F}_p^n$ by eliminating the $i$th and the $(n+i)$th components ($1 \leq i \leq n$) of all vectors in $C$. Let $C^J_{(s)}$ be the code obtained by puncturing the linear code $C$ for the element corresponding to the index set $J \subset \{1, \ldots, n\}$. We define the symplectic weight of $(a|b) \in C$ as $w_a(a|b) = \#\{i \mid (a_i, b_i) \neq 0\}$. We define the minimum weight of $C$ as $d_{\text{min}}(C) = \min\{w_a(a|b) \mid (a|b) \in C, (a|b) \neq 0\}$.

The following sufficient condition can be verified without computing dimensions of linear spaces.

**Theorem 2.** Let $S$ be a stabilizer contained in $E_n$. Let $Q(S)$ be a $[[n, k, 1]]$ stabilizer code. A set of shares $J$ to be advance shareable in our proposal with $Q(S)$, i.e.,

$$\dim f(S)^{(J)}_{(s)} = \dim f(S) - 2|J|$$

(29)

if

$$|J| < d_{\text{min}}(f(S)\downarrow)$$

(30)

holds.

**Proof.** According to Lemma 1.1 of the reference [14], for $[[n, k, 1]]_p$ stabilizer code $Q(S)$, if $|J| < d_{\text{min}}(f(S)\downarrow)$ holds, then we have $\dim f(S)^\downarrow = \dim (f(S)^{(J)})_{(p)}$. We have $f(S)_{(s)} = ((f(S)^\downarrow)^{(J)})_{(p)}$. Then,

$$\dim f(S)^{(J)}_{(s)} = \dim ((f(S)^\downarrow)^{(J)})_{(p)}$$

(31)

$$= 2n - 2|J| - \dim (f(S)^\downarrow)^{(J)}_{(p)}$$

(32)

$$= 2n - 2|J| - \dim f(S)^\downarrow$$

(33)

$$= \dim f(S) - 2|J|.$$  

(34)

Therefore, if $|J| < 2$ holds, an index set $J$ is advance shareable in our proposal for this stabilizer $S$.

4. Conclusion

In our paper, we propose a quantum secret sharing scheme that can distribute some shares before a given secret. In Sect. 3, we provide a construction of an EAQECC from a stabilizer, whose erasure correcting ability is the same as the original stabilizer code. Then, we clarify the access structures of our proposed quantum secret sharing. In Example 4, we confirm that our proposal can construct $((3, 2, 4))$-ramp QSS with 1-qubit shares. This ramp QSS cannot be constructed by the schemes of Lie et al. [10] nor Ogawa et al. [8]. We clarify a necessary and sufficient condition on advance shareable sets. In Remark 1, our proposal shows the significance of constructing an EAQECC with a large number of maximally entangled pairs. We give a sufficient condition of advance shareable set that can be verified without using the dimensions of linear spaces. Therefore, our proposal can provide a useful method of advance sharing when a dealer unable to communicate with some participants after the dealer obtains a secret.

Acknowledgments

The author would like to thank Professor Tomohiko Uematsu for a helpful advice. This work was supported by JST SPRING Grant Number JPMJSP2106 and JSPS Grant No. 23K10980.

References

Mamoru Shibata received the B.E. degree in computer science, the M.E. degree in communication engineering from the Tokyo Institute of Technology, Japan, in 2019, and 2021, respectively, where he is currently pursuing the Ph.D. degree with the Department of Information and Communications Engineering.

Ryutaroh Matsumoto received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1996, 1998, and 2001, respectively. From 2001 to 2004, he was an Assistant Professor with the Department of Information and Communications Engineering, Tokyo Institute of Technology, where he was an Associate Professor, from 2004 to 2017. From 2017 to 2020, he was an Associate Professor with the Department of Information and Communication Engineering, Nagoya University, Nagoya, Japan. Since 2020, he has been an Associate Professor, and promoted to a Full Professor, in August 2022, with the Department of Information and Communications Engineering, Tokyo Institute of Technology. In 2011 and 2014, he was as a Velux Visiting Professor with the Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark. His research interests include error-correcting codes, quantum information theory, information theoretic security, and communication theory. Dr. Matsumoto was a recipient of the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He was also a recipient of the Best Paper Awards from IEICE in 2001, 2008, 2011, and 2014.