PAPER

Advance Sharing of Quantum Shares for Quantum Secrets

Mamoru SHIBATA [†a)], *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. Lie et al. found a $((2,3))$-threshold secret sharing for quantum secrets can 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 σ_B be an ancilla quantum mixed state of a quantum system B. A quantum masker applies a unitary matrix to $|\psi\rangle$ and σ_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 $|\psi\rangle$.

Manuscript received April 17, 2023.
Manuscript revised September 1, 2023.
Manuscript publicized November 24, 2023.

[†]Department of Information and Communications Enginnering, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
a) E-mail: shibata@it.ict.e.titech.ac.jp

DOI: 10.1587/transfun.2023EAP1041

Let K be a purification of σ_B meaning that there exists a bipartite pure state $|\Sigma\rangle_{BK}$ such that $\mathrm{Tr}_K |\Sigma\rangle\langle\Sigma|_{BK} = \sigma_B$. 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 with non-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 qudits with the help of c maximally entangled pairs. An $[[n,k;c]]_p$ EAQECC works as follows:

1. Before the qunautum communication begins, a sender and a receiver share some maximally entangled pairs.
2. The sender encodes k information qudits $|\psi_k\rangle$ together with $\ell = n - c - k$ ancilla qudits and the sender's half of the c entangled pairs into n qudits ρ_n.
3. The sender sends ρ_n to the receiver through a noisy communication channel.
4. The receiver combines the received noisy qudits with the receiver's half of the c entangled pairs and performs measurements on all $(n + c)$ qudits to distinguish the error.
5. The receiver performs a recovery operation to restore the k information qudits.

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 ρ_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.

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 $\{|i\rangle \mid i = 0,\dots,p-1\}$ be an orthonormal basis for p-dimensional Hilbert space $\mathbb{C}^p$. Let ω be a complex number such that is $\omega^p = 1$ and $\omega^1, \omega^2, \dots, \omega^{p-1}$ are different. We define two unitary matrices X_p, Z_ω that change $|i\rangle$ as $X_p|i\rangle = |i+1 \mod p\rangle$ and $Z_\omega|i\rangle = \omega^i|i\rangle$ for $i = 0,\dots,p-1$. Consider the set $E_n = \{\omega^i X_p^{a_1} Z_\omega^{b_1} \otimes \cdots \otimes X_p^{a_n} Z_\omega^{b_n} \mid i, a_j, b_j \in \{0,\dots,p-1\} \text{ for } j = 1,\dots,n\}$. 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 $\vec{a} = (a_1,\dots,a_n)$ and $\vec{b} = (b_1,\dots,b_n) \in \mathbb{F}_p^n$, we define $X_p(\vec{a}) = X_p^{a_1} \otimes \cdots \otimes X_p^{a_n}$ and $Z_\omega(\vec{b}) = Z_\omega^{b_1} \otimes \cdots \otimes Z_\omega^{b_n}$. For two vectors $(\vec{a} \mid \vec{b}), (\vec{c} \mid \vec{d}) \in \mathbb{F}_p^{2n}$, the sympectic inner product is defined by

$$\langle(\vec{a} \mid \vec{b}), (\vec{c} \mid \vec{d})\rangle_s = \langle\vec{a}, \vec{d}\rangle_E - \langle\vec{b}, \vec{c}\rangle_E, \tag{1}$$

where $\langle\cdot \mid \cdot\rangle_E$ is the Euclidean inner product. We define the weight of $\omega^i X_p(\vec{a}) Z_\omega(\vec{b}) \in E_n$ as $w(\omega^i X_p(\vec{a}) Z_\omega(\vec{b})) = \sharp\{i \mid (a_i, b_i) \neq 0\}$. We call a commutative subgroup of E_n as a stabilizer. Let S be a stabilizer contained in E_n. Let $S' = \{M \in E_n \mid MN = NM \text{ for } \forall N \in S\}$, and let $\overline{S}$ be the commutative subgrous of E_n generated by $\omega I_p^{\otimes n}$ and S. Here I_p is the identity matrix on $\mathbb{C}^p$. We define the minimum distance of a stabilizer S by $d(S) = \min\{w(M) \mid M \in S' \backslash \overline{S}\}$.

Suppose that eigenspaces of a stabilizer S have dimension p^k. An $[[n,k]]_p$ quantum stabilizer code $Q(S)$ encoding k qudits into n qudits can be defined as a simultaneous eigenspace of all elements of S. Sometimes we will write $[[n,k,d]]_p$ stabilizer code to indicate that the distance of the code is d. An $[[n,k,d]]_p$ stabilizer code is capable of correcting less than d erasures. The erasure correcting procedure of an $[[n,k]]_p$ stabilizer code $Q(S)$ is as follows. Let a

generators of S be $\{X_p(\vec{a_1})Z_\omega(\vec{b_1}),\ldots,X_p(\vec{a_{n-k}})Z_\omega(\vec{b_{n-k}}))\}$. The projective measurement corresponding to the simultaneous eigenspaces gives an error syndrome $\vec{e}=(e_1,\ldots,e_{n-k})$. Then, it is possible to find an unitary matrix $M_E = X_p(\vec{a_E})Z_\omega(\vec{b_E})$ such that satisfy $\langle(\vec{a_i}|\vec{b_i}),(\vec{a_E}|\vec{b_E})\rangle_s = e_i$ for every $i=1,\ldots,n-k$. If the erasures are less than d, these can be corrected by applying $M_E^\dagger$.

Now, we explain a way to describe a stabilizer S by finite fields. For an $(n-k)$-dimensional $\mathbb{F}_p$-linear subspace C of $\mathbb{F}_p^{2n}$, we define $C^\perp = \{\vec{a}\in\mathbb{F}_p^{2n} \mid \forall\vec{b}\in C, \langle\vec{a},\vec{b}\rangle_s = 0\}$. We define $M(\vec{a}|\vec{b})$ as $M(\vec{a}|\vec{b}) = X_p(\vec{a})Z_\omega(\vec{b}) \in E_n$ with $\vec{a},\vec{b}\in\mathbb{F}_p^n$. We define a mapping $f(\omega^i M(\vec{a}|\vec{b}))$ from E_n to $\mathbb{F}_p^{2n}$ by $f(\omega^i M(\vec{a}|\vec{b})) = (\vec{a}|\vec{b})$. For a stabilizer S, $f(S)$ is an $\mathbb{F}_p$-linear space. We define a check matrix of a stabilizer S as a matrix $H_S = [H_X \mid H_Z]$ whose row space is $f(S)$.

Example 1. We define a stabilizer generator $\{M_1, M_2\}$ as follows:

$$\begin{array}{rcccccccc} M_1 &=& X_2 &\otimes& X_2 &\otimes& X_2 &\otimes& X_2, \\ M_2 &=& Z_{-1} &\otimes& Z_{-1} &\otimes& Z_{-1} &\otimes& Z_{-1}. \end{array} \tag{2}$$

We define a basis of the simultaneous $+1$ eigenspace Q of this stabilizer $\{|00_L\rangle, |01_L\rangle, |10_L\rangle, |11_L\rangle\}$ as follows:

$$\begin{array}{rcl} |00_L\rangle &=& \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle), \\ |01_L\rangle &=& \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle), \\ |10_L\rangle &=& \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle), \\ |11_L\rangle &=& \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle) \end{array} \tag{3}$$

The dimension of Q is 4 and the minimum distance of this stabilizer is 2. Thus, Q is a $[[4,2,2]]_2$ stabilizer code. A check matrix of this stabilizer can be written as follows:

$$H = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]. \tag{4}$$

This stabilizer code is capable of correcting 1 erasure.

2.2 EAQECC

We review p-ary EAQECC [11], [12]. Suppose that a sender and a receiver share c pairs of maximally entangled states. For an arbitrary non-abelian subgroup $G\subset E_n$, there exist a set of generators $\{\overline{Z}_1,\overline{Z}_2,\ldots,\overline{Z}_{c+\ell},\overline{X}_1,\ldots,\overline{X}_c\}$ for G where $c\geq 1, k\geq 0, \ell = n-c-k$ with the following commutative relations:

$$\begin{array}{ll} [\overline{X}_i,\overline{X}_j]=0, & \forall 1\leq i,j\leq c, \\ [\overline{Z}_i,\overline{Z}_j]=0, & \forall 1\leq i,j\leq c+\ell, \\ [\overline{X}_i,\overline{Z}_j]=0, & \forall i\neq j, 1\leq i\leq c, 1\leq j\leq c+\ell, \\ [\overline{X}_i,\overline{Z}_i]\neq 0, & \forall 1\leq i\leq c. \end{array} \tag{5}$$

Here $[\cdot,\cdot]$ is the commutator, $[A,B]=AB-BA$ for $A,B\in E_n$. Let μ_i be an integer such that $\overline{X}_i\overline{Z}_i = \omega^{-\mu_i}\overline{Z}_i\overline{X}_i$. We define $X_{(i)}, Z_{(j)}$ for $i=1,2,\ldots,c$ and $j=1,2,\ldots,c+\ell$ as:

$$\begin{array}{l} X_{(i)} = I^{\otimes i-1}\otimes X_p^{\mu_i}\otimes I^{\otimes n-i}, \\ Z_{(j)} = I^{\otimes j-1}\otimes Z_\omega\otimes I^{\otimes n-j}. \end{array} \tag{6}$$

We define a subgroup B_G of E_n generated by $\{Z_{(1)},\ldots,Z_{(c+\ell)},X_{(1)},\ldots,X_{(c)}\}$.

Since the groups B_G and G are isomorphic as groups, we can relate B_G to G by following lemma [12]:

Lemma 1. If B_G is defined as above, then there exists a unitary U such that for all $b\in B_G$ there exists an $g\in G$ such that $b = UgU^\dagger$ up to an overall phase. □

We define $X'_{(i)}, Z'_{(j)}$, as:

$$\begin{array}{ll} X'_{(i)} = X_{(i)}\otimes I^{\otimes i-1}\otimes X_p^{\mu_i}\otimes I^{\otimes c-i}, & 1\leq i\leq c, \\ Z'_{(j)} = Z_{(j)}\otimes I^{\otimes j-1}\otimes Z_\omega^{-1}\otimes I^{\otimes c-j}, & 1\leq j\leq c, \\ Z'_{(j)} = Z_{(j)}\otimes I^{\otimes c}, & c<j\leq c+\ell. \end{array} \tag{7}$$

Let B'_G be a group generated by $\{Z'_{(1)},\ldots,Z'_{(c+\ell)},X'_{(1)},\ldots,X'_{(c)}\}$. Then, B'_G is a stabilizer contained in E_{n+c} because B'_G is a commutative subgroup of E_{n+c}. For an arbitrary k qudits $|\psi_k\rangle$, the codeword $|\Psi\rangle$ of a stabilizer code $Q(B'_G)$ can be written as follows:

$$|\Psi\rangle = \sum_{(i_1,\ldots,i_c)\in\mathbb{F}_p^c} \frac{1}{\sqrt{p^c}}|i_1\rangle\ldots|i_c\rangle|0\rangle^{\otimes\ell}|\psi_k\rangle|i_1\rangle\ldots|i_c\rangle \tag{8}$$

where the pairs of jth and $(n+j)$th 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 $\overline{Z}'_i, \overline{X}'_i$ as

$$\begin{array}{ll} \overline{X}'_i = \overline{X}_i\otimes I^{\otimes i-1}\otimes X_p^{\mu_i}\otimes I^{\otimes c-i}, & 1\leq i\leq c, \\ \overline{Z}'_j = \overline{Z}_j\otimes I^{\otimes j-1}\otimes Z_\omega^{-1}\otimes I^{\otimes c-j}, & 1\leq j\leq c, \\ \overline{Z}'_j = \overline{Z}_j\otimes I^{\otimes c}, & c<j\leq c+\ell. \end{array} \tag{9}$$

Let G' be a group generated by $\{\overline{Z'}_1,\ldots,\overline{Z'}_{c+\ell},\overline{X'}_1,\ldots,\overline{X'}_c\}$. Then, G' is a stabilizer contained in E_{n+c} because G' is a commutative subgroup of E_{n+c}. We define a stabilizer code $Q(G')$. From Lemma 1, a code space $Q(G')$ is given by

$$Q(G') = \{(U\otimes I^{\otimes c})|\Psi\rangle \mid |\Psi\rangle\in Q(B'_G)\}. \tag{10}$$

The sender applies the encoding operation U on information qudits $|\psi_k\rangle$, the sender's halves of the entangled pair, and $\ell = n-k-c$ ancilla qudits. The sender then sends n qudits through a noisy channel to the receiver. The receiver combines the received n qudits and the receiver's c halves of the entangled pair. The receiver correct the erasures in the resulting $(n+c)$ qudits by the stabilizer code $Q(G')$, and decode the information qudits $|\psi_k\rangle$ by applying $(U\otimes I^{\otimes c})^{-1}$.

Then $Q(G,G',U)$ is an $[[n,k,d;c]]_p$ EAQECC that employs c maximally entangled pairs and $\ell = n-k-c$ ancilla qudits to encode k information qudits. The erasure correcting ability of $Q(G,G',U)$, including receiver's halves of maximally entangled pairs, is the same as a stabilizer code $Q(G')$.

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

$$\begin{array}{rcccccc} \overline{X}_1 & = & X_2 & \otimes & X_2 & \otimes & X_2, \\ \overline{Z}_1 & = & Z_{-1} & \otimes & Z_{-1} & \otimes & Z_{-1}. \end{array} \tag{11}$$

Then, generators of B_G can be written as follows:

$$\begin{array}{rcccccc} X_{(1)} & = & X_2 & \otimes & I_2 & \otimes & I_2, \\ Z_{(1)} & = & Z_{-1} & \otimes & I_2 & \otimes & I_2. \end{array} \tag{12}$$

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

$$\begin{aligned} U = &|000\rangle\langle 000| + |001\rangle\langle 111| + |010\rangle\langle 110| + |011\rangle\langle 010| \\ &+ |100\rangle\langle 011| + |101\rangle\langle 100| + |110\rangle\langle 110| + |111\rangle\langle 001|. \end{aligned}$$

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

$$\begin{array}{rcccccccc} X'_{(1)} & = & X_2 & \otimes & I_2 & \otimes & I_2 & \otimes & X_2, \\ Z'_{(1)} & = & Z_{-1} & \otimes & I_2 & \otimes & I_2 & \otimes & Z_{-1}. \end{array} \tag{13}$$

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

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

Then, generators $\{\overline{X'}_1, \overline{Z'}_1\}$ of G' can be written as follows:

$$\begin{array}{rcccccccc} \overline{X'}_1 & = & X_2 & \otimes & X_2 & \otimes & X_2 & \otimes & X_2, \\ \overline{Z'}_1 & = & Z_{-1} & \otimes & Z_{-1} & \otimes & Z_{-1} & \otimes & Z_{-1}. \end{array} \tag{15}$$

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

$$Q(G') = \{(U \otimes I_2)|\Psi\rangle \mid |\Psi\rangle \in Q(B'_G)\}. \tag{16}$$

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 infromation 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 $\mathbb{F}_p^{\overline{J}}$ for J as

$$\begin{aligned} \mathbb{F}_p^{\overline{J}} = \{(a_1, \ldots, a_n | b_1, \ldots, b_n) \in \mathbb{F}_p^{2n} | \\ j \in J \Rightarrow (a_j, b_j) = (0, 0)\} \end{aligned} \tag{17}$$

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

$$f(S)^{\perp} \cap \mathbb{F}_p^{\overline{J}} = f(S) \cap \mathbb{F}_p^{\overline{J}} \tag{18}$$

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 $j \in J$, jth column of H_S has 1 at only jth 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:

$$H'_S = \left[\begin{array}{ccccc|ccc} h_{1,1} & \cdots & 0 & \cdots & & \cdots & 0 & \cdots & h_{1,2n} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ h_{i,1} & \cdots & \mu_i & \cdots & & \cdots & 0 & \cdots & h_{i,2n} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ h_{i+|J|,1} & \cdots & 0 & \cdots & & \cdots & -1 & \cdots & h_{i+|J|,2n} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ h_{n-k,1} & \cdots & 0 & \cdots & & \cdots & 0 & \cdots & h_{n-k,2n} \end{array}\right]$$

where $\mu_i = \sum_{j=1, j\neq i}^{n} h_{i,j} h_{i+|J|,n+j} - \sum_{j=1, j\neq i}^{n} h_{i+|J|,j} h_{i,n+j}$. Since S is an abelian subgroup of E_n, we have $\mu_i \neq 0$.

We denote the j-th column of H_S as $\vec{h_{Sj}}$. Here $\vec{h_{Sj}} = (0,\ldots,0,\mu_i,0,\ldots,0)^\top$ and $\vec{h_{Sn+j}} = (0,\ldots,0,-1,0,\ldots,0)^\top$ 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 $\overline{J} = \{1,\ldots,n\}\backslash J$.

Lemma 3. There exist a unitary matrix U_J and non-abelian subgroup S^J of $E_{n-|J|}$ such that $Q(S^J,S,U_J)$ 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 satisfy 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:

$$H'_S = \left[\begin{array}{cccc|cccc} h_{1,1} & \cdots & 0 & \cdots & \cdots & 0 & \cdots & h_{1,2n} \\ \vdots & & \vdots & & & \vdots & & \vdots \\ h_{i,1} & \cdots & \mu_i & \cdots & \cdots & 0 & \cdots & h_{i,2n} \\ \vdots & & \vdots & & & \vdots & & \vdots \\ h_{i+|J|,1} & \cdots & 0 & \cdots & \cdots & -1 & \cdots & h_{i+|J|,2n} \\ \vdots & & \vdots & & & \vdots & & \vdots \\ h_{n-k,1} & \cdots & 0 & \cdots & \cdots & 0 & \cdots & h_{n-k,2n} \end{array}\right] \tag{19}$$

where $\vec{h_{Sj}} = (0,\ldots,0,\mu_i,0,\ldots,0)^\top$ and $\vec{h_{Sn+j}} = (0,\ldots,0,-1,0,\ldots,0)^\top$ for $j \in J$. Then, we can define generators $\{G_1,\ldots,G_{n-k}\}$ of S as follows:

$$G_i = \bigotimes_{j=1}^n X_p^{h_{i,j}} Z_\omega^{h_{i,n+j}}, \quad i = 1,\ldots,n-k \tag{20}$$

where $h_{i,j}$ is the (i,j) component of H'_S. We define $\{G^J_1,\ldots,G^J_{n-k}\}$ as follows:

$$G^J_i = \bigotimes_{\substack{j=1,\\ j\notin J}}^n X_p^{h_{i,j}} Z_\omega^{h_{i,n+j}}, i = 1,\ldots,n-k. \tag{21}$$

Let S^J be a subgroup of $E_{n-|J|}$ generated by $\{G^J_1,\ldots,G^J_{n-k}\}$. We define $\{x_1,x_2,\ldots,x_{|J|}\} \subset \overline{J}$ and $\{z_{2|J|+1},z_{2|J|+2},\ldots,z_{n-k}\} \subset \overline{J}$ such that all of x_i,z_i are different from each other. We define $g_{j,l}$ as follows:

$$\begin{array}{cc} g_{j,j} = g_{j,x_j} = X_p^{\mu_j}, & j \in J, \\ g_{j+|J|,j} = Z_\omega, & j \in J, \\ g_{j+|J|,x_j} = Z_\omega^{-1}, & j \in J, \\ g_{i,z_i} = Z_\omega, & i \in \{2|J|+1,\ldots,n-k\}, \\ g_{i,j} = I_p, & \text{otherwise.} \end{array} \tag{22}$$

We define $\{G'^J_1,\ldots,G'^J_{n-k}\}$ and $\{G'_1,\ldots,G'_{n-k}\}$ as follows:

$$G'^J_j = \bigotimes_{\substack{l=1,\\ l\notin J}}^n g_{j,l}, \tag{23}$$

$$G'_j = \bigotimes_{l=1}^n g_{j,l}. \tag{24}$$

Let B^J_S be a subgroup of $E_{n-|J|}$ generated by $\{G'^J_1,\ldots,G'^J_{n-k}\}$. Considering the mapping $G^J_j \mapsto G'^J_j$, we see that S^J and B^J_S are isomorphic. Since the groups B^J_S and S^J are isomorphic as groups, there exists a unitary U_J such that for all $b \in B^J_S$ there exists an $g \in S^J$ such that $b = U_J g U_J^\dagger$ up to overall phase. Let B_S be a subgroup of E_n generated by $\{G'_1,\ldots,G'_{n-k}\}$. Let $Q(B_S)$ be a stabilizer code of B_S. Since S^J and B^J_S are isomorphic and we have $X_p^{h_{i,j}} Z_\omega^{h_i,n+j} = g_{i,j}$ for $j \in J$, $i = 1,\ldots,n-k$, the groups S and B_S are isomorphic. Then, we can construct an $[[n-|J|,k,d;|J|]]_p$ EAQECC $Q(S^J,S,U_J)$ by the procedure in Sect. 2. In the decoding procedure of (S^J,S,U_J), we correct the erasures by the stabilizer code $Q(S)$. So, $Q(S^J,S,U_J)$ has the same erasure correcting ability as $Q(S)$. □

Example 3. Let S be the stabilizer defined in Example 1. Let $J = \{4\}$ be an index set. Here, the check matrix H_S of S, which is defined in Example 1, satisfies the conditions C1 and C2. We define S^J and its generator $\{G^J_1,G^J_2\}$ as follows:

$$\begin{array}{rcccccc} G^J_1 & = & X_2 & \otimes & X_2 & \otimes & X_2, \\ G^J_2 & = & Z_{-1} & \otimes & Z_2 & \otimes & Z_2. \end{array} \tag{25}$$

Then, S^J is the same as G in Example 2. Therefore, $Q(S^J,S,U_J)$ is a $[[3,2,2;1]]_p$ EAQECC. In the decoding procedure of $Q(S^J,S,U_J)$, we correct the erasures by the $[[4,2,2]]_p$ stabilizer code $Q(S)$.

3.2 Our Proposed Encoding Method for QSS

When a set of shares corresponding to an index set J can be distributed before a given secret, the index set J is called an "advance shareable set". We give an example of a QSS for quantum secrets with an index set J being advance shareable as follows:

Example 4. Let S be the stabilizer defined in Example 1. We define an index set $J = \{4\}$ as an advance shareable set. Let $Q(S^J,S,U_J)$ be the $[[3,2,2;1]]_p$ EAQECC defined in Example 3. The procedure of a QSS with an index set J being advance shareable is as follows:

1. A dealer prepares a maximally entangled pair and distribute a half of the maximally entangled state to 4th participant.
2. The dealer encodes a 2-qubit quantum secret $|\psi_2\rangle$ into 3 qudits of a codeword of the EAQECC.
3. The dealer distributes each qubit of the encoded state to the remaining participants.

All the shares constitute of a codeword of $Q(S)$ that is capable of correcting 1 erasure, so 3 or more participants can restore the secret. This QSS encodes 2 qubits of a quantum secret into 4 shares in such a way that any 3 or more shares can

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-qudit quantum secret $|\psi_k\rangle$ into $n-|J|$ qudits of a codeword of $Q(S^J, S, U_J)$.
3: The dealer distributes each qudit 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 $n+1-d$ or 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 $U_J^\dagger$ 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 $C' \subset \mathbb{F}_p^{2n-2}$ from a linear code $C \subset \mathbb{F}_p^{2n}$ by selecting vectors in C where the ith and the $(n+i)$th components $(1 \le i \le n)$ are both zero and then eliminating the ith 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 $J \subset \{1,\dots,n\}$.

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 $J \subset \{1,\dots,n\}$ and a check matrix H_S satisfy the conditions C1 and C2 if and only if the equation

$$\dim f(S)_{(s)}^{(J)} = \dim f(S) - 2|J| \tag{26}$$

holds.

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

$$H_S = \left[\begin{array}{cc|cc} D_{|J|} & A & 0 & B' \\ 0 & A' & -I_{|J|} & B \\ 0 & E & 0 & F \end{array}\right], \tag{27}$$

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 ith diagonal components are μ_i that is defined in Lemma 2. Since the row space of H_S is $f(S)$, we obtain $\dim f(S)_{(s)}^{(J)} = \dim f(S) - 2|J|$.

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

$$H_S = \left[\begin{array}{ccccc|ccccc} h_{1,1} & \cdots & 0 & \cdots & & \cdots & 0 & \cdots & h_{1,2n} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ h_{j,1} & \cdots & 1 & \cdots & & \cdots & 0 & \cdots & h_{j,2n} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ h_{j+|J|,1} & \cdots & 0 & \cdots & & \cdots & 1 & \cdots & h_{j+|J|,2n} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ h_{n-k,1} & \cdots & 0 & \cdots & & \cdots & 0 & \cdots & h_{n-k,2n} \end{array}\right]. \tag{28}$$

For all of $j \in J$, the dimension of $f(S)$ is reduced by 2 by shortening for jth 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 $J = \{4\}$ be an index set. Since we have $f(S)^{(J)}_{(s)} = \{\vec{0}\}$, we have $\dim f(S)^{(J)}_{(s)} = 0$. Therefore, we have $\dim f(S)^{(J)}_{(s)} = \dim f(S) - 2|J|$.

3.4 Suffcient 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 $C \subset \mathbb{F}_p^{2n}$ by eliminating the ith and the $(n+i)$th components $(1 \le i \le n)$ of all vectors in C. Let $C^{(J)}_{(p)}$ 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 $(\vec{a}|\vec{b}) \in C$ as $w_s(\vec{a}|\vec{b}) = \sharp\{i \mid (a_i, b_i) \neq 0\}$. We define the minimum weight of C as $d_{min}(C) = \min\{w_s(\vec{a}|\vec{b}) \mid (\vec{a}|\vec{b}) \in C, (\vec{a}|\vec{b}) \neq \vec{0}\}$.

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 $[[n,k]]_p$ stabilizer code. A set of shares J to be advance shareable in our proposal with $Q(S)$, i.e.,

$$\dim f(S)^{(J)}_{(s)} = \dim f(S) - 2|J| \tag{29}$$

if

$$|J| < d_{min}(f(S)^{\perp}) \tag{30}$$

holds.

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

$$\begin{aligned}
\dim f(S)^{(J)}_{(s)} &= \dim ((f(S)^{\perp})^{(J)}_{(p)})^{\perp} && (31)\\
&= 2n - 2|J| - \dim (f(S)^{\perp})^{(J)}_{(p)} && (32)\\
&= 2n - 2|J| - \dim f(S)^{\perp} && (33)\\
&= \dim f(S) - 2|J|. && (34)
\end{aligned}$$

□

So, an index set J is advance shareable set in QSS based on a $[[n,k]]_p$ stabilizer code $Q(S)$ if $|J| < d_{min}(f(S)^{\perp})$ holds.

Example 6. Let S be a stabilizer defined in Example 1. The following set is a basis of $f(S)$:

$$\left\{ \begin{array}{l} (1111|0000), \\ (0000|1111) \end{array} \right\}. \tag{35}$$

Then the following set is a basis of $f(S)^{\perp}$:

$$\left\{ \begin{array}{l} (0011|0000), \\ (0101|0000), \\ (1001|0000), \\ (0000|0011), \\ (0000|0101), \\ (0000|1001) \end{array} \right\}. \tag{36}$$

We have following identity:

$$d_{min}(f(S)^{\perp}) = 2. \tag{37}$$

Therefore, if $|J| < 2$ holds, an index set J is advance shareable in our propsal 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

[1] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, Nov. 1979.
[2] G.R. Blakley, "Safeguarding cryptographic keys," 1979 International Workshop on Manageing Requirements Knowledge (MARK), pp.313–318, 1979.
[3] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol.59, pp.1829–1834, March 1999.
[4] R. Cleve, D. Gottesman, and H.K. Lo, "How to share a quantum secret," Phys. Rev. Lett., vol.83, no.3, pp.648–651, Jul6 1999.
[5] D. Gottesman, "Theory of quantum secret sharing," Phys. Rev. A, vol.61, no.4, p.042311, March 2000.
[6] K. Senthoor and P.K. Sarvepalli, "Communication efficient quantum secret sharing," Phys. Rev. A, vol.100, no.5, p.052313, Nov. 2019.

[7] K. Senthoor and P.K. Sarvepalli, "Theory of communication efficient quantum secret sharing," IEEE Trans. Inf. Theory, vol.68, no.5, pp.3164–3186, 2022.
[8] 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, 032318, Sept. 2005.
[9] R. Miyajima and R. Matsumoto, "Advance sharing of quantum shares for classical secrets," IEEE Access, vol.10, pp.94458–94468, 2022.
[10] S.H. Lie and H. Jeong, "Randomness cost of masking quantum information and the information conservation law," Phys. Rev. A, vol.101, no.5, p.052322, May 2020.
[11] T. Brun, I. Devetak, and M.H. Hsieh, "Correcting quantum errors with entanglement," Science, vol.314, no.5798, pp.436–439, Oct. 2006.
[12] L. Luo, Z. Ma, Z. Wei, and R. Leng, "Non-binary entanglement-assisted quantum stabilizer codes," Sci. China Inf. Sci., vol.60, no.4, p.042501, 2017.
[13] R. Matsumoto, "Unitary reconstruction of secret for stabilizer-based quantum secret sharing," Quantum Inf. Process., vol.16, no.8, p.202, 2017.
[14] D. Ueno and R. Matsumoto, "Explicit method to make shortened stabilizer EAQECC from stabilizer QECC," arXiv:2205.13732, May 2022.
[15] C-Y. Lai and T. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," Phys. Rev. A, vol.86, no.3, p.032319, Sept. 2012.

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.