Unified Approach to Secret Sharing and Symmetric Private Information Retrieval With Colluding Servers in Quantum Systems

Masahito Hayashi®, Fellow, IEEE, and Seunghoan Song®, Member, IEEE

Abstract—This paper unifiedly addresses two kinds of key quantum secure tasks, i.e., quantum versions of secret sharing (SS) and symmetric private information retrieval (SPIR) by using multi-target monotone span program (MMSP), which characterizes the classical linear protocols of SS and SPIR. SS has two quantum extensions; One is the classical-quantum (CQ) setting, in which the secret to be sent is classical information and the shares are quantum systems. The other is the quantum-quantum (QQ) setting, in which the secret to be sent is a quantum state and the shares are quantum systems. The relation between these quantum protocols and MMSP has not been studied sufficiently. We newly introduce the third setting, i.e., the entanglement-assisted (EA) setting, which is defined by modifying the CQ setting with allowing prior entanglement between the dealer and the end-user who recovers the secret by collecting the shares. Showing that the linear version of SS with the EA setting is directly linked to MMSP, we characterize linear quantum versions of SS with the CQ ad QQ settings via MMSP. Further, we introduce the EA setting of SPIR, which is shown to link to MMSP. In addition, we discuss the quantum version of maximum distance separable codes.

Index Terms—Mutual information, maximization, channel capacity, classical-quantum channel, analytical algorithm.

I. INTRODUCTION

RECENTLY, quantum information processing technology attracts much attention as a future technology. In particular, it is considered that quantum information processing technology has a strong advantage for cryptographic protocols. Therefore, it is desired to develop an efficient method for constructing various cryptographic protocols in a unified viewpoint. This paper focuses on the quantum versions of two fundamental cryptographic protocols, secret sharing (SS) and private information retrieval (PIR). Since these are key tools for cryptographic tasks, their quantum versions are expected to take crucial roles in future quantum technologies.

In SS [1], [2], a dealer is required to encode a secret into n shares so that the end-user can reconstruct the secret by using some subsets of shares but nobody obtains any part of the secret from the other subsets. In PIR [3], a user is required to retrieve one of the multiple files from server(s) without revealing which file is retrieved. Since PIR with one server has no efficient solution [3], it has been extensively studied with multiple non-communicating servers, and thus, in the following, we simply denote multi-server PIR by PIR. When the user obtains no information other than the retrieved file, the PIR protocol is called symmetric PIR (SPIR), which is also called oblivious transfer [4] in the one-server case.

SS and SPIR have a similar structure because the secrecy of both protocols is obtained by partitioning the confidential information. On the other hand, the two protocols have different structures because in SS, the secret is both confidential and targeted information but in PIR, the targeted file is not confidential. Using the similarity, several studies constructed PIR protocols from SS protocols [5], [6], [7], [8], [9]. Recently, the paper [10] derived a one-to-one correspondence between linear SS protocols and linear SPIR protocols even with general access structure. In this correspondence, all linear SS protocols and a special class of linear SPIR protocols are algebraically characterized by using a multi-target monotone span program (MMSP) [11], [12], [13].

As quantum versions of SS, existing studies investigated two problem settings. One is classical-quantum SS (CQSS), in which the secret message to be sent is given as classical information [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], which is illustrated as Fig. 1 (a). The other is quantum-quantum SS (QQSS), in which the secret message to be sent is given as a quantum state [14], [16], [17], [19], [20], [24], [25], [26], [27], [28], [29], [30], [31], which is illustrated as Fig. 1 (b). The studies [17], [21], [22], [23], [25], [26], [27] discussed the security of these problem settings by using a general access structure. Although the papers [14], [16], [17], [19], [20], [24] studied both settings, no existing study a unified framework for both problem settings. That is, no preceding study clarified the algebraic structure of...
Fig. 1. Quantum SS protocols where the end-user receives the shares from Player 2 and Player 3. Fig. (a), (b), and (c) show a CQSS protocol, a QQSS protocol, and an EASS protocol, respectively. The notations in the above figures will be defined in Section III.

CQSS protocols and QQSS protocols. In fact, since linear SS protocols are characterized algebraically by MMSP completely, we can expect that CQSS protocols and QQSS protocols can be characterized by a variant of MMSP. That is, it is expected that such characterization would be helpful to understand what type of CQSS and QQSS are possible. However, such useful characterizations of CQSS and QQSS protocols with general access structure by MMSP have not been obtained. In addition, for classical SS protocol, ramp-type SS protocols have been actively studied in [32], [33], [34], [35], and [36]. However, while its CQSS and QQSS versions were introduced, their analysis is very limited and did not discuss general access structure [22], [23], [26], [27].

In this paper, to resolve the above problems for CQSS protocols and QQSS protocols from a unified framework, as illustrated in Fig. 1 (c), we introduce the third problem setting, entanglement-assisted SS (EASS), in which the secret message to be sent is given as a classical information, and prior entanglement is allowed between the dealer and the end-user who intends to decode the message while the above two problem settings allow no prior entanglement. Analyzing two special cases of EASS, we derive our analyses of CQSS and QQSS. Here, CQSS is simply given as a special case of EASS. In contrast, we derive a notable conversion between QQSS and a special case of EASS by considering notable relations between dense coding and noiseless quantum state transmission.

To cover the security with general access structure, we study the relation between the security of EASS and the property of MMSP under a linearity condition while the paper [25] discussed this relation with a special case of access structure. For this analysis, we introduce a new concept, the symplectification for each access structure. Through the symplectification for each access structure, linear EASS protocols are characterized by MMSP because the symplectic structure plays a central role in this problem although such a symplectification for an access structure has not been considered by any existing study. Then, using this concept, we characterize CQSS protocols. To characterize QQSS protocols, we additionally invent new relations between dense coding and noiseless quantum state transmission. Then, we characterize QQSS protocols by combining our obtained characterization for EASS protocols and the above relations. In addition, we clarify the relation between QQSS protocols and quantum maximum distance separable (MDS) codes while a special case of such relations was mentioned in [16].

As quantum versions of SPIR, many existing papers [37], [38], [39], [40], [41], [42], [43], [44], [45] studied classical-quantum SPIR (CQSPIR), in which the file to be sent is given as a classical information. However, no existing paper studied the relation between CQSPIR and quantum versions of SS while such relation in the classical version was studied in [10]. In addition, several existing papers [10], [46], [47], [48], [49], [50] for the classical setting considered the reconstruction of the message only from the answers from a part of servers, which is called a qualified set of servers. Also, several existing papers [10], [51], [52], [53], [54] considered various cases for the set of colluding servers. Therefore, the analysis with various qualified sets of servers and various sets of colluding servers can be considered as a hot topic in the area of SPIR. However, no existing paper studied the reconstruction of a CQSPIR protocol with a general qualified set of servers because all existing papers [37], [38], [39], [40], [41], [42], [43], [44], [45] of the quantum setting considered this task under the condition that all servers send the answer to the user. In this paper, to develop the above relation, as another quantum setting of SPIR, we introduce entanglement-assisted SPIR (EASPIR), in which the file to be sent is given as a classical information, and prior entanglement is allowed between the servers and the user while CQSPIR does not allow such prior entanglement. Although the papers [55], [56], [57] considered use of prior entanglement between the server and the user and the papers [55], [57] showed its great advantages over the case without prior entanglement in the quantum non-symmetric PIR, no existing paper discussed the use of this type of prior entanglement in the quantum SPIR. Using MMSP, we derive the conversion relation between EASS and EASPIR.
protocols under the linearity condition. Due to this conversion, we address these two settings under a general access structure. In SPIR, a general access structure characterizes what a set of servers is qualified to recover the file information and what a set of colluded servers is disqualified to identify what file the user wants. That is, under this problem setting, we can discuss the case when only a part of servers answers the query sent by the user. In fact, no existing study addressed general access structure for CCQSP because all existing studies considered only two settings: the existence or non-existence of an access structure. In this paper, we address these two settings under a general access structure. We show notable relations between dense coding and noiseless state transmission. Section VIII introduces EASPIR protocols and presents our results for CCQSPIR protocols, which implies our results for EASS protocols, which is summarized in Tables II, III, and IV. Furthermore, we derive notable characterizations for the achievable rates of EASS and EASPIR, which are summarized in Section V and VI and guarantees the existences of several types of MMSPs.

II. PRELIMINARIES

A. Vector Space and Matrix Over a Finite Field

In this paper, our information is described as an element of a vector space on a finite field \( \mathbb{F}_q \) whose order is a prime power \( q = p^r \) because we address linear protocols. For preliminary results, we derive several notations over the finite field \( \mathbb{F}_q \). First, we define \( \text{tr} z := \text{Tr} T_z \in \mathbb{F}_p \) for \( z \in \mathbb{F}_q \), where \( T_z \in \mathbb{F}_p^{x \times x} \) denotes the matrix representation of the linear map \( y \in \mathbb{F}_q \mapsto zy \in \mathbb{F}_q \) by identifying the finite field \( \mathbb{F}_q \) with the vector space \( \mathbb{F}_p^x \).

**Example 1:** Consider the algebraic extension \( \mathbb{F}_q \) of \( \mathbb{F}_p \) with an irreducible polynomial \( f(x) = -x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 \), i.e., \( q = p^r \). The finite field \( \mathbb{F}_q \) is written as a vector space \( \mathbb{F}_p^x \) with basis \( 1, x, \ldots, x^{r-1} \). Then, for \( \alpha \in \{0, \ldots, r-1\} \) we have

\[
x^\alpha x = \begin{cases} x^{\alpha+1} & \text{when } \alpha \leq r-2 \\ a_{r-1}x^{r-1} + \cdots + a_1x + a_0 & \text{when } \alpha = r-1.
\end{cases}
\]

Therefore, \( \text{Tr} T_x = a_{r-1} \), i.e., \( \text{tr} x = a_{r-1} \).

A linear map from a vector space \( \mathbb{F}_q^x \) to \( \mathbb{F}_p^x \) is written as an \( n \times y \) matrix \( G \). We say that \((G, F)\) is an \( n \times (y + x) \) matrix when \( G \in \mathbb{F}_n \times \mathbb{F}_y \) and \( F \in \mathbb{F}_y \times \mathbb{F}_x \). The column vectors of \( G \) are written as \( g_1, \ldots, g_n \in \mathbb{F}_q^n \). The image \( \text{Im}(G) \) of \( G \) is given as the vector space spanned by \( g_1, \ldots, g_n \). Once the linear map \( G \) is given, we have a subspace \( \text{Im}(G) \subset \mathbb{F}_y \). We identify vectors \( h_1, h_2 \in \mathbb{F}_y \) satisfying \( h_1 - h_2 \in \text{Im}(G) \), we define the quotient vector space \( \mathbb{F}_q^y / \text{Im}(G) \). Considering this identification, we define the natural map from \( \mathbb{F}_q^y / \text{Im}(G) \) to \( \mathbb{F}_y / \text{Im}(G) \). This map is written as \( \pi \text{Im}(G) \).

For a given positive integer \( n \), we denote the set \( \{1, \ldots, n\} \) by [\( n \)]. For a subset \( C \) of \( \{n\} \), we define the linear map \( P_C \) from \( \mathbb{F}_q^C \) to \( \mathbb{F}_q^C \) as follows. Given a vector \( g = (g_1, \ldots, g_n)^T \in \mathbb{F}_q^n \), the vector \( P_C g \in \mathbb{F}_q^C \) is defined as \( P_C g = (g_x)_{x \in C} \).

Next, we consider the case with \( n = 2m \). For \( x, y \in \mathbb{F}_q^n \), we denote \((x, y) := \text{tr} \sum_{i=1}^{2m} x_i y_i \in \mathbb{F}_p \). Then, we define the symplectic inner product \( \langle (x, y), (x', y') \rangle := \langle x, y \rangle - \langle x', y' \rangle \in \mathbb{F}_p \). We say that a vector \( g \in \mathbb{F}_q^n \) is orthogonal to another vector \( h \in \mathbb{F}_q^n \) in the sense of the symplectic inner product when \( (g, h) = 0 \). We say that a matrix \( G = (g_1, \ldots, g_n)^T \in \mathbb{F}_q^{n \times x} \) is self-column-orthogonal when vectors \( g_1, \ldots, g_n \) are orthogonal to each other in the sense of the symplectic inner product. In addition, we say that an \( n \times x \) matrix \( F \) is column-orthogonal to an \( n \times y \) matrix \( G \) when vectors \( f_1, \ldots, f_x \) are orthogonal to vectors \( g_1, \ldots, g_n \) in the sense of the symplectic inner product.

B. Fundamentals of Quantum Information Theory

In this subsection, we briefly introduce the fundamentals of quantum information theory. More detailed introduction can be found at [58] and [59]. A quantum system is a Hilbert space \( \mathcal{H} \). Throughout this paper, we only consider finite-dimensional Hilbert spaces. A quantum state is defined by a density matrix, which is a Hermitian matrix \( \rho \) on \( \mathcal{H} \) such that

\[
\rho \geq 0, \quad \text{Tr} \rho = 1.
\]

The set of states on \( \mathcal{H} \) is written as \( S(\mathcal{H}) \). A state \( \rho \) is called a pure state if \( \text{rank} \rho = 1 \), which can also be described by a unit vector of \( \mathcal{H} \). If a state \( \rho \) is not a pure state, it is called a mixed state. The state \( \rho_{\text{mix}} := I_{\mathcal{H}} / \dim \mathcal{H} \) is called the completely mixed state, where \( I_{\mathcal{H}} \) is the identity operator.
on $\mathcal{H}$. The composite system of two quantum systems $A$ and $B$ is given as the tensor product of the systems $A \otimes B$. For a state $\rho \in S(A \otimes B)$, the reduced state on $A$ is written as
\begin{equation}
\rho_A = \text{Tr}_B \rho,
\end{equation}
where $\text{Tr}_B$ is the partial trace with respect to the system $B$.

A state $\rho \in S(A \otimes B)$ is called a separable state if $\rho$ is written as
\begin{equation}
\rho = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i},
\end{equation}
for some distribution $p = \{p_i\}$ and states $\rho_{A,i} \in S(A)$, $\rho_{B,i} \in S(B)$. A state $\rho \in S(A \otimes B)$ is called an entangled state if it is not separable.

A quantum measurement is defined by a positive-operator valued measure (POVM), which is the set of Hermitian matrices $\{\Pi_x\}_{x \in \mathcal{X}}$ on $\mathcal{H}$ such that
\begin{equation}
\Pi_x \geq 0, \quad \sum_{x \in \mathcal{X}} \Pi_x = I_H,
\end{equation}
When the elements of POVM are orthogonal projections, i.e., $\Pi_x^2 = \Pi_x$ and $\Pi_x \Pi_y = 0$, we call the POVM a projection-valued measure (PVM). A quantum operation is described by a trace-preserving completely positive (TP-CP) map $\kappa$, which is a linear map such that
\begin{equation}
\text{Tr} \kappa(\rho) = 1 \quad \forall \rho \in S(\mathcal{H}),
\end{equation}
\begin{equation}
\kappa \otimes \iota_{\mathbb{C}^d}(\rho) \geq 0 \quad \forall \rho \in S(\mathcal{H} \otimes \mathbb{C}^d), \quad \forall d \geq 1,
\end{equation}
where $\iota_{\mathbb{C}^d}$ is the identity map on $\mathbb{C}^d$. We often omit the identity map $\iota_{\mathbb{C}^d}$.

An example of TP-CP maps is the unitary map, which is defined by $\kappa_U(\rho) = U \rho U^* \text{ for a unitary matrix } U$.

C. Stabilizer Formalism Over Finite Fields

In this subsection, we introduce the stabilizer formalism for finite fields. Stabilizer formalism gives an algebraic structure for quantum information processing. We use this formalism for the construction of the QPIR protocol. Stabilizer formalism is often used for quantum error-correction. More detailed introduction of the stabilizer formalism can be found at [60], [61], [62], and [63].

In this paper, we denote the $q$-dimensional Hilbert space with a basis $\{|j\} \mid j \in \mathbb{F}_q^n\}$ by $\mathcal{H}$. For $a, b \in \mathbb{F}_q$, we define unitary matrices on $\mathcal{H}$
\begin{align*}
X(a) &:= \sum_{j \in \mathbb{F}_q} |j + a\rangle \langle j|, \\
Z(b) &:= \sum_{j \in \mathbb{F}_q} \omega^{j b} |j\rangle \langle j|, \\
W(a, b) &:= X(a) Z(b),
\end{align*}
where $\omega := \exp(2\pi i/p)$. For $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, and $w = (a, b) \in \mathbb{F}_q^{2n}$, we define a unitary matrix on $\mathcal{H}^{\otimes n}$
\begin{equation*}
W_{[w]}(w) = W_{[w]}(a, b) := X(a_1) Z(b_1) \otimes X(a_2) Z(b_2) \otimes \cdots \otimes X(a_n) Z(b_n).
\end{equation*}

Since $X(a) Z(b) = \omega^{- ab} Z(b) X(a)$, for any $(a, b), (c, d) \in \mathbb{F}_q^{2n}$, we have
\begin{equation}
W_{[w]}(a, b) W_{[w]}(c, d) = \omega^{(a, b), (c, d)} W_{[w]}(c, d) W_{[w]}(a, b).
\end{equation}

When the above operator is defined on a subset $A \subset [n]$, it is written as $W_A(w')$ with $w' \in \mathbb{F}_q^{|A|}$.

D. Information Quantities

To discuss information leakage, we often employ the mutual information. To address the mutual information, we prepare the quantum relative entropy. For two states $\rho$ and $\sigma$ on the quantum system $\mathcal{H}$, the quantum relative entropy is defined as
\begin{equation*}
D(\rho || \sigma) := \begin{cases} 
\text{Tr} \rho (\log \rho - \log \sigma) & \text{if supp}(\rho) \subset \text{supp}(\sigma) \\
\infty & \text{otherwise},
\end{cases}
\end{equation*}
where $\text{supp}(\rho) := \{|x\} \in \mathcal{H} \mid \rho(x) \neq 0\}$.

When the state on the joint system of two quantum systems $\mathcal{H}_A$ and $\mathcal{H}_B$ is given as $\rho_{AB}$, the mutual information $I(A; B)_{\rho_{AB}}$ is defined as
\begin{equation}
I(A; B)_{\rho_{AB}} := D(\rho_{AB} || \rho_A \otimes \rho_B),
\end{equation}
where $\rho_A := \text{Tr}_B \rho_{AB}$ and $\rho_B := \text{Tr}_A \rho_{AB}$. The above quantity will be employed for the discussion on the relation between two types of SS protocols.

E. Access Structure

In this paper, we discuss a general access structure when $n$ players or $n$ servers exist. The family of subsets of $[n]$ is identified with $\{0, 1\}^n$. We call $A \subset \{0, 1\}^n$ a monotone increasing collection if $A \subset \mathcal{A}$ implies $A \subset \mathcal{A}$ for any $A \subset C \subset [n]$. In contrast, we call $B \subset \{0, 1\}^n$ a monotone decreasing collection if $B \subset \mathcal{B}$ implies $B \subset \mathcal{B}$ for any $C \subset B$. In addition, we call $C \subset \{0, 1\}^n$ an $f$-collection if $C \subset \mathcal{C}$ implies $|C| = f$. An access structure on $[n]$ is defined as a pair $(\mathcal{A}, \mathcal{B})$ of monotone increasing and decreasing collections $\mathcal{A} \subset \mathcal{B} \subset \{0, 1\}^n$ such that $\mathcal{A} \cap \mathcal{B} = \emptyset$.

When $n$ is an even number $2n$, for a subset $A \subset 2^n$, we denote its cardinality by $|A|$. Then, we define the symmetrification of a subset $\overline{A} \subset 2^n$ and an access structure $\mathcal{A}$ as follows. When $A = \{a_0, \ldots, a_t\} \subset [n]$, $\overline{A}$ is defined as $\{a_0, \ldots, a_t, a_1 + n, \ldots, a_t + n\} \subset [n]$. Then, given a monotone increasing collection $\mathcal{A} \subset 2^n$, we define a monotone increasing collection $\overline{\mathcal{A}} \subset \{0, 1\}^n$ as follows. When $\mathcal{A} = \{A_0, \ldots, A_t\} \subset 2^n$, $\overline{\mathcal{A}}$ is defined as $\{\overline{A_0}, \ldots, \overline{A_t}\} \subset \{0, 1\}^n$, which is called the symmetrification of $\mathcal{A}$. For a monotone decreasing collection $\overline{\mathcal{B}} \subset 2^n$, we define the monotone decreasing collection $\overline{\mathcal{B}} \subset 2^n$ in the same way.

In fact, a general access structure covers the case when several players have access to multiple systems as follows. Assume that there are $z$ players and the $s$-th player has access to the systems labeled by elements in the subset $A_s \subset [n]$. Here, we assume that $A_s \cap A_s' = \emptyset$ for $s \neq s'$ and $\cup_{s \in C} A_s = [n]$. Any general access structure of this case is written by the pair of $\mathcal{A}$ and $\mathcal{B}$ to satisfy the condition that any elements of $\mathcal{A}$ and $\mathcal{B}$ are written as a form $\cup_{s \in C} A_s$ with $C \subset [z]$. 
Example 2: We choose $n$ is 3. Then, $\bar{n}$ is 6. When we choose $\mathfrak{A} = \{\{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$ and $\mathfrak{B} = \{\{1\}, \{2\}, \{3\}\}$ on [3], we have a general access structure $\mathfrak{A} = \{\{1, 2, 4, 5\}, \{2, 3, 5, 6\}, \{1, 2, 3, 4, 5, 6\}\}$ and $\mathfrak{B} = \{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$ on [6]. When we choose $\mathfrak{A} = \{\{1, 2, 3\}\}$ and $\mathfrak{B} = \{\{1\}, \{2\}, \{3\}, \{1, 3\}\}$ on [3], we have a general access structure $\mathfrak{A} = \{\{1, 2, 3, 4, 5, 6\}\}$ and $\mathfrak{B} = \{\{1, 4\}, \{2, 5\}, \{3, 6\}, \{1, 3, 4, 6\}\}$ on [6].

III. OUR MODELS

A. Formulation of Quantum Versions of SS Protocols

First, we consider secret sharing, where the secret is a classical information and the dealer uses quantum states. Hence, our problem setting is called classical-quantum secret sharing (CQSS). In this problem setting, shares the secret is a classical information and is given as a random variable $M \in \mathcal{M}$ and $m := |M|$. We denote the quantum system to be sent to the $j$-th player by $D_j$, and define the system $\mathcal{D}[A]$ as $\otimes_{j \in A} D_j$ for any subset $A \subset [n]$. Then, the dealer generates shares as quantum states, and distributes the shares to $n$ players. Finally, the end-user intends to recover the secret by collecting shares from several players. As illustrated in Fig. 1 (a), a CQSS protocol with one dealer, $n$ players, and one end-user is defined as Protocol 1. In this paper, the dealer and the end-user are assumed to be honest, i.e., they follow the protocol. Players are assumed to be semi-honest, i.e., they follow the protocol, but players of $B \in \mathcal{B}$ may collude together.

Protocol 1 CQSS protocol

STEP 1: Share generation: Depending on the message $M \in \mathcal{M}$, the dealer prepares $n$ shares as a state $\rho[M]$ on the joint system $D_1 \otimes \cdots \otimes D_n$, and sends the $j$-th share system $D_j$ to the $j$-th player.

STEP 2: Decoding: For a subset $A \in \mathfrak{A}$, the end-user decodes the message from the received state from players $A$ by a decoder, which is defined as a POVM $\text{Dec}[A] := \{Y_A(w) \mid w \in [m]\}$ on $\mathcal{D}[A]$. The end-user outputs the measurement outcome $W$ as the decoded message.

Then, in Protocol 1, the share cost and the rate of a CQSS protocol are defined by

$$D := \dim \left( \bigotimes_{j=1}^{n} D_j \right), \quad R := \frac{\log m}{\log D}. \quad (12)$$

The security of CQSS protocols are defined as follows.

Definition 1 ($\mathfrak{A}, \mathfrak{B}$)-security: For an access structure $\mathfrak{A}, \mathfrak{B}$ on $[n], a$ CQSS protocol defined as Protocol 1 is called $\mathfrak{A}$-correct if the following correctness condition is satisfied. It is called $(\mathfrak{A}, \mathfrak{B})$-secure if the following both conditions are satisfied.

- Correctness: The relation

$$\text{Tr} \rho[m](Y_A(m) \otimes I_{A^c}) = 1$$

holds for $A \in \mathfrak{A}$ and $m \in \mathcal{M}$.

- Secrecy: The state $\text{Tr}_{B^c} \rho[m]$ does not depend on $m \in \mathcal{M}$ for $B \in \mathcal{B}$.

In particular, we define the $(r, t, n)$-security as the $(\mathfrak{A}, \mathfrak{B})$-security under the choice $\mathfrak{A} = \{A \subset [n] \mid |A| \geq r\}$ and $\mathfrak{B} = \{B \subset [n] \mid |B| \leq t\}$.

The classical case of ramp type SS protocols has been actively studied in [32], [33], [34], [35], and [36]. When the secret is given as a quantum state, we need a different problem setting. Since this problem uses quantum systems to generate shares, our protocol is called a quantum-quantum secret sharing (QQSS) protocol. To consider this problem, we need the system $D_M$ with $\dim D_M = m$ to describe our secret. As illustrated in Fig. 1 (b), a QQSS protocol with one dealer, $n$ players, and one end-user is defined by Protocol 2.

Protocol 2 QQSS protocol

STEP 1: Share generation: Applying a TP-CP map $\Gamma$ from $D_M$ to $D_1 \otimes \cdots \otimes D_n$, the dealer prepares $n$ shares as the joint system $D_1 \otimes \cdots \otimes D_n$, and sends the $j$-th share system $D_j$ to the $j$-th player.

STEP 2: Decoding: For a subset $A \in \mathfrak{A}$, the end-user decodes the message from the received state from players $A$ by a decoder, which is defined as a TP-CP map $\text{Dec}[A]$ from $D[A]$ to $D_M$.

Definition 2 ($\mathfrak{A}, \mathfrak{B}$)-QQSS: For an access structure $\mathfrak{A}, \mathfrak{B}$ on $[n], a$ QQSS protocol defined as Protocol 2 is called $(\mathfrak{A}, \mathfrak{B})$-secure when the following condition holds. $\mathfrak{A}$-correctness is defined in the same way as Definition (1).

- Correctness: The relation

$$\text{Dec}[A](\text{Tr}_{A^c} \Gamma(\rho)) = \rho$$

holds for any state $\rho$ on $D_M$.

- Secrecy: The state $\text{Tr}_{B^c} \Gamma(\rho)$ does not depend on the state $\rho$ on $D_M$.

B. Formulation of Quantum Versions of SPIR Protocol

We consider the following type of SPIR. The files are given as classical information. The query is limited to classical information. The servers can use quantum system and their answers are quantum states. In addition, the servers are allowed to share prior entangled states. This problem setting is called classical-quantum SPIR (CQSPIR). In this setting, the files $M_1, \ldots, M_t \in [m]$ are uniformly and independently distributed. Each of $n$ servers $\sigma_1, \ldots, \sigma_n$ contains a copy of all files $\vec{M} := (M_1, \ldots, M_t)^T$. The $n$ servers are assumed to share an entangled state. A user chooses a file index $K \in \{1, \ldots, t\}$ uniformly and independently of $\vec{M}$ in order to retrieve the file $M_K$. The requirement is to construct a protocol that allows the user to retrieve $M_K$ from
the collection of the answers from servers $A \in \mathfrak{A}$ without revealing $K$ to the collection of servers $B \in \mathfrak{B}$. The user uses a random variables $Q^{(K)} = (Q^{(K)}_1, \ldots, Q^{(K)}_n) \in Q_1 \times \cdots \times Q_n$ depending on $K$ as a query, where $Q_1, \ldots, Q_n$ are finite sets. As illustrated in Fig. 2 (a), a CQSPIR protocol is defined as Protocol 3. In this paper, the user is assumed to be semi-honest, i.e., he/she follows the protocol, but he/she tries to know the information other than the retrieved file. Servers are assumed to be semi-honest, i.e., they follow the protocol, but servers of $B \in \mathfrak{B}$ may collude together.

That is, given the numbers of servers $n$ and files $f$, a CQSPIR protocol of the file size $m$ is described by

$$(\rho_{\text{prev}}, \text{Enc}_{\text{user}}, \text{Enc}_{\text{serv}}, \text{Dec})$$

of the shared entangled state, user encoder, server encoder, and decoder, where $\text{Enc}_{\text{serv}} := (\text{Enc}_{\text{serv}1}, \ldots, \text{Enc}_{\text{serv}n})$.

Then, in Protocol 3, the upload cost, the download cost, and the rate of a CQSPIR protocol $\Lambda$ are defined by

$$U(\Lambda) := \sum_{j=1}^n |Q_j|, \quad D(\Lambda) := \dim \bigotimes_{j=1}^n \mathcal{D}_j,$$

$$R(\Lambda) := \frac{\log m}{\log D(\Lambda)}.$$ (13) (14)

The security of CQSPIR protocols are defined as follows.

**Definition 3:** For an access structure $(\mathfrak{A}, \mathfrak{B})$ on $[n]$, a CQSPIR protocol defined as Protocol 3 is called $(\mathfrak{A}, \mathfrak{B})$-secure if the following conditions are satisfied.

- **Correctness:** For any $A \in \mathfrak{A}$, $k \in [f]$, and $\vec{m} = (m_1, \ldots, m_t)^T \in [m]^t$, the relation

$$\text{Tr} \rho(\vec{m}, q, k)(Y_{k,q,A}(m_k) \otimes I_{\mathcal{A}^c}) = 1$$

holds when $q$ is any possible query $Q^{(K)}$.

- **User Secrecy:** The distribution of $(Q_j^{(K)})_{j \in B}$ does not depend on $k \in [f]$ for any $B \in \mathfrak{B}$.

- **Server Secrecy:** We fix $K = k$, $M_k = m_k$, and $Q^{(K)} = q$. Then, the state $\rho(m_1, \ldots, m_f, q, k)$ does not depend on $(m_j)_{j \neq k} \in \mathcal{M}^{f-1}$.

**Protocol 3 CQSPIR protocol**

**STEP 1: Preparation:** The state of the quantum system $\mathcal{D}_1' \otimes \cdots \otimes \mathcal{D}_n'$ is initialized as $\rho_{\text{prev}}$ and is distributed so that the $j$-th server $\text{serv}_j$ contains $\mathcal{D}_j$. Let $U_S$ be random variable, called the random seed for servers, and the random seed $U_S$ is encoded as $\text{Enc}_{\text{serv}}(U_S) = R = (R_1, \ldots, R_n)^T \in \mathcal{R} = \mathcal{R}_1 \times \cdots \times \mathcal{R}_n$ by the shared randomness encoder $\text{Enc}_{\text{SR}}$. The randomness $R$ is distributed so that the $j$-th server contains $R_j$.

**STEP 2: User’s encoding:** The user randomly encodes the index $K$ to classical queries $Q^{(K)}_1, \ldots, Q^{(K)}_n$, i.e.,

$$\text{Enc}_{\text{user}}(K) = (Q^{(K)}_1, \ldots, Q^{(K)}_n) \in \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_n,$$

where $Q_1, \ldots, Q_n$ are finite sets. Then, the user sends $Q_j$ to the $j$-th server $\text{serv}_j$ ($j = 1, \ldots, n$).

**STEP 3: Servers’ encoding:** Let $\mathcal{D}_1, \ldots, \mathcal{D}_n$ be $d$-dimensional Hilbert spaces and $\mathcal{D}_A[\mathcal{A}]$. After receiving the query $Q_j^{(K)}$, depending on the random variable $R_j$, the $j$-th server $\text{serv}_j$ constructs a TP-CP map $\Lambda_j$ from $\mathcal{D}_j$ to $\mathcal{D}_j$ by the server encoder $\text{Enc}_{\text{serv}_j}$ as

$$\text{Enc}_{\text{serv}_j}(\vec{M}, Q^{(K)}_j, R_j) = \Lambda_j.$$ Then, the $j$-th server $\text{serv}_j$ applies $\Lambda_j$, and sends $D_j$ to the user. The state on $D_1 \otimes \cdots \otimes D_n$ is written as

$$\rho(\vec{M}, Q^{(K)}_1, K) := \Lambda_1 \otimes \cdots \otimes \Lambda_n(\rho_{\text{prev}}).$$

**STEP 4: Decoding:** For a subset $A \in \mathfrak{A}$, the user decodes the message from the received state from servers $A$ by a decoder, which is defined as a POVM $\text{Dec}(K, Q^{(K)}_A, A) := \{Y_{K,Q^{(K)}_A}(w) \mid w \in [m]\}$ on $\mathcal{D}_A[\mathcal{A}]$ depending on the variables $K$ and $Q^{(K)}$. The user outputs the measurement outcome $W$ as the retrieval result.

**TABLE I**

| Symbol | CQSPIR | CQSS |
|--------|--------|------|
| $n$ | Number of servers | Number of shares |
| $f$ | Number of files | - |
| $m$ | Size of one file | Size of secret |
| $r$ | Number of responsive servers | Reconstruction threshold |
| $t$ | Number of colluding servers | Secrecy threshold |

**IV. CLASSICAL LINEAR PROTOCOLS**

**A. Linear CSS**

Section III formulates various quantum protocols. This section reviews their classical version with the linearity condition. As the first step, we formulate linear CSS as a special case of CQSS.

**Definition 4 (Linear CSS):** A CQSS protocol $\Phi_{\text{QCSS}}^m$ is called a linear CSS protocol with $(G, F)$ if the following conditions are satisfied. In this definition, the number of shares is written as $n$ instead of $n$.

**Vector representation of secret** The secret $M$ is written as a vector in $[q]_q^n$.
Vector representation of randomness

The dealer’s private randomness $U_D$ is written as a uniform random vector in $\mathbb{F}_q^n$.

Linearity of share generation

The $j$-th share is a random variable $Z_j \in \mathbb{F}_q$. The encoder is given as a linear map, i.e., an $n \times (y+x)$ matrix $(G, F)$. That is, $(Z_1, \ldots, Z_n)^T = FM + GU_D$.

In the notation $(G, F)$, the first matrix $G$ identifies the direction of the randomization for secrecy, and the second matrix $F$ identifies the direction of the message imbedding. Due to the above conditions, the rate of this linear CSS is $x/n$.

As a special case, we define MDS codes as follows.

Definition 5 ((n, x) - MDS code): We consider the with $y = 0$, i.e., we have only an $n \times x$ matrix $(\emptyset, F)$. In this case, the linear CSS protocol with $(\emptyset, F)$ is called an $(n, x)$-maximum distance separable (MDS) code when it is $\mathbb{F}$-correct with $\mathbb{A} = \{ A \subset [n] \mid |A| \geq x \}$. In addition, when the linear CSS protocol with $(\emptyset, F)$ is an $(n, x)$-MDS code, we say that the matrix $F$ is an $(n, x)$-MDS code.

In the following, we identify the MDS protocol with the linear CSS protocol with $(\emptyset, F)$.

Remark 1: Usually, an MDS code is defined as a code whose minimum distance is $n - x + 1$ [64]. In fact, given a linear subspace $C \subseteq \mathbb{F}_q^n$, the relation $n - \min_{x \in C \setminus \{0\}} |x| = x - 1$ holds if and only if $\dim P_A C = |A|$ for any $A \subset \{0, 1\}$ with $|A| = x$. Thus, our definition for an MDS code is equivalent to the above conventional definition of an MDS code.

B. Multi-Target Monotone Span Program (MMSP)

A linear CSS is characterized by a multi-target monotone program (MMSP) [10], [11], [12], [13]. Hence, to discuss its correctness and its secrecy with a general access structure, we focus on the following lemma. To state the following lemma, we focus on the vector space $\mathbb{F}_q^{y+y}$, and define the vector $e_j \in \mathbb{F}_q^{y+y}$ as the row vector with 1 in the $j$-th coordinate and 0 in the others. Also, we define the vector space $\mathbb{E}$ spanned by $\{e_{y+1}, \ldots, e_{y+x}\}$.

Lemma 1: The following conditions are equivalent for an $n \times (y+x)$ matrix $(G, F)$ and a subset $A \subset [n]$.

(A1) The column vectors $\pi[\text{Im} P_A G] P_A F$ are linearly independent.

(A2) The vector space spanned by the row vectors $(P_A G, P_A F)$ contains $\mathbb{E}$.

Also, the following conditions are equivalent for a $n \times (y+x)$ matrix $(G, F)$ and a subset $B \subset [n]$.

(B1) Any column vector $P_B G$ is included in the linear span of column vectors $P_B G$.

(B2) The vector space spanned by the row vectors $(P_B G, P_B F)$ does not contain any non-zero element of $\mathbb{E}$.

Proof: The condition (A1) is equivalent to the following condition (A3).

(A3) There exists an $|A| \times |A|$ invertible matrix $H$ such that $H(P_A G, P_A F) = \begin{pmatrix} 0 & I_n \\ * & * \end{pmatrix}$, where $*$ means an arbitrary form.

Also, the condition (A2) is equivalent to the following condition (A3). Hence, we obtain the equivalence between (A1) and (A2).

The condition (B1) does not hold if and only if the following condition (B3*) holds.

(B3*) There exist an $|B| \times |B|$ invertible matrix $H$ and a column vector $a$ such that $H(P_B G, P_B F) = \begin{pmatrix} 0 & a \\ * & \end{pmatrix}$.

Also, the condition (B2) does not hold if and only if the following condition (B3*) holds. Hence, we obtain the equivalence between (B1) and (B2).

Then, MMSP is defined as follows.

Definition 6 (Multi-Target Monotone Span Program (MMSP)): Given an $n \times (y+x)$ matrix $(G, F)$, we say the following:

- (Acceptance) $(G, F)$ accepts $\mathbb{A}$ if the condition (A1) or (A2) holds for any $A \in \mathbb{A}$.
- (Rejection) $(G, F)$ rejects $\mathbb{B}$ if the condition (B1) or (B2) holds for any $B \in \mathbb{B}$.

Then, the matrix $(G, F)$ is called $(\mathbb{A}, \mathbb{B})$-MMSP if $(G, F)$ accepts $\mathbb{A}$ and rejects $\mathbb{B}$.

Example 3: For $n = 6$, we choose

$$G := \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 2 & 2 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{6 \times 2}, \quad F := \begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 1 & 2 \\ 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{6 \times 2}. \quad (15)$$

Then, we choose a general access structure $\mathbb{A} = \{ \{1, 2, 4, 5\}, \{2, 3, 5, 6\}, \{1, 2, 3, 4, 5, 6\} \}$ and $\mathbb{B} = \{ \emptyset, \{1, 4\}, \{2, 5\}, \{3, 6\} \}$ on $[6]$. Since

$$P_{\{1,2,4,5\}}(G, F) = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix},$$

$$P_{\{2,3,5,6\}}(G, F) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 2 & 2 & 1 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 2 & 1 & 2 \end{pmatrix} \quad (16)$$

are invertible, the MMSP $(G, F)$ accepts $\mathbb{A}$. Since the matrices

$$P_{\{1,4\}} G = P_{\{2,5\}} G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad P_{\{3,6\}} G = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad (17)$$

are invertible, the MMSP $(G, F)$ rejects $\mathbb{B}$. Hence, $(G, F)$ is an $(\mathbb{A}, \mathbb{B})$-MMSP.

Example 4: For $n = 6$, we choose $G^*$ and $F^*$ as

$$G^* := \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 2 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \in \mathbb{F}_3^{6 \times 3}, \quad F^* := \begin{pmatrix} 2 & 0 \\ 1 & 1 \\ 1 & 2 \\ 0 & 0 \\ 0 & 2 \\ 0 & 2 \end{pmatrix} \in \mathbb{F}_3^{6 \times 2}. \quad (18)$$
Then, we choose $\mathfrak{A}^* = \{1, 2, 3, 4, 5, 6\}$ and $\mathfrak{B}^* = \{\emptyset, \{1\}, \{2, 5\}, \{3, 6\}, \{1, 3, 4, 8\}\}$. Since
\[
P_{1, 3, 4, 6}G^* = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 2 \\ 1 & 0 & 0 \\ 0 & 2 & 2 \end{pmatrix}, \quad P_{1, 3}F^* = \begin{pmatrix} 2 & 0 \\ 1 & 2 \\ 0 & 0 \end{pmatrix},
\] (19)
the column vectors of $P_{1, 3, 4, 6}F^*$ is written as linear sums of the column vectors of $P_{1, 3, 4, 6}G(1)^*$. Also, since the rank of $P_{2, 5}G$ is 2, the column vectors of $P_{2, 5}F^*$ is written as linear sums of the column vectors of $P_{2, 5}G^*$. Hence, the MMSP $(G^*, F^*)$ rejects $\mathfrak{B}^*$. Since the column vectors of $(G^*, F^*)$ are linearly independent, the MMSP $(G^*, F^*)$ accepts $\mathfrak{A}^*$. Hence, $(G(1)^*, F^*)$ is an $(\mathfrak{A}^*, \mathfrak{B}^*)$-MMSP.

A MMSP characterizes the security of CSS as follows.

**Proposition 1** ([10, Corollary 5]): A linear CSS protocol with $(G, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure if and only if $(G, F)$ is $(\mathfrak{A}^*, \mathfrak{B}^*)$-MMSP.

Therefore, a linear CSS protocol is completely characterized by an MMSP. That is, to consider the security of a given linear CSS protocol with $(G, F)$, it is sufficient to consider its corresponding MMSP defined by $(G, F)$.

*Proof:* For a linear CSS protocol with $(G, F)$, the decodable information is given as $(\text{Im } P_A F + \text{Im } P_A G)/\text{Im } P_A G$. Thus, if and only if the map $x \in \mathbb{F}^n_q \mapsto \pi(\text{Im } P_A G)(P_A F x) \in (\text{Im } P_A F + \text{Im } P_A G)/\text{Im } P_A G$ is injective, the correctness holds. Also, if and only if $P_B F x \in \text{Im } P_B G$ for $x \in \mathbb{F}^n_q$, the secrecy holds. Therefore, the acceptance condition for MMSP guarantees correctness, and the rejection condition for MMSP guarantees secrecy. Hence, we have the following proposition.

**Remark 2:** Our definition of MMSP is the same as the definition in [10] while the paper [10] uses the conditions (A2) and (B2). Hence, Proposition 1 was shown in [10] by using the conditions (A2) and (B2). This paper mainly uses the conditions (A1) and (B1) while other preceding studies also use the conditions (A2) and (B2) as well as the reference [10]. The definition in [10] generalized the definition in [11], [12], and [13]. The MMSP defined in [11], [12], and [13] corresponds to the definition in [10] with $\mathfrak{A} \cup \mathfrak{B} = \{0, 1\}$ and $\mathfrak{A} \cap \mathfrak{B} = \emptyset$, i.e., every subset of $[n]$ is either authorized or forbidden. Our definition of MMSP also generalizes the monotone span programs [65], which corresponds to the case $x = 1$ and $\mathfrak{A} \cup \mathfrak{B} = \{0, 1\}$[6] for our MMSP definition. The papers [65], [66], [67] proved the one-to-one correspondence of linear CSS protocols with complete security and monotone span programs.

As special cases, we define $(\mathfrak{A}, \mathfrak{B})$-MMSPs with thresholds as follows [10].

**Definition 7** $(\mathfrak{r}, \mathfrak{n})$-MMSP: When $\mathfrak{A} = \{A \subseteq \mathfrak{n} | |A| \geq \mathfrak{r}\}$ and $\mathfrak{B} = \{B \subseteq \mathfrak{n} | |B| \leq \mathfrak{t}\}$, an $(\mathfrak{A}, \mathfrak{B})$-MMSP are called an $(\mathfrak{r}, \mathfrak{n})$-MMSP.

An $(\mathfrak{r}, \mathfrak{n})$-MMSP is related with an MDS code. A matrix $A \in \mathbb{F}_q^{n \times f}$ is an $(\mathfrak{n}, f)$-MDS code if and only if any $f$ rows of $A$ are linearly independent because the linear independence guarantees the correctness. Then, we have the following proposition [10].

**Proposition 2:** An $\mathfrak{n} \times (t + (r - t))$ matrix $(G, F)$ is an $(\mathfrak{r}, t)$-MMSP if and only if the matrix $(G, F)$ is an $(\mathfrak{n}, r)$-MDS code, and the matrix $G$ is an $(\mathfrak{n}, t)$-MDS code.

### C. Linear CSPIR

Next, we formulate linear CSPIR as a special case of CQSPIR as follows.

**Definition 8** (Linear CSPIR): A protocol is called a linear CSPIR protocol if the following conditions are satisfied. In this definition, the number of servers is written as $\mathfrak{n}$ instead of $n$.

**Vector representation of files** The files $M_i$ are written as a vector in $\mathbb{F}_q^n$. The entire file is written by the concatenated vector $\bar{M} = (M_1, \ldots, M_t)^T \in \mathbb{F}_q^n$.

**Linearity of shared randomness** The random seed $U_S$ is written by a uniform random vector in $\mathbb{F}_q^n$. The randomness encoder is written as a matrix $G \in \mathbb{F}_q^{n \times t}$ and the shared randomness is written as $R = GU_S \in \mathbb{F}_q^n$. The randomness of the $j$-th server is written as $R_j = G_jU_S \in \mathbb{F}_q^n$, where $G = (G(1), \ldots, G(n))^T$, i.e., $G_j$ is a row vector of $G$.

**Linearity of servers** The $j$-th server’s system $D_j$ is a classical system, i.e., is given as a random variable $D_j \in \mathbb{F}_q^n$. The answer of the $j$-th server $D_j$ is written as the sum of the shared randomness $R_j$ and the encoded output of the files $\bar{M}$ by an $f_\mathfrak{x}$-dimensional random column vector $Q_j^{(K)}$, which depends on the query, i.e.,

$$D_j = Q_j^{(K)}\bar{M} + R_j \in \mathbb{F}_q^n.$$ (20)

Therefore, we can consider that the query to the $j$-th server is given as the linear function, a random matrix, $Q_j^{(K)}(\forall j = 1, \ldots, \mathfrak{f})$. The above protocol is called the linear CSPIR protocol with $G, Q_j^{(K)}$.

Due to the above conditions, the PIR rate and the shared randomness rate of a linear CSPIR protocol are $x/\mathfrak{f}$ and $y/x$, respectively.

In the case of linear CSPIR protocols, the server secrecy can be characterized as follows.

**Lemma 2:** Assume that $Q_j^{(k)} = (Q_j^{(k)})_{j=1}^\mathfrak{f}$ is an $\mathfrak{n} \times f_k$ random matrix for $k = 1, \ldots, \mathfrak{f}$. A linear CSPIR protocol with $G, Q_j^{(K)}$ satisfies the server secrecy if and only if any column vector of $Q_j^{(K)} \in \mathbb{F}_q^{n \times f_k}$ belongs to the linear span of column vectors of $\bar{G}$ for $j \neq k$.

*Proof:* The user cannot distinguish elements in $\text{Im } G$. Hence, the server secrecy holds if only if the following holds. Let $k$ be an arbitrary element in $[\mathfrak{f}]$ and $m_k$. The element $\pi(\text{Im } G_i(Q_j^{(k)})\bar{m})$ does not depend on $(m_j)_{j \neq k}$. Since the above condition is equivalent to the condition stated in this lemma. Hence, the desired statement is obtained.

For the choice of the query $Q_j^{(K)}$, we consider the following construction in a similar way to [46], [51], [54], [68], [69], and [10].

**Definition 9** (Standard form): Let $F$ be an $\mathfrak{n} \times f$ matrix taking values in $\mathbb{F}_q$. A query $Q_j^{(K)}$ is called the standard form with matrix $F$ when it is given as follows. The user prepares uniform random variable $U_q \in \mathbb{F}_q^{n \times f}$ independently of $K$. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Then,\[ Q^{(k)} := FE_k + GU_Q, \]
where $E_k := (\delta_{1,k}I_n, \ldots, \delta_{n,k}I_n)$. A linear CSPIR protocol with $(G, Q^{(k)})$ is called a standard linear CSPIR protocol with $(G, F)$ when the query $Q^{(k)}$ is the standard form with matrix $F$.

The security of a standard linear CSPIR protocol is characterized as follows.

**Proposition 3:** The standard linear CSPIR protocol with $(G, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure if and only if the matrix $(G, F)$ is $(\mathfrak{A}, \mathfrak{B})$-MMSP.

Although Proposition 3 was shown in [10] by using the conditions (A1) and (B1), we use the conditions (A1) and (B1) in the latter discussion.

**Proof:** The choice (21) of $Q^{(k)}$ satisfies the condition of Lemma 2. Hence, it is sufficient to discuss the user secrecy and the correctness. The user secrecy holds for $B \in \mathfrak{B}$ if and only if $P_B(F + GU)$ and $P_BGU$ cannot be distinguished when $U \in \mathbb{F}_q^{\times n}$ is subject to the uniform distribution. This condition is equivalent to the rejection condition for $(\mathfrak{A}, (G, F))$. The correctness holds for $A \in \mathfrak{A}$ if and only if the map $m \in \mathbb{F}_q^n \mapsto \pi[\text{Im } P_A G](P_A F x) \in (\text{Im } P_A F + \text{Im } P_A G)/\text{Im } P_A G$ is injective. This condition is equivalent to the acceptance condition for $(\mathfrak{A}, (G, F))$. Therefore, the desired statement is obtained. \[ \square \]

V. LINEAR QUANTUM PROTOCOLS WITHOUT PRESHARED ENTANGLEMENT WITH USER

A. Linear CQSS Protocol

We assume that an $\bar{n} \times n$ matrix $G^{(1)}$, an $\bar{n} \times y_2$ matrix $G^{(2)}$, and an $\bar{n} \times x$ matrix $F$ on the finite field $\mathbb{F}_q$ with $\bar{n} = 2n$ satisfy the following conditions. All column vectors of $(G^{(1)}, G^{(2)}, F)$ are linearly independent, and all column vectors of $G^{(1)}$ are commutative with each other, which is equivalent to the self-column-orthogonal condition. Then, we define a CQSS protocol as follows. We choose the message set $M = \mathbb{F}_q^n$. We choose the Hilbert space $\mathcal{H}$ as the space spanned by $\{|x\rangle\}_{x \in \mathbb{F}_q^n}$. We choose the vectors $g^1, \ldots, g^n$ as column vectors of $G^{(1)}$. We define a normalized vector $|\psi[G^{(1)}]\rangle \in \mathcal{D}_D := \mathcal{H}^{\otimes \bar{n}}$ as the common eigenvector with eigenvalue 1 of $\mathbf{W}_n[|g^1\rangle], \ldots, \mathbf{W}_n[|g^n\rangle]$, i.e.,

$$\mathbf{W}_n[|G^{(1)}y\rangle|\psi[G^{(1)}]\rangle] = |\psi[G^{(1)}]\rangle \quad \text{for } y \in \mathbb{F}_q^n.$$ \[ (22) \]

Then, we define the linear CQSS protocol with $(G^{(1)}, G^{(2)}, F)$ as Protocol 4.

A usual linear CQSS protocol does not have randomization $U_D \in \mathbb{F}_q^{2n}$. That is, $y_2 = 0$ and it does not have the matrix $G^{(2)}$. Such a protocol is called the randomless linear CQSS protocol with $(G^{(1)}, F)$. In this case, the state with message $M = 0$ is determined as the stabilizer of the group generated by $G^{(1)}$. That is, any CQSS protocol given as the application of $\mathbf{W}_n$ to the stabilizer state is written as the above way. Then, we have the following theorem.

**Theorem 1:** Given a $2n \times n$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and a $2n \times x$ matrix $F$, the following conditions for $(G^{(1)}, G^{(2)}, F)$ are equivalent.

(C1) The linear CQSS protocol with $(G^{(1)}, G^{(2)}, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

(C2) The linear CSS protocol with $((G^{(1)}, G^{(2)}), F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

(C3) The matrix $((G^{(1)}, G^{(2)}), F)$ is an $(\mathfrak{A}, \mathfrak{B})$-MMSP.

Also, we have the following proposition.

**Proposition 4:** In Protocol 4, even when STEP 3 is replaced by another decoder, the decoder can be simulated by the decoder given in Protocol 4, without loss of generality, we can assume that our decoder is given as STEP 3.

We will prove the above theorem and proposition after we introduce linear EASS protocols in the next section.

**Example 5:** For $n = 3$, we choose

$$G^{(1)} := \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 2 & 2 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} \in \mathbb{F}_3^{6 \times 2}, \quad F := \begin{pmatrix} 2 & 0 \\ 1 & 1 \\ 0 & 2 \\ 2 & 1 \end{pmatrix} \in \mathbb{F}_3^{6 \times 2}. \quad (24)$$

The column vectors of $(G^{(1)})^*, F^*$ are linearly independent. $(G^{(1)})^*$ is self-column-orthogonal, and $F$ is column-orthogonal to $G^{(1)}$. Hence, according to Protocol 4, the randomless linear CQSS protocol with $(G^{(1)}, F)$ can be constructed.

We choose $\mathfrak{A} = \{\{1, 2\}, \{2, 3\}\} \cup \{1, 2, 3\}$ and $\mathfrak{B} = \emptyset$. Using observations in Examples 2 and 3, we have

$$P_{\mathfrak{A}, \mathfrak{B}}[G^{(1)}, F] = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$
TABLE II

| general | relation to MMSP | ramp scheme |
|---------|-----------------|-------------|
| access structure | | |
| [17], [21] | Yes | No | No |
| [25] | Yes | special cases | No |
| [22], [23] | No | No | special cases |
| This paper | Yes | general case (Theorem 1) | general case (Corollary 1) |

To characterize CQSS protocols with two thresholds, i.e.,
with the ramp scheme, we define the following special case of ($\mathcal{A}, \mathcal{B}$)-MMSPs.

**Definition 10** ($\mathcal{A}, \mathcal{B}$-CQMMSP): We choose $\mathcal{A} = \{A \in [n] | |A| \geq r\}$ and $\mathcal{B} = \{B \subset [n] | |B| \leq t\}$. Given a $2n \times n$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and a $2n \times x$ matrix $F$, the matrix $(G^{(1)}, G^{(2)}, F)$ is called an $(\mathcal{A}, \mathcal{B})$-CQMMSP when the matrix $((G^{(1)}, G^{(2)}), F)$ is an $(\mathcal{A}, \mathcal{B})$-MMSP.

**Theorem 2:** When $n \geq r \geq t > 0$, and $r > n/2$, there exist a positive integer $s$, a $2n \times n$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times [2t-n]_+$ matrix $G^{(2)}$, and a $2n \times (2r - \max(2t, n))$ matrix $F$ on $\mathbb{F}_q$ with $q = p^s$ such that the matrix $((G^{(1)}, G^{(2)}), F)$ is an $(\mathcal{A}, \mathcal{B})$-CQMMSP. Here, we use the notation $[x]_+ := \max(0, x)$.

**Theorem 2** is shown in Appendix C. Combining Theorems 1 and 2, we obtain the following corollary.

**Corollary 1:** When $n \geq r \geq t > 0$ and $r > n/2 > 0$, there exists an $(\mathcal{A}, \mathcal{B})$-secure CQSS protocol of rate $(2r - \max(2t, n))/n$. In particular, when $n \geq r > n/2 \geq t > 0$, there exists an $(\mathcal{A}, \mathcal{B})$-secure CQSS protocol of rate $(2r - n)/n$.

In the classical case with the ramp scheme, the optimal rate of $(r, t, n)$-secure SS protocol is $(r - t)/n$ [34], [70], [71]. Hence, the rate of Corollary 1 is twice of the classical case. In fact, the existence of the above rate of the ramp case was not shown in the general case. Only a limited case of the ramp case was discussed in [22] and [23]. That is, the achievability of the rate $(2r - \max(2t, n))/n$ was not shown in existing studies.

**B. Linear QQSS**

Next, we discuss linear QQSS protocols. For this aim, we focus on a $2n \times (n-x)$ self-column-orthogonal matrix $G^{(1)}$ and a $2n \times y_2$ matrix $G^{(2)}$. Also, we focus on a $2n \times 2x$ matrix $F$ that is column-orthogonal to $G^{(1)}$. In this construction, we use the notation given in Section V-A, and use the matrix $G^{(1)}$ as the stabilizer. That is, we define the subset $D_D[y, G^{(1)}] \subset D_D$ in the same way as $D_E[y, G^{(1)}]$ for $y \in \mathbb{F}_q^{n-x}$. Then, we define a QQSS protocol as Protocol 5. This protocol is called the linear QQSS protocol with $(G^{(1)}, G^{(2)}, F)$.

**Protocol 5** Linear QQSS protocol with $(G^{(1)}, G^{(2)}, F)$

**STEP 1:** Share generation: The dealer encodes the system $\mathcal{H}^{(s) \otimes [x]}$ into the subspace $D_D[0, G^{(1)}]$. Hence, the message system $D_M$ is identified with $D_D[0, G^{(1)}]$. The dealer prepares a uniform random variable $U_{D, 2} \in \mathbb{F}_{q^2}$, and applies $W_{D_D}(G^{(2)} U_{D, 2})$ on $D_D$.

**STEP 2:** Decoding: For a subset $A \in \mathcal{A}$, the end-user applies a suitable TP-CP map $\Gamma$ to recover the original state.

**Theorem 3:** Given a $2n \times (n-x)$ self-column-orthogonal matrix $G^{(1)}$ and a $2n \times y_2$ matrix $G^{(2)}$, we choose a $2n \times 2x$ matrix $F$ column-orthogonal to $G^{(1)}$. Then, the following conditions for $G^{(1)}, G^{(2)}, F$ are equivalent:

$$
\sum_{a \in \mathbb{F}_q^{n-x-1}} \left| F^{\top} \left( \begin{array}{c} a \\ 0 \end{array} \right) \right|.
$$

(28)
Choose there exist positive integers $(E_1)$ $r$ $(\mathcal{A}, \mathcal{B})$-secure. That is, there exists a suitable TP-CP map \( \Gamma \) to recover the original state in step 2.

(D2) The linear CSS protocol with $\{(G^{(1)}, G^{(2)}), F \}$ is $(\mathcal{A}, \mathcal{B})$-secure.

(D3) The matrix $\{(G^{(1)}, G^{(2)}), F \}$ is an $(\mathcal{A}, \mathcal{B})$-MMSP.

This theorem will be shown by Theorem 8 including the construction of the decoder in Section VII-B. The papers [17] studied QQSS protocols with a general access structure. However, the paper [17] did not discuss its relation with MMSP.

Example 7: For $n = 3$, we choose $G^{(1)}$ and $F$ in the same way as Example 5. Since the column vectors of $(G^{(1)}, F^n)$ are linearly independent, $G^{(1)}$ is self-column-orthogonal, and $F$ is column-orthogonal to $G^{(1)}$, according to Protocol 5, the randomless linear QQSS protocol with $(G^{(1)}, F)$ can be constructed.

We choose $\mathcal{A} = \{\{1, 2\}, \{1, 2, 3\}\}$ and $\mathcal{B} = \{\emptyset, \{1\}, \{2\}, \{3\}\}$. Since Example 5 guarantees that $(G^{(1)}, F)$ is an $(\mathcal{A}, \mathcal{B})$-MMSP, due to Theorem 3, the randomless linear QQSS protocol with $(G^{(1)}, F)$ is $(\mathcal{A}, \mathcal{B})$-secure, i.e., there exists a suitable TP-CP map $\Gamma$ to recover the original state in step 2.

To characterize QQSS protocols with the threshold case, i.e., the ramp scheme, we define the following special case of $(\mathcal{A}, \mathcal{B})$-MMSPs.

**Definition 11** $\{(r, t, n)$-QQMMSP$: We choose $\mathcal{A} = \{A \subset [n] \mid |A| \geq r \}$ and $\mathcal{B} = \{B \subset [n] \mid |B| \leq t \}$. Given a $2n \times (n - x)$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times 2y$ matrix $G^{(2)}$, and a $2n \times 2x$ matrix $F$ column-orthogonal to $G^{(1)}$, the matrix $(G^{(1)}, G^{(2)}, F)$ is called an $(r, t, n)$-QQMMSP when the matrix $\{(G^{(1)}, G^{(2)}), F \}$ is an $(\mathcal{A}, \mathcal{B})$-MMSP.

When the matrix $(G^{(1)}, G^{(2)}, F)$ is an $(r, t, n)$-QQMMSP, the linear QQSS protocol with $(G^{(1)}, G^{(2)}, F)$ has the perfect secrecy for $t$ colluded players. In this case, the secret can be recovered by the end-user when the end-user collects the shares from $r$ players. Such a linear QQSS protocol is called an $(r, t, n)$-linear QQSS protocol.

**Theorem 4:** Let $p$ be a prime number. Then, the following conditions for positive integers $r, t, n$ with $n \geq r > t > 0$ are equivalent.

(E1) The condition $r \geq (n + 1)/2$ holds.

(E2) There exist positive integers $s$, $y_2$, and $x$, a $2n \times (n - x)$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and a $2n \times 2x$ matrix $F$ column-orthogonal to the matrix $G^{(1)}$ on $\mathbb{F}_q$ with $q = p^s$ such that the matrix $(G^{(1)}, G^{(2)}, F)$ is an $(r, t, n)$-QQMMSP.

(E3) Choose $t' := \max(t, n - r)$. There exist a positive integer $s$, a $2n \times (n - r + t')$ self-column-orthogonal matrix $G^{(1)}$, $a 2n \times (t' + r - n)$ matrix $G^{(2)}$, and a $2n \times 2(t - t')$ matrix $F$ column-orthogonal to the matrix $G^{(1)}$ on $\mathbb{F}_q$ with $q = p^s$ such that the matrix $(G^{(1)}, G^{(2)}, F)$ is an $(r, t, n)$-QQMMSP.

Theorem 4 is shown in Appendix D. Therefore, the threshold scheme, i.e., a $(r, n - r - 1, n)$-secure QQSS protocol exists when $n \geq r \geq (n + 1)/2$ [29]. Combining Theorem 3 and Theorem 4, we obtain the following corollary.

**Corollary 2:** When the condition $r \geq (n + 1)/2$ holds, there exists an $(r, t, n)$-secure QQSS protocol with rate $(r - \max(t, n - r))/n$.

Only a limited case of the ramp case for QQSS protocols was discussed in existing studies [26], [27]. That is, the achievability of the rate $(r - \max(t, n - r))/n$ was not shown in existing studies. In addition, as a special case of QQSS protocol, we define the QQ version of MDS codes as follows.

**Definition 12** $\{(n, r)$-QMQMD$)$ code$: We consider the case with $t = n - r$. Assume that $G^{(1)}$ is a $2n \times 2(n - r)$ self-column-orthogonal matrix and $F$ is a $2n \times 2(2r - n)$ matrix column-orthogonal to $G^{(1)}$. We say that the randomless linear QQSS protocol with $(G^{(1)}, F)$ is an $(n, r)$-QMQMD code when it is $\mathcal{A}$-correct with $\mathcal{A} = \{A \subset [n] \mid |A| \geq r \}$.

Usually, a QMQMD code is called a quantum MDS code [72], [73], [74]. Hence, any $(r, n - r, n)$-secure QQSS protocol is an $(n, r)$-QMQMD code while its special case was mentioned in [75]. We have the following characterization for QMQMD codes.

**Lemma 3:** Given a $2n \times 2(n - r)$ self-column-orthogonal matrix $G^{(1)}$ and a $2n \times 2(2r - n)$ matrix $F$ column-orthogonal to $G^{(1)}$, the following conditions are equivalent.

(F1) The randomless linear QQSS protocol with $(G^{(1)}, F)$ is an $(n, r)$-QMQMD code.

(F2) The matrix $(G^{(1)}, F)$ accepts $\mathcal{A}$ with $\mathcal{A} = \{A \subset [n] \mid |A| \geq r \}$ in the sense of Definition 6.

This Lemma will be shown as Corollary 6 in Section VII-B. Considering the special case of Theorem 4 with $t = n - r$, we have the following corollary because an $(r, n - r, n)$-QQMMSP $(G^{(1)}, \emptyset, F)$ accepts $\mathcal{A}$ with $\mathcal{A} = \{A \subset [n] \mid |A| \geq r \}$.

**Corollary 3:** For any positive integers $r, n$ with $n \geq r > 0$ and any prime $p$, there exist a positive integer $s$, a $2n \times 2(n - r)$ self-column-orthogonal matrix $G^{(1)}$, and a $2n \times 2(2r - n)$ matrix $F$ column-orthogonal to the matrix $G^{(1)}$ on $\mathbb{F}_q$ with $q = p^s$ such that the matrix $(G^{(1)}, F)$ accepts $\mathcal{A}$ with $\mathcal{A} = \{A \subset [n] \mid |A| \geq r \}$.

Therefore, due to Lemma 3 and Corollary 3, there exists an $(r, n - r, n)$-secure QQSS protocol that gives an $(n, r)$-QMQMD code with a sufficiently large prime power $q$ of any prime number $p$.

**Remark 3:** Usually, a quantum MDS code is defined as a code minimum distance $d$ whose dimension is $n + 2 - 2d$ [72], [73], [74]. Reference [76] showed that the following conditions for stabilizer codes are equivalent to the condition that the minimum distance is $d$.

(G1) It is possible to detect the existence of error only with $d - 1$ systems.

(G2) It is possible to recover the original state when errors occur only in $\lfloor (d - 1)/2 \rfloor$ systems.

(G3) It is possible to recover the original state even when $\lfloor d - 1 \rfloor$ systems are lost at most.

Our definition (Definition 12) is based on the condition (G3).

**Remark 4:** We remark the relation with stabilizer codes. When $G^{(2)}$ is empty, the randomless linear QQSS protocol with $(G^{(1)}, F)$ with a $2n \times (n - x)$ matrix $G^{(1)}$ and a $2n \times x$ matrix $F$ has a relation with a stabilizer code. Since $G^{(1)}$ is self-column-orthogonal, the group $N := \{G^{(1)}y\}_{y \in \mathbb{F}_q^{(n-x)}}$
TABLE III

| general access structure | relation to MMSP | ramp scheme | relation between QMMDs code and QCSSS protocol |
|--------------------------|-----------------|------------|-----------------------------------------------|
| [26], [27]              | No              | No         | No                                            |
| [72], [73], [74], [76]  | No              | No         | No (They studied only QMMDs code.)            |
| This paper              | Yes             | general case (Thm. 3) | Yes (Lem. 3) |

The linear QCSIIR protocol with $G^{(1)}$, $G^{(2)}$, $Q^{(K)}$ is called the standard linear QCSIIR protocol with $(G^{(1)}, G^{(2)}, F)$ when the query $Q^{(K)}$ is given as (21) by using $F$. In addition, linear QCSIIG protocols discussed in [37], [38], and [39] do not have randomization $U_{y_2} \in F_{q^2}$. That is, $y_2 = 0$ and it does not have the matrix $G^{(2)}$. Such a protocol is called the randomless standard linear QCSIIR protocol with $(G^{(1)}, F)$. Then, we have the following theorem.

**Theorem 5:** Given a $2n \times n$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and a query $Q^{(K)}$, the following conditions are equivalent.

- (H1) The linear QCSIIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.
- (H2) The linear QCSIIR protocol with $G^{(1), G^{(2)}}, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

In addition, we assume that $F$ is a $2n \times x$ matrix. the following conditions for $G^{(1)}, G^{(2)}$, and $F$ are equivalent.

- (H3) The standard linear QCSIIR protocol with $(G^{(1)}, G^{(2)}, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.
- (H4) The standard linear QCSIIR protocol with $((G^{(1)}, G^{(2)}), F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.
- (H5) The matrix $((G^{(1)}, G^{(2)}), F)$ is an $(\mathfrak{A}, \mathfrak{B})$-MMSP.

C. Linear QCSIIR Protocol

We choose an $n \times n$ matrix $G^{(1)}$, an $n \times y_2$ matrix $G^{(2)}$, and an $n \times x$ matrix $F$ on the finite field $F_{q^2}$ with $n = 2n$ in the same way as Section V-A. Then, similar to Section V-A, we define a normalized vector $|\psi(G^{(1)})\rangle \in D_1 \otimes \cdots \otimes D_n$ as the stabilizer of the column vectors of $G^{(1)}$. Then, using the state $|\psi(G^{(1)})\rangle$, we define the linear QCSIIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ as Protocol 6.

**Protocol 6** Linear QCSIIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$.

**STEP 1: Preparation:** We set the initial state $|\rho_D\rangle$ on $D_1 \otimes \cdots \otimes D_n$ to be $|\psi(G^{(1)})\rangle$. Let $U_{S,2}$ be a random variable subject to the uniform distribution on $F_{q^2}^n$. The shared randomness $R = (R_1, \ldots, R_{2n})^T$ is generated as $R_j := G^{(2)} U_{S,2}$ for $j = 1, \ldots, 2n$. The randomness $R$ is distributed so that $j$-th server contains $R_j$ and $R_{n+j}$ for $j = 1, \ldots, n$.

**STEP 2: User’s encoding:** The user randomly encodes the index $K$ to classical queries $Q^{(K)} := (Q^{(1)}_1, \ldots, Q^{(2n)}_K)^T$, which is an $n \times 1$ random matrix for $k = 1, \ldots, f$. The user sends $Q^{(K)}$, $Q^{(K)}_{n+j}$ to the $j$-th server $\sigma_j$.

**STEP 3: Servers’ encoding:** The $j$-th server $\sigma_j$ applies unitary $W_j(Q^{(K)}_j \hat{m} + R_j, Q^{(K)}_{n+j} \hat{m} + R_{n+j})$ on $D_1$.

**STEP 4: Decoding:** For a subset $A \in \mathfrak{A}$, the user makes the measurement given by the POVM $\{W_A(y)(\tr_A^* |\psi(G^{(1)})\rangle \langle |\psi(G^{(1)})\rangle |W_A^T(y)\}_{y \in F_{q^2}^{n+1}}$. Based on the obtained outcome, the user outputs the measurement outcome $m$ as the retrieval result.

The linear QCSIIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ is called the standard linear QCSIIR protocol with $(G^{(1)}, G^{(2)}, F)$ when the query $Q^{(K)}$ is given as (21) by using $F$. In addition, linear QCSIIR protocols discussed in [37], [38], and [39] do not have randomization $U_{y_2} \in F_{q^2}$. That is, $y_2 = 0$ and it does not have the matrix $G^{(2)}$. Such a protocol is called the randomless standard linear QCSIIR protocol with $(G^{(1)}, F)$. Then, we have the following theorem.

**Theorem 5:** Given a $2n \times n$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and a query $Q^{(K)}$, the following conditions are equivalent.

- (H1) The linear QCSIIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.
- (H2) The linear QCSIIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

In addition, we assume that $F$ is a $2n \times x$ matrix. the following conditions for $G^{(1)}, G^{(2)}$, and $F$ are equivalent.

- (H3) The standard linear QCSIIR protocol with $(G^{(1)}, G^{(2)}, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.
- (H4) The standard linear QCSIIR protocol with $((G^{(1)}, G^{(2)}), F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.
- (H5) The matrix $((G^{(1)}, G^{(2)}), F)$ is an $(\mathfrak{A}, \mathfrak{B})$-MMSP.

Also, we have the following proposition.

**Proposition 5:** In Protocol 6, even when STEP 4 is replaced by another decoder, the decoder can be simulated by the decoder given in STEP 4. That is, once STEPs 1, 2, and 3 are given in Protocol 6, without loss of generality, we can assume that our decoder is given as STEP 4.

The above theorem and proposition will be shown after Corollary 7 later. Combining Theorems 2 and 5, we obtain the following corollary.

**Corollary 4:** When $n \geq r > t \geq n/2 > 0$, there exists an $(r, t, n)$-secure linear QCSIIR protocol of rate $2(r - t)/n$.

**Example 8:** For $n = 3$, we choose $G^{(1)}$ and $F$ in the same way as Example 5. Since the column vectors of $(G^{(1)+}, F^*)$ are linearly independent, $G^{(1)}$ is self-column-orthogonal, and $F$ is column-orthogonal to $G^{(1)}$, according to Protocol 6 with (21), the randomless standard linear QCSIIR protocol with $(G^{(1)}, F)$ can be constructed.

We choose $\mathfrak{A} = \{\emptyset, \{1\}, \{2\}, \{3\}\}$ and $\mathfrak{B} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. Since Example 5 guarantees that $(G^{(1)}, F)$ is an $(\mathfrak{A}, \mathfrak{B})$-MMSP, the randomless standard linear QCSIIR protocol with $(G^{(1)}, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure due to Theorem 5.

**Example 9:** For $n = 3$, we choose $G^{(1)+}$ and $F^*$ in the same way as Example 6. The column vectors of $(G^{(1)+}, F^*)$ are linearly independent. $G^{(1)+}$ is self-column-orthogonal. Hence, according to Protocol 6 with (21), the randomless standard linear QCSIIR protocol with $(G^{(1)+}, F^*)$ can be constructed.

We choose $\mathfrak{A}^* = \{\{1, 2\}\}$ and $\mathfrak{B}^* = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 3\}\}$ in the same way as Example 6. As shown in Example 6, $(G^{(1)+}, F^*)$ is an $(\mathfrak{A}, \mathfrak{B})$-MMSP. Thus, the randomless standard linear QCSIIR protocol with $(G^{(1)+}, F^*)$ is $(\mathfrak{A}, \mathfrak{B})$-secure due to Theorem 5.

The preceding paper [40] proposed a protocol with the rate $2(n - t)/n$ when $r = n$. That is, no existing study considered QCSIIR protocols with general qualified sets $\mathfrak{A}$ including the case with $r < n$. Hence, Corollary 4 can be considered as a generalization of the existing result [40]. The comparison with the existing QCSIIR results is summarized in Table IV. In the
TABLE IV
Comparison for Analysis for CQSPIR Protocols

|                | general qualified set | relation to MMSP | threshold type qualified set |
|----------------|-----------------------|------------------|------------------------------|
| [37]–[39]      | No                    | No               | case with $t = n$ and special 1 |
| [40]           | No                    | No               | case with $t = n$ and general 1 |
| This paper     | Yes                   | general case (Theorem 5) | general case (Corollary 4) |

classical case, the optimal rate of $(r, t, n)$-secure SPIR protocol is $(r-t)/n$ [10, Corollary 4]. Hence, the rate of Corollary 8 is twice of the classical case. In addition, the rate of CQSPIR cannot exceed 1 due to the condition $t \geq n/2$.

Remark 5: One may consider that SPIR for quantum states can be discussed in this framework. However, a simple application of this method to SPIR for quantum states does not work due to the following reasons. To transmit quantum states, we need to perform a quantum operation across several subsystems. In the case of SS, only the dealer makes encoding. Hence, a quantum operation across several subsystems is possible. However, in the case of SPIR, several servers perform encoding operations individually. Hence, it is impossible to perform a quantum operation across several subsystems. This is reason why we cannot apply the same scenario to SPIR for quantum states.

VI. QUANTUM SS PROTOCOLS WITH PRESHARED ENTANGLEMENT WITH END-USER

This section introduces EASS protocols and presents our results for EASS protocols, which implies our results for CQSS protocols.

A. Formulation

Modifying the CQSS setting by allowing prior entanglement between the dealer and the end-user, we formulate an SS protocol with preshared entanglement between the dealer and the end-user. Since this problem setting employs entanglement assistance, this protocol is called an entanglement-assisted secret sharing (EASS) protocol. As illustrated in Fig. 1 (c), an EASS protocol with one dealer, $n$ players, and one end-user is defined as Protocol 7.

Definition 13 ($\mathcal{A}, \mathcal{B}$)-EASS: For an access structure $(\mathcal{A}, \mathcal{B})$ on $[n]$, an EASS protocol defined as Protocol 7 is called $(\mathcal{A}, \mathcal{B})$-secure if the following conditions are satisfied.

$\mathcal{A}$-correctness is defined in the same way as Definition (1).

- Correctness: The relation

$$\text{Tr} \Gamma[m](\rho_{DE})(Y_{A,E}(m) \otimes I_{A'}) = 1$$

holds for $m \in \mathcal{M}$.

- Secrecy: The state $\text{Tr}_{(B,E)} \Gamma[m](\rho_{DE})$ does not depend on $m \in \mathcal{M}$.

In particular, when the system $D_E$ has the same dimension as $D_D$ and the state $\rho_{DE}$ is a maximally entangled state, the EASS protocol is called fully EASS (FEASS) protocol.

Protocol 7 EASS protocol

STEP 1: Preparation: The dealer and the end-user have quantum systems $D_D$ and $D_E$, respectively, and share a state $\rho_{DE}$ on the joint quantum system $D_D \otimes D_E$ before the protocol.

STEP 2: Share generation: Depending on the message $m \in \mathcal{M}$, the dealer prepares $n$ shares as the joint system $D_1 \otimes \cdots \otimes D_n$ by applying a TP-CP map $\Gamma[m]$ from $D_D$ to $D_1 \otimes \cdots \otimes D_n$, and sends the $j$-th share system $D_j$ to the $j$-th player.

STEP 3: Decoding: For a subset $A \in \mathcal{A}$, the end-user decodes the message from the received state from players $A$ by a decoder, which is defined as a POVM Dec($A, E$) := $\{Y_{A,E}(w) \mid w \in [m]\}$ on $D[D] \otimes D_E$. The end-user outputs the measurement outcome $W$ as the decoded message.

Protocol 8 Linear FEASS protocol with $(G, F)$

STEP 1: Preparation: We set the initial state $\rho_{DE}$ on $D_D \otimes D_E$ to be $|\Phi\rangle$.

STEP 2: Share generation: The dealer prepares a uniform random variable $U_D \in \mathcal{F}_q^*$. For $m \in \mathcal{M}$, the dealer applies $W_{[m]}(Fm + GU_D)$ on $D_D$. That is, the encoding operation $\Gamma[m]$ on $D_D$ is defined as

$$\Gamma[m](\rho) := \sum_{u_D \in \mathcal{F}_q^*} \frac{1}{q^t} W_{[m]}(Fm + GU_D) \rho W_{[m]}^\dagger(Fm + GU_D).$$

(30)

The shares are given as parts of the state $\Gamma[m](|\Phi\rangle \langle \Phi|)$. 

STEP 3: Decoding: For a subset $A \in \mathcal{A}$, the end-user takes the partial trace on $D_E[A']$, and makes the measurement on the basis $\{W_{A}(y)|\Phi\rangle \langle \Phi|\}_{y \in \mathcal{Y}[A]}$. Based on the obtained outcome, the end-user recovers $m$.

B. Linear FEASS Protocol

Next, we formulate linear protocols with preshared entanglement with user. Given an $n \times (y + x)$ matrix $(G,F)$ on the finite field $\mathbb{F}_q$ with $n = 2n$, we define an EASS protocol as follows. We choose the message set $\mathcal{M}$ as $\mathbb{F}_q^*$ and choose the Hilbert space $\mathcal{H}$ as the space spanned by $\{|x\rangle\}_{x \in \mathbb{F}_q^*}$. We define $D_J$ and $D_{E,J}$ as $\mathcal{H}$, and define $D_D$, $D_E$, $D_A$, $D_{E,A}$, and $D_{E,A,J}$, respectively, for any subset $A \subset [n]$. Hence, $D_D$ and $D_E$ are $\mathcal{H}^{\otimes n}$. In the following sections, we adopt the above definitions. Also, we use the maximally entangled state $|\phi\rangle := \sum_{x \in \mathbb{F}_q^*} \frac{1}{\sqrt{q^t}} |x\rangle$ on $\mathcal{H}^{\otimes 2}$. In particular, we define the state $|\Phi\rangle$ as the state on the composite $D_D \otimes D_E$ whose reduced density on $D_J \otimes D_{E,J}$ is $|\phi\rangle$.

Then, we define the linear FEASS protocol with $(G,F)$ as Protocol 8.

Lemma 4: The following conditions for $(G,F)$ are equivalent.

(11) The linear FEASS protocol with $(G,F)$ is $(\mathcal{A}, \mathcal{B})$-secure.

(12) The linear CSS protocol with $(G,F)$ is $(\mathcal{A}, \mathcal{B})$-secure.

(13) The matrix $(G,F)$ is an $(\mathcal{A}, \mathcal{B})$-MMSP.
Proof: Since the equivalence between (I2) and (I3) follows from Proposition 1, we show the equivalence between (I1) and (I2).

Given a subset $A \subset [n]$ and $x \in \mathbb{F}_q^n$, we consider a linear FEASS protocol with $(G, F)$. In this protocol, we have

$$\text{Tr}_{(A,E)} W_n(x) \langle \phi \rangle \langle \bar{\phi} \rangle W_n^\dagger(x) = W_A(P_A x) \langle |\phi\rangle \langle |\bar{\phi}\rangle |A\rangle W_A^\dagger(P_A x) \otimes \rho_{\text{mix}}^{|A\rangle}.$$  \hspace{0.5cm} (31)

Hence, the above state can be identified with the classical information $P_A x$. That is, the analysis on the correctness and the secrecy in the linear FEASS protocol with $(G, F)$ is equivalent with the correctness and the secrecy in the linear CSS protocol with $(G, F)$. We obtain the equivalence between (I1) and (I2).

Proposition 6: In Protocol 8, even when STEP 3 is replaced by another decoder, the decoder can be simulated by the decoder given in STEP 3. That is, once STEPs 1 and 2 are given in Protocol 8, without loss of generality, we can assume that our decoder is given as STEP 3.

Proof: When the end-user can access all shares, any possible state $\Gamma[m]\langle \rho \rangle$ is a diagonal state with respect to the basis $\{W_n(x)|\Phi\rangle\}_{x \in \mathbb{F}_q^n}$. For any subset $A \subset [n]$, the state reduced density with respect to $(A,E)$ is given as (31). Since the state $\rho_{\text{mix}}$ has no information, without loss of generality, we can consider that the state is $W_A(P_A x)\langle |\phi\rangle \langle |\bar{\phi}\rangle |A\rangle W_A^\dagger(P_A x)$, which is a diagonal state with respect to the basis $\{W_A(x)\langle |\phi\rangle \langle |\bar{\phi}\rangle |A\rangle\}_{x \in \mathbb{F}_q^n}$. Therefore, even when STEP 3 is replaced by another decoder, the decoder can be simulated by the decoder given in STEP 3.

C. Linear EASS Protocol

Next, we focus on a $2n \times y_1$ self-column-orthogonal matrix $G^{(1)}$ and a $2n \times y_2$ matrix $G^{(2)}$. We denote $y_1$ column vectors of $G^{(1)}$ by $g^{(1)}, \ldots, g^{y_1}$. In this section, we propose another EASS protocol. For this aim, we choose $n - y_1$ column vectors $\bar{g}^{1}, \ldots, \bar{g}^{n-y_1}$ such that all the vectors $g^{1}, \ldots, g^{y_1}, \bar{g}^{1}, \ldots, \bar{g}^{n-y_1}$ are orthogonal to each other in the sense of the symplectic inner product. We also choose vectors $h^{1}, \ldots, h^{y_1}$ such that $\langle h^{1}, g^{1}\rangle = \delta_{1,1'}$ and $\langle h^{1}, h^{y_1}\rangle = 0$. We denote the matrix $(h^{1}, \ldots, h^{y_1})$ by $H^{(1)}$.

For $y \in \mathbb{F}_q$ and $x \in \mathbb{F}_q^{n-y_1}$, we define the vector $|x,y\rangle$ as

$$W_n(g_j)|x,y\rangle = \omega_{jy}\langle x,y\rangle$$ \hspace{0.5cm} (32)

$$W_n(\bar{g}_j)|x,y\rangle = \omega_{jx}\langle x,y\rangle$$ \hspace{0.5cm} (33)

$$W_n(H^{(1)}\bar{y})|x,y\rangle = \langle x,y + \bar{y}\rangle.$$ \hspace{0.5cm} (34)

We define the space $D_E[y,G^{(1)}]$ as the space spanned by $\{|x,y\rangle\}_{x \in \mathbb{F}_q^{n-y_1}}$. We define the entangled state

$$|\Phi[y,G^{(1)}]\rangle := \sum_{x \in \mathbb{F}_q^{n-y_1}} \frac{1}{\sqrt{q^{n-y_1}}} |x,y\rangle|x,y\rangle.$$ \hspace{0.5cm} (35)

To consider the relation with CSS protocols, we modify Protocol 8 as follows. The initial state $|\Phi\rangle$ is replaced by $|\Phi[0,G^{(1)}]\rangle$. The random variable $U_D$ is written as $(U_{D,1},U_{D,2})$ with $U_{D,1} \in \mathbb{F}_q^2$ and $U_{D,2} \in \mathbb{F}_q^2$ so that $G_{U_D} = G^{(1)}U_{D,1} + G^{(2)}U_{D,2}$. The applied unitary $W_n(Fm + GU_D)$ is replaced by $W_n(Fm + G^{(2)}U_{D,2})$. In this protocol, the end-user’s space $D_E$ is given as $D_E[0,G^{(1)}]$. This protocol is formally written as Protocol 9, and is called the linear EASS protocol with $(G^{(1)},G^{(2)},F)$. In this notation, the first matrix $G^{(1)}$ identifies the initial state, the second matrix $G^{(2)}$ identifies the direction of the randomization for secrecy, and the third matrix $F$ identifies the direction of the message imbedding. That is, the linear EASS protocol with $(G^{(1)},G^{(2)},F)$ is different from the linear FEASS protocol with $(G^{(1)},G^{(2)},F)$ because the latter is characterized as follows: The initial state is the maximally entangled state between $D_D \otimes D_E$ and the matrix $(G^{(1)},G^{(2)})$ determines the direction of the randomization for secrecy.

Protocol 9 Linear EASS protocol with $(G^{(1)},G^{(2)},F)$

STEP 1: Preparation: We set the initial state $\rho_{DE}$ on $D_D \otimes D_E[0,G^{(1)}]$ to be $|\Phi[0,G^{(1)}]\rangle$.

STEP 2: Share generation: The dealer prepares a uniform random variable $U_{D,2} \in \mathbb{F}_q^2$. For $m \in A$, the dealer applies $W_n(Fm + G^{(2)}U_{D,2})$ on $D_D$. That is, the encoding operation $\Gamma[m]$ on $D_D$ is defined as

$$\Gamma[m]|\rho\rangle := \sum_{u_{D,2} \in \mathbb{F}_q^2} \frac{1}{q^{y_2}} W_n(Fm + G^{(2)}u_{D,2}) \rho \cdot W_n^\dagger(Fm + G^{(2)}u_{D,2}).$$ \hspace{0.5cm} (36)

The shares are given as parts of the state $\Gamma[m]|\Phi[0,G^{(1)}]\rangle|\Phi[0,G^{(1)}]\rangle$.

STEP 3: Decoding: For a subset $A \subset \mathfrak{A}$, the end-user takes partial trace on $D_E[A^{\perp}]$, and makes the measurement given by the POVM $\{\Pi_E[A]\}_{z \in \mathbb{F}_q^{y_2}}$, where $\Pi_E[A]$ is defined as

$$W_A(z) \langle \text{Tr}_{D[A^{\perp}],D_E[A]}|\Phi[0,G^{(1)}]\rangle|\Phi[0,G^{(1)}]\rangle W_A^\dagger(z).$$ \hspace{0.5cm} (37)

Based on the obtained outcome, the end-user recovers $m$. In particular, when $y_2 = 0$, the protocol does not have the matrix $G^{(2)}$ and the protocol does not have the random variable $U_{D,2}$. Such a protocol is called the ransomless linear EASS protocol with $(G^{(1)},F)$. Similar to Lemma 4, we have the following theorem for linear EASS protocols, Protocol 9.

Theorem 6: Given a $2n \times y_1$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and a $2n \times x$ matrix $F$, the following conditions are equivalent.

(J1) The linear EASS protocol with $(G^{(1)},G^{(2)},F)$ is $(\mathfrak{A},\mathfrak{B})$-secure.
(J2) The linear FEASS protocol with \(((G^{(1)}, G^{(2)}), F)\) is \((\mathfrak{A}, \mathfrak{B})\)-secure.
(J3) The linear CSS protocol with \(((G^{(1)}, G^{(2)}), F)\) is \((\mathfrak{A}, \mathfrak{B})\)-secure.
(J4) The matrix \(((G^{(1)}, G^{(2)}), F)\) is an \((\mathfrak{A}, \mathfrak{B})\)-MMSP.

The above theorem shows the one-to-one correspondence between a special class of linear FEASS protocols and linear EASS protocols.

Example 10: In this example, we give an example of MMSP which can be converted to a randomless linear EASS protocol that overperforms a linear CQSS protocol.

Let \(p\) be a prime. For \(n = p\), we define the \(2p \times 2p\) matrix \(G^{**} = (g_{j,k})\) and the \(2p \times 2p\) matrix \(F^{**} = (f_{j,k})\) over \(\mathbb{F}_p\) as \(g_{j,1} = 1, g_{j,p+1} = 0, g_{j,2} = 0, g_{j,p+2} = 1, f_{j,1} = j - 1, f_{j,p+1} = 0, f_{j,2} = 0, f_{j,p+2} = j - 1\) for \(j = 1, \ldots, p\). The column vectors of \((G^{**}, F^{**})\) are linearly independent. \(G^{**}\) is self-column-orthogonal.

When \(p > 2\), \((G^{**}, F^{**})\) cannot be used for a randomless linear CQSS protocol nor a randomless linear QQSS protocol, because \(G^{**}\) is not a \(2p \times p\) matrix. But, the randomless linear EASS protocol with \((G^{**}, F^{**})\) can be constructed according to Protocol 9.

We choose \(\mathfrak{A}^{**} = \{A \subset [p] \mid |A| \geq 2\}\) and \(\mathfrak{B}^{**} = \{B \subset [p] \mid |B| \leq 1\}\). For \(i < j \in [p]\), we have

\[
P_{(i,j)}(G^{**}, F^{**}) = \begin{pmatrix} 1 & 0 & i - 1 & 0 \\ 0 & 1 & 0 & i - 1 \\ 0 & 1 & 0 & i - 1 \\ 0 & 1 & 0 & j - 1 \end{pmatrix}.
\]

The first relation shows that the MMSP \((G^{**}, F^{**})\) rejects \(\mathfrak{B}^{**}\), and the second relation shows that the MMSP \((G^{**}, F^{**})\) accepts \(\mathfrak{A}^{**}\). Therefore, the MMSP \((G^{**}, F^{**})\) is an \((\mathfrak{A}^{**}, \mathfrak{B}^{**})\)-MMSP.

Thus, the randomless linear EASS protocol with \((G^{**}, F^{**})\) is \((\mathfrak{A}^{**}, \mathfrak{B}^{**})\)-secure due to Theorem 6. The randomless linear EASS protocol with \((G^{**}, F^{**})\) has the rate \(2/p\).

In addition, the equivalence between (J1) and (J2), we have a statement similar to Proposition 6 as follows while its proof is given in Section VI-D.

Proposition 7: In Protocol 9, even when STEP 3 is replaced by another decoder, the decoder can be simulated by the decoder given in STEP 3. That is, once STEPs 1 and 2 are given in Protocol 9, without loss of generality, we can assume that our decoder is given as STEP 3.

When \(y_1 = n/2 = n, D_{E}[0, G^{(1)}]\) is a one-dimensional system and the summand for \(x\) does not appear in (35). Hence, the state \(|\Phi[0, G^{(1)}]\) is a product state, and can be considered as a state on \(D_{E}\). Since the state on \(D_{E}\) in Protocol 9 is fixed to \(|0_0\rangle\), Protocol 9 is essentially the same as Protocol 4, a linear CQSS protocol. Therefore, as corollaries of Theorem 6 and Proposition 6, we obtain Theorem 1 and Proposition 4.

Since \(G^{(1)}\) is self-column-orthogonal, the group \(N := \{G^{(1)}y \mid y \in \mathbb{F}_p^n\}\) satisfies the self-orthogonal condition \(N \subset N^\perp := \{v \in \mathbb{F}_p^n \mid \langle v, v' \rangle = 0, \forall v' \in N\}\). In particular, the dimension of \(N\) is \(n\), \(N = N^\perp\). Hence, the state \(|\Phi[0, G^{(1)}]\) is given as the stabilizer state of \(N\). That is, the encoded state is given as the application of \(\Gamma[n]\) to the stabilizer state of \(N\).

Therefore, as a generalization of \((r, t, n)\)-CQMMSP, we define the following special case of \((\mathfrak{A}, \mathfrak{B})\)-MMSPs.

Definition 14 \((\mathfrak{A}, \mathfrak{B})\)-MMSP: We choose \(\mathfrak{A} = \{A \subset [n] \mid |A| \geq r\}\) and \(\mathfrak{B} = \{B \subset [n] \mid |B| \leq t\}\). Given a \(2n \times y_1\) self-column-orthogonal matrix \(G^{(1)}\), a \(2n \times y_2\) matrix \(G^{(2)}\), and a \(2n \times \times\) matrix \(F\), the matrix \((G^{(1)}, G^{(2)}, F)\) is called an \((\mathfrak{A}, \mathfrak{B})\)-MMSP when the matrix \(((G^{(1)}, G^{(2)}, F)\) is an \((\mathfrak{A}, \mathfrak{B})\)-MMSP.

Theorem 7: For any positive integers \(r, t, n, y_1\) with \(n \geq r > t \geq y_1/2 \geq 0\) and any prime \(p\), there exists a prime integer \(s\), a \(2n \times y_1\) self-column-orthogonal matrix \(G^{(1)}\), a \(2n \times (2t - y_1)\) matrix \(G^{(2)}\), and a \(2n \times (2r - 2t)\) matrix \(F\) on \(\mathbb{F}_p\) with \(q = p^s\) such that the matrix \((G^{(1)}, G^{(2)}, F)\) is an \((\mathfrak{A}, \mathfrak{B})\)-MMSP.

Theorem 7 is shown in Appendix B. Combining Theorem 7, we obtain the following corollary.

Corollary 5: When \(n \geq r > t \geq 0\), there exists an \((r, t, n)\)-secure EASS protocol with rate \(2(r-t)/n\).

In the case of classical case, the optimal rate of \((r, t, n)\)-secure SS protocol is \((r-t)/n\) [34, 70, 71]. Hence, the rate of Corollary 5 is twice of the classical case. However, the rate of CQSS cannot exceed 1 due to the condition \(t \geq n/2\). This constraint always holds beyond the condition in Corollary 5 because CQSS does not have shared entanglement. Since EASS has shared entanglement, the rate of CQSS exceeds 1 by removing the condition \(t \geq n/2\), which can be considered as an advantage of EASS over CQSS. In addition, in the case of threshold type, i.e., the case with \(r = t + 1\), a CQSS protocol requires the condition \(t \geq n/2\) in Corollary 1. In contrast, an EASS protocol works even with \(n/2 \geq t = t + 1\), which is another advantage of use of preshared entanglement with user over CQSS protocols.

Remark 6: We compare the above EASS protocols, Protocol 9, with the combination of QQSS protocol and dense coding. As discussed in Corollary 2, QQSS protocol has the rate \((r - \max(t, n - r))/n\) under the condition \(n \geq r > (n + 1)/2\). Combining it with dense coding, the obtained protocol has the rate \(2(r - \max(t, n - r))/n\). In contrast, as mentioned in Corollary 5, the EASS protocol has the rate \((r - t)/n\) under the condition \(n \geq r > t \geq 0\). Since \(2(r-t)/n-2(r-\max(t, n-r))/n = \max(0, n-r-t)/n \geq 0\), the EASS protocol has a strictly better performance than the simple combination of QQSS protocol and dense coding when \(n - r - t > 0\).

Remark 7: As another comparison, we can consider the comparison between a QQSS protocol and a combination of an EASS protocol and teleportation. This combined protocol is given as follows. Assume that the dealer and the end-user share entangled states. The dealer performs a generalized Pauli measurement across the input system and the entanglement half. The dealer sends the measurement outcome (classical messages) to the end-user via an EASS protocol. The end-user recovers the original quantum state by applying generalized Pauli operations to the other entanglement half based on the obtained measurement outcome. However, a QQSS protocol
allows no preshared entanglement between the dealer and the end-user. To discuss this comparison, we need to discuss an entanglement-assisted QKSS protocol, which is not defined in this paper. Studying this class of protocols is an interesting future study.

Further, as a special case of EASS protocol, we define the EA version of MDS codes as follows. This concept is useful for discussing the QQ version of MDS codes.

Definition 15 ((n, x)-EAMDS code): We consider the case with \( y_2 = 0 \). Assume that \( G(1) \) is an \( n \times y_1 \) self-column-orthogonal matrix and \( F \) is an \( n \times x \) matrix. We say that the randomless linear EASS protocol with \( (G(1), F) \) is a \( (n, [\frac{y_2 + x}{2}]) \)-EAMDS code when it is \( \mathfrak{A} \)-correct with \( \mathfrak{A} = \{ A \subset [n] \mid |A| \geq [\frac{y_2 + x}{2}] \} \).

By considering the case when \( \mathfrak{A} \) is the empty set, Theorem 6 implies the following lemma.

Lemma 5: Assume that \( G(1) \) is an \( n \times y_1 \) self-column-orthogonal matrix and \( F \) is an \( n \times x \) matrix. The randomless linear EASS protocol with \( (G(1), F) \) is \( \mathfrak{A} \)-correct with \( \mathfrak{A} = \{ A \subset [n] \mid |A| \geq [\frac{y_2 + x}{2}] \} \).

D. Proofs of Theorem 6 and Proposition 7

We show only Theorem 6 by using the idea by references [77], [78]. Lemma 4 guarantees the equivalence among (J2), (J3), and (J4). In the following, we show the equivalence between (J1) and (J2), and Proposition 7.

As the preparation, we notice the relation:

\[
\sum_{y \in \mathbb{F}_q} \frac{1}{q^y} \mathbf{W}_n[(G(1)y)\Phi][\Phi][G(1)y] = \sum_{y \in \mathbb{F}_q} \frac{1}{q^y} \langle \Phi[y, G(1)] \langle \Phi[y, G(1)] \rangle
\]

\[\tag{39}\]

\[= (a) \mathcal{W}_A(P_A H(1)y) \otimes W(H(1)y) \Phi[0, G(1)] \Phi[0, G(1)]
\]

\[\cdot (W_A(P_A H(1)y) \otimes W(H(1)y))^\dagger, \tag{40}\]

where \((a)\) follows from (34). Taking the partial trace on \( D[A^c] \) and \( D_E[A^c], \) for \( z \in \mathbb{F}_q^{|A^c|}, \) we have

\[
\Pi_z := \mathcal{W}_A(z)
\]

\[\cdot \left( \sum_{y \in \mathbb{F}_q} \frac{1}{q^y} \mathcal{W}_A(P_A G(1)y) \right)
\]

\[= \mathcal{W}_A(z) \left( \sum_{y \in \mathbb{F}_q} \frac{1}{q^y} \mathcal{W}_A(P_A G(1)y) \right) \mathcal{W}_A(z)^\dagger \tag{41}
\]

Proposition 10 Modified linear EASS protocol with \( (G(1), G(2), F) \)

STEP 1: Preparation: We set the initial state \( \rho_{DE} \) on \( D_D \otimes D_E \) to be \( \sum_{y \in \mathbb{F}_q} \frac{1}{q^y} [\Phi[y, G(1)] \Phi[y, G(1)]] \).

STEP 2: Share generation: The dealer prepares a uniform random variable \( U_D \in \mathbb{F}_q^y. \) For \( m \in \mathcal{M}, \) the dealer applies \( \mathbf{W}_n(Fm + G(2) U_{D, 2}) \) on \( D_D. \) That is, the encoding operation \( \Gamma[m] \) on \( D_D \) is defined as

\[
\Gamma[m](\rho) := \sum_{y \in \mathbb{F}_q} \frac{1}{q^y} \mathbf{W}_n(Fm + G(2) U_{D, 2}) \rho \cdot \mathbf{W}_n(Fm + G(2) U_{D, 2}). \tag{43}
\]

The shares are given as parts of the state \( \Gamma[m](\sum_{y \in \mathbb{F}_q} \frac{1}{q^y} [\Phi[y, G(1)] \Phi[y, G(1)]]). \)

STEP 3: Decoding: For a subset \( A \in \mathfrak{A}, \) the end-user takes partial trace on \( D_E[A^c], \) and makes the measurement on the basis \( \{ \mathcal{W}_A(z) [\Phi[0, A]] \}_{x \in \mathbb{F}_q^{|A|}}. \) Based on the obtained outcome, the end-user recovers \( m. \)

The relation (39) guarantees that their final states in STEP2 are the same, which implies that Protocol 8 has the same performance as Protocol 10.

Protocol 9 and Protocol 10 are converted to each other in decoding process as follows. For a subset \( A \in \mathfrak{A}, \) we modify the decoder of Protocol 9 as follows. First, the end-user randomly generates \( Y \in \mathbb{F}_q^y \) subject to the uniform distribution. The end-user applies the unitary \( \mathbf{W}_A(P_A H(1)y) \otimes \mathbf{W}(H(1)y) \) on \( (\otimes_{y \in A} D_T) \otimes D_E, \) Then, the end-user applies the measurement \( \{ \Pi_z \}_{x \in \mathbb{F}_q^{|A|}} \) defined in (42). This measurement has the same output statistics as the measurement given in STEP3 of Protocol 9.

Due to (40), the resultant state by the above unitary application on \( (\otimes_{y \in A} D_T) \otimes D_E \) is the same state as the final state of STEP 2 of Protocol 10. Since the final state of STEP 2 of Protocol 10 is invariant for \( \mathcal{W}_A(P_A G(1)y), \) the measurement in STEP 3 of Protocol 10 can be replaced by the POVM \( \{ \Pi_z \}_{x \in \mathbb{F}_q^{|A|}} \) defined in (41). The relation (42) guarantees that the POVM is the same as the POVM given in STEP 3 of Protocol 9. Therefore, the decoder of Protocol 9 has the same output statistics as the decoder of Protocol 10. That is, the correctness and the secrecy of Protocol 8 is equivalent to those of Protocol 9. Hence, we obtain the equivalence between (J1) and (J2).

Next, we proceed to the proof of Proposition 7. Any decoding measurement \( \{ \Pi_\omega \}_\omega \) in Protocol 9 is given as a POVM on the space \( D_D \otimes D_E[0, G(1)]. \) For a subset \( A \in \mathfrak{A}, \) we modify this decoding measurement as follows. First, the end-user randomly generates \( Y \in \mathbb{F}_q^y \) subject to the uniform distribution. The end-user applies the unitary \( \mathbf{W}_A(P_A H(1)y) \otimes \mathbf{W}(H(1)y) \) on \( (\otimes_{y \in A} D_T) \otimes D_E. \) Then, the end-user applies the measurement \( \{ \mathbf{W}_A(\bar{\rho}_A H(1)y) \Pi_\omega \mathbf{W}_A(P_A H(1)y) \}_{\omega} \) to \( D_D \otimes D_E[Y, G(1)]. \) This modified measurement has the same output statistics as the original measurement \( \{ \Pi_\omega \}_\omega \) in Protocol 9.

Also, we define the POVM \( \{ \Pi_\omega \}_\omega \) on \( D_D \otimes D_E := \otimes_{y \in \mathbb{F}_q} D_D \otimes D_E[y, G(1)] \) as \( \bar{\Pi}_\omega := \sum_{y \in \mathbb{F}_q} \omega \pi \mathbf{W}_n(Fm + G(2) U_{D, 2}) \rho \cdot \mathbf{W}_n(Fm + G(2) U_{D, 2}). \)
\(W_A(-P_A H(1)^{y}) \Pi_x W_A(P_A H(1)^{y}).\) Since the state on \(D_D \otimes D_E\) is the same as the state as the final state of STEP 2 of Protocol 10, which is the same as the final state of STEP 2 of Protocol 8. Due to Proposition 6, the output of this measurement can be simulated by the decoder given in STEP 3 of Protocol 8. The above proof of Theorem 6 guarantees that the decoder given in STEP 3 of Protocol 8 can be simulated by the decoder given in STEP 3 of Protocol 9. Hence, we obtain Proposition 7.

VII. PROOFS OF THEOREM 3 AND LEMMA 3 AND DECODER FOR LINEAR QSS PROTOCOL

This section presents the proofs for our results of QSS protocols stated in Section V by showing notable relations between dense coding and noiseless quantum state transmission.

A. Dense Coding and Noiseless Quantum State Transmission

For a preparation for the discussion on QSS protocols, we investigate the relation between dense coding and noiseless quantum state transmission. When noiseless transmission with \(d\)-dimensional quantum system is allowed, the noiseless classical message transmission with size \(d^2\) is possible with a shared entangled state. It is called dense coding. Here, we investigate its converse statement.

We choose \(H_A = H^{\otimes n}\). We prepare the system \(H_B\) as the same dimensional system as \(H_A\). Here, to clarify that the operator \(W_{A,[n]}(x)\) is applied on \(H_A\), we denote it by \(W_{A,[n]}(x)\). This usage of the subscript will be applied in the latter parts. For a given POVM \(\Pi = \{\Pi_x\}_{x} \in P^{2^n}\) on the joint system \(H_R \otimes H_B\), we define the TP-CP map \(\Gamma[\Pi]\) from the system \(H_B\) to the system \(H_A\) as follows. We prepare the maximally entangled state \(|\psi\rangle \langle \psi|^{\otimes n}\) on \(H_R \otimes H_B\). Then, \(\Gamma[\Pi]\) is defined as

\[
\Gamma[\Pi](\rho) := \sum_{x} W_{A,[n]}(x)^{\dagger} Tr_{B,R}(\rho \otimes |\psi\rangle \langle \psi|^{\otimes n} \Pi_x) W_{A,[n]}(x)
\]

(44)

for a density \(\rho\) on the system \(H_B\).

\textbf{Lemma 6:} Let \(H_A\) and \(H_B\) be the systems equivalent to \(H^{\otimes n}\) and \(H_B\) be an arbitrary quantum system. Let \(\Lambda\) be a TP-CP map from \(H_A\) to \(H_B\). Assume that a POVM \(\Pi = \{\Pi_x\}_{x} \in P^{2^n}\) on the joint system \(H_R \otimes H_B\) satisfies that

\[
Tr_{R,B} \Lambda(W_{A,[n]}(x) |\psi\rangle \langle \psi|^\otimes n W_{A,[n]}^{\dagger}(x)) = \delta_{x,x'}.
\]

(45)

Then, \(\Gamma[\Pi] \circ \Lambda\) is the identity channel.

\textit{Proof:} We define the adjoint map \(\Lambda^*\) from the Hermitian matrices on \(H_B\) to those on \(H_A\) as

\[
\text{Tr} \Lambda(X) Y = \text{Tr} X \Lambda^*(Y).
\]

(46)

Then, we have

\[
\Gamma[\Pi] \circ \Lambda(\rho) = \sum_{x} W_{A,[n]}^{\dagger}(x) Tr_{B,R}(\Lambda(\rho) \otimes |\psi\rangle \langle \psi|^\otimes n \Pi_x) W_{A,[n]}(x).
\]

(47)

Due to the condition (45), \(\{\Lambda^*(\Pi_x)\}_x\) equals the POVM \(\{W_{A,[n]}(x) |\psi\rangle \langle \psi|^\otimes n W_{A,[n]}^{\dagger}(x)\}_x\). Hence, the process in (47) can be considered as the process of quantum teleportation. Thus, \(\Gamma[\Pi] \circ \Lambda\) is the identity channel.

\textbf{Lemma 7:} Let \(H_A\) and \(H_B\) be the systems equivalent to \(H^{\otimes n}\) and \(H_B\) be an arbitrary quantum system. Let \(\Lambda\) be a TP-CP map from \(H_A\) to \(H_B\). We generate the random variable \(X \in \mathbb{F}_{2^n}\) subject to the uniform distribution. Using the variable \(X\), we generate the state \(\Lambda(W_{A,[n]}(x) |\psi\rangle \langle \psi|^\otimes n W_{A,[n]}^{\dagger}(x))\). We consider the mutual information between \(X\) and the joint system \(BR\). That is, we consider the state \(\rho_{BRX} := \sum_{x} \frac{1}{2^n} |x\rangle \langle x| \otimes \Lambda(W_{A,[n]}(x) |\psi\rangle \langle \psi|^\otimes n W_{A,[n]}^{\dagger}(x))\). Also, we consider another state \(\sigma_{BR} := \Lambda(|\psi\rangle \langle \psi|^\otimes n)\). Then, we have the following relation.

\[
I(\{X;BR\}|\rho_{BRX}) = I(\{R;B\}|\sigma_{RB}).
\]

(48)

Therefore, the joint system \(BR\) has no information for the random variable \(X\) in the dense coding scheme if and only if the output system \(B\) of the channel \(\Lambda\) has no information for the input state on \(H_A\).

\textit{Proof:} For \(x = (a,b)\), we define \(\bar{x} = (a,-b)\). Then, we have

\[
I(\{X;BR\}|\rho_{BRX}) = \sum_{x} \frac{1}{2^n} D(\Lambda \left( W_{A,[n]}(x) |\psi\rangle \langle \psi|^\otimes n W_{A,[n]}^{\dagger}(x) \right))
\]

\[
\left\| \Lambda \left( \sum_{x} \frac{1}{2^n} W_{A,[n]}(x') |\psi\rangle \langle \psi|^\otimes n W_{A,[n]}^{\dagger}(x') \right) \right\|
\]

\[
= \sum_{x} \frac{1}{2^n} D(\Lambda(\rho_{mix,A}) \otimes \rho_{mix,R})
\]

(49)

B. Proofs of Theorem 3 and Lemma 3 and Decoder for Linear QSS Protocol

Now, we show Theorem 3 and Lemma 3 by using the contents of Section VII-A. Considering linear EASS protocols, we restate Theorem 3 as follows.

\textbf{Theorem 8:} Given a \(2n \times (n-x)\) self-column-orthogonal matrix \(G^{(1)}\) and a \(2n \times y_2\) matrix \(G^{(2)}\), we choose a \(2n \times 2x\) matrix \(F\) column-orthogonal to \(G^{(1)}\). Then, the following conditions for \(G^{(1)}, G^{(2)}, F\) are equivalent.
(J1) The linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\) is \((\mathfrak{A}, \mathfrak{B})\)-secure. That is, there exists a suitable TP-CP map \(\bar{T}\) to recover the original state in STEP 2.

(J2) The linear CSS protocol with \(((G^{(1)}, G^{(2)}), F)\) is \((\mathfrak{A}, \mathfrak{B})\)-secure.

(J3) The matrix \(((G^{(1)}, G^{(2)}), F)\) is an \((\mathfrak{A}, \mathfrak{B})\)-MMSP.

(J4) The linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\) is \((\mathfrak{A}, \mathfrak{B})\)-secure.

In particular, when Condition (J4) holds, the decoder of the linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\) is given as \(\bar{T}[\Pi]\) defined in (44), where the POVM \(\Pi = \{\Pi_m\}_{m\in\mathbb{F}_2^n}\) is the decoder of the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\).

In the following proof, we give a construction of the decoder for Condition (J1).

**Proof:** Since Theorem 6 guarantees the equivalence among the conditions (J2), (J3), and (J4), we show only the equivalence between the conditions (J1) and (J4).

First, we show the direction (J1)⇒(J4). We assume Condition (J1). We combine the linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\) and dense coding [79]. Then, the obtained protocol is the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\). The correctness and secrecy of the linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\) for \((\mathfrak{A}, \mathfrak{B})\) imply those of the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\) for \((\mathfrak{A}, \mathfrak{B})\). Hence, Condition (J4) holds.

Next, we show the direction (J4)⇒(J1). We assume Condition (J4). Hence, the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\) satisfies the correctness with respect to \(A \in \mathfrak{A}\). We choose \(H_A = D_D[0, G^{(1)}]\) and \(H_B\) as \(\otimes_{i\in A} D_{D_i}\). Hence, we choose \(n'\) to be \(n\). Since \(F\) is column orthogonal to \(G^{(1)}\), the action of the unitaries \((W_n(F_m))_{m\in\mathbb{F}_2^n}\) preserves the subspace \(D_D[0, G^{(1)}]\). We choose \(\Lambda\) as

\[
\Lambda(\rho) := \text{Tr}_{A^c} \sum_{u_D, z \in \mathbb{F}_2^n} \frac{1}{q^{k^2}} W_n[(G^{(2)}u_D, 2)\rho W_n]G^{(2)}u_D, 2).
\]

Due to the correctness of the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\) for \(A \in \mathfrak{A}\), there is a POVM \(\Pi = \{\Pi_m\}_{m\in\mathbb{F}_2^n}\) on the joint system \(H_B \otimes H_B\) such that

\[
\text{Tr}_{\Pi_m}(\Lambda(W_n(F_m)|\phi)\langle\phi|\otimes W_n^\dagger(F_m)) = \delta_{m, m'}.
\]

We choose \(\bar{T}[\Pi]\) defined in (44). Then, Lemma 6 guarantees that \(\bar{T}[\Pi] \circ \Lambda\) is the identity channel. Hence, we obtain the correctness of the linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\) with respect to \(A \in \mathfrak{A}\) when \(\bar{T}[\Pi]\) is chosen as the decoder.

In addition, the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\) satisfies the secrecy with respect to \(B \in \mathfrak{B}\). We choose \(H_A = D_D[0, G^{(1)}]\) and \(H_B\) as \(\otimes_{i\in E} D_{D_i}\). We apply Lemma 7 in the same way as the above. In this application, \(I(R; B)|\sigma_{RB}\) expresses the information obtained by the players in \(B\) under the above linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\), and \(I(X; B)|\sigma_{RBX}\) expresses the information obtained by the players in \(B\) under the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\). Hence, the linear EASS protocol with \((G^{(1)}, G^{(2)}, F)\) with respect to \(B \in \mathfrak{B}\) implies the secrecy of the linear QQSS protocol with \((G^{(1)}, G^{(2)}, F)\) with respect to \(B \in \mathfrak{B}\). Hence, Condition (J1) holds.

Combining Lemma 5 and the same idea as Theorem 8, we obtain the following corollary. This corollary is a recasted statement of Lemma 3 with adding the new condition (F3).

**Corollary 6:** Given a \(2n \times 2(2r - n)\) self-column-orthogonal matrix \(G^{(1)}\) and \(2n 	imes 2[n - 2r + n]_{\text{column-orthogonal}}\) to \(G^{(1)}\), the following conditions are equivalent.

(F1) The randomless linear QQSS protocol with \((G^{(1)}, F)\) is an \((n, 2)^{-}\)-QMDS code.

(F2) The matrix \((G^{(1)}, F)\) accepts \(\mathfrak{A}\) with \(\mathfrak{A} = \{A \subset [n] \mid |A| \geq r\}\).

(F3) The randomless linear EASS protocol with \((G^{(1)}, F)\) is an \((n, 2)^{-}\)-EAMDS code.

**Proof:** The equivalence between (F2) and (F3) follows from Lemma 5. The equivalence between (F1) and (F3) follows from the discussion only for the correctness in the proof of Theorem 8.

**VIII. QUANTUM SPIR PROTOCOLS WITH PRESHARED ENTANGLEMENT WITH USER**

This section introduces EASPIR protocols and presents our results for EASPIR protocols, which implies our results for CQSPIR protocols.

**A. Formulation**

Modifying the CQSPIR setting by allowing prior entanglement between the user and the servers, we introduce a quantum SPIR protocol with preshared entanglement with user. Since this problem setting employs entanglement assistance, this protocol is called an entanglement-assisted SPIR (EASPIR) protocol. As illustrated in Fig. 2 (b), an EASPIR protocol is defined as Protocol 11.

**Protocol 11 EASPIR protocol**

**STEP 1: Preparation:** The user has a quantum system \(D_U\) before the protocol and the state of the quantum system \(D'_U \otimes \cdots \otimes D'_n \otimes D_U\) is initialized as the initial state \(\rho_{\text{pre}}\). The random seed \(\text{Enc}_{SR}(U_S) = R = (R_1, \ldots, R_n)\) is defined as the same way as Protocol 3.

**STEP 2: User’s encoding:** This step is done in the same way as Protocol 3.

**STEP 3: Servers’ encoding:** This step is done in the same way as Protocol 3.

**STEP 4: Decoding:** For a subset \(A \in \mathfrak{A}\), the user decodes the message from the received state from servers \(A\) by a decoder, which is defined as a POVM \(\text{Dec}(K, Q^{(K)}, A) := \{Y_{k, Q^{(K)}, A} \mid w \in [m]\} \subset D[A] \otimes D_U\) depending on the variables \(K\) and \(Q^{(K)}\). The user outputs the measurement outcome \(W\) as the retrieval result.

The \((\mathfrak{A}, \mathfrak{B})\)-security for an EASPIR protocol is defined in the same way as Definition 3 as follows.

**Definition 16:** For an access structure \((\mathfrak{A}, \mathfrak{B})\) on \([n]\), an EASPIR protocol defined as Protocol 11 is called \((\mathfrak{A}, \mathfrak{B})\)-secure if the following conditions are satisfied.

- **Correctness:** For any \(A \in \mathfrak{A}\), \(k \in [f]\), and \(m = (m_1, \ldots, m_f)^\dagger \in \mathbb{F}_q^f\), the relation
  \[
  \text{Tr}(\rho(m, q, k)y_{k, q, A}(m_k) \otimes I_{A^c}) = 1
  \]
Fig. 3. Entanglement-assisted (EA) SPIR protocols where Server 1 and Server 2 collude and Server 2 and Server 3 respond to the user.

TABLE VI
SYMBOLS FOR FEASPIR AND EASPIR PROTOCOLS

| symbol         | meaning            | definition |
|----------------|--------------------|------------|
| $D_{U,j}$      | User’s $j$-th system | $H_j$      |
| $D_U$          | User’s whole system | $\Phi_0, D_{U,j} = H^{\otimes n}$ |
| $D_{U}[A]$     | User’s system with subset $A$ | $\Phi_{IA, D_{U,j}}$ |

holds when $q$ is any possible query $Q^{(K)}$.

- **User Secrecy**: The distribution of $(Q^{(j)})_{j \in B}$ does not depend on $j \in [f]$ for any $B \subseteq \mathbb{B}$.

- **Server Secrecy**: We fix $K = k$, $M_k = m_k$, and $Q^{(K)} = q$. Then, the state $\rho(m_1, \ldots, m_f, q, k)$ does not depend on $(m_j)_{j \in k} \subset M^{f-1}$.

In particular, when the system $D'_1 \otimes \cdots \otimes D'_n$ has the same dimension as $D_U$ and the encoded states are maximally entangled states on $D'_1 \otimes \cdots \otimes D'_n$ and $D_U$, the EASPIR protocol is called fully EASPIR (FEASPIR) protocol. Indeed, it is difficult to consider quantum-quantum SPIR (QQSPIR) in a similar way as QQSS. Remark 5 in Section V-B explains its reason.

### B. Linear Protocols With Preshared Entanglement With User

Given a $2n \times n$ matrix $G$ and a $2n \times f$ matrix $Q^{(K)}$ with index $K$, we define an FEASPIR protocol as follows. The set $M$ is given as $\mathbb{F}_{q}^n$. We set $D_j$, $D'_j$ and $D_{U,j}$ as $H$ for $j = 1, \ldots, n$, and define $D[A], D'_j$, and $D_{U}[A]$ as $\otimes_{j \in A} D_j$, $\otimes_{j \in A} D'_j$, and $\otimes_{j \in A} D_{U,j}$, respectively, for any subset $A \subset [n]$. Hence, $D_U$ is $H^{\otimes n}$.

Then, we define the linear FEASPIR protocol with $G, Q^{(K)}$ as Protocol 12.

**Lemma 8**: The following conditions for the matrix $G$ and the query $Q^{(K)}$ are equivalent.

**(K1)** The linear FEASPIR protocol with $G, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

**(K2)** The linear CSPIR protocol with $G, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

**Proof**: Given a subset $A \subset [n]$ and $x \in \mathbb{F}_{q}^n$, we have

$$
\text{Tr}_{(A,U)} \left[ W_{[n]}(x) |\Phi\rangle \langle \Phi| W_{[n]}^\dagger(x) \right] = W_{\mathcal{A}}(P_{\mathcal{A}}x) \otimes \rho_{\text{mix}}^{(\otimes |A|)}.
$$

Hence, the above state can be identified with the classical information $P_{\mathcal{A}}x$. That is, the analysis on the correctness and the secrecy of the linear FEASPIR protocol with $G, Q^{(K)}$ follows from those of the linear CSPIR protocol with $G, Q^{(K)}$.

Next, we assume that the $2n \times y_1$ matrix $G$ is written as $(G^{(1)}, G^{(2)})$ with a $2n \times y_1$ self-column-orthogonal matrix $G^{(1)}$ and a $2n \times y_2$ matrix $G^{(2)}$. Then, to discuss the relation with CSQSPIR protocols, we modify Protocol 12 as follows. The initial state $|\Phi\rangle$ is replaced by $|\Phi[0, G^{(1)}]\rangle$. The random seed $U_S$ is written as $(U_{S,1}, U_{S,2})$ with $U_{S,1} \in \mathbb{F}_{q}^{y_1}$ and $U_{S,2} \in \mathbb{F}_{q}^{y_2}$ so that $GU_S = G^{(1)}U_{S,1} + G^{(2)}U_{S,2}$. The applied unitary $W(G^{(K)}_{j}, m) + G_j U_S, Q^{(K)}_{j+n} + G_{n+j} U_C)$ on $D_j$. In this protocol, the end-user’s space $D_E$ is given as $D_E[0, G^{(1)}]$. This protocol is formally written as Protocol 13, and is called the linear EASPIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$. When $y_2$ is zero, i.e., $G^{(2)}$ is not given, the linear EASPIR protocol with $G^{(1)}, Q^{(K)}$ does not require shared randomness among servers, and is called the random linear EASPIR protocol with $G^{(1)}, Q^{(K)}$.

**Theorem 9**: Given a $2n \times y_1$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times y_2$ matrix $G^{(2)}$, and query $Q^{(K)}$, the following conditions are equivalent.

**(L1)** The linear EASPIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

**(L2)** The linear EASPIR protocol with $(G^{(1)}, G^{(2)}), Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

**(L3)** The linear CSPIR protocol with $(G^{(1)}, G^{(2)}), Q^{(K)}$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

Theorem 9 can be shown in the same way as Theorem 6. That is, the equivalence between (L2) and (L3) follows from Lemma 8, and the equivalence between (L1) and (L2) can be shown in the same way as Theorem 6.
**Protocol 13** Linear EASPIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$

**STEP 1: Preparation:** We set $D_{UV}$ to be $\mathcal{H}^{\otimes n}$. We set the initial state $\rho_{DV}$ on $D_1 \otimes \cdots \otimes D_n \otimes D_U$ to be $\ket{\Phi[0, G^{(1)}]}$. Let $U_{S,2}$ be a random variable subject to the uniform distribution on $\mathbb{F}_q^T$. The shared randomness $R = (R_1, \ldots, R_n)^T$ is generated as $R_j := G_j^{(2)} U_{S,2}$ for $j = 1, \ldots, 2n$. The randomness $R$ is distributed so that the $j$-th server contains $R_j$ and $R_{n+j}$ for $j = 1, \ldots, n$.

**STEP 2: User’s encoding:** The user randomly encodes the index $K$ to classical queries $Q^{(K)} := (Q^{(K)}_1, \ldots, Q^{(K)}_{2n})^T$, which is an $n \times f$ random matrix for $k = 1, \ldots, f$. The user sends $Q^{(K)}_j, Q^{(K)}_{n+j}$ to the $j$-th server $s_j$.

**STEP 3: Servers’ encoding:** The $j$-th server $s_j$ applies unitary $W(Q^{(K)}_j \vec{m} + R_j, Q^{(K)}_{n+j} \vec{m} + R_{n+j})$ on $D_j$.

**STEP 4: Decoding:** For a subset $A \subseteq \mathfrak{A}$, the user takes partial trace on $D_U[A]$, and makes the measurement given by the POVM $\{\Pi_U[A] \}_y \in \mathbb{F}_q^{|B|}$, where $\Pi_U[A]_y$ is defined as $W_{A}(y) \langle \Theta_{D_U[A], D_U[A]} | \Phi[0, G^{(1)}] \langle \Phi[0, G^{(1)}] \rangle | W_A^\dagger(y)$. Based on the obtained outcome, the user outputs the measurement outcome $m$ as the retrieval result.

**Example 11:** In this example, we give an example of MMSP which can be converted to a randomness standard linear EASPIR protocol that overperforms linear CQSPIR protocol.

Let $p$ be a prime. For $n = p$, we define the $2p \times 2$ matrix $G^{**} = (g_{y,k})$ and the $2p \times 2$ matrix $F^{**} = (f_{j,k})$ over $\mathbb{F}_p$ in the same way as Example 10. When $p > 2$, $(G^{**}, F^{**})$ cannot be used for a randomness standard linear CQSPIR protocol. But, the randomness standard linear EASPIR protocol with $(G^{**}, F^{**})$ can be constructed according to Protocols 13.

We choose $\mathfrak{A}^{**} = \{A \subset [p] | |A| \geq 2\}$ and $\mathfrak{B}^{**} = \{B \subset [p] | |B| \leq 1\}$ similar to Example 10. Since Example 10 shows that the MMSP $(G^{**}, F^{**})$ is an $(\mathfrak{A}^{**}, \mathfrak{B}^{**})$-MMSP, the randomness standard linear EASPIR protocol with $(G^{**}, F^{**})$ is $(\mathfrak{A}^{**}, \mathfrak{B}^{**})$-secure due to Theorem 9. The randomness standard linear EASPIR protocol with $(G^{**}, F^{**})$ has the rate $2/p$.

In the same way as Proposition 7, we have the following proposition.

**Proposition 8:** In Protocol 13, even when STEP 4 is replaced by another decoder, the decoder can be simulated by the decoder given in STEP 3. That is, once steps 1, 2, and 3 are given in Protocol 6, without loss of generality, we can assume that our decoder is given as STEP 4.

In addition, the linear FEASPIR protocol with $G, Q^{(K)}$ is called the standard linear FEASPIR protocol with $(G, F)$ when the query $Q^{(K)}$ is given as $Q$ by using $F$. Under the same condition, the linear EASPIR protocol with $G^{(1)}, G^{(2)}, Q^{(K)}$ is called the standard linear EASPIR protocol with $(G^{(1)}, G^{(2)}, F)$. In particular, when $\gamma_2 = 0$, the protocol does not have the matrix $G^{(2)}$, i.e., the protocol does not have the random variable $U_{S,2}$. Such a protocol is called the randomness standard linear EASPIR protocol with $(G^{(1)}, F)$.

Therefore, we obtain the following corollary by combining Theorem 9 and Proposition 3.

**Corollary 7:** Given a $2n \times \gamma_1$ self-column-orthogonal matrix $G^{(1)}$, a $2n \times \gamma_2$ matrix $G^{(2)}$, and a $2n \times \gamma_1$ matrix $F$, the following conditions are equivalent.

(M1) The standard linear EASPIR protocol with $(G^{(1)}, G^{(2)}, F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

(M2) The standard linear FEASPIR protocol with $((G^{(1)}, G^{(2)}), F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

(M3) The standard linear CQSPIR protocol with $((G^{(1)}, G^{(2)}), F)$ is $(\mathfrak{A}, \mathfrak{B})$-secure.

(M4) The matrix $((G^{(1)}, G^{(2)}), F)$ is an $(\mathfrak{A}, \mathfrak{B})$-MMSP.

When $\gamma_1 = n/2$, as discussed in Section VI-C, $D_\epsilon[0, G^{(1)}]$ is a one-dimensional system. Hence, the state $\ket{\Phi[0, G^{(1)}]}$ is a product state. Therefore, Protocol 13 essentially coincides with the linear CQSPIR protocol with $(G^{(1)}, G^{(2)}, Q^{(K)})$. Since a (standard) linear CQSPIR protocol with $((G^{(1)}, G^{(2)}, Q^{(K)}))$ is a special case of a (standard) linear EASPIR protocol with $((G^{(1)}, G^{(2)}, F))$, the relations among Conditions (L1), (L3), (M1), (M3), and (M4) yields Theorem 5. In the same way, Proposition 8 implies Proposition 5.

Combining Corollary 7 and Theorem 7, we obtain the following corollary as a generalization of Corollary 4.

**Corollary 8:** When $n \leq t > 0$, there exists an $(r, t, n)$-secure EASPIR protocol with rate $2(r-t)/n$.

Remember that the rate of CQSPIR cannot exceed 1 due to the condition $t \geq n/2$. This constraint always holds beyond the condition in Corollary 8 because CQSPIR does not have shared entanglement. Since EASPIR has shared entanglement, the rate of CQSPIR exceeds 1 by removing the condition $t \geq n/2$, which can be considered as an advantage of EASPIR over CQSPIR. Further, we have the following lemma, which implies Lemma 10.

**Lemma 9:** When we apply the conversion given in Theorem 10 to the standard linear FEASPIR protocol with $(G, F)$, the resultant EASS protocol is the linear FEASS protocol with $(G, F)$.

**Proof:** First, we calculate the share of the resultant EASS protocol. Combining Protocol 14 and Protocol 13, we find that it is calculated as

$$\begin{align*}
\otimes_{j=1}^n W(Q_j^{(1)} \vec{m} + G_j U_{S}, Q_{n+j}^{(1)} \vec{m} + G_{n+j} U_{S})|\Phi\rangle \\
= \otimes_{j=1}^n W(F_j E_1 \vec{m} + G_j U_{S}, F_{n+j} E_1 \vec{m} + G_{n+j} U_{S})|\Phi\rangle \\
= \otimes_{j=1}^n W(F_j m_1 + G_j U_{S}, F_{n+j} m_1 + G_{n+j} U_{S})|\Phi\rangle \\
= W_P(F_1 m_1 + G_1 U_{S})|\Phi\rangle,
\end{align*}$$

where $(a)$ follows from (21). The RHS of (53) is the same as the share of the linear FEASS protocol with $(G, F)$.

The decoding of the resultant EASS protocol is the standard linear EASPIR protocol with $(G, F)$, which is given as follows. For a subset $A \subseteq \mathfrak{A}$, the user makes the measurement on the basis $\{ W_{A}(y) | \phi[0, A] \}_y \in \mathbb{F}_q^{|B|}$. Based on the obtained outcome, the user outputs the measurement outcome $m$ as the retrieval result. It is the same as the decoder of the linear FEASS protocol with $(G, F)$ presented as Protocol 8.

In fact, the same property holds for the standard linear EASPIR protocol with $((G^{(1)}, G^{(2)}), F)$, which includes a standard linear CQSPIR protocol as a special case.
IX. CONVERSION FROM EASPIR PROTOCOL TO EASS PROTOCOL

A. Conversion From General EASPIR Protocol

As stated in [10], a CSPIR protocol can be converted to a CSS protocol. In this subsection, we present how an EASPIR protocol is converted to an EASS protocol. Protocol 14 shows the converted protocol from an EASPIR protocol. Protocol 14 contains the conversion from a CSPIR protocol to a CQSS protocol as the special case when $\mathcal{D}_E = \mathcal{D}_U$ is one-dimensional.

Protocol 14 EASS protocol converted from EASPIR protocol

STEP 1: Preparation: The dealer chooses the quantum systems $\mathcal{D}_D$ to be $\mathcal{D}'_D \otimes \cdots \otimes \mathcal{D}'_n$, and the end-user chooses the quantum system $\mathcal{D}_E$ to be $\mathcal{D}'_n$, respectively. They share the state $\rho_{\text{prev}}$ as the state $\rho_{\text{DE}}$ on the joint quantum system $\mathcal{D}_D \otimes \mathcal{D}_E$ before the protocol.

STEP 2: Share generation: The dealer prepares a uniform random variable $U_{D,2} \in \mathbb{F}_q^2$. For $m \in \mathcal{M}$, the dealer applies $\mathcal{W}_{[n]}(Q_j^{(1)}(m,0,\ldots,0) + G_j^{(2)}U_{D,2})$ to $\mathcal{D}_j$. That is, the encoding operation $\Gamma[m]$ on $\mathcal{D}_D$ is defined as

$$\Gamma[m](\rho) := \sum_{u_{D,2} \in \mathbb{F}_q^2} \frac{1}{q^2} \mathcal{W}_{[n]}(Q_j^{(1)}(m,0,\ldots,0) + G_j^{(2)}U_{D,2})\rho \cdot \mathcal{W}_{[n]}(Q_j^{(1)}(m,0,\ldots,0) + G_j^{(2)}U_{D,2}).$$

(55)

The shares are given as parts of the state $\Gamma[m](\Phi[0, G_j^{(1)}](\Phi[0, G_j^{(1)}]))$.

STEP 3: Decoding: For a subset $A \in \mathcal{A}$, the end-user takes partial trace on $\mathcal{D}_E[A^c]$, and makes the measurement given by the POVM $\{\Pi_E[A]_z\}_{z \in \mathbb{F}_q^2 : A}$, where $\Pi_E[A]_z$ is defined in (37). Based on the obtained outcome, the end-user recovers $m$.

Next, we consider the case when the query $Q^K$ has the standard form (21). In this case, the uniform random number $U_q$ in (21) is rewritten as $(U_{Q,1}^1, U_{Q,2}^1)$ by using the uniform random numbers $U_{Q,1}$ and $U_{Q,2}$ on $\mathbb{F}_q^3$ and $\mathbb{F}_q^2$. Hence, $Q_j^{(1)}(m,0,\ldots,0) + G_j^{(2)}U_{D,2}$ is rewritten as

$$Q_j^{(1)}(m,0,\ldots,0) + G_j^{(2)}U_{D,2} = Fm + (G_j^{(1)}, G_j^{(2)})U + G_j^{(2)}U_{D,2} = Fm + G_j^{(1)}U_{Q,1} + G_j^{(2)}U_{Q,2} + U_{D,2}.$$  (56)

Since $\mathcal{W}_{[n]}(G_j^{(1)}U_{Q,1})$ does not change the state $\Phi[0, G_j^{(1)}]$, the application of (56) is equivalent to the application of $Fm + G_j^{(2)}(U_{Q,2} + U_{D,2})$, which is Step 2 of Protocol 9. Therefore, we find that the standard linear EASPIR protocol with $(G_j^{(1)}, G_j^{(2)}, F)$ is converted to the linear EASS protocol with $(G_j^{(1)}, G_j^{(2)}, F)$ via the conversion protocol, Protocol 14. That is, the standard linear EASPIR protocols with $(G_j^{(1)}, G_j^{(2)}, F)$ have a one-to-one correspondence with linear EASS protocols.

When we restrict our protocols to standard linear CQSPIR protocols, we have the following lemma.

Lemma 10: When we apply the conversion given in Theorem 10 to the standard linear CQSPIR protocol with $(G_j^{(1)}, G_j^{(2)}, F)$, the resultant CQSS protocol is the linear CQSS protocol with $(G_j^{(1)}, G_j^{(2)}, F)$.

When the CQSPIR protocol is a standard linear CQSPIR protocol, the converted CQSS protocol is characterized by the same matrices. That is, the reverse conversion is possible in this case. This fact shows the one-to-one correspondence between a linear CQSS protocol and a standard linear CQSPIR protocol.

X. CONCLUSION

We have characterized CQSS and QQSS protocols and CQSPIR protocols under general access structure by using MMSS with symplectic structure. These characterizations...
TABLE VII
Characterizations for Matrices Used for respective Protocols

|                              | $G^{(1)}$                          | $G^{(2)}$                          | $F$                        |
|------------------------------|------------------------------------|------------------------------------|-----------------------------|
| linear standard FEASPIR     | one $2n \times y$ matrix           | $2n \times y$                      | $2n \times x$              |
| linear FEASS (general form)  |                                    |                                    |                             |
| linear standard EASS        | $2n \times y_1$ self-column-orthogonal | $2n \times y_2$ self-column-orthogonal | $2n \times (2t - y)$        |
| linear EASPIR (general form) |                                    |                                    |                             |
| (r, t, n)-secure linear standard EASPIR | $2n \times y_1$ self-column-orthogonal | $2n \times y_2$ self-column-orthogonal | $2n \times (2t - 2t)$      |
| (r, t, n)-secure linear EASS |                                    |                                    |                             |
| linear CQSS                 | $2n \times n$ self-column-orthogonal | $2n \times y_2$ self-column-orthogonal | $2n \times x$              |
| linear CQSPIR (general form) |                                    |                                    |                             |
| (r, t, n)-secure linear CQSPIR | $2n \times n$ self-column-orthogonal | $2n \times (2t - n)$ self-column-orthogonal | $2n \times (2t - 2t)$      |
| (r, t, n)-secure linear CQSS |                                    |                                    |                             |
| linear QQSS (general form)   | $2n \times (n - x)$ self-column-orthogonal | $2n \times y_2$ self-column-orthogonal | $2n \times 2x$ column-orthogonal to $G^{(1)}$ |
| (r, t, n)-secure linear QQSS |                                    |                                    |                             |

Fig. 4. One-to-one relations among various linear protocols. In this figure, the word “linear” is omitted. Arrows of each color show a one-to-one relation among several protocols. ① shows the restriction that $G = (G^{(1)}, G^{(2)})$ and $G^{(1)}$ is self-column-orthogonal, ② shows the restriction that $G^{(2)} = \emptyset$ and $F$ is column-orthogonal to $G^{(1)}$.

Linear protocols presented in this paper

yield ramp type of CQSS and QQSS protocols and CQSPIR protocols with a general qualified set, which were not studied sufficiently until this paper. Also, these characterizations yield interesting constructions QMDS codes. However, the derivation of these characterizations cannot be derived from a simple application of similar relations in the classical case. To overcome this problem, we have introduced EASS and EASPIR protocols. Since these two types of protocols can be converted to classical protocols, we have easily derived their relation with general access structure and MMSP while these analyses require column-orthogonality for MMSP. Fortunately, CQSS and QQSS protocols and CQSPIR protocols can be considered as special cases of EASS and EASPIR protocols, respectively. That is, the relation among these settings is summarized as Fig. 4, and matrices used for respective protocols are summarized as Table VII. In addition, we have shown the existence of desired types of MMSP in Appendix, which implies the existence of CQSS, QQSS, and CQSPIR protocols parameterized by two threshold parameters $t$ and $r$.

For this discussion, as subclasses of EASS and EASPIR protocols, we have newly introduced linear EASS and linear EASPIR protocols and the symplectification for an access structure. In particular, we have focused on linear FEASS and FEASPIR protocols because they are directly linked to linear classical protocols as Lemmas 4 and 8 thanks to the orthogonality of generalized Bell basis. Such a simple structure has never appeared in CQSS and QQSS protocols and CQSPIR protocols. Under the self-column-orthogonality for the matrix $G^{(1)}$, linear FEASS and FEASPIR protocols are converted to linear EASS and EASPIR protocols as Theorems 6 and 9. Since the classical linear protocols are linked to MMSP as Proposition 1 and Lemma 3, linear EASS and EASPIR protocols are linked to MMSP via the above relations. Since CQSS and CQSPIR protocols are special classes of EASS and EASPIR protocols, CQSS and CQSPIR protocols are characterized by using MMSP in this way.

However, the relation with QQSS is more complicated. To establish the relation between QQSS and EASS protocols, we have introduced new relation between dense coding and quantum state transmission. It was known that noiseless quantum state transmission implies dense coding with zero error. However, no existing study clarified whether dense coding protocol with zero error yields noiseless quantum state transmission. In this paper, we have constructed a concrete protocol for noiseless quantum state transmission from dense coding protocol with zero error. That is, we constructed a decoder for quantum state transmission with zero error from a decoder for dense coding protocol with zero error as Lemma 6. Also, we have derived the equivalence relation between the mutual information between dense coding and quantum state transmission as Lemma 7. Using these relations, we have made the conversion between QQSS and EASS protocols as Theorem 8. Also, we have pointed out that a special class of QQSS protocols yields QMDS codes, which are often called quantum MDS codes. In addition, as Remark 4, we have shown that any stabilizer code can be characterized as the performance of QQSS protocols in our method. Overall, our main contribution can be summarized as revealing the relation between EASS and EASPIR protocols and the symplectification for an access structure, which is a hidden simple structure behind CQSS, QQSS, and CQSPIR protocols.

Although we have constructed various types of MMSP with column-orthogonality, these constructions are based on
algebraic extension similar to [40] and [80]. In contrast, existing studies [74] discussed how a small size of field can realize QMDS codes under a certain condition. Therefore, it is an interesting future study to find efficient constructions of various types of MMSP with column-orthogonality depending on two threshold parameters \( t \) and \( r \). This is because these constructions are essential for constructing our linear protocols. In addition, the existing study [81, Section IV-B] discussed SPIR with a quantum noisy multiple access channel. Since a noisy setting is realistic, it is another interesting study to extend our results to the setting with quantum noisy channels.

**APPENDIX A**

**PREPARATION FOR PROOFS OF THEOREMS 7 AND 4**

This appendix prepares several lemmas to be used in our proofs of Theorems 2, 7, and 4. For this, we prepare the following lemma.

**Lemma 11:** We consider a \((d+1) \times (d+1)\) matrix \( A = (a_{i,j})_{1 \leq i \leq d+1, 1 \leq j \leq d+1} \) over a finite field \( \mathbb{F}_q \) to satisfy the following conditions. (i) The \( d \times d \) matrix \((a_{i,j})_{1 \leq i \leq d, 1 \leq j \leq d}\) is an invertible matrix. (ii) The components \( a_{i,j} \) except for \( a_{d+1, d+1} \) belong to \( \mathbb{F}_q \). Then, the \((d+1) \times (d+1)\) matrix \( A \) is invertible.

**Proof:** We show the desired statement by contradiction. We assume that \( A \) is not an invertible matrix. We denote the \( d+1 \) column vectors of \( A \) by \( a^1, \ldots, a^{d+1} \). Since the \( d \) column vectors of \( a^1, \ldots, a^d \) are linearly independent, there exist \( d \) elements \( \beta_1, \ldots, \beta_d \) of \( \mathbb{F}_q \) such that

\[
\sum_{j=1}^{d} \beta_j a_{i,j} = a_{i,d+1}
\]

for \( i = 1, \ldots, d+1 \). The finite field \( \mathbb{F}_q \) is a vector space over the finite field \( \mathbb{F}_q \) generated by \( a^0 = 1, a^1, \ldots, a^n \) with a certain positive integer \( n \geq 1 \), where \( a := a_{d+1, d+1} \).

We choose elements \( \beta_{i,j} \in \mathbb{F}_q \) such that \( \beta_{j} = \sum_{i=0}^{n} \beta_{j,i} a^i \). Then, (57) with \( i = d+1 \) is rewritten as

\[
\sum_{i=0}^{n} \sum_{j=1}^{d} \beta_{i,j} a_{d+1,j} a^i = \sum_{j=1}^{d} \sum_{i=0}^{n} \beta_{j,i} a^i a_{d+1,j} = a_{d+1,d+1} = 1.
\]

Considering the case with \( i = 1 \), we have

\[
\sum_{j=1}^{d} \beta_{j,1} a_{d+1,j} = 1,
\]

which implies that the vector \( (\beta_{j,1})_{j=1}^{d} \) is a non-zero vector. We denote the \( d+1 \) column vectors of \( A \) only with the initial \( d \) components by \( b^1, \ldots, b^{d+1} \) in \( \mathbb{F}_q^d \). Since \( b^1, \ldots, b^d \) are linearly independent, the vector \( \sum_{j=1}^{d} \beta_{j,1} b^j \) is a non-zero vector.

Next, we rewrite (57) with \( i = 1, \ldots, d \) as

\[
\sum_{i=0}^{n} \sum_{j=1}^{d} \beta_{i,j} b^j a^i = \sum_{j=1}^{d} \beta_{j,1} b^j a^i = \sum_{j=1}^{d} \beta_{j,1} b^j a^i = b^{d+1}.
\]

We focus on the case with \( i = 1 \), which implies

\[
\sum_{j=1}^{d} \beta_{j,1} b^j = 0.
\]

However, the LHS is a non-zero vector, we obtain a contradiction. Hence, we obtain the desired statement.

**Lemma 12:** Assume that a \((d+f) \times d\) matrix \( D \) over a finite field \( \mathbb{F}_q \) is a \((d+f, d)\)-MDS code. We consider a \((d+f) \times g \) matrix \( F = (f_{i,j})_{1 \leq i \leq d+f, 1 \leq j \leq g} \) over the finite field \( \mathbb{F}_q \). We assume the following conditions. (i) \( f \geq g \). (ii) The component \( f_{i,j} \) \( \beta_{i,j} \in \mathbb{F}_q \) when \( i + j \leq d + g \). (iii) The component \( f_{i,j} \in \mathbb{F}_q \) when \( i + j > d + g \). Then, the \((d+f) \times (d+g)\) matrix \( G := (D, F) \) is a \((d+f, g+d)\)-MDS code.

**Proof:** We denote the matrix \( G \) as \((g_{i,j})_{1 \leq i \leq d+f, 1 \leq j \leq g+d} \). We choose a strictly increasing function \( \pi \) from \( [d+g] \) to \([d+f] \). We define the subset \( A_{\pi} \) as \( \{ \pi(1), \ldots, \pi(d+g) \} \). Hence, it is sufficient to show that the \((d+g) \times (d+g)\) matrix \( P_{A_{\pi}}(D, F) \) is invertible for any map \( \pi \). To show this statement, we show that the matrix \( G_{k} := (g_{i,j})_{1 \leq i \leq d+k, 1 \leq j \leq d+k} \) is invertible for \( k = 0, 1, \ldots, g \) by the induction for \( k \). The case with \( k = 0 \) holds because \( D \) is a \((d+f, d)\)-MDS code.

Now, we assume that \( G_{k} \) is invertible for \( k = t - 1 \). The component \( g_{\pi(t),t} \) \( \beta_{\pi(t),t} \in \mathbb{F}_q \) for \( 1 \leq t \leq g \). Also, other components of \( G_{t} \) belong to \( \mathbb{F}_q \). Hence, Lemma 11 guarantees that \( G_{t} \) is invertible.

Now, we recall Proposition 4 of [40, Appendix D], which is a generalization of Appendix of [80].

**Proposition 9 (Appendix D):** Given positive integers \( l < r \) and a prime \( p \), we choose \( q \) such that \( \mathbb{F}_q \) is an algebraic extension \( \mathbb{F}_p \). We choose \( \alpha_{i,j} \) as an element of \( \mathbb{F}_p \). We define \( l \) vectors \( v^1, \ldots, v^n \in \mathbb{F}_p^r \) as

\[
v^i := \begin{cases} 
\delta_{i,j} & \text{when } i \leq l \\text{ and } j \leq 1, \\
\alpha_{i-1,j} & \text{when } i > l \text{ and } j \leq 1.
\end{cases}
\]

In addition, we assume that \( \alpha_{1,1} = 1 \). Then, the matrix \( (v^1, \ldots, v^n) \) is an \((r, l)\)-MDS code.

**Lemma 13:** Given positive integers \( l < k \) and a prime \( p \), we choose \( q \) such that \( \mathbb{F}_q \) is an algebraic extension \( \mathbb{F}_p \). We choose \( \alpha_{i,j} \) as an element of \( \mathbb{F}_p \). We define \( k \) vectors \( v^1, \ldots, v^k \in \mathbb{F}_p^r \) as

\[
v^i := \begin{cases} 
\delta_{i,j} & \text{when } i \leq l \\text{ and } j \leq 1, \\
\alpha_{i-1,j} & \text{when } i > l \text{ and } j \leq 1.
\end{cases}
\]

In addition, we assume that \( \alpha_{1,1} = 1 \). Then, the matrix \( (v^1, \ldots, v^k) \) is an \((r, k)\)-MDS code.

**Proof:** We apply Lemma 12 to the case when \( D = (v^1, \ldots, v^n), F = (v^{n+1}, \ldots, v^k), d = l, f = r - l, g = k - l, \) and \( \mathbb{F}_q \) is \( \mathbb{F}_p \). Then, we find that the matrix \( (v^1, \ldots, v^k) \) is an \((r, k)\)-MDS code.

**Lemma 14:** We consider a finite field \( \mathbb{F}_p \). We choose a \((b-a) \times a\) matrix \( A_1 = (a_{i,j})_{1 \leq i \leq b-a, 1 \leq j \leq a} \) and a \((b-a) \times a\) matrix \( A_2 = (a_{i,j})_{b-a+1 \leq i \leq 2b-a, 1 \leq j \leq a} \) over \( \mathbb{F}_p \) to satisfy the following conditions. The component \( a_{i,j} \) is an element of \( \mathbb{F}_p \) for \( 1 \leq i \leq 2(b-a) \) and \( 1 \leq j \leq a \). We choose a \( a \times a \) matrix \( A_3 = (a_{i,j})_{2(b-a)+1 \leq i \leq 2b-a, 1 \leq j \leq a} \) over \( \mathbb{F}_p \). Then, the LHS is a non-zero vector, we obtain a contradiction. Hence, we obtain the desired statement.
satisfy the conditions; The component $a_{i,j}$ is an element of $F_p[e_1, \ldots, e_{i+j-1}] \setminus F_p[e_1, \ldots, e_{i+j-2}]$ for $2(b-a)+1 \leq i \leq 2b-a$ and $1 \leq j \leq a$. The relation

$$a_{2(b-a)+j,i} + \sum_{k=1}^{b-a} a_{k,j}a_{b-a+k,i} = a_{2(b-a)+j,i} + \sum_{k=1}^{b-a} a_{k,j}a_{b-a+k,i}$$

holds for $1 \leq i \leq a$ and $1 \leq j \leq a$. Notice that the above choice is always possible. Then, we define a $2b \times a$ matrix $A$ and a $2b \times (2b-a)$ matrix $B$ as follows

$$A = \begin{pmatrix} A_2 \\ A_3 \\ A_1 \\ I \end{pmatrix}, \quad B = \begin{pmatrix} I \\ -A_1^T \ A_2^T \ A_3^T \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$ (65)

In addition, we assume that $a_{1,1} = 1$. Then, we have the following conditions.

(N1) The relation $A^TJA = 0$ holds.

(N2) The relation $A^TJB = 0$ holds.

(N3) The $2b \times a$ matrix $A$ is a $(2b,a)$-MDS code.

(N4) The $2b \times (2b-a)$ matrix $B$ is a $(2b,(2b-a))$-MDS code.

In fact, since the set $F_p[e_1, \ldots, e_{i+j-1}] \setminus F_p[e_1, \ldots, e_{i+j-2}]$ is not empty, it is possible to choose the component $a_{i,j}$ in the above way.

Proof: The condition (N1) follows from the condition (64). The condition (N2) follows from the definitions of $A$ and $B$. The condition (N3) holds if and only if the $2b \times a$ matrix

$$A = \begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$$

is a $(2b,a)$-MDS code. The latter condition follows from Proposition 9. Hence, we obtain the condition (N3). The condition (N4) holds if and only if the $2b \times (2b-a)$ matrix

$$B = \begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$$

is a $(2b,(2b-a))$-MDS code. The latter condition follows from Proposition 9. Hence, we obtain the condition (N4).

Lemma 15: We choose matrices $A$ and $B$ in the same way as Lemma 14. We choose a prime power $q$ such that $F_q = F_p[e_1, \ldots, e_{2b-1}]$. We choose a $(b-a) \times c$ matrix $C = \begin{pmatrix} g_{ij} \end{pmatrix}_{1 \leq i \leq b-a, 1 \leq j \leq c}$ and a $(b-a) \times c$ matrix $C_2 = \begin{pmatrix} g_{ij} \end{pmatrix}_{1 \leq i \leq 2(b-a), 1 \leq j \leq c}$ over $F_q[e_1', \ldots, e_{2(b-a)-1}']$ to satisfy the following conditions. The component $g_{i,j}$ is an element of $F_q[e_1', \ldots, e_{i+j-1}] \setminus F_q[e_1', \ldots, e_{i+j-2}']$ for $1 \leq i \leq 2(b-a)$ and $1 \leq j \leq c$. We choose a $c \times c$ matrix $C_3 = \begin{pmatrix} g_{ij} \end{pmatrix}_{2(b-a)+1 \leq i \leq 2b-a, 1 \leq j \leq c}$ to satisfy the conditions; The component $g_{i,j}$ is an element of $F_q[e_1', \ldots, e_{i+j-1}] \setminus F_q[e_1', \ldots, e_{i+j-2}']$ for $2(b-a)+1 \leq i \leq 2b-a$ and $1 \leq j \leq c$.

Then, we define a $2b \times c$ matrix $C$ as follows

$$C = \begin{pmatrix} C_2 \\ C_3 \\ C_1 \\ 0 \end{pmatrix}.$$ (66)

Then, we have the following conditions.

(N5) The $2b \times (a+c)$ matrix $(A,C)$ is a $(2b,(a+c))$-MDS code.

(N6) Let $C^{(s)}$ be the matrix composed of the first $s$ column vectors of $C$. The $2b \times (a+s)$ matrix $(A,C^{(s)})$ is a $(2b,(a+s))$-MDS code.

(N7) The $2b \times (2b-a+c)$ matrix $(B,C)$ is a $(2b,(2b-a+c))$-MDS code.

Proof: The condition (N5) holds if and only if the $2b \times (a+c)$ matrix

$$\begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$$

is a $(2b,a)$-MDS code. We apply Lemma 12 to the case with $D = \begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$, $F = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}$, $l = a$, $k = a+s$, $r = 2b$, and $F' = F_q[e_1', \ldots, e_{a-1}']$. Then, due to the condition (N3) of Lemma 14, we obtain the condition (N5).

To show the condition (N6), we apply Lemma 12 to the case with $D = \begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$, $F = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}$, $l = a$, $k = a+s$, $r = 2b$, and $F' = F_q[e_1', \ldots, e_{a-1}']$. Hence, we obtain the condition (N6).

The condition (N7) holds if and only if the $2b \times (a+c)$ matrix

$$\begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$$

is a $(2b,(2b-a))$-MDS code. We apply Lemma 12 to the case with $D = \begin{pmatrix} I \\ A_1 \\ A_2 \\ A_3 \end{pmatrix}$, $F = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}$, $l = 2b-a$, $k = 2b-a+c$, $r = 2b$, and $F' = F_q[e_1', \ldots, e_{2(b-a)-c+1}']$. Then, due to the condition (N4) of Lemma 14, we obtain the latter condition. Hence, we obtain the condition (N7).
Theorem 2 is completed.

APPENDIX C

Proof of Theorem 2

To show Theorem 2, we apply Lemma 15 with \( b = n, a = n, c = 2r \) that is given in Appendix A. Then, we choose the matrices \( G^{(1)}, G^{(2)} \) as \( A \), the matrix composed of the first \( y_2 := [2t-n]_+ \) column vectors of \( C \), the matrix composed of the remaining \( 2r - y_2 \) column vectors of \( C \), respectively. Due to the condition (64), the matrix \( G^{(1)} \) is self-column-orthogonal.

The condition (N6) with \( s = y_2 \) guarantees that \( (G^{(1)}, G^{(2)}) \) is a \((2n, n + y_2)\)-MDS code. This property guarantees the rejection condition with \( B \) that has the choice \( B = \{B \subset [n] \mid |B| \leq t \} \) because \( n + y_2 \geq 2t \). Also, the condition (N5) guarantees that \( ((G^{(1)}, G^{(2)}), F) \) is a \((2n, 2r)\)-MDS code. This property guarantees the acceptance condition with \( A \) that has the choice \( A = \{A \subset [n] \mid |A| \geq r \} \). Therefore, the proof of Theorem 2 is completed.

APPENDIX D

Proof of Theorem 4

Since Condition (E3) implies Condition (E2), we show the directions (E2) \( \Rightarrow \) (E1) and (E1) \( \Rightarrow \) (E3).

To show the direction (E2) \( \Rightarrow \) (E1), we assume Condition (E2). Due to Theorem 3, there exists a linear QCSS protocol that satisfies the correctness with \( A = \{A \subset [n] \mid |A| \geq r \} \) if \( \text{Condition (E1)} \) holds, i.e., \( t < (n + 1)/2 \), there are two disjoint subsets \( A_1, A_2 \subset A \). Hence, the players in \( A_1 \) and the players in \( A_2 \) can recover the original state, which contradicts the no-cloning theorem [82], [83]. Hence, Condition (E2) implies Condition (E1).

To show the direction (E1) \( \Rightarrow \) (E3), we assume Condition (E1), and choose \( t^* := \max\{t, n - r\} \). Then, we choose a positive integer \( s \), a \( 2n \times (n - r + t^*) \) self-column-orthogonal matrix \( G^{(1)} \), a \( 2n \times (t^* + r - n) \) matrix \( G^{(2)} \), and a \( 2n \times 2(t^* - r) \) matrix \( F \) column-orthogonal to the matrix \( G^{(1)} \) on \( \mathbb{F}_q \) with \( q = p^s \) such that the matrix \( (G^{(1)}, G^{(2)}, F) \) is an \((r, t^*, n)\)-QQMMP. Since \( t^* \geq t \), this statement implies Condition (E3).

For this aim, we apply Lemma 15 to the case with \( b = n, a = n - r + t^*, c = t^* + r - n \) that is given in Appendix A. We choose the \( 2n \times (n - r + t^*) \) matrix \( G^{(1)} \), the \( 2n \times (t^* + r - n) \) matrix \( G^{(2)} \), and the \( 2n \times 2(t^* - r) \) matrix \( F \), as \( A, C, \) and \( D \), respectively. The matrix \( G^{(1)} \) is self-column-orthogonal due to the condition (N1). The matrix \( F \) is column-orthogonal to \( G^{(1)} \) due to the condition (N2).

The matrix \( (G^{(1)}, G^{(2)}) \) is \((2n, 2t^*)\)-MDS code due to the condition (N5). Since the \( n+r - t^* \) column vectors of \( G^{(1)}, F \) form the orthogonal space to the \( n + r - t^* \) column vectors of \( G^{(1)}, F \), the linear space spanned by the \( n + r - t^* \) column vectors of \( G^{(1)}, F \) equals the linear space spanned by the \( n + r - t^* \) column vectors of \( B \). Hence, the matrix \( (G^{(1)}, G^{(2)}, F) \) is \((2n, 2r)\)-MDS code if and only if The matrix \( (B, G^{(2)}) \) is \((2n, 2r)\)-MDS code, which is guaranteed by the condition (N6). Therefore, the matrix \( (G^{(1)}, G^{(2)}, F) \) is an \((r, t^*, n)\)-QQMMP, which implies Condition (E3).

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,” in Proc. Int. Workshop. Requirements Knowl. (MARK), Jun. 1979, pp. 313–318.
[3] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
[4] M. Rabim, “How to exchange secrets by oblivious transfer,” Aiken Comput. Lab., Harvard Univ., Cambridge, MA, USA, Tech. Rep., TR-81, 1981.
[5] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, “Protecting data privacy in private information retrieval schemes,” J. Comput. Syst. Sci., vol. 60, no. 3, pp. 592–629, Jun. 2000.
[6] A. Beimel, Y. Ishai, E. Kushilevitz, and I. Orlov, “Share conversion and private information retrieval,” in Proc. IEEE 27th Conf. Comput. Complex., Jun. 2012, pp. 258–268.
[7] L. Li, M. Militzer, and A. Datta, “rPIR: Ramp secret sharing-based communication-efficient private information retrieval,” Int. J. Inf. Secur., vol. 16, pp. 603–625, Jan. 2017.
[8] H. Yang, W. Shin, and J. Lee, “Private information retrieval for secure distributed storage systems,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 12, pp. 2953–2964, Dec. 2018.
[9] R. G. L. D’Oliveira and S. E. Rouayheb, “Lifting private information retrieval from two to any number of messages,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2018, pp. 1744–1748.
[10] S. Song and M. Hayashi, “Equivalence of non-perfect secret sharing and symmetric private information retrieval with general access structure,” IEEE J. Sel. Areas Commun., vol. 40, no. 3, pp. 999–1012, Mar. 2022.
[11] A. Beimel et al., “Secret-sharing schemes: A survey,” in Coding and Cryptology (Lecture Notes in Computer Science), vol. 6639, Y. M. Chee, Ed. Berlin, Germany: Springer, 2011.
[12] M. Bertilsson and I. Ingemarsson, “A construction of practical secret sharing schemes using linear block codes,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 718, J. Seberry and Y. Zheng, Eds. Berlin, Germany: Springer, 1992, pp. 67–79.
[13] M. van Dijk, “A linear construction of perfect secret sharing schemes,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 950, A. De Santis, Ed. Cham, Switzerland: Springer-Verlag, 1995, pp. 23–34.
[14] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” Phys. Rev. A, Gen. Phys., vol. 59, pp. 1829–1834, Mar. 1999.
[15] A. Karlsson, M. Koashi, and N. Imoto, “Quantum entanglement for secret sharing and secret splitting,” Phys. Rev. A, Gen. Phys., vol. 59, no. 1, pp. 162–168, Jan. 1999.
[16] D. Gottesman, “Theory of quantum secret sharing,” Phys. Rev. A, Gen. Phys., vol. 61, no. 4, Mar. 2000, Art. no. 042311.
[17] P. Sarvepalli, “Non-threshold quantum secret sharing schemes in the graph state formalism,” Phys. Rev. A, Gen. Phys., vol. 86, Jan. 2012, Art. no. 042303.
[18] E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix, “Information flow in secret sharing protocols,” 2009, arXiv:0909.4479.
[19] D. Markham and B. C. Sanders, “Graph states for quantum secret sharing,” Phys. Rev. A, Gen. Phys., vol. 78, no. 4, Oct. 2008, Art. no. 042309.
[20] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, “Quantum secret sharing with qudit graph states,” Phys. Rev. A, Gen. Phys., vol. 82, no. 6, Dec. 2010, Art. no. 062315.
[21] M.-M. Wang, X.-B. Chen, and Y.-X. Yang, “Quantum secret sharing for general access structures based on multipartite entanglements,”Quantum Inf. Process., vol. 13, no. 2, pp. 429–443, Feb. 2014.
[22] R. Matsumoto, “Quantum stabilizer codes can realize access structures,” IEICE Trans. Fundamentals Electron., Commun. Comput. Sci., vol. 100, no. 12, pp. 2738–2739, 2017.
[23] R. Matsumoto, “Classical access structures of ramp secret sharing based on quantum stabilizer codes,” Quantum Inf. Process., vol. 19, no. 1, pp. 1–10, Jan. 2020.
[24] A. Marin and D. Markham, “Equivalence between sharing quantum and classical secrets and error correction,” Phys. Rev. A, Gen. Phys., vol. 88, no. 4, Oct. 2013, Art. no. 042332.
[76] M. Grassl, T. Beth, and T. Pellizzari, “Codes for the quantum erasure channel,” Phys. Rev. A, Gen. Phys., vol. 56, no. 1, pp. 33–38, Jul. 1997.
[77] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, “Private quantum channels,” in Proc. 41st Annu. Symp. Found. Comput. Sci., 2000, pp. 547–553.
[78] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett., vol. 85, no. 2, pp. 441–444, Jul. 2000.
[79] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states,” Phys. Rev. Lett., vol. 69, no. 20, pp. 2881–2884, Nov. 1992.
[80] N. Cai and M. Hayashi, “Secure network code for adaptive and active attacks with no-randomness in intermediate nodes,” IEEE Trans. Inf. Theory, vol. 66, no. 3, pp. 1428–1448, Mar. 2020.
[81] M. Hayashi and Á. Vázquez-Castro, “Computation-aided classical-quantum multiple access to boost network communication speeds,” Phys. Rev. Appl., vol. 16, no. 5, Nov. 2021, Art. no. 054021.
[82] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
[83] D. Dieks, “Communication by EPR devices,” Phys. Lett. A, vol. 92, no. 6, pp. 271–272, Nov. 1982.

Masahito Hayashi (Fellow, IEEE) was born in Japan in 1971. He received the B.S. degree from the Faculty of Sciences, Kyoto University, Japan, in 1994, and the M.S. and Ph.D. degrees in mathematics from Kyoto University, in 1996 and 1999, respectively.

He was a Research Fellow of the Japan Society of the Promotion of Science (JSPS), Kyoto University, from 1998 to 2000, and a Researcher with the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN, from 2000 to 2003. He was the Research Head of the ERATO Quantum Computation and Information Project, Japan Science and Technology Agency (JST), from 2003 to 2006, and a Group Leader with the ERATO-SORST Quantum Computation and Information Project, JST, from 2006 to 2007. He was also with the Superrobust Computation Project Information Science and Technology Strategic Core (21st Century COE by MEXT), Graduate School of Information Science and Technology, The University of Tokyo, as an Adjunct Associate Professor, from 2004 to 2007. He was an Associate Professor with the Graduate School of Information Sciences, Tohoku University, from 2007 to 2012. In 2012, he joined the Graduate School of Mathematics, Nagoya University, as a Full Professor. He was with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China, as a Chief Research Scientist, from 2020 to 2023. In 2023, he joined the School of Data Science, The Chinese University of Hong Kong Shenzhen (CUHK-Shenzhen), as a Full Professor, and joined the International Quantum Academy (SIQA) as a Chief Research Scientist. Also, he was with the Centre for Quantum Technologies, National University of Singapore, as a Visiting Research Associate Professor, from 2009 to 2012, and has been a Visiting Research Professor since 2012. He was with the Center for Advanced Intelligence Project, RIKEN, as a Visiting Scientist, from 2017 to 2020. He was with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, as a Visiting Professor, from 2018 to 2020, and the Peng Cheng Laboratory, Center for Quantum Computing, Shenzhen, as a Visiting Professor, from 2019 to 2020. In 2006, he published the book Quantum Information: An Introduction (Springer), whose revised version was published as Quantum Information Theory: Mathematical Foundation from Graduate Texts in Physics (Springer, 2016). In 2016, he has published other two books Group Representation for Quantum Theory and A Group Theoretic Approach to Quantum Information (Springer). He is on the editorial board of International Journal of Quantum Information. His research interests include classical and quantum information theory and classical and quantum statistical inference.

Prof. Hayashi was elected as an Institute of Mathematical Statistics (IMS) Fellow and an Asia-Pacific Artificial Intelligence Association (AAIA) Fellow in 2022. In 2011, he received the Information Theory Society Paper Award for “Information-Spectrum Approach to Second-Order Coding Rate in Channel Coding.” In 2016, he received the Japan Academy Medal from the Japan Academy and the JSPS Prize from the Japan Society for the Promotion of Science.

Seunghoan Song (Member, IEEE) received the B.E. degree from Osaka University, Japan, in 2017, and the M.Math. and Ph.D. degrees in mathematical science from Nagoya University, Japan, in 2019 and 2020, respectively. He was a Research Fellow of the Japan Society of the Promotion of Science (JSPS) from 2020 to 2021. He was a JSPS Post-Doctoral Fellow with the Graduate School of Mathematics, Nagoya University, from 2021 to 2022. He is currently working in industry. His research interests include classical and quantum information theory and its applications to secure communication protocols. He was awarded the School of Engineering Science Outstanding Student Award from Osaka University in 2017 and the Graduate School of Mathematics Award for Outstanding Masters Thesis from Nagoya University in 2019.