Allaix, Matteo; Song, Seunghoan; Holzbaur, Lukas; Pllaha, Tefjol; Hayashi, Masahito; Hollanti, Camilla

On the Capacity of Quantum Private Information Retrieval From MDS-Coded and Colluding Servers

Published in:
IEEE Journal on Selected Areas in Communications

DOI:
10.1109/JSAC.2022.3142363

Published: 01/03/2022

Document Version
Publisher's PDF, also known as Version of record

On the Capacity of Quantum Private Information Retrieval From MDS-Coded and Colluding Servers

Matteo Allaix, *Student Member, IEEE*, Seunghoan Song, *Member, IEEE*, Lukas Holzbaur, *Graduate Student Member, IEEE*, Tefjol Pllaha, Masahito Hayashi, *Fellow, IEEE*, and Camilla Hollanti, *Member, IEEE*

***Abstract*— In quantum private information retrieval (QPIR), a user retrieves a classical file from multiple servers by downloading quantum systems without revealing the identity of the file. The QPIR capacity is the maximal achievable ratio of the retrieved file size to the total download size. In this paper, the capacity of QPIR from MDS-coded and colluding servers is studied for the first time. Two general classes of QPIR, called stabilizer QPIR and dimension-squared QPIR induced from classical strongly linear PIR are defined, and the related QPIR capacities are derived. For the non-colluding case, the general QPIR capacity is derived when the number of files goes to infinity. A general statement on the converse bound for QPIR with coded and colluding servers is derived showing that the capacities of stabilizer QPIR and dimension-squared QPIR induced from any class of PIR are upper bounded by twice the classical capacity of the respective PIR class. The proposed capacity-achieving scheme combines the star-product scheme by Freij-Hollanti *et al.* and the stabilizer QPIR scheme by Song *et al.* by employing (weakly) self-dual Reed–Solomon codes.**

Manuscript received June 1, 2021; revised November 1, 2021; accepted December 21, 2021. Date of publication January 12, 2022; date of current version February 17, 2022. The work of Matteo Allaix and Camilla Hollanti was supported by the Academy of Finland, under Grant 318937 and Grant 336005. The work of Seunghoan Song was supported by the Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for JSPS Fellows under Grant JP20J11484. The work of Lukas Holzbaur was supported by the German Research Foundation [Deutsche Forschungsgemeinschaft (DFG)] under Grant WA 3907/1-1. The work of Masahito Hayashi was supported in part by the Guangdong Provincial Key Laboratory under Grant 2019B121203002. An earlier version of this paper was presented in part at the 2021 IEEE International Symposium on Information Theory (ISIT) [1] [DOI: 10.1109/ISIT45174.2021.9517846]. *(Matteo Allaix and Seunghoan Song contributed equally to this work.) (Corresponding author: Matteo Allaix.)*

Matteo Allaix and Camilla Hollanti are with the Department of Mathematics and System Analysis, Aalto University, 02150 Espoo, Finland (e-mail: matteo.allaix@aalto.fi; camilla.hollanti@aalto.fi).

Seunghoan Song is with the Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan (e-mail: m17021a@math.nagoya-u.ac.jp).

Lukas Holzbaur is with the Institute for Communications Engineering, Technical University of Munich, 80333 Munich, Germany (e-mail: lukas.holzbaur@tum.de).

Tefjol Pllaha is with the Department of Mathematics, University of Nebraska, Lincoln, NE 68588 USA (e-mail: tefjol.pllaha@unl.edu).

Masahito Hayashi is with the Shenzhen Institute for Quantum Science and Engineering and the Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China, and also with the Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan (e-mail: hayashi@sustech.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSAC.2022.3142363.

Digital Object Identifier 10.1109/JSAC.2022.3142363

***Index Terms*— Private information retrieval (PIR), information theoretic privacy, quantum information theory, capacity.**

I. Introduction

With the amount of data stored in distributed storage systems steadily increasing, the demand for user privacy has surged in recent years. One notion that has received considerable attention is private information retrieval (PIR), where the user's goal is to access a file of a (distributed) storage system without revealing the identity (index) of this desired file. In their seminal work Chor *et al.* [2] introduced the concept of PIR from multiple non-colluding servers, each storing a copy of every file. More recently, the capacity, *i.e.*, the highest achievable rate, for this setting [3] was derived, which led to similar derivations in more general settings admitting for colluding servers [4], coded storage [5], and symmetric privacy [6], [7]. While the capacity of PIR from coded storage with colluding servers remains an open problem, some progress was made in [8]–[10]. Among other things, [9], [10] introduce the practical notion of strongly linear PIR. Informally, this class is given by PIR schemes where both the computation of the server responses and the decoding of the desired file from these responses is achieved by applying linear functions. The capacity of this class of schemes coincides with a conjecture on the asymptotic (in the number of files) capacity for this setting [11] and is known to be achievable by schemes with requiring only small subpacketization, such as the star-product scheme of [12].

Quantum PIR (QPIR) considers accomplishing the PIR task with quantum communication between the user and the servers [13]–[20]. Following the study on the classical PIR capacity [4], the papers [21]–[24] considered the capacity of QPIR and quantum symmetric PIR (QSPIR), where the user obtains no other information than the desired file in addition to the requirements of PIR. The QPIR schemes in [21]–[24] are conducted by the following procedure: a user uploads classical queries; multiple servers sharing entanglement apply quantum operations on their quantum systems depending on the queries and the files and respond quantum systems to the user; the user finally retrieves the desired file by quantum measurement on the responded systems. When each of the n servers stores a copy of every file, the QPIR/QSPIR capacity with multiple non-colluding

TABLE I

KNOWN ASYMPTOTIC ($m \to \infty$) CAPACITY RESULTS WITH n SERVERS. THE RESULT IN RED IS A CONJECTURE IN ITS FULL GENERALITY [12], BUT SHOWN TO HOLD FOR STRONGLY LINEAR [10] AND FULL SUPPORT RANK [9] PIR. A SCHEME ACHIEVING THAT RATE WAS PROPOSED IN [12]. THE RESULTS IN GREEN ARE PROVED IN THIS PAPER FOR STRONGLY LINEAR PIR

CAPACITIES	PIR	ref.	SPIR	ref.	QPIR	ref.
Replicated storage, no collusion	$1-\frac{1}{\mathsf{n}}$	[3]	$1-\frac{1}{\mathsf{n}}$	[6]	1	[21]
Replicated storage, t-collusion	$1-\frac{\mathsf{t}}{\mathsf{n}}$	[4]	$1-\frac{\mathsf{t}}{\mathsf{n}}$	[25]	$\min\{1, \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}\}$	[23]
$[\mathsf{n},\mathsf{k}]$-MDS coded storage, no collusion	$1-\frac{\mathsf{k}}{\mathsf{n}}$	[5]	$1-\frac{\mathsf{k}}{\mathsf{n}}$	[7]	$\min\{1, \frac{2(\mathsf{n}-\mathsf{k})}{\mathsf{n}}\}$	–
$[\mathsf{n},\mathsf{k}]$-MDS coded storage, t-collusion	$1-\frac{\mathsf{k}+\mathsf{t}-1}{\mathsf{n}}$	[12]	$1-\frac{\mathsf{k}+\mathsf{t}-1}{\mathsf{n}}$	[7]	$\min\{1, \frac{2(\mathsf{n}-\mathsf{k}-\mathsf{t}+1)}{\mathsf{n}}\}$	–

servers [21] and t colluding servers [23] are proved to be 1 and $\min\{1, 2(\mathsf{n}-\mathsf{t})/\mathsf{n}\}$, respectively. On the other hand, when the files are stored in a distributed storage system coded by an $[\mathsf{n},\mathsf{k}]$ maximum distance separable (MDS) code, QSPIR schemes with colluding servers are constructed [24], but the result was limited to the case $\mathsf{t}+\mathsf{k}=\mathsf{n}$.

A. Contributions

As a generalization of [24], we study the QPIR/QSPIR capacity from $[\mathsf{n},\mathsf{k}]$ MDS coded storage with t colluding servers for any $\mathsf{t}+\mathsf{k} \leq \mathsf{n}$. Since the capacity of this setting is even unsolved for the classical case, similar to [9] and [10], we define two new classes of QPIR, which include the existing QPIR schemes [21]–[24], and derive the capacity for these classes. The first class is *stabilizer QPIR induced from classical PIR*. Stabilizer QPIR is a class of QPIR that naturally imports linear PIR schemes in quantum settings while doubling the PIR rate. More specifically, the user and the servers simulate the classical PIR scheme, except that the servers' prior entangled state is a state in a stabilizer code and the servers apply Pauli X and Z operations on each quantum system depending on the answers of the classical PIR. The second class is *dimension-squared QPIR*, which is a broader class of QPIR that includes stabilizer QPIR. Whereas the stabilizer QPIR is defined with restrictions on the encoding, decoding, and shared entanglement, dimension-squared QPIR is defined only with restriction on dimensions of the answered quantum systems, which is a sufficient condition for our converse proof. Similar to the stabilizer QPIR, dimension-squared QPIR can also be induced from classical PIR and the existing QPIR schemes [21]–[24] are dimension-squared QPIR induced from strongly linear PIR.

For stabilizer QPIR and dimension-squared QPIR induced from strongly-linear PIR, we prove that the asymptotic QPIR/QSPIR capacities with MDS-coded and colluding servers are $\min\{1, 2(\mathsf{n}-\mathsf{k}-\mathsf{t}+1)/\mathsf{n}\}$. Furthermore, for non-colluding case $\mathsf{t}=1$, we prove that the general asymptotic QPIR/QSPIR capacity is $\min\{1, 2(\mathsf{n}-\mathsf{k})/\mathsf{n}\}$. The derived quantum capacities double the classical asymptotic capacities of PIR and SPIR, as compared in Table I.

The capacity achieving scheme is based on the strongly-linear star-product scheme of [12] for classical PIR from MDS-coded storage and the QPIR scheme of [23] for replicated storage, both in the presence of t colluding servers. A generalization of these schemes, which employs (weakly) self-dual Generalized Reed–Solomon (GRS) codes, results in the first known QPIR scheme from MDS-coded storage in the considered setting. The scheme is non-trivial for two main reasons. First, the chosen codes must behave well with the star-product operation: one example is the polynomial-based codes class, that includes GRS codes. This requirement comes from the classical PIR scheme described in [12]. Second, the star-product of the storage code and the query code must be a (weakly) self-dual code in order to employ the stabilizer formalism and get the advantage of quantum communication. To the best of our knowledge the combination of these two properties was not considered in previous literature. In this paper, we prove that for any given GRS storage code we can find a GRS query code such that their star-product is a (weakly) self-dual code.

The converse bounds are proved separately for the colluding and non-colluding cases. First, the converse for colluding case is derived generally for any PIR classes. Namely, when the classical capacity of any PIR class is C, we prove that the rates of stabilizer QPIR and dimension-squared QPIR induced from the same class of PIR are upper bounded by $\min\{1, 2C\}$. Then, from the capacity of strongly linear PIR for coded and colluding servers $(\mathsf{n}-\mathsf{k}-\mathsf{t}+1)/\mathsf{n}$ [9], [10], we obtain our converse bound for colluding case. Second, the converse for non-colluding case is proved for general QPIR schemes with the following idea. We prove that the k servers obtain negligible information of the user's information. Combining this fact and the entanglement-assisted classical capacity [26], we prove that the desired converse bound $C \leq \min\{1, 2(\mathsf{n}-\mathsf{k})/\mathsf{n}\}$.

Similar to the existing multi-server QPIR studies [21]–[24], the communication model in this paper is classical query and quantum answers with entanglement. This model is the hybrid model of classical and quantum communication for classical file retrieval. Compared to the non-quantum model, our main theorem implies that the capacity doubles only with the one-way quantum communication from the servers to the user. On the other hand, compared to the purely quantum model, which allows quantum queries, our model has three practical advantages. First, since the quantum communication is hard to be implemented with the current technology, our one-way communication model is a more realizable model than the two-way quantum communication. Second, in our scheme, most of the quantum resources and computations are operated by the servers, and the only

quantum device required for the user is a fixed measurement apparatus.[1] The same kind of outsourcing also appears in the computation by measurement-based quantum computation [28]. Third, since the storage is still classical, we can just employ quantum communication technology and quantum memory to double the rate of an already existing MDS-coded storage implementing a classical PIR scheme.

B. Organization

The remainder of the paper is organized as follows. Section II is a preliminary section for notation, linear codes and distributed data storage, quantrum information theory, and stabilizer formalism. In Section III, we formally define classical PIR, QPIR, and the related QPIR classes. In Section IV, we present our main capacity results. Our capacity-achieving QPIR scheme with MDS-coded storage and colluding servers is proposed in Section V and the converse bound is derived in Section VI. Section VII is the conclusion of the paper.

II. Preliminaries

A. Notation

We denote by $[n]$ and $[n_1{:}n_2]$ the sets $\{1,2,\dots,n\}, n\in\mathbb{N}$ and $\{n_1,n_1+1,\dots,n_2\}, n_1,n_2\in\mathbb{N}$, respectively, and by $\mathbb{F}_q$ the finite field of q elements. For a linear code of length n and dimension k over $\mathbb{F}_q$ we write $[\mathsf{n},\mathsf{k}]$. For random variables $A_1,\dots,A_n$, quantum systems $\mathcal{A}_1,\dots,\mathcal{A}_n$ and a set $\mathcal{S}\subset[n]$, we denote $A_{\mathcal{S}} := (A_j|j\in\mathcal{S})$ and $\mathcal{A}_{\mathcal{S}} := \bigotimes_{j\in\mathcal{S}}\mathcal{A}_j$. For a matrix $\mathbf{A}$ we write $\mathbf{A}^\top$ for its transpose and $\mathbf{A}^\dagger$ for its conjugate transpose. The function $\delta_{i,j}$ is the Kronecker delta and $\mathbf{I}_\nu$ is the $\nu\times\nu$ identity matrix. For an $n\times m$ matrix $\mathbf{A}=(a_{ij})_{i\in[n],j\in[m]}$, $\mathcal{S}_1\subset[n]$, and $\mathcal{S}_2\subset[m]$, we denote $\mathbf{A}^{\mathcal{S}_1}_{\mathcal{S}_2}=(a_{ij})_{i\in\mathcal{S}_1,j\in\mathcal{S}_2}$ and $\mathbf{A}^{\mathcal{S}_1}=(a_{ij})_{i\in\mathcal{S}_1,j\in[m]}$, $\mathbf{A}_{\mathcal{S}_2}=(a_{ij})_{i\in[n],j\in\mathcal{S}_2}$. Throughout this paper, we use $\log$ for the logarithm to the base 2.

B. Linear Codes and Distributed Data Storage

We consider a distributed storage system employing error/erasure correcting codes to protect against data loss. To this end, let $\mathbf{X}$ be an $\mathsf{m}\beta\times\mathsf{k}$ matrix containing m files $\mathbf{X}^i\in\mathbb{F}_q^{\beta\times\mathsf{k}}$, $i\in[\mathsf{m}]$. This matrix is encoded with a linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$. The $\mathsf{m}\beta\times\mathsf{n}$ matrix of encoded files is given by $\mathbf{Y}=\mathbf{X}\cdot\mathbf{G}_{\mathcal{C}}$, where $\mathbf{G}_{\mathcal{C}}\in\mathbb{F}_q^{\mathsf{k}\times\mathsf{n}}$ is the generator matrix of $\mathcal{C}$. Server $s\in[\mathsf{n}]$ stores the s-th column of $\mathbf{Y}$, which is denoted by $\mathbf{Y}_s$.

In this work we consider systems encoded with MDS codes. A linear code $\mathcal{C}$ is called an MDS code if any k columns of the generator matrix $\mathbf{G}_{\mathcal{C}}$ are linearly independent. Since we consider a MDS coded data storage, we have the following properties.

1) The matrix $\mathbf{X}^i$ can be recovered from any k elements of $\{\mathbf{Y}^i_1,\dots,\mathbf{Y}^i_{\mathsf{n}}\}$ for any $i\in[\mathsf{m}]$.
2) Any k columns of $\mathbf{Y}$ are linearly independent.

[1]QPIR problem can also be considered for the retrieval of quantum states, i.e., QPIR with quantum storage. A part of authors discussed this problem in a recent paper [27].

C. Preliminaries on Quantum Information Theory

In this subsection, we introduce the preliminaries on quantum information theory. To be precise, we introduce quantum systems, states, operations, and measurements. Further, after the introduction, we explain the quantum information theory is a generalization of classical information theory. For more details the reader is referred to [29] and [30].

A quantum system $\mathcal{H}$ is represented by a finite dimensional complex vector space. Vectors in a quantum system are written with bra-ket notation as $|\psi\rangle\in\mathcal{H}$ and their complex conjugates are as $\langle\psi|$. The *computational basis* of a d-dimensional quantum system $\mathcal{H}$ is a fixed orthonormal basis written as $\{|0\rangle,\dots,|d-1\rangle\}$. The composite system of multiple quantum systems $\mathcal{H}_1,\dots,\mathcal{H}_n$ is represented by the tensor product $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_n$.

A state σ on $\mathcal{H}$ is represented by a positive-semidefinite matrix on $\mathcal{H}$ with trace 1, which is called a *density matrix*. When a density matrix σ is a rank-one matrix, i.e., $\sigma=|\psi\rangle\langle\psi|$, the state is equivalently represented by a unit vector $|\psi\rangle$, called a *pure state*. When a state is not a pure state, the state is called a *mixed state*. On a composite system $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_n$, a state is called *separable* if the state is written as $\sigma=\sum_i p_i\sigma_1\otimes\cdots\otimes\sigma_n$ with $p_i\geq 0$, $\sum_i p_i=1$, and density matrices σ_i for all i. A state on a composite system is called *entangled* if it is not a separable state. When the state on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_n$ is σ, the *reduced state* on $\mathcal{H}_k$ is written as $\mathrm{Tr}_{k^c}\sigma$, where Tr_{k^c} is the partial trace over $\bigotimes_{i\neq k}\mathcal{H}_i$.

A quantum operation κ from $\mathcal{H}_1$ to $\mathcal{H}_2$ is represented by *completely positive trace-preserving (CPTP) map* defined as follows. A linear map κ from matrices on $\mathcal{H}_1$ to matrices on $\mathcal{H}_2$ is called *completely positive* if for all positive integer n, the map $\kappa\otimes\mathrm{id}_{\mathbb{C}^n}$ maps positive-semidefinite matrices to positive-semidefinite matrices, where $\mathrm{id}_{\mathbb{C}^n}$ is the identity map over the matrices on $\mathrm{id}_{\mathbb{C}^n}$, and *trace-preserving* if $\mathrm{Tr}(\kappa(M))=\mathrm{Tr}(M)$ for all matrices M on $\mathcal{H}_1$. A CPTP map κ is called a *unitary map* if $\kappa(M)=U^\dagger MU$ with a unitary matrix U on $\mathcal{H}$.

A measurement on a quantum system $\mathcal{H}$ is represented by a set of positive-semidefinite matrices $\mathbf{M}=\{M_\omega\}_{\omega\in\Omega}$ on $\mathcal{H}$ with $\sum_\omega M_\omega=I$, called a *positive operation-valued measure (POVM)*. When a POVM is performed on a state σ, the measurement outcome is ω with probability $\mathrm{Tr}(M_\omega\sigma M_\omega)$. If all elements of a POVM $\{M_\omega\}_{\omega\in\Omega}$ are orthogonal projections, the POVM is called *the projection-valued measure (PVM)*.

Classical information theory is included in the framework of quantum information theory in the following sense. A finite set $[0:d-1]$ corresponds to a d-dimensional quantum system with computational basis $\{|0\rangle,\dots,|d-1\rangle\}$. An instance $x\in[0:d-1]$ and a random variable X with probability $\{p_x|x\in[0:d-1]\}$ correspond, respectively, to a pure state $|x\rangle$ and a mixed state $\sigma=\sum_{x\in[0:d-1]}p_x|x\rangle\langle x|$. A transition matrix $Q=(Q_{x,y})_{x\in[0:d-1],y\in[0:d'-1]}$, which satisfies $Q_{x,y}\in[0,1]$ and $\sum_y Q_{x,y}=1$, corresponds to a CPTP map $\kappa(\sigma)=\sum_{x,y}Q_{x,y}|y\rangle\langle x|\sigma|x\rangle\langle y|$. For example, if the state σ corresponds to the random variable X, i.e., $\sigma=\sum_{x\in[0:d-1]}p_x|x\rangle\langle x|$, the resultant state after applying κ is $\sum_y(\sum_x p_xQ_{x,y})|y\rangle\langle y|$, i.e., the random variable after applying Q on X. Sampling a random variable X with the outcome

x corresponds to performing PVM $\mathbf{M} = \{P_x = |x\rangle\langle x|\}$ and obtaining the measurement outcome x with probability p_x.

D. Stabilizer Formalism

Stabilizer formalism is an algebraic structure in quantum information theory and is often used for the quantum error correction [31], [32]. In the context of QPIR, it is also an essential tool to design most of the existing multi-server QPIR schemes [21]–[24]. With the stabilizer formalism, we will define a new class of QPIR, called stabilizer QPIR in Section III-B.1, and design our capacity-achieving schemes in Section V. As a preliminary, in this section, we first define stabilizer formalism over finite fields $\mathbb{F}_q$. Then, to help understanding how the mathematical definition of the stabilizer formalism is used for information processing tasks, we briefly explain the application to the quantum error correction.

1) Stabilizer Formalism Over Finite Fields: Let $q = p^r$ with a prime number p and a positive integer r. Let $\mathcal{H}$ be a q-dimensional Hilbert space spanned by orthonormal states $\{|j\rangle | j \in \mathbb{F}_q\}$. For $x \in \mathbb{F}_q$, we define $\mathbf{T}_x$ on $\mathbb{F}_p^r$ as the linear map $y \in \mathbb{F}_q \mapsto xy \in \mathbb{F}_q$ by identifying the finite field $\mathbb{F}_q$ with the vector space $\mathbb{F}_p^r$. Let $\operatorname{tr} x := \operatorname{Tr} \mathbf{T}_x \in \mathbb{F}_p$ for $x \in \mathbb{F}_q$. Let $\omega := \exp(2\pi i/p)$. For $a, b \in \mathbb{F}_q$, we define unitary matrices $\mathsf{X}(a) := \sum_{j\in\mathbb{F}_q} |j+a\rangle\langle j|$ and $\mathsf{Z}(b) := \sum_{j\in\mathbb{F}_q} \omega^{\operatorname{tr} bj} |j\rangle\langle j|$ on $\mathcal{H}$. For $\mathbf{s} = (s_1, \dots, s_{2\mathsf{n}}) \in \mathbb{F}_q^{2\mathsf{n}}$, we define a unitary matrix $\tilde{\mathbf{W}}(\mathbf{s}) := \mathsf{X}(s_1)\mathsf{Z}(s_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(s_{\mathsf{n}})\mathsf{Z}(s_{2\mathsf{n}})$ on $\mathcal{H}^{\otimes \mathsf{n}}$. For $\mathbf{x} = (x_1, \dots, x_{\mathsf{n}})$, $\mathbf{y} = (y_1, \dots, y_{\mathsf{n}}) \in \mathbb{F}_q^{\mathsf{n}}$, we define the tracial bilinear form $\langle \mathbf{x}, \mathbf{y}\rangle := \operatorname{tr} \sum_{i=1}^{\mathsf{n}} x_i y_i \in \mathbb{F}_p$ and the trace-symplectic bilinear form $\langle \mathbf{x}, \mathbf{y}\rangle_{\mathbb{S}} := \langle \mathbf{x}, \mathbf{J}\mathbf{y}\rangle$, where $\mathbf{J}$ is a $2\mathsf{n} \times 2\mathsf{n}$ matrix

$$\mathbf{J} = \begin{pmatrix} \mathbf{0} & -\mathbf{I}_{\mathsf{n}} \\ \mathbf{I}_{\mathsf{n}} & \mathbf{0} \end{pmatrix}.$$

The Heisenberg-Weyl group is defined as $\mathrm{HW}_q^{\mathsf{n}} := \{*\} c\tilde{\mathbf{W}}(\mathbf{s}) | \mathbf{s} \in \mathbb{F}_q^{2\mathsf{n}},\ c \in \mathbb{C}$. A commutative subgroup of $\mathrm{HW}_q^{\mathsf{n}}$ not containing $c\mathbf{I}_{q^{\mathsf{n}}}$ for any $c \neq 0$ is called a *stabilizer*. A subspace $\mathcal{V}$ of $\mathbb{F}_q^{2\mathsf{n}}$ is called *self-orthogonal* with respect to the bilinear form $\langle \cdot, \cdot \rangle_{\mathbb{S}}$ if $\mathcal{V} \subset \mathcal{V}^{\perp_{\mathbb{S}}} := \{\mathbf{s} \in \mathbb{F}_q^{2\mathsf{n}} | \langle \mathbf{v}, \mathbf{s}\rangle_{\mathbb{S}} = 0 \text{ for any } \mathbf{v} \in \mathcal{V}\}$. Any self-orthogonal subspace of $\mathbb{F}_q^{2\mathsf{n}}$ defines a stabilizer by the following proposition.

Proposition 2.1 ([23, Sec. IV-A]): Let $\mathcal{V}$ be a self-orthogonal subspace of $\mathbb{F}_q^{2\mathsf{n}}$. There exists $\{c_{\mathbf{v}} \in \mathbb{C} | \mathbf{v} \in \mathcal{V}\}$ such that

$$\mathcal{S}(\mathcal{V}) := \{\mathbf{W}(\mathbf{v}) := c_{\mathbf{v}} \tilde{\mathbf{W}}(\mathbf{v}) | \mathbf{v} \in \mathcal{V}\} \subset \mathrm{HW}_q^{\mathsf{n}} \tag{1}$$

is a stabilizer.

In the next proposition, we denote the elements of the quotient space $\mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}$ by $\overline{\mathbf{s}} := \mathbf{s} + \mathcal{V}^{\perp_{\mathbb{S}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}$.

Proposition 2.2 ([23, Sec. IV-A]): Let $\mathcal{V}$ be a d-dimensional self-orthogonal subspace of $\mathbb{F}_q^{2\mathsf{n}}$ and $\mathcal{S}(\mathcal{V})$ be a stabilizer defined from Proposition 2.1. Then, we obtain the following statements.

(a) For any $\mathbf{v} \in \mathcal{V}$, the operation $\mathbf{W}(\mathbf{v}) \in \mathcal{S}(\mathcal{V})$ is simultaneously and uniquely decomposed as

$$\mathbf{W}(\mathbf{v}) = \sum_{\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}} \omega^{\langle \mathbf{v}, \mathbf{s}\rangle_{\mathbb{S}}} \mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \tag{2}$$

with orthogonal projections $\{\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}}\}$ such that

$$\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} \mathbf{P}_{\overline{\mathbf{t}}}^{\mathcal{V}} = \mathbf{0} \text{ for any } \overline{\mathbf{s}} \neq \overline{\mathbf{t}}, \tag{3}$$

$$\sum_{\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}} \mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} = \mathbf{I}_{q^{\mathsf{n}}}. \tag{4}$$

(b) Let $\mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} := \operatorname{Im} \mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}}$. We have $\dim \mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} = q^{\mathsf{n}-d}$ for any $\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}$ and the quantum system $\mathcal{H}^{\otimes \mathsf{n}}$ is decomposed as

$$\mathcal{H}^{\otimes \mathsf{n}} = \bigotimes_{\overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}} \mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} = \mathcal{W} \otimes \mathbb{C}^{q^{\mathsf{n}-d}}, \tag{5}$$

where the system $\mathcal{W}$ is the q^d-dimensional Hilbert space spanned by $\{|\overline{\mathbf{s}}\rangle | \overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}\}$ with the property $\mathcal{H}_{\overline{\mathbf{s}}}^{\mathcal{V}} = |\overline{\mathbf{s}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}} := \{|\overline{\mathbf{s}}\rangle \otimes |\psi\rangle || \psi\rangle \in \mathbb{C}^{q^{\mathsf{n}-d}}\}$.

(c) For any $\mathbf{s}, \mathbf{t} \in \mathbb{F}_q^{2\mathsf{n}}$, we have

$$\mathbf{W}(\mathbf{t}) |\overline{\mathbf{s}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}} = |\overline{\mathbf{s}+\mathbf{t}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}}, \tag{6}$$

$$\mathbf{W}(\mathbf{t}) \left(|\overline{\mathbf{s}}\rangle\langle\overline{\mathbf{s}}| \otimes \mathbf{I}_{q^{\mathsf{n}-d}} \right) \mathbf{W}(\mathbf{t})^\dagger = |\overline{\mathbf{s}+\mathbf{t}}\rangle\langle\overline{\mathbf{s}+\mathbf{t}}| \otimes \mathbf{I}_{q^{\mathsf{n}-d}}. \tag{7}$$

(d) For any $\mathbf{v} \in \mathcal{V}$ and any $|\psi\rangle \in |\overline{\mathbf{0}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}}$, we have

$$\mathbf{W}(\mathbf{v}) |\psi\rangle = |\psi\rangle. \tag{8}$$

2) Application to Quantum Error Correction: Next, we explain how the stabilizer formalism is used for quantum error correction [31], [32]. Similar to the classical case, the structure of error correction will be used for accomplishing PIR tasks in the later sections.

Consider the transmission of a quantum state from a sender to a receiver over a noisy channel. When the sender's message state is σ on $\mathbb{C}^{q^{\mathsf{n}-d}}$, the sender encodes the state σ as $|\overline{\mathbf{0}}\rangle\langle\overline{\mathbf{0}}| \otimes \sigma$ on the quantum system $|\overline{\mathbf{0}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}} \subset \mathcal{H}^{\otimes \mathsf{n}}$ defined in (b) of Proposition 2.2, and send the quantum system $\mathcal{H}^{\otimes \mathsf{n}}$ to the receiver. Suppose the noise of the channel is $\mathbf{W}(\mathbf{s})$, *i.e.*, the operation $\mathbf{W}(\mathbf{s})$ is applied to the state. Then, the receiver's state is in the space $|\overline{\mathbf{s}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}}$ by (c) of Proposition 2.2. For the decoding of the error, the receiver detects $\overline{\mathbf{s}}$ by performing the PVM measurement $\{\mathbf{P}_{\overline{\mathbf{s}}}^{\mathcal{V}} | \overline{\mathbf{s}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}\}$, defined from the projections in (a) of Proposition 2.2. This PVM is called *syndrome measurement* in the similar context to the classical error correction. Then, the receiver applies error correction by choosing an element $\mathbf{s}' \in \overline{\mathbf{s}}$ and applying $\mathbf{W}(-\mathbf{s}')$, which maps the received state to the original space $|\overline{\mathbf{0}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}}$. Since the noise and error correction operation are combined as the unitray matrix $\mathbf{W}(\mathbf{s})\mathbf{W}(-\mathbf{s}') = \mathbf{W}(\mathbf{s}-\mathbf{s}')$, if $\mathbf{s}-\mathbf{s}' \in \mathcal{V}$, the decoded state is $|\overline{\mathbf{0}}\rangle\langle\overline{\mathbf{0}}| \otimes \sigma$ from (d) of Proposition 2.2. That is, σ is correctly recovered by the receiver. The characterization of the noise $\mathbf{s}$ and the corresponding choice of $\mathbf{s}'$ in decoding are essential problem in quantum error correction to achieve more reliable communication.

III. Notions of PIR

A. Classical PIR

We formally define a classical PIR scheme with MDS-coded storage (MDS-PIR). In a general MDS-PIR scheme, one user and n servers participate.

Distributed Storage The m files are given as uniformly and independently distributed random variables $X^1, \ldots, X^{\mathsf{m}}$ in $\mathbb{F}_q^{\beta \times \mathsf{k}}$. As described in Section II-B, the files $X = ((X^1)^\top, \ldots, (X^{\mathsf{m}})^\top)^\top$ are encoded with an MDS code $\mathcal{C}$ as $Y = (Y_1, \ldots, Y_{\mathsf{n}}) = X\mathbf{G}_{\mathcal{C}} \in \mathbb{F}_q^{\beta \mathsf{m} \times \mathsf{n}}$ and is distributed as the s-th server contains $Y_s \in \mathbb{F}_q^{\beta \mathsf{m}}$.

Shared Randomness The servers possibly share randomness $H = (H_1, \ldots, H_{\mathsf{n}})$, where $\mathcal{H}_s$ is owned by server s.

Query Let K be a uniform random variable with values in $[\mathsf{m}]$. The user desiring the K-th file X^K prepares $Q^K = (Q_1^K, \ldots, Q_{\mathsf{n}}^K)$ with local randomness R by the encoder $\mathsf{Enc}_{\mathrm{user}}$:$[\mathsf{m}] \times \mathcal{R} \to \mathcal{Q} := \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_{\mathsf{n}}$, where $\mathcal{R}$ is the alphabet of the user's local randomness and $\mathcal{Q}_s$ is the alphabet of the query to server s, and sends Q_s^K to server s.

Response With the encoder $\mathsf{Enc}_{\mathrm{serv}_s}$:$\mathbb{F}_q^{\beta \mathsf{m}} \times \mathcal{H}_s \times \mathcal{Q}_s \to \mathcal{B}_s$, the s-th server responds $B_s^K = \mathsf{Enc}_{\mathrm{serv}_s}(Y_s, H_s, Q_s) \in \mathcal{B}_s$ to the user. We denote $B^K = (B_1^K, \ldots, B_{\mathsf{n}}^K)$ and $\mathcal{B} = \mathcal{B}_1 \times \cdots \times \mathcal{B}_{\mathsf{n}}$.

Decoding With the decoder Dec:$[\mathsf{m}] \times \mathcal{Q} \times \mathcal{B} \to \mathbb{F}_q^{\beta \times \mathsf{k}}$, the user obtains an estimate $\hat{X}^K = \mathsf{Dec}(K, Q^K, B^K) \in \mathbb{F}_q^{\beta \times \mathsf{k}}$ of X^K.

As described above, an MDS-PIR scheme Φ is defined as $\Phi_C = (\mathcal{C}, \sigma_{\mathrm{init}}, \mathsf{Enc}_{\mathrm{user}}, \mathsf{Enc}_{\mathrm{serv}}, \mathsf{Dec})$ with the MDS code for storage $\mathcal{C}$, the initial state σ_{init}, the query encoder of the user $\mathsf{Enc}_{\mathrm{user}}$, the answer encoders of the servers $\mathsf{Enc}_{\mathrm{serv}} := \{\mathsf{Enc}_{\mathrm{serv}_s} | \forall s \in [\mathsf{n}]\}$, and the decoder of the user Dec.

The correctness of MDS-PIR is defined as follows.

Definition 3.1 (Correctness): The correctness of a MDS-PIR scheme Φ_C is evaluated by the error probability

$$P_{\mathrm{err}}(\Phi_C) := \max_{\iota \in [\mathsf{m}]} \Pr[X^\iota \neq \hat{X}^\iota]. \tag{9}$$

We also consider the following secrecy conditions with a positive integer t with $1 \leq \mathsf{t} < \mathsf{n}$.

Definition 3.2 (Privacy With t-Collusion): User t-secrecy*: Any set of at most t colluding servers gains no information about the index ι of the desired file,* i.e.*, $p_{Q_\mathcal{T}|K=\iota} = p_{Q_\mathcal{T}|K=\iota'}$ for any $\iota, \iota' \in [\mathsf{m}]$ and $\mathcal{T} \subset [\mathsf{n}]$ with $|\mathcal{T}| \leq \mathsf{t}$, where $p_{Q_\mathcal{T}|K=\iota}$ is the distribution of $Q_\mathcal{T}$ conditioned with $K = \iota$.*

Server secrecy*: The user does not gain any information about the files other than the requested one,* i.e.*,

$$I(B^\iota; X | Q^\iota, K = \iota) = H(X^\iota). \tag{10}$$

As customary, we assume that the size of the query alphabet is negligible compared to the size of the files. This is well justified if the files are assumed to be large, as the upload cost is independent of the size of the files. For simplicity, we only consider files of sizes $\mathsf{k}\beta \log q$ in the following. However, note that repeatedly applying the scheme with the same queries allows for the download of files that are any multiple of $\mathsf{k}\beta \log q$ in size at the same rate and without additional upload cost.

When user t-secrecy is satisfied, the scheme is called $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-PIR and leaks no information of the index K to any t colluding servers. When both user t-secrecy and server secrecy are satisfied, the scheme is called *symmetric* and we denote it by $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-SPIR.

As a measure of efficiency of the MDS-PIR scheme Φ_C is defined as follows.

Definition 3.3 (MDS-PIR Rate): The MDS-PIR scheme Φ_C is defined as

$$R(\Phi_C) = \frac{H(X^i)}{\sum_{j=1}^{\mathsf{n}} \log |\mathcal{B}|}. \tag{11}$$

Definition 3.4 (Achievable MDS-PIR Rate): A rate R is called ϵ-error achievable $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-PIR ($[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-SPIR) rate with m files *if there exists a sequence of $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-PIR ($[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-SPIR) schemes with m files $\{\Phi_\ell\}_\ell$ such that the PIR rate $R(\Phi_\ell)$ approaches R and the error probability satisfies $\lim_{\ell \to \infty} P_{\mathrm{err}}(\Phi_\ell) \leq \epsilon$.*

Definition 3.5 (MDS-PIR Capacity): The ϵ-error $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-PIR ($[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-SPIR) capacity with m files $C_{\mathsf{m}, \epsilon, \mathrm{cl}}^{[\mathsf{n}, \mathsf{k}, \mathsf{t}]}$ ($C_{\mathsf{m}, \epsilon, \mathrm{cl}}^{[\mathsf{n}, \mathsf{k}, \mathsf{t}], \mathrm{s}}$) *is the supremum of ϵ-error achievable $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-PIR ($[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-SPIR) rate with m files.*

Remark 1: Our definition of the achievable rate and capacity with asymptotic ϵ error generalizes the case of $\epsilon = 0$, which have been discussed in other PIR studies [3], [6].

We define two well-known classes of classical PIR. For a set $\mathcal{I} \subseteq [\mathsf{n}]$ and $\gamma \in \mathbb{N}$, we define $\psi_\gamma(\mathcal{I}) := \bigcup_{i \in \mathcal{I}} [(i-1)\gamma + 1 : i\gamma]$. For example, if $\mathcal{I} = [\mathsf{n}]$, we have $\psi_\gamma([\mathsf{n}]) = [\gamma \mathsf{n}]$.

Definition 3.6 (Linear PIR [9, Definition 1]): A PIR scheme is called linear *if*

- *the query Q is represented by a matrix $\mathbf{Q} \in \mathbb{F}_q^{\beta \mathsf{m} \times \gamma \mathsf{n}}$, where $\mathbf{Q}_{\psi_\gamma(s)}$ is the query to server s, and*
- *the classical answer B_s of server s is represented by*

$$\mathbf{B}_{\psi_\gamma(s)} = \mathbf{Y}_s^\top \mathbf{Q}_{\psi_\gamma(s)} \in \mathbb{F}_q^{1 \times \gamma}. \tag{12}$$

We also define strongly linear PIR, which requires the linearity also for the reconstruction of the targeted file.

Definition 3.7 (Strongly Linear PIR [9]): A linear PIR scheme is called strongly linear *if there exist linear maps $\{f_{i,j} | (i,j) \in [\beta] \times [\mathsf{k}]\}$ such that*

$$\mathbf{X}_j^i = f_{i,j}\Big((\mathbf{B}_{(s-1)\gamma + t_{i,j}} | s \in [\mathsf{n}])\Big) \text{ for some } t_{i,j} \in [\gamma].$$

One of our main results is on the MDS-QPIR capacity induced from strongly linear PIR. The capacity of strongly linear PIR is derived in [9] as follows.

Proposition 3.1 ([9], [10]): The zero-error capacity of any strongly linear PIR with $[\mathsf{n}, \mathsf{k}]$-MDS coded storage and t colluding servers is

$$\sup \frac{\mathsf{k}\beta \log q}{\sum_{i=1}^{\mathsf{n}} H(B_i)} = 1 - \frac{\mathsf{k} + \mathsf{t} - 1}{\mathsf{n}} \tag{13}$$

for any number of files m.

B. Quantum PIR (QPIR)

1) QPIR From MDS-Coded Storage: We formally define a QPIR scheme with MDS-coded storage (MDS-QPIR), depicted in Figure 1.

Distributed Storage The same as classical PIR.

Shared Entanglement The initial state of the n servers is given as a density matrix σ_{init} on quantum system $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{\mathsf{n}}$, where $\mathcal{H}_s$ is distributed to server s. The state σ_{init} is possibly entangled.

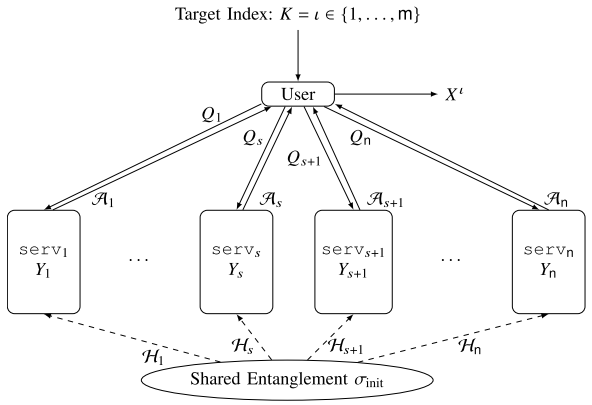

Fig. 1. Quantum private information retrieval scheme.

Query The same as classical PIR.

Response Each server s applies a CPTP map $\mathsf{Enc}_{\mathrm{serv}_s}[Q_s^K, Y_s]$ from $\mathcal{H}_s$ to $\mathcal{A}_s$ depending on Q_s^K and Y_s, where $\mathcal{A}_s$ is a d-dimensional quantum system, and returns $\mathcal{A}_s$ to the user.

Decoding Depending on K and Q^K, the user applies a POVM $\mathsf{Dec}[K, Q^K]$ on $\mathcal{A} = \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_\mathsf{n}$ and obtains the measurement outcome $\hat{X}^K$.

As described above, an MDS-QPIR scheme Φ is defined as $\Phi = (\mathcal{C}, \sigma_{\text{init}}, \mathsf{Enc}_{\text{user}}, \mathsf{Enc}_{\text{serv}}, \mathsf{Dec})$ with the MDS code for storage $\mathcal{C}$, the initial state σ_{init}, the query encoder of the user $\mathsf{Enc}_{\text{user}}$, the answer encoders of the servers $\mathsf{Enc}_{\text{serv}} := \{\mathsf{Enc}_{\mathrm{serv}_s} | \forall s \in [\mathsf{n}]\}$, and the decoding measurement of the user Dec.

Definition 3.8: The correctness, privacy, rate, and capacity of QPIR are defined in the same way as Definitions 3.1, 3.2, 3.3, and 3.5, respectively, except that (10) *and* (11) *are replaced as*

$$I(\mathcal{A}; X | Q^\iota, K = \iota) = H(X^\iota), \tag{14}$$

and

$$R(\Phi) = \frac{H(X^i)}{\sum_{j=1}^{\mathsf{n}} \log \dim \mathcal{A}}. \tag{15}$$

Notation 3.1: We denote by $C_{\mathsf{m},\epsilon}^{[\mathsf{n},\mathsf{k},\mathsf{t}]}$ *(*$C_{\mathsf{m},\epsilon}^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathsf{s}}$*) the* ϵ-error $[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-QPIR ($[\mathsf{n}, \mathsf{k}, \mathsf{t}]$-QSPIR) capacity with m files.

In Definition 3.2, user t-secrecy is defined as the independence of the index K and the queries $Q_\mathcal{T}$ of the colluding servers. Although this user secrecy condition is natural in classical PIR, one may be unsure whether this condition is sufficient for the QPIR setting because the servers share quantum entanglement. To justify this condition in the QPIR setting, we consider the malicious scenario where the servers apply malicious operations on the answered systems in order to extract the information of the user's request K. Even in this malicious scenario, the servers cannot exploit entanglement to break the user's secrecy because of the no-signaling principle [33]. No-signaling principle states that two parties sharing an entangled state cannot communicate any information from their local measurements. From this principle, even if the colluding servers share entanglement with the other servers or the user throughout the scheme, the only information obtained by the colluding servers is the queries $Q_\mathcal{T}$. Thus, the user t-secrecy condition guarantees the secrecy of K from the colluding servers.

2) Example of QPIR Scheme: With stabilizer formalism, we give an example of two-server QPIR, which corresponds to the QPIR scheme in [21]. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two-dimensional quantum systems, which are also called *qubits*. From Proposition 2.1, we define a stabilizer on $\mathcal{H}_1 \otimes \mathcal{H}_2$ with the self-orthogonal subspace

$$\mathcal{V} = \{(0,0,0,0), (1,1,0,0), (0,0,1,1), (1,1,1,1)\} \subset \mathbb{F}_2^4.$$

The space $\mathcal{V}$ satisfies $\mathcal{V} = \mathcal{V}^{\perp_\mathsf{s}}$. With this stabilzer, we set the initial entangled state of the two servers as $|\overline{\mathbf{0}}\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\overline{\mathbf{s}} = \mathbf{s} + \mathcal{V}^{\perp_\mathsf{s}}$ for all $\mathbf{s} \in \mathbb{F}_2^4$. The two servers have $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. The files are prepared as $\mathbf{m}_i = (m_{iX}, m_{iZ}) \in \mathbb{F}_2^2$ for all $i \in [\mathsf{m}]$. For querying the k-th file, the user sends queries

$$\mathbf{q}_1 = (\mathbf{e}_k, \mathbf{e}_k) + \mathbf{r} \in \mathbb{F}_2^{2\mathsf{m}}, \tag{16}$$

$$\mathbf{q}_2 = \mathbf{r} \in \mathbb{F}_2^{2\mathsf{m}}, \tag{17}$$

where $\mathbf{e}_k$ is the k-th standard vector in $\mathbb{F}_2^\mathsf{m}$ and $\mathbf{r}$ is a random vector in $\mathbb{F}_2^{2\mathsf{m}}$. After receiving queries, the servers generates

$$(a_1, b_1) = \mathbf{q}_1 \cdot \mathbf{m} = \mathbf{m}_k + \mathbf{r} \cdot \mathbf{m}, \tag{18}$$

$$(a_2, b_2) = \mathbf{q}_2 \cdot \mathbf{m} = \mathbf{r} \cdot \mathbf{m}, \tag{19}$$

where $\mathbf{m} = ((m_{1X}, m_{2X}, \ldots, m_{\mathsf{m}X}), (m_{1Z}, m_{2Z}, \ldots, m_{\mathsf{m}Z})) \in \mathbb{F}_2^{2\mathsf{m}}$. Then, the server i applies $\mathsf{X}(a_i)\mathsf{Z}(b_i)$ on $\mathcal{H}_i$ and sends $\mathcal{H}_i$ to the user. The user receives the states

$$\tilde{\mathbf{W}}(a_1, a_2, b_1, b_2)|\overline{\mathbf{0}}\rangle = |\overline{(a_1, a_2, b_1, b_2)}\rangle \tag{20}$$

$$= |\overline{(m_{kX}, 0, m_{kZ}, 0)}\rangle, \tag{21}$$

where the first equality follows from (6) and the second equality follows from $(1,1,1,1) \in \mathcal{V}^{\perp_\mathsf{s}} = \mathcal{V}$. By applying measurement on the received state, the user retrieves $\mathbf{m}_k = (m_{kX}, m_{kZ}) \in \mathbb{F}_2^2$ correctly. The user secrecy is satisfied from the query structure, and the server secrecy is satisfied because the user's state only depends on $\mathbf{m}_k$ as in (21). The QPIR rate is 1 because 2 bits are retrieved and 2 qubits are downloaded.

3) Classes of QPIR: As a general class of QPIR schemes, we introduce a new class called stabilizer QPIR, which includes the example in Section III-B.2 and most of the known multi-server QPIR schemes [21]–[24].

Definition 3.9 (Stabilizer QPIR): A QPIR scheme is called a stabilizer QPIR induced from a classical PIR scheme Φ_C *if*

- *the initial state of the servers* σ_{init} *is a state in* $\mathcal{H}_{\overline{\mathbf{0}}}^{\mathcal{V}} = |\overline{\mathbf{0}}\rangle \otimes \mathbb{C}^{q^{\mathsf{n}-d}} \subset \mathcal{H}^{\otimes \mathsf{n}}$ *defined with a self-orthogonal subspace* $\mathcal{V}$ *by Proposition 2.2,*
- *the query is the same as* Φ_C*, and*
- *the* s*-th server's operation is the Weyl operation* $\mathsf{X}(a_s)\mathsf{Z}(b_s)$*, where* $(a_s, b_s) \in \mathbb{F}_q^2$ *is the* s*-th server's answer of* Φ_C*.*

In Section V, we construct a stabilizer QPIR scheme, which achieves the capacities in Corollaries 4.1 and 4.2.

Further, we define a more general class of QPIR as follows.

TABLE II
SUMMARY OF SYMBOLS

Symbol	Description
n	Number of servers / Length of a code
k	Dimension of $[\mathsf{n},\mathsf{k}]$-MDS code
t	Number of colluding servers / Dimension of query code
$(i),\mathsf{m}$	(Index running over) Number of files
d	Dimension of the answer $\mathcal{A}_s$ $(\forall s \in [\mathsf{n}])$
$(b),\beta$	(Index running over) Number of stripes in a file
$(r),\rho$	(Index running over) Number of rounds
p,s	Indices of pair and server, respectively
$\mathcal{C},\mathcal{D},\mathcal{S}$	Storage, query and star-product codes
$(\sigma),\mathcal{H}$	(State of) Quantum system
$\mathcal{V}$	Self-orthogonal subspace of $\mathbb{F}_q^{2\mathsf{n}}$
X,Z	Pauli operators
$\mathbf{X},\mathbf{Y}$	Matrices of files and encoded symbols
$\mathbf{Z},\mathbf{B}$	Matrices of queries and responses
Φ_C,Φ	Classical, quantum PIR scheme

Definition 3.10 (Dimension-Squared QPIR): A QPIR scheme is said to be dimension-squared *if the s-th server's operation is determined by classical information $B_s \in \mathcal{B}_s$ with $|\mathcal{B}_s| \leq \mathsf{d}^2$ for all $s \in [\mathsf{n}]$.*

Furthermore, if $B = (B_1,\ldots,B_{\mathsf{n}})$ is the answer of a classical PIR scheme Φ_C and the query of the QPIR scheme is the same as Φ_C, the QPIR scheme is called a dimension-squared QPIR induced from the classical PIR scheme Φ_C.

Any stabilizer QPIR scheme is a dimension-squared scheme induced from a classical PIR scheme. Accordingly, the example in Section III-B.2 and the multi-server QPIR schemes [21]–[24] are also dimension-squared schemes induced from strongly linear schemes. In Section VI, we derive the converse bound for dimension-squared QPIR schemes.

When a classical PIR scheme Φ_C induces a QPIR scheme without the condition of dimensions, then the scheme can be modified to induce dimension-squared QPIR in the following way. First, we make the n answers the same size by repeating Φ_C multiple times while reordering the roles of the servers for all possible cases. Let d' be the size of one answer and Φ'_C be the repeated PIR scheme. Again, let Φ''_C be the PIR scheme made by repeating Φ'_C d' times, and then, the size of each answer of Φ''_C is $(\mathsf{d}')^2$. Thus, a dimension-squared QPIR scheme Φ_Q is induced from Φ''_C if Φ_Q can be made to satisfy the correctness condition. For convenience, we consider a dimension-squared QPIR scheme induced from Φ''_C as induced from Φ_C.

Notation 3.2: We denote by $C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},\epsilon,\mathrm{stab}}$, $C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},\epsilon,\mathrm{dim}}$ ($C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},\epsilon,\mathrm{stab}}$, $C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},\epsilon,\mathrm{dim}}$) the ϵ-error $[\mathsf{n},\mathsf{k},\mathsf{t}]$-QPIR ($[\mathsf{n},\mathsf{k},\mathsf{t}]$-QSPIR) capacities of stabilizer QPIR induced from strongly linear PIR and dimension-squared QPIR induced from strongly linear PIR.

From the definitions, the capacities are decreasing for t and increasing for ϵ, and satisfy

$$\begin{array}{ccccc} C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},\epsilon,\mathrm{stab}} & \leq & C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},\epsilon,\mathrm{dim}} & \leq & C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},\epsilon} \\ \wedge & & \wedge & & \wedge \\ C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},\epsilon,\mathrm{stab}} & \leq & C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},\epsilon,\mathrm{dim}} & \leq & C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},\epsilon}. \end{array} \tag{22}$$

IV. MAIN RESULTS

In this section, we give our two main results of the paper. The first result is the asymptotic capacity of stabilizer QPIR and dimension-squared QPIR induced from strongly linear PIR. The second result is the general asymptotic capacity without collusion, i.e., the case $\mathsf{t} = 1$. Before our capacity result, we state a general upper bound of dimension-squared QPIR capacity.

Theorem 4.1 (Converse for Dimension-Squared QPIR Induced From Classical PIR): Let A be a set of assumptions on classical PIR and $C_\epsilon[A]$ be the ϵ-error capacity of the classical PIR with assumptions A. Then, for any $\epsilon' \in [0,1)$, the ϵ'-error capacity of dimension-squared QPIR induced from classical ϵ-error PIR with the assumptions A is upper bounded by $\min\{1, 2C_\epsilon[A]\}$.

Theorem 4.1 will be proved in Section VI-A. Notice that Theorem 4.1 is proved for dimension-squared QPIR induced from any classical PIR class. Intuitively, the dimensional condition in the dimension-squared QPIR is the key factor for doubling the capacity of any classical PIR. On the other hand, it should be noted that classical PIR schemes do not necessarily induce QPIR schemes, *i.e.*, the existence and the construction of QPIR induced from the classical PIR is not trivial as discussed in Section I-A.

Our first capacity result is on the capacities of stabilizer QPIR and dimension-squared QPIR induced from strongly linear PIR. An upper bound of the capacities $C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},\epsilon,\mathrm{dim}}$ and $C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},\epsilon,\mathrm{dim}}$ is derived by Theorem 4.1 and Proposition 3.1 as

$$C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},0,\mathrm{dim}}, C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},0,\mathrm{dim}} \leq 2\left(1 - \frac{\mathsf{k}+\mathsf{t}-1}{\mathsf{n}}\right). \tag{23}$$

Furthermore, we prove the following theorem in Section V.

Theorem 4.2 (Achievability): Let $\mathsf{n},\mathsf{k},\mathsf{t}$ be positive integers with $1 \leq \mathsf{n}/2 \leq \mathsf{k}+\mathsf{t}-1 < \mathsf{n}$. There exists a stabilizer QPIR scheme induced from strongly linear PIR with $[\mathsf{n},\mathsf{k}]$-MDS coded storage and t-colluding servers achieving (23) *with equality for any number of files m and without error.*

Combining Eqs. (22), (23), and Theorem 4.2, we obtain the first capacity result.

Corollary 4.1 (MDS-Q(S)PIR Capacity With Colluding Servers): Let $\mathsf{n},\mathsf{k},\mathsf{t}$ be positive integers such that $1 \leq \mathsf{k} \leq \mathsf{n}$ and $1 \leq \mathsf{t} < \mathsf{n}$. Then, for any $C_{\mathsf{m},0} \in \{C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},0,\mathrm{stab}}, C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},0,\mathrm{stab}}, C^{[\mathsf{n},\mathsf{k},\mathsf{t}]}_{\mathsf{m},0,\mathrm{dim}}, C^{[\mathsf{n},\mathsf{k},\mathsf{t}],\mathrm{s}}_{\mathsf{m},0,\mathrm{dim}}\}$,

$$C_{\mathsf{m},0} = \begin{cases} 1 & \text{if } \mathsf{k}+\mathsf{t}-1 \leq \mathsf{n}/2, \\ 2\left(1 - \dfrac{\mathsf{k}+\mathsf{t}-1}{\mathsf{n}}\right) & \text{otherwise}. \end{cases} \tag{24}$$

In Corollary 4.1, the case for $\mathsf{k}+\mathsf{t}-1 \leq \mathsf{n}/2$ is proved as follows. When $\mathsf{k}+\mathsf{t}-1 = \mathsf{n}/2$, Theorem 4.2 proves the rate 1 is achievable. If $\mathsf{t} \leq \mathsf{t}'$, the QPIR scheme for t' colluding servers also has the user secrecy against t colluding servers. Therefore, when $\mathsf{k}+\mathsf{t}-1 \leq \mathsf{n}/2$, we can apply the scheme for $\mathsf{k}+\mathsf{t}'-1 = \mathsf{n}/2$ with n even to achieve the rate 1. Finally, the tightness of the rate 1 follows trivially from definition. If n is odd, we just consider $\mathsf{n}-1$ servers and $\mathsf{t} = (\mathsf{n}+1)/2 - \mathsf{k}$ in order to achieve rate 1.

As the second result, when no servers collude, *i.e.*, $\mathsf{t} = 1$, we prove the general asymptotic capacity theorem. Without

the assumption of dimension-squared QPIR, we prove the following upper bound of QPIR.

Theorem 4.3 (Converse of QPIR Without Collusion): Let n, k *be positive integers with* $1 \leq \mathsf{n}/2 \leq \mathsf{k} < \mathsf{n}$. *Then, we have*

$$\lim_{\epsilon \to 0} \lim_{\mathsf{m} \to \infty} C_{\mathsf{m},\epsilon}^{[\mathsf{n},\mathsf{k},1]} \leq 2\left(1 - \frac{\mathsf{k}}{\mathsf{n}}\right). \tag{25}$$

Theorem 4.3 will be proved in Section VI-A. Combining Eq. (22), Theorem 4.3, and Theorem 4.2 for the case $\mathsf{t} = 1$, we obtain the second capacity result.

Corollary 4.2 (MDS-Q(S)PIR Capacity): Let n, k *be positive integers such that* $1 \leq \mathsf{k} \leq \mathsf{n}$. *For any* $C_{\mathsf{m},\epsilon} \in \{C_{\mathsf{m},\epsilon,\text{stab}}^{[\mathsf{n},\mathsf{k},1]}, C_{\mathsf{m},\epsilon,\text{stab}}^{[\mathsf{n},\mathsf{k},1],\text{s}}, C_{\mathsf{m},\epsilon,\text{dim}}^{[\mathsf{n},\mathsf{k},1]}, C_{\mathsf{m},\epsilon,\text{dim}}^{[\mathsf{n},\mathsf{k},1],\text{s}}, C_{\mathsf{m},\epsilon}^{[\mathsf{n},\mathsf{k},1]}, C_{\mathsf{m},\epsilon}^{[\mathsf{n},\mathsf{k},1],\text{s}}\}$,

$$\lim_{\epsilon \to 0} \lim_{\mathsf{m} \to \infty} C_{\mathsf{m},\epsilon} = \begin{cases} 1 & \text{if } \mathsf{k} \leq \mathsf{n}/2, \\ 2\left(1 - \dfrac{\mathsf{k}}{\mathsf{n}}\right) & \text{otherwise}. \end{cases} \tag{26}$$

In Corollary 4.2, the smallest capacity in the six capacities is $C_{\mathsf{m},\epsilon,\text{stab}}^{[\mathsf{n},\mathsf{k},1],\text{s}}$ from (22), and this value is asymptotically lower bounded by the RHS of (26) from Theorem 4.2. On the other hand, the greatest capacity is $C_{\mathsf{m},\epsilon}^{[\mathsf{n},\mathsf{k},1]}$, which is upper bounded by the RHS of (26) from Theorem 4.3.

V. Achievability

We will frequently deal with $\mathsf{m}\beta \times 2\mathsf{n}$ matrices, where sub-blocks of β rows and the pair of columns s and $\mathsf{n}+s$ semantically belong together. We therefore index such a matrix $\mathbf{Y}$ by two pairs of indices (i,b), $i \in [\mathsf{m}]$, $b \in [\beta]$ and (p,s), $p \in [2]$, $s \in [\mathsf{n}]$, where $\mathbf{Y}_{p,s}^{i,b}$ denotes the symbol in row $(i-1)\beta + b$ and column $(p-1)\mathsf{n} + s$, *i.e.*, the symbol in the b-th row of the i-th sub-block of rows and the s-th column of the p-th sub-block of columns. Omitting of an index implies that we take all positions, *i.e.*, $\mathbf{Y}^i$ denotes the i-th sub-block of β rows, $\mathbf{Y}^{i,b}$ the row $(i-1)\beta + b$, $\mathbf{Y}_p$ the p-th sub-block of n columns, and $\mathbf{Y}_{p,s}$ the column $(p-1)\mathsf{n}+s$. For the reader's convenience, we sometimes imply the separation of the sub-blocks of columns by a vertical bar in the following. We denote by $\mathbf{e}_\gamma^\lambda$ the standard basis column vector of length λ in $\mathbb{F}_q^\lambda$ with a 1 in position $\gamma \in [\lambda]$. Given $a \in [\alpha]$, $b \in [\beta]$, it will help our notation to call *coordinate* (a,b) the position $\beta(a-1)+b$ in a vector of length $\alpha\beta$. For instance, $\mathbf{e}_{(2,1)}^{2\cdot 3} = \mathbf{e}_4^6 = (0,0,0,1,0,0)$. For a zero matrix $\mathbf{0}$ and matrices $\mathbf{M}_1, \mathbf{M}_2 \in \mathbb{F}_q^{\mu \times \nu}$

$$\operatorname{diag}(\mathbf{M}_1, \mathbf{M}_2) = \begin{pmatrix} \mathbf{M}_1 \mathbf{0} \\ \mathbf{0} \mathbf{M}_2 \end{pmatrix} \in \mathbb{F}_q^{2\mu \times 2\nu}.$$

For a matrix $\mathbf{M}$, the space spanned by the rows of $\mathbf{M}$ is denoted by $\langle \mathbf{M} \rangle_{\mathsf{row}}$.

For two vectors $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^{\mathsf{n}}$ we define the (Hadamard-) star-product as $\mathbf{c} \star \mathbf{d} = (c_1 d_1, c_2 d_2, \ldots, c_{\mathsf{n}} d_{\mathsf{n}})$. For two codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}^{\mathsf{n}}$ we denote $\mathcal{C} \star \mathcal{D} = \langle \{\mathbf{c} \star \mathbf{d} \mid \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{D}\} \rangle$. Observe that, as the star-product is an element-wise operation, we have

$$(\mathcal{C} \times \mathcal{C}) \star (\mathcal{D} \times \mathcal{D}) = (\mathcal{C} \star \mathcal{D}) \times (\mathcal{C} \star \mathcal{D}). \tag{27}$$

A. Generalized Reed–Solomon Codes

We consider systems encoded with (the Cartesian product of) Generalized Reed–Solomon (GRS) codes (cf. [34, Ch. 10]), a popular class of MDS codes.

Definition 5.1: Let $\mathcal{L} = \{\alpha_i \in \mathbb{F}_q : i \in [n]\}$ *and* $\mathcal{M} = \{\beta_i \in \mathbb{F}_q : i \in [n]\}$ *be the sets of the* code locators *and of the* column multipliers, *respectively. The* Generalized Reed–Solomon *(GRS) code* $\mathcal{C}$ *of dimension* k *is given by*

$$\mathcal{C} = \{(\beta_1 f(\alpha_1), \ldots, \beta_n f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\}.$$

Among coded storage systems, these have proven to be particularly well-suited for PIR and general schemes exist for a wide range of parameters [11], [12], [35]. The key idea is to design the queries such that the retrieved symbols are the sum of a codeword of another GRS code (of higher dimension), which we refer to as the *star-product code*, plus a vector depending only on the desired file. To obtain the desired file, the codeword part is projected to zero, leaving only the desired part of the responses. In the QPIR system we consider in the following, this projection is part of the quantum measurement. This imposes a constraint on this star-product code, namely, that the code is (weakly) self-dual. In the following, we collect/establish the required theoretical results on GRS codes and their star-products.

Definition 5.2 (Weakly Self-Dual Code): We say that an $[\mathsf{n}, \mathsf{k}]$ *code* $\mathcal{C}$ *is* weakly self-dual *if* $\mathcal{C}^\perp \subseteq \mathcal{C}$ *and* self-dual *if* $\mathcal{C}^\perp = \mathcal{C}$. *It is easy to see that any such code with parity-check matrix* $\mathbf{H}$ *has a generator matrix of the form* $\mathbf{G} = (\mathbf{H}^\top \ \mathbf{F}^\top)^\top$ *for some* $(2\mathsf{k} - \mathsf{n}) \times \mathsf{n}$ *matrix* $\mathbf{F}$.

Lemma 5.1 (Follows From [36, Theorem 3]): For $q = 2^r$ *there exist self-dual GRS* $[2\mathsf{k}, \mathsf{k}]$ *codes over* $\mathbb{F}_q$ *for any* $\mathsf{k} \in [2^{r-1}]$ *and code locators* $\mathcal{L}$.

Lemma 5.2: Let q *be even with* $q \geq \mathsf{n}$. *Then there exists a weakly self-dual* $[\mathsf{n}, \mathsf{k}]$ *GRS code* $\mathcal{C}$ *for any integer* $\mathsf{k} \geq \frac{\mathsf{n}}{2}$ *and code locators* $\mathcal{L}$.

Proof: First consider the case of even n. Let $\mathcal{S}$ be an $[\mathsf{n}, \mathsf{n}/2]$ self-dual GRS code with code locators $\mathcal{L} \subseteq \mathbb{F}_q$, as shown to exist in [36, Theorem 3] (see Lemma 5.1). It is easy to see that this code is a subcode of the $[\mathsf{n}, \mathsf{k}]$ GRS code $\mathcal{C}$ with the same locators and column multipliers. The property $\mathcal{C}^\perp \subset \mathcal{C}$ follows directly from observing that $\mathcal{C}^\perp \subseteq \mathcal{S}^\perp = \mathcal{S} \subseteq \mathcal{C}$.

Now consider the case of odd n. First, observe that this implies $\mathsf{n} < q$ and $\lceil \frac{\mathsf{n}}{2} \rceil = \frac{\mathsf{n}+1}{2}$. Then, by Lemma 5.1, there exists a self-dual $[\mathsf{n}+1, \lceil \frac{\mathsf{n}}{2} \rceil]$ GRS code $\mathcal{S}'$ with code locators $\mathcal{L}' = \mathcal{L} \cup \{\alpha\}$, where $\alpha \in \mathbb{F}_q \setminus \mathcal{L}$. Let $j \in [\mathsf{n}+1]$ be the index of the position corresponding to α. Now consider the code $\mathcal{C}$ obtained from puncturing this position j, *i.e.*, the set

$$\mathcal{S} = \{\mathbf{c}_{[\mathsf{n}+1] \setminus \{j\}} \mid \mathbf{c} \in \mathcal{S}'\}.$$

It is well-known that the operation dual to puncturing is shortening and therefore the corresponding $[\mathsf{n}, \lceil \frac{\mathsf{n}}{2} \rceil - 1]$ dual code $\mathcal{S}^\perp$ is given by

$$\begin{aligned} \mathcal{S}^\perp &= \{\mathbf{c}_{[\mathsf{n}+1] \setminus \{j\}} \mid c_j = 0, \mathbf{c} \in (\mathcal{S}')^\perp\} \\ &= \{\mathbf{c}_{[\mathsf{n}+1] \setminus \{j\}} \mid c_j = 0, \mathbf{c} \in \mathcal{S}'\}. \end{aligned}$$

Clearly, this operation preserves the weak duality, *i.e.*, $\mathcal{S}^\perp \subset \mathcal{S}$. Again, it is easy to see that $\mathcal{S}$ is a subcode of the $[\mathsf{n}, \mathsf{k}]$

GRS code $\mathcal{C}$ with the same locators and column multipliers for any $\mathsf{k} \geq \frac{\mathsf{n}}{2}$. The statement follows from observing that we have $\mathcal{C}^{\perp} \subseteq \mathcal{S}^{\perp} \subset \mathcal{S} \subseteq \mathcal{C}$ □

Lemma 5.3: Let q be even with $q \geq n$. For any $[\mathsf{n}, \mathsf{k}]$ GRS code $\mathcal{C}$ there exists an $[\mathsf{n}, \mathsf{t}]$ GRS code $\mathcal{D}$ such that their star-product $\mathcal{S} = \mathcal{C} \star \mathcal{D}$ is an $[\mathsf{n}, \mathsf{k}+\mathsf{t}-1]$ weakly self-dual GRS code.

Proof: By [37] the star product between an $[\mathsf{n}, \mathsf{k}]$ GRS code $\mathcal{C}$ with column multipliers $\mathcal{M}_{\mathcal{C}}$ and an $[\mathsf{n}, \mathsf{t}]$ GRS code $\mathcal{D}$ with column multipliers $\mathcal{M}_{\mathcal{D}}$, both with the same locators $\mathcal{L}$, is the $[\mathsf{n}, \mathsf{k}+\mathsf{t}-1]$ GRS code with column multipliers $\mathcal{M}_{\mathcal{C}} \star \mathcal{M}_{\mathcal{D}}$ and code locators $\mathcal{L}$. Denote by $\mathcal{M}_{\mathcal{S}}$ the column multipliers of a weakly-self dual $[\mathsf{n}, \mathsf{k}+\mathsf{t}-1]$ GRS code with code locators $\mathcal{L}$, as shown to exist in Lemma 5.2. Then, the lemma statement follows from setting $\mathcal{M}_{\mathcal{D}} = (\mathcal{M}_{\mathcal{C}})^{-1} \star \mathcal{M}_{\mathcal{S}}$, where we denote by $(\mathcal{M}_{\mathcal{C}})^{-1}$ the element-wise inverse of $\mathcal{M}_{\mathcal{C}}$. □

B. Description of the Coded QPIR Scheme

In this subsection we describe the required preliminaries for the capacity-achieving QPIR scheme. Afterwards, we give a compact list of the steps followed by the protocol.

1) Storage: We consider a linear code $\mathcal{C}$ of length $2\mathsf{n}$ and dimension $2\mathsf{k}$, which is the Cartesian product of an $[\mathsf{n}, \mathsf{k}]$ GRS code $\mathcal{C}'$ over $\mathbb{F}_q$ with itself,[2] *i.e.*, $\mathcal{C} = \mathcal{C}' \times \mathcal{C}'$. It therefore has a generator matrix $\mathbf{G}_{\mathcal{C}} = \operatorname{diag}(\mathbf{G}_{\mathcal{C}'}, \mathbf{G}_{\mathcal{C}'})$, where $\mathbf{G}_{\mathcal{C}'}$ is a generator matrix of $\mathcal{C}'$. The $\mathsf{m}\beta \times 2\mathsf{n}$ matrix of encoded files is given by $\mathbf{Y} = \mathbf{X} \cdot \mathbf{G}_{\mathcal{C}}$. Server $s \in [\mathsf{n}]$ stores columns s and $\mathsf{n}+s$ of $\mathbf{Y}$, *i.e.*, it stores $\mathbf{Y}_{1,s}$ and $\mathbf{Y}_{2,s}$ (for an illustration see Figure 2). For a given integer c, which will be defined in the next paragraph, the parameter β is fixed to $\beta = \operatorname{lcm}(c, \mathsf{k})/\mathsf{k}$.

2) Query and Star-Product Code: Let t be the collusion parameter with $\frac{\mathsf{n}}{2} \leq \mathsf{k}+\mathsf{t}-1 < \mathsf{n}$. By Lemma 5.3 there exists an $[\mathsf{n}, \mathsf{t}]$ GRS code $\mathcal{D}'$ such that $\mathcal{S}' = \mathcal{C}' \star \mathcal{D}'$ is an $[\mathsf{n}, \mathsf{k}+\mathsf{t}-1]$ weakly self-dual GRS code. We define the query code as the Cartesian product $\mathcal{D} = \mathcal{D}' \times \mathcal{D}'$. Thus, for a generator matrix $\mathbf{G}_{\mathcal{D}'}$ of $\mathcal{D}'$, the matrix $\mathbf{G}_{\mathcal{D}} = \operatorname{diag}(\mathbf{G}_{\mathcal{D}'}, \mathbf{G}_{\mathcal{D}'}) \in \mathbb{F}_q^{2\mathsf{t} \times 2\mathsf{n}}$ is a generator matrix of $\mathcal{D}$.

Define $\mathcal{S} = \mathcal{C} \star \mathcal{D}$ and $\mathcal{S}' = \mathcal{C}' \star \mathcal{D}'$. By (27) we have $\mathcal{S} = \mathcal{C} \star \mathcal{D} = \mathcal{S}' \times \mathcal{S}'$, so $\mathcal{S}$ is the Cartesian product of two star product codes. Define $c = d_{\mathcal{S}'} - 1$, where $d_{\mathcal{S}'} = \mathsf{n}-\mathsf{k}-\mathsf{t}+2$ is the minimum distance of $\mathcal{S}'$.

Let $\mathbf{H}_{\mathcal{S}'} \in \mathbb{F}_q^{(\mathsf{n}-\mathsf{k}-\mathsf{t}+1) \times \mathsf{n}}$ be a parity-check matrix of $\mathcal{S}'$. By Definition 5.2, the code $\mathcal{S}'$ has a generator matrix of the form $\mathbf{G}_{\mathcal{S}'} = (\mathbf{H}_{\mathcal{S}'}^{\top} \quad \mathbf{F}_{\mathcal{S}'}^{\top})^{\top}$ for some $\mathbf{F}_{\mathcal{S}'} \in \mathbb{F}_q^{[2(\mathsf{k}+\mathsf{t}-1)-\mathsf{n}] \times \mathsf{n}}$. Hence, $\mathcal{S}$ has a generator matrix of form

$$\mathbf{G}_{\mathcal{S}} = \begin{pmatrix} \operatorname{diag}(\mathbf{H}_{\mathcal{S}'}, \mathbf{H}_{\mathcal{S}'}) \\ \operatorname{diag}(\mathbf{F}_{\mathcal{S}'}, \mathbf{F}_{\mathcal{S}'}) \end{pmatrix} \in \mathbb{F}_q^{2(\mathsf{k}+\mathsf{t}-1) \times 2\mathsf{n}}. \tag{28}$$

Lemma 5.4: Let $\mathbf{G}_{\mathcal{S}}$ be the matrix defined in Eq. (28) *and let $\mathbf{H}_{\mathcal{S}}$ be the submatrix of $\mathbf{G}_{\mathcal{S}}$ containing its first $2(\mathsf{n}-\mathsf{k}-\mathsf{t}+1)$ rows. Let $\mathbf{w}_1, \ldots, \mathbf{w}_{2\mathsf{n}}$ be the column vectors of $\mathbf{G}_{\mathcal{S}}$. Then, they satisfy conditions (a) and (b) of [23, Lemma 2],* i.e.,

(a) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{k}+\mathsf{t}-1)}, \mathbf{w}_{\pi(1)+n}, \ldots, \mathbf{w}_{\pi(\mathsf{k}+\mathsf{t}-1)+n}$ *are linearly independent for any permutation π of* $[\mathsf{n}]$.

(b) $\mathbf{H}_{\mathcal{S}} \mathbf{J}^{\top} \mathbf{G}_{\mathcal{S}}^{\top} = \mathbf{0}$.

Proof: It is well-known that any subset of $\mathsf{k}+\mathsf{t}-1$ columns of the generator matrix of an $[\mathsf{n}, \mathsf{k}+\mathsf{t}-1]$ MDS code are linearly independent. Hence, the columns $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{k}+\mathsf{t}-1)}$ are linearly independent, as the first n columns of $\mathbf{G}_{\mathcal{S}}$ generate $\mathcal{S}$. The same holds for $\mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{k}+\mathsf{t}-1)+\mathsf{n}}$. Trivially, any non-zero columns of a diagonal matrix are linearly independent and property (a) follows.

Property (b) follows directly from observing that, by definition, $\mathbf{H}_{\mathcal{S}} \mathbf{G}_{\mathcal{S}}^{\top} = \mathbf{0}$ for any linear code with generator matrix $\mathbf{G}_{\mathcal{S}}$ and parity-check matrix $\mathbf{H}_{\mathcal{S}}$. □

Let $\mathcal{V}$ be the space spanned by the first $2(\mathsf{n}-\mathsf{k}-\mathsf{t}+1)$ rows of $\mathbf{G}_{\mathcal{S}}$, *i.e.*, $\mathcal{V} = \langle \operatorname{diag}(\mathbf{H}_{\mathcal{S}'}, \mathbf{H}_{\mathcal{S}'}) \rangle_{\mathsf{row}}$. By Lemma 5.4, the space $\mathcal{V}$ is self-orthogonal and the rows of $\mathbf{G}_{\mathcal{S}}$ span the space $\mathcal{V}^{\perp_{\mathbb{S}}}$. Notice that $\mathcal{V}$ is defined from a classical code $\mathcal{E} = \langle \mathbf{H}_{\mathcal{S}'} \rangle_{\mathsf{row}}$, which satisfies $\mathcal{E} \subset \mathcal{E}^{\perp_{\mathbb{S}}}$. Thus, the stabilizer $\mathcal{S}(\mathcal{V})$ defines a Calderbank–Steane–Shor (CSS) code [38], [39], which is defined from the self-orthogonal space $\langle \operatorname{diag}(\mathbf{G}_{\mathcal{C}_1}, \mathbf{G}_{\mathcal{C}_2}) \rangle_{\mathsf{row}}$ with the generator matrices $\mathbf{G}_{\mathcal{C}_1}$ and $\mathbf{G}_{\mathcal{C}_2}$ of two classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ satisfying $\mathcal{C}_1 \subset \mathcal{C}_2^{\perp_{\mathbb{S}}}$. Our QPIR scheme will be constructed with the CSS code.

3) Targeted Positions: Let $\rho = \operatorname{lcm}(c, \mathsf{k})/c$. Fix $\mathcal{J} = \{1, \ldots, \max\{c, \mathsf{k}\}\}$ to be the set of server indices from which the user obtains the symbols of $\mathbf{Y}^{\iota}$. We consider $\mathcal{J}_1 = [c] \subseteq \mathcal{J}$ and we partition it into subsets $\mathcal{J}_1^b = \{i + (b-1)c/\beta | i \in [c/\beta]\}$, $b \in [\beta]$. Then, for $r \in [2 : \rho]$ we define recursively $\mathcal{J}_r^b = \{(j + c/\beta - 1) \pmod{|\mathcal{J}|} + 1 | j \in \mathcal{J}_{r-1}^b\}$ and $\mathcal{J}_r = \bigcup_{b \in [\beta]} \mathcal{J}_r^b$. We will construct our scheme so that during the r-th iteration the user obtains the symbols $(\mathbf{Y}_{1,a}^{\iota,b}, \mathbf{Y}_{2,a}^{\iota,b})$ for every $a \in \mathcal{J}_r^b$ and $b \in [\beta]$.

We define

$$\mathbf{N}^{(r)} = (\mathbf{e}_a^{\mathsf{n}})_{a \in \mathcal{J}_r}^{\top} \in \mathbb{F}_q^{c \times \mathsf{n}}, \tag{29}$$

where $\mathbf{e}_a^{\mathsf{n}}$ is the standard basis column vector of length n with a 1 in position a. Then, the matrix $(\mathbf{G}_{\mathcal{S}}^{\top} \quad (\mathbf{M}^{(r)})^{\top})^{\top}$, with $\mathbf{M}^{(r)} = \operatorname{diag}(\mathbf{N}^{(r)}, \mathbf{N}^{(r)}) \in \mathbb{F}_q^{2c \times 2\mathsf{n}}$, is a basis for $\mathbb{F}_q^{2\mathsf{n}}$. To see that this is in fact a basis observe that the row span of $\mathbf{N}^{(r)}$, by definition, contains vectors of weight at most c. The span of $\mathbf{G}_{\mathcal{S}'}$ contains vectors of weight at least $d_{\mathcal{S}'} = c+1$. It follows that the spans of $\mathbf{N}^{(r)}$ and $\mathbf{G}_{\mathcal{S}'}$ intersect trivially, which implies that their ranks add up.

4) A Capacity-Achieving QPIR Scheme: In our scheme, we use the the stabilizer formalism for the transmission of the classical files. On the other hand, as discussed in Section II-D, the stabilizer formalism is often used for the transmission of quantum states, which is performed by four steps of the encoding of the state, transmission over the error channel, syndrome measurement, and error-correction. For the transmission of the classical files, similar to the QPIR scheme [23], we construct our scheme so that the desired file is extracted by the syndrome measurement of the stabilizer code. Then, by the same property as the superdense coding [40], our scheme can convey twice more classical information compared to the classical PIR schemes. We refer to [23, Sec. IV-B] for the detailed explanation of this idea.

[2]We choose this description of the storage code because this structure is required for the quantum PIR scheme. However, note that the system can equivalently be viewed as being encoded with an $[\mathsf{n}, \mathsf{k}]$ code over $\mathbb{F}_{q^2}$, where each of the servers stores one column of the resulting codeword matrix.

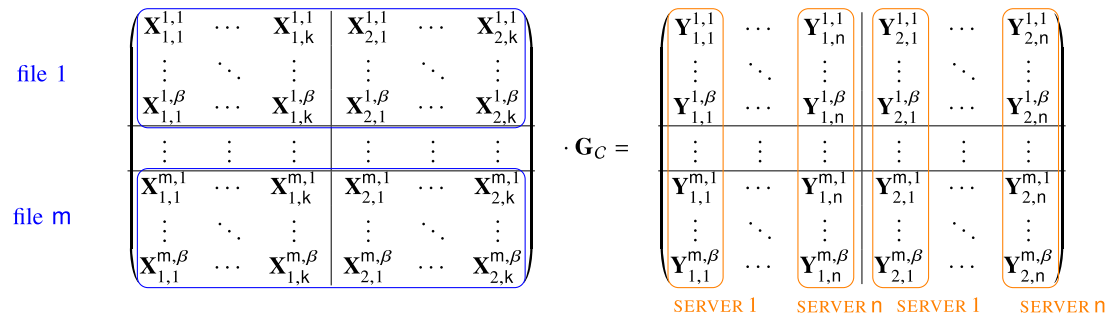

Fig. 2. Illustration of a DSS storing m files, each consisting of $2\beta\mathsf{k}$ symbols. The matrix $\mathbf{G}_{\mathcal{C}}$ is a generator matrix of a $[2\mathsf{n}, 2\mathsf{k}]$ code $\mathcal{C}$.

Suppose the desired file is $\mathbf{X}^{\iota}$. The queries are constructed so that the total response vector during one iteration is the sum of a codeword in $\mathcal{S}$ and a vector containing $2c$ distinct symbols of $\mathbf{Y}^{\iota}$ in known locations, and zeros elsewhere.

We now describe the five steps of the capacity-achieving QPIR scheme $\Phi^{\star}$.

Protocol 5.1: The first four steps are repeated in each round $r \in [\rho]$.

1) ***Distribution of entangled state.*** *Let $\mathcal{H}_1, \ldots, \mathcal{H}_{\mathsf{n}}$ be q-dimensional quantum systems, $\sigma_{\text{init}} = q^{\mathsf{n}-2(\mathsf{k}+\mathsf{t}-1)} \cdot \mathbf{I}_{q^{2(\mathsf{k}+\mathsf{t}-1)-\mathsf{n}}}$ and $\mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}} = \{\overline{\mathbf{w}} = \mathbf{w} + \mathcal{V}^{\perp_{\mathbb{S}}} : \mathbf{w} \in \langle \mathbf{M}^{(r)} \rangle_{\mathsf{row}}\}$. By Proposition 2.2.(b) the composite quantum system $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ is decomposed as $\mathcal{H} = \mathcal{W} \otimes \mathbb{C}^{q^{2(\mathsf{k}+\mathsf{t}-1)-\mathsf{n}}}$, where $\mathcal{W} = \operatorname{span}\{|\overline{\mathbf{w}}\rangle | \overline{\mathbf{w}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}\}$. The state of $\mathcal{H}$ is initialized as $|\overline{\mathbf{0}}\rangle\langle\overline{\mathbf{0}}| \otimes \sigma_{\text{init}}$ and distributed such that server $s \in [\mathsf{n}]$ obtains $\mathcal{H}_s$.*
2) ***Query.*** *The user chooses a matrix $\mathbf{Z}^{(r)} \in \mathbb{F}_q^{\mathsf{m}\beta \times 2\mathsf{t}}$ uniformly at random. We define $\mathbf{E}_{(\iota)} \in \mathbb{F}_q^{\mathsf{m}\beta \times 2c}$ with $\mathbf{E}_{(\iota),p,a} = \mathbf{e}^{\mathsf{m}\beta}_{(\iota,a)}$, $p \in [2]$, $a \in [c]$, where $\mathbf{e}^{\mathsf{m}\beta}_{(\iota,a)}$ is the standard basis column vector of length $\mathsf{m}\beta$ with a 1 in coordinate (ι, a). We denote by $\mathbf{Q}^{(r)} \in \mathbb{F}_q^{\mathsf{m}\beta \times 2\mathsf{n}}$ the matrix of all the queries, which are computed as*

$$\mathbf{Q}^{(r)} = \left(\mathbf{Z}^{(r)}\mathbf{E}_{(\iota)}\right) \cdot \begin{pmatrix} \mathbf{G}_{\mathcal{D}} \\ \mathbf{M}^{(r)} \end{pmatrix} = \mathbf{Z}^{(r)} \cdot \mathbf{G}_{\mathcal{D}} + \mathbf{E}_{(\iota)} \cdot \mathbf{M}^{(r)}. \tag{30}$$

   Each server $s \in [\mathsf{n}]$ receives two vectors $\mathbf{Q}^{(r)}_{1,s}$, $\mathbf{Q}^{(r)}_{2,s} \in \mathbb{F}_q^{\mathsf{m}\beta}$.
3) ***Response.*** *The servers compute the dot product of each column of their stored symbols and the respective column of the queries received,* i.e., *they compute the response $\mathbf{B}^{(r)}_{p,s} = \mathbf{Y}^{\top}_{p,s} \cdot \mathbf{Q}^{(r)}_{p,s} \in \mathbb{F}_q$, $s \in [\mathsf{n}]$, $p \in [2]$. Server s applies $\mathsf{X}\left(\mathbf{B}^{(r)}_{1,s}\right)$ and $\mathsf{Z}\left(\mathbf{B}^{(r)}_{2,s}\right)$ to its quantum system and sends it to the user.*
4) ***Measurement.*** *The user applies the PVM $\mathcal{B}^{\mathcal{V}} = \{\mathbf{P}_{\overline{\mathbf{w}}} | \overline{\mathbf{w}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathcal{V}^{\perp_{\mathbb{S}}}\}$ on $\mathcal{H}$ defined in Proposition 2.2 and obtains the output $\mathbf{o}^{(r)} \in \mathbb{F}_q^{2c}$.*
5) ***Retrieval.*** *Finally, after ρ rounds the user has retrieved $2\rho c = 2\beta\mathsf{k}$ symbols of $\mathbb{F}_q$ from which he can recover the desired file $\mathbf{X}^{\iota}$.*

C. Properties of the Coded QPIR Scheme

Lemma 5.5: The scheme $\Phi^{\star}$ of Section V-B is correct, i.e., *fulfills Definition 3.1.*

Proof: Let us fix the round $r \in [\rho]$ and let $\mathbf{B}^{(r)}$ be the vector of responses computed by the servers. By Prop. 2.2.(c) the state after the servers' encoding is

$$\mathsf{W}(\mathbf{B}^{(r)})(|\overline{\mathbf{0}}\rangle\langle\overline{\mathbf{0}}| \otimes \sigma_{\text{init}})\mathsf{W}(\mathbf{B}^{(r)})^{\dagger} = |\overline{\mathbf{B}^{(r)}}\rangle\langle\overline{\mathbf{B}^{(r)}}| \otimes \sigma_{\text{init}}.$$

We observe that $\mathcal{V}^{\perp_{\mathbb{S}}} = \mathcal{S}$ since both spaces are spanned by the rows of $\mathbf{G}_{\mathcal{S}}$. Notice that the row in coordinate (i, b) of the product $\mathbf{E}_{(\iota)} \cdot \mathbf{M}^{(r)}$ is $\sum_{p=1}^{2}\sum_{a\in\mathcal{J}_r^b} \delta_{i,\iota}(\mathbf{e}^{2\mathsf{n}}_{(p,a)})^{\top}$. Remembering that $\mathbf{e}^{2\mathsf{n}}_{(p,a)}$ is the standard basis column vector of length $2\mathsf{n}$ with a 1 in coordinate (p, a), by definition of the star product scheme the response vector is

$$\begin{aligned}
\mathbf{B}^{(r)} = \left(\mathbf{B}^{(r)}_1 \middle| \ \mathbf{B}^{(r)}_2\right) &= \sum_{i=1}^{\mathsf{m}}\sum_{b=1}^{\beta} \mathbf{Y}^{i,b} \star \mathbf{Q}^{(r),i,b} \\
&= \sum_{i=1}^{\mathsf{m}}\sum_{b=1}^{\beta} \left(\mathbf{X}^{i,b} \cdot \mathbf{G}_{\mathcal{C}}\right) \star \left(\mathbf{Z}^{(r),i,b} \cdot \mathbf{G}_{\mathcal{D}}\right) \\
&\quad + \sum_{i=1}^{\mathsf{m}}\sum_{b=1}^{\beta} \mathbf{Y}^{i,b} \star \Big(\sum_{a\in\mathcal{J}_r^b} \delta_{i,\iota}\left(\mathbf{e}^{2n}_{(1,a)} + \mathbf{e}^{2n}_{(2,a)}\right)^{\top} \Big) \\
&\in \mathcal{S} + \sum_{b=1}^{\beta}\sum_{a\in\mathcal{J}_r^b} \left(\mathbf{Y}^{\iota,b}_{1,a}\mathbf{e}^{2\mathsf{n}}_{(1,a)} + \mathbf{Y}^{\iota,b}_{2,a}\mathbf{e}^{2\mathsf{n}}_{(2,a)}\right)^{\top} \\
&= \mathcal{V}^{\perp_{\mathbb{S}}} + \left(\mathbf{Y}^{\iota,b}_{1,a} \middle| \ \mathbf{Y}^{\iota,b}_{2,a}\right)_{a\in\mathcal{J}_r^b, b\in[\beta]} \cdot \mathbf{M}^{(r)}.
\end{aligned} \tag{31}$$

The random part is encoded into a vector in $\mathcal{V}^{\perp_{\mathbb{S}}}$ while the vector $\left(\mathbf{Y}^{\iota,b}_{1,a} \mid \mathbf{Y}^{\iota,b}_{2,a}\right)_{a\in\mathcal{J}_r^b, b\in[\beta]} \in \mathbb{F}_q^{2c}$ is encoded with $\mathbf{M}^{(r)}$ and hence independent of the representative of $\overline{\mathbf{o}^{(r)}}$. Therefore, the user obtains the latter without error after measuring the quantum systems with the PVM $\mathcal{B}^{\mathcal{V}}$. Recall that we fixed $\beta = \operatorname{lcm}(c, \mathsf{k})/\mathsf{k}$ for $c = d_{\mathcal{S}'} - 1$. To allow the user to download exactly the desired file over ρ iterations, we defined $\rho = \operatorname{lcm}(c, \mathsf{k})/c$. During each iteration, the user can download $2c/\beta = 2\mathsf{k}/\rho$ symbols from each of the β rows of $\mathbf{Y}^{\iota}$, where the factor 2 is achieved by utilizing the properties of superdense coding [40]. After ρ rounds the user obtained the $2\mathsf{k}$ symbols $\mathbf{Y}^{\iota,b} \in \mathbb{F}_q^{2\mathsf{k}}$ of each codeword corresponding to a block $\mathbf{X}^{\iota,b}$, $b \in [\beta]$ and is therefore able to recover the file. □

Lemma 5.6: The scheme $\Phi^{\star}$ of Section V-B is symmetric and protects against t-collusion in the sense of Definition 3.2.

Proof: The idea is that user privacy is achieved since, for each subset of t servers, the corresponding joint distribution of queries is the uniform distribution over $\mathbb{F}_q^{\mathsf{m}\beta\times 2\mathsf{t}}$. Consider a set of t colluding servers. The set of queries these servers

receive is given by $\mathbf{Q}^{(r)}$ during round $r \in [\rho]$. By the MDS property of the code $\mathcal{D}$ any subset of t columns of $\mathbf{G}_{\mathcal{D}}$ is linearly independent. As the columns of $\mathbf{Z}^{(r)}$ are uniformly distributed and chosen independently for each $r \in [\rho]$, any subset of t columns of $\mathbf{Z}^{(r)} \cdot \mathbf{G}_{\mathcal{D}}$ is statistically independent and uniformly distributed. The sum of a uniformly distributed vector and an independently chosen vector is again uniformly distributed, and therefore adding the matrix $\mathbf{E}_{(\iota)} \cdot \mathbf{M}^{(r)}$ does not incur any dependence between any subset of t columns and the file index ι.

For each $r \in [\rho]$, server secrecy is achieved because in every round the received state of the user is $|\overline{\mathbf{B}^{(r)}}\rangle\langle\overline{\mathbf{B}^{(r)}}| \otimes \sigma_{\text{init}}$ with $\mathbf{B}^{(r)} = \left(\mathbf{Y}_{1,a}^{\iota,b} \mid \mathbf{Y}_{2,a}^{\iota,b}\right)_{a \in \mathcal{J}_r^b, b \in [\beta]}$ from (31) and this state is independent of $\mathbf{Y}^i$ with $i \neq \iota$. □

Unlike in the classical setting, the servers in the quantum setting do not need access to a source of shared randomness that is hidden from the user to achieve server secrecy. However, this should not be viewed as an inherent advantage since the servers instead share entanglement.

Theorem 5.1: The QPIR rate of the scheme in Section V-B is

$$R(\Phi^\star) = \frac{2(\mathsf{n} - \mathsf{k} - \mathsf{t} + 1)}{\mathsf{n}}$$

Proof: The user downloads $\rho\mathsf{n}$ quantum systems while retrieving $2\mathsf{k}\beta\log(q)$ bits of information, thus the rate is given by

$$\begin{aligned} R(\Phi^\star) &= \frac{2k\beta\log(q)}{\log(q^{\rho\mathsf{n}})} \\ &= \frac{2\rho c\log(q)}{\rho\mathsf{n}\log(q)} = \frac{2(\mathsf{n} - \mathsf{k} - \mathsf{t} + 1)}{\mathsf{n}}. \end{aligned}$$

□

The presented scheme is an adapted version of the star-product scheme of [12], which is strongly linear [10]. To see that the QPIR scheme is induced by this strongly linear scheme, it suffices to observe that for each $p \in [2]$ the second and third step in Protocol 5.1, up to the definition of the *classical* responses $\mathbf{B}_{p,s}^{(r)}$ with $s \in [\mathsf{n}]$, are the same as in the star-product scheme. Hence, these steps can be viewed as two parallel instances of the star-product scheme and it follows directly from Definition 3.7 that this scheme is strongly linear.

VI. Converse

In this section, we prove Theorem 4.1 and Theorem 4.3.

A. Proof of Theorem 4.1

Since the upper bound 1 is trivial, we prove the quantum capacity in Theorem 4.1 is upper bounded by $2C_\epsilon[A]$. Let Φ_C be an arbitrary classical PIR scheme with assumptions A and error probability ϵ, and $\Phi_Q[\Phi_C]$ be an arbitrary dimension-squared QPIR scheme induced from Φ_C with error probability ϵ'. The PIR rate of Φ_C is upper bounded as

$$\frac{\mathsf{k}\beta\log q}{\sum_{s=1}^{\mathsf{n}} H(B_s)} \leq C_\epsilon[A]. \tag{32}$$

From the definition of dimension-squared QPIR, we have $H(B_i) \leq 2\log\mathsf{d}$ for all $s \in [\mathsf{n}]$ for Φ_Q. Thus, the QPIR rate $R(\Phi_Q)$ is upper bounded as

$$R(\Phi_Q) = \frac{\mathsf{k}\beta\log q}{\mathsf{n}\log\mathsf{d}} \leq \frac{2\mathsf{k}\beta\log q}{\sum_{s=1}^{\mathsf{n}} H(B_s)} \leq 2C_\epsilon[A]. \tag{33}$$

Thus, the desired QPIR capacity is upper bounded by $2C_\epsilon[A]$.

B. Proof of Theorem 4.3

Theorem 4.3 is proved with the following idea. If the answered state from some k servers is independent of the targeted file X^ι, the user and the remaining $(\mathsf{n}-\mathsf{k})$ servers can use the answers from the k servers as entanglement shared with the user. Then, the entanglement-assisted classical-quantum channel capacity [26] implies that the user can obtain at most $2(\mathsf{n}-\mathsf{k})\log\mathsf{d}$ bits of X^ι, which implies Theorem 4.3. Thus, we show that the answered state of the servers $1, \ldots, \mathsf{k}$ have no information of X^ι. For the proof, we consider the process in which the k servers apply quantum operations sequentially, and evaluate the information of X^ι contained in the quantum systems. Initially, the k servers have quantum systems $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{\mathsf{k}}$ and the state is independent of X^ι. After server 1's operation, the state on $\mathcal{A}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_{\mathsf{k}}$ has at most $(\log\mathsf{d})/\mathsf{m}$ bits of X^ι from the user secrecy. Furthermore, we prove that as one more server applies the operation, at most $(\log\mathsf{d})/\mathsf{m}$ bits of X^ι is added to the state of the k servers, from the MDS-coded storage structure and the user secrecy. Consequently, after all servers' operations, the k servers' quantum systems contain at most $(\mathsf{k}\log\mathsf{d})/\mathsf{m}$ bits of X^ι, which converges 0 as $\mathsf{m} \to \infty$.

Throughout the proofs, we use superscripts c (resp. u, s, m) over equalities and inequalities for denoting they are derived from correctness (resp. user secrecy, server secrecy, MDS coded storage structure) of the QPIR scheme. For example, $\overset{u}{=}$ denotes that the equality is derived from the user secrecy of QPIR scheme.

The following proofs are written with quantum mutual information and quantum relative entropy defined as follows. When a quantum system $\mathcal{A}$ has a state $\sigma = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, the von Neumann entropy is defined as $H(\mathcal{A})_\sigma = \mathrm{Tr}(\sigma\log\sigma) = -\sum_i p_i\log p_i$. Similar to the classical case, the mutual information and conditional mutual information are defined as $I(\mathcal{A};\mathcal{B})_\sigma = H(\mathcal{A})_\sigma + H(\mathcal{B})_\sigma - H(\mathcal{A}\mathcal{B})_\sigma$ and $I(\mathcal{A};\mathcal{B}|\mathcal{C})_\sigma = I(\mathcal{A};\mathcal{B}\mathcal{C})_\sigma - I(\mathcal{A};\mathcal{C})_\sigma$, respectively. For two states σ and σ' on $\mathcal{A}$, the quantum relative entropy is defined as $D(\sigma\|\sigma') = \mathrm{Tr}(\sigma(\log\sigma - \log\sigma'))$. Similar to classical case, we have $I(\mathcal{A};\mathcal{B})_\sigma = D(\sigma\|\sigma_{\mathcal{A}} \otimes \sigma_{\mathcal{B}})$

For the proof, we prepare two propositions.

Proposition 6.1 (Fano's Inequality): Let X, Y be random variables with values in $[n]$ and Z be any random variable. Then, $H(X|YZ) \leq \epsilon\log n + h_2(\epsilon)$, where $\varepsilon = \Pr[X \neq Y]$.

Proposition 6.2: Let κ be a CPTP map from $\mathcal{A}$ to $\mathcal{B}$ and σ be a state on $\mathcal{A}\otimes\mathcal{C}$. Then, $I(\mathcal{A};\mathcal{C})_\sigma \geq I(\mathcal{B};\mathcal{C})_{\kappa\otimes\mathrm{id}_{\mathcal{C}}(\sigma)}$, where $\mathrm{id}_{\mathcal{C}}$ is the identity operator on $\mathcal{C}$.

Proof: The proposition follows from the following inequality

$$\begin{aligned} I(\mathcal{A};\mathcal{C})_\sigma &= D(\sigma\|\sigma_{\mathcal{A}} \otimes \sigma_{\mathcal{C}}) \\ &\geq D(\kappa\otimes\mathrm{id}_{\mathcal{C}}(\sigma)\|\kappa(\sigma_{\mathcal{A}}) \otimes \sigma_{\mathcal{C}}) = I(\mathcal{B};\mathcal{C})_{\kappa\otimes\mathrm{id}_{\mathcal{C}}(\sigma)}, \end{aligned}$$

where $\sigma_{\mathcal{A}}$ and $\sigma_{\mathcal{C}}$ are reduced states on $\mathcal{A}$ and $\mathcal{C}$, and the inequality is from the data-processing inequality of the quantum relative entropy. □

Theorem 4.3 is proved by the following two lemmas.

Lemma 6.1: The size of one file is upper bounded as

$$\mathsf{k}\beta \log q \le \frac{2(\mathsf{n}-\mathsf{k})\log \mathsf{d} + I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota) + h_2(\epsilon)}{1-\epsilon}, \quad (34)$$

where $\epsilon = \max_{\iota \in [\mathsf{m}]} \Pr[X^\iota \neq \tilde{X}^\iota]$.

Proof: Fix the index of the targeted file as $K = \iota = \operatorname{argmax}_{\iota \in [\mathsf{m}]} \Pr[X^\iota \neq \tilde{X}^\iota]$. The uniformity of $X^\iota \in \mathbb{F}_q^{\beta \times \mathsf{k}}$ and the Fano's inequality (Proposition 6.1) imply

$$I(\hat{X}^\iota; X^\iota | Q^\iota) = H(X^\iota | Q^\iota) - H(X^\iota | \hat{X}^\iota Q^\iota) \quad (35)$$
$$\ge (1-\epsilon)\mathsf{k}\beta \log q - h_2(\epsilon). \quad (36)$$

From Proposition 6.2, the mutual information in the above inequality is upper bounded as

$$I(\mathcal{A}; X^\iota | Q^\iota) \ge I(\hat{X}^\iota; X^\iota | Q^\iota). \quad (37)$$

Furthermore, the left-hand side of the above inequality is upper bounded as

$$\begin{aligned} I(\mathcal{A}; X^\iota | Q^\iota) &= I(\mathcal{A}_{[\mathsf{k}+1:\mathsf{n}]}; X^\iota | \mathcal{A}_{[\mathsf{k}]} Q^\iota) + I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota) \\ &\le 2 \log \dim \mathcal{A}_{[\mathsf{k}+1:\mathsf{n}]} + I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota) \\ &= 2(\mathsf{n}-\mathsf{k})\log \mathsf{d} + I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota). \end{aligned}$$

Thus, combining (36), (37), and (38), we obtain the desired lemma. □

Lemma 6.2: $\lim_{\mathsf{m}\to\infty} I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota) = 0$.

With Lemmas 6.1 and 6.2, we prove Theorem 4.3 as follows. From Lemma 6.1, the $[\mathsf{n}, \mathsf{k}, 1]$-QPIR capacity is upper bounded as

$$C^{[\mathsf{n},\mathsf{k},1]}_{\mathsf{m},\epsilon} = \sup \frac{\mathsf{k}\beta \log q}{\mathsf{n} \log \mathsf{d}} \quad (38)$$
$$\le \frac{1}{1-\epsilon}\left(\frac{2(\mathsf{n}-\mathsf{k})}{\mathsf{n}} + \frac{I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota) + h_2(\epsilon)}{\mathsf{n}\log \mathsf{d}} \right). \quad (39)$$

Furthermore, Lemma 6.2 proves that $I(\mathcal{A}_{[\mathsf{k}]}; X^\iota | Q^\iota)$ approaches zero as the number of files m goes to infinity, and $h_2(\epsilon) \to 0$ as $\epsilon \to 0$. Thus, as $\mathsf{m} \to \infty$ and $\epsilon \to 0$, the capacity is upper bounded by $2(1 - \mathsf{k}/\mathsf{n})$, which implies Theorem 4.3.

In the remainder of this subsection, we prove Lemma 6.2. For the proof, we prepare the following lemma.

Lemma 6.3: Suppose that $t \in [\mathsf{n}]$ *and* $\mathcal{T} \subset [\mathsf{n}]$ *satisfy* $t \notin \mathcal{T}$. *Then,*

$$I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}}; Y_t^\iota | Q^\iota) \le \frac{2 \log \mathsf{d}}{\mathsf{m}}. \quad (40)$$

Proof: Since the operation from $\mathcal{H}_t$ to $\mathcal{A}_t$ is applied on the quantum system of dimension of d, we have

$$I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}}; Y_t | Q^\iota) \le 2 \log \mathsf{d}. \quad (41)$$

On the other hand, we have

$$I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}}; Y_t | Q^\iota) = \sum_{j=1}^{\mathsf{m}} I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}}; Y_t^j | Y_t^{[j-1]} Q^\iota) \quad (42)$$
$$= \sum_{j=1}^{\mathsf{m}} I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}} Y_t^{[j-1]}; Y_t^j | Q^\iota) \ge \sum_{j=1}^{\mathsf{m}} I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}}; Y_t^j | Q^\iota) \quad (43)$$
$$\overset{u}{=} \mathsf{m} I(\mathcal{A}_t \mathcal{H}_{\mathcal{T}}; Y_t^\iota | Q^\iota), \quad (44)$$

where the last equality follows from the user secrecy condition. Thus, combining (41) and (44), we obtain the desired inequality (40). □

Now, we prove Lemma 6.2. *Proof:* [Proof of Lemma 6.2] By mathematical induction, we prove

$$\lim_{\mathsf{m}\to\infty} I(\mathcal{A}_{[j]} \mathcal{H}_{[j+1:\mathsf{k}]}; Y_{[j]}^\iota | Q^\iota) = 0 \quad (45)$$

for any $j \in [\mathsf{k}]$. Then, the case for $j = \mathsf{k}$ proves the lemma.

First, the case $j = 1$ follows from Lemma 6.3. Next, assuming

$$\lim_{\mathsf{m}\to\infty} I(\mathcal{A}_{[j]} \mathcal{H}_{[j+1:\mathsf{k}]}; Y_{[j]}^\iota | Q^\iota) = 0, \quad (46)$$

we prove

$$\lim_{\mathsf{m}\to\infty} I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]}; Y_{[j+1]}^\iota | Q^\iota) = 0 \quad (47)$$

for $j \in [\mathsf{k}-1]$. Since

$$I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]}; Y_{[j+1]}^\iota | Q^\iota) \quad (48)$$
$$= I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]}; Y_{[j]}^\iota | Q^\iota) + I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]}; Y_{j+1}^\iota | Y_{[j]}^\iota Q^\iota), \quad (49)$$

we prove that the two terms of (49) approaches 0 as $\mathsf{m} \to \infty$. Then, we obtain the desired statement by induction.

The first term of (49) is upper bounded as

$$I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]}; Y_{[j]}^\iota | Q^\iota) \le I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]} Y_{j+1}; Y_{[j]}^\iota | Q^\iota)$$
$$\overset{(a)}{\le} I(\mathcal{A}_{[j]} \mathcal{H}_{[j+1:\mathsf{k}]} Y_{j+1}; Y_{[j]}^\iota | Q^\iota) \overset{m}{=} I(\mathcal{A}_{[j]} \mathcal{H}_{[j+1:\mathsf{k}]}; Y_{[j]}^\iota | Q^\iota),$$

where (a) follows from Proposition 6.2 and the last equality holds because Y_{j+1} is independent of all other quantum systems and random variables. Thus, by the assumption (46), the first term of (49) approaches 0 as $\mathsf{m} \to \infty$.

The second term of (49) is upper bounded as

$$I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]}; Y_{j+1}^\iota | Y_{[j]}^\iota Q^\iota) \quad (50)$$
$$\overset{m}{=} I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]} Y_{[j]}^\iota; Y_{j+1}^\iota | Q^\iota) \quad (51)$$
$$\le I(\mathcal{A}_{[j+1]} \mathcal{H}_{[j+2:\mathsf{k}]} Y_{[j]}; Y_{j+1}^\iota | Q^\iota) \quad (52)$$
$$\le I(\mathcal{A}_{j+1} \mathcal{H}_{[\mathsf{k}]\setminus\{j+1\}} Y_{[j]}; Y_{j+1}^\iota | Q^\iota) \quad (53)$$
$$\overset{m}{=} I(\mathcal{A}_{j+1} \mathcal{H}_{[\mathsf{k}]\setminus\{j+1\}}; Y_{j+1}^\iota | Q^\iota) \le \frac{\log \mathsf{d}}{\mathsf{m}}, \quad (54)$$

where (53) follows from Proposition 6.2 and the last inequality is from Lemma 6.3. Thus, the second term of (49) approaches 0 as $\mathsf{m} \to \infty$. □

VII. Conclusion

In this paper, we have studied the capacity of QPIR/QSPIR with $[\mathsf{n}, \mathsf{k}]$-MDS coded storage and t colluding servers. As general classes of QPIR, we defined stabilizer QPIR and dimension-squared QPIR induced from classical strongly linear PIR. We have proved that the capacities of stabilizer QPIR/QSPIR and dimension-squared QPIR/QSPIR induced from strongly linear PIR are $2(\mathsf{n} - \mathsf{k} - \mathsf{t} + 1)/\mathsf{n}$. When there is no collusion, *i.e.*, $\mathsf{t} = 1$, we have proved that the asymptotic capacity of QPIR/QSPIR is $2(\mathsf{n} - \mathsf{k})/\mathsf{n}$, when the number of files m approaches infinity. These capacities are greater than the known classical counterparts. For the achievability, we have proposed a capacity-achieving QSPIR scheme. The proposed scheme combined the star product PIR

scheme [12] and the QPIR scheme with the stabilizer formalism [23].

As open problems, we state three directions for extending our results. The first direction is to find the general capacity of QPIR/QSPIR with MDS coded storage and colluding servers. This problem in full generality is also unsolved in the classical setting. Partial solutions were given in [8] and [9], which imply that the combination of collusion and coded storage leads to involved linear dependencies that need to be taken into account for a general converse proof. Note that as the capacities proved in these works depend on the number of files m, it is possible that they exceed the asymptotic QPIR capacity proved in this work for a very small number of files.

The second direction is to find non-stabilizer QPIR schemes. Most of the existing multi-server QPIR schemes are stabilizer QPIR schemes. Finding non-stabilizer QPIR schemes is the first step towards the achievability part of the general non-asymptotic capacity theorem.

The third direction is to clarify the trade-off between the amount of entanglement and the capacity. However, even in the case of only two servers, it is very challenging to derive the capacity with restricted entanglement. As a related study, the entanglement-assisted classical capacity for a noisy quantum channel [41] has been recently studied with several new techniques.

REFERENCES

[1] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti, "High-rate quantum private information retrieval with weakly self-dual star product codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 1046–1051.

[2] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proc. IEEE 36th Annu. Found. Comput. Sci.*, Jan. 1995, pp. 41–50.

[3] H. Sun and S. A. Jafar, "The capacity of private information retrieval," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4075–4088, Jul. 2017.

[4] H. Sun and S. A. Jafar, "The capacity of robust private information retrieval with colluding databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2361–2370, Apr. 2018.

[5] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1945–1956, Mar. 2018.

[6] H. Sun and S. A. Jafar, "The capacity of symmetric private information retrieval," *IEEE Trans. Inf. Theory*, vol. 65, no. 1, pp. 322–329, Jan. 2019.

[7] Q. Wang and M. Skoglund, "Symmetric private information retrieval from MDS coded distributed storage with non-colluding and colluding servers," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5160–5175, Aug. 2019.

[8] H. Sun and S. A. Jafar, "Private information retrieval from MDS coded data with colluding servers: Settling a conjecture by Freij-Hollanti et al.," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 1000–1022, Feb. 2018.

[9] L. Holzbaur, R. Freij-Hollanti, J. Li, and C. Hollanti, "Towards the capacity of private information retrieval from coded and colluding servers," 2019, *arXiv:1903.12552*.

[10] L. Holzbaur, R. Freij-Hollanti, and C. Hollanti, "On the capacity of private information retrieval from coded, colluding, and adversarial servers," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Aug. 2019, pp. 1–5.

[11] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, and C. Hollanti, "Private information retrieval from coded storage systems with colluding, Byzantine, and unresponsive servers," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3898–3906, Jun. 2019.

[12] R. Freij-Hollanti, O. W. Gnilke, C. Hollanti, and D. A. Karpuk, "Private information retrieval from coded databases with colluding servers," *SIAM J. Appl. Algebra Geometry*, vol. 1, no. 1, pp. 647–664, 2017.

[13] I. Kerenidis and R. de Wolf, "Exponential lower bound for 2-query locally decodable codes via a quantum argument," in *Proc. 25th ACM Symp. Theory Comput.*, New York, NY, USA, 2003, pp. 106–115, doi: 10.1145/780542.780560.

[14] I. Kerenidis and R. de Wolf, "Quantum symmetrically-private information retrieval," *Inf. Process. Lett.*, vol. 90, no. 3, pp. 109–114, May 2004.

[15] F. Le Gall, "Quantum private information retrieval with sublinear communication complexity," *Theory Comput.*, vol. 8, no. 16, pp. 369–374, 2012.

[16] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, 2011, Art. no. 022313, doi: 10.1103/PhysRevA.84.022313.

[17] Ä. Baumeler and A. Broadbent, "Quantum private information retrieval has linear communication complexity," *J. Cryptol.*, vol. 28, no. 1, pp. 161–175, Jan. 2015.

[18] I. Kerenidis, M. Laurière, F. Le Gall, and M. Rennela, "Information cost of quantum communication protocols," *Quantum Inf. Comput.*, vol. 16, nos. 3–4, pp. 181–196, 2016.

[19] D. Aharonov, Z. Brakerski, K. Chung, A. Green, C.-Y. Lai, and O. Sattath, "On quantum advantage in information theoretic single-server PIR," in *Advances in Cryptology* (Lecture Notes in Computer Science), Y. Ishai and V. Rijmen, Eds. Berlin, Germany: Springer-Verlag, 2019, pp. 219–246.

[20] W. Y. Kon and C. C. W. Lim, "Provably secure symmetric private information retrieval with quantum cryptography," *Entropy*, vol. 23, no. 1, p. 54, 2021. [Online]. Available: https://www.mdpi.com/1099-4300/23/1/54

[21] S. Song and M. Hayashi, "Capacity of quantum private information retrieval with multiple servers," *IEEE Trans. Inf. Theory*, vol. 67, no. 1, pp. 452–463, Jan. 2021.

[22] S. Song and M. Hayashi, "Capacity of quantum symmetric private information retrieval with collusion of all but one of servers," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 380–390, Oct. 2021.

[23] S. Song and M. Hayashi, "Capacity of quantum private information retrieval with colluding servers," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5491–5508, Aug. 2021.

[24] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti, "Quantum private information retrieval from coded and colluding servers," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 599–610, Aug. 2020.

[25] Q. Wang and M. Skoglund, "Secure symmetric private information retrieval from colluding databases with adversaries," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2017, pp. 1083–1090.

[26] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Phys. Rev. Lett.*, vol. 83, no. 15, pp. 3081–3084, 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.83.3081

[27] S. Song and M. Hayashi, "Quantum private information retrieval for quantum messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 1052–1057.

[28] M. Hayashi and T. Morimae, "Verifiable measurement-only blind quantum computing with stabilizer testing," *Phys. Rev. Lett.*, vol. 115, Nov. 2015, Art. no. 220502. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.115.220502

[29] M. A. Nielsen and I. L. Chuang, *Quantum Computing Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[30] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Graduate Texts in Physics). Cham, Switzerland: Springer, 2017.

[31] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, Dept. Division Phys., Math. Astron., California Inst. Technol., Pasadena, CA, USA, 1997.

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

[33] J. S. Bell, "On the Einstein podolsky rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, Oct. 1964. [Online]. Available: https://cds.cern.ch/record/111654

[34] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes* (North-Holland Mathematical Library), vol. 16. Amsterdam, The Netherlands: Elsevier, 1977.

[35] R. Tajeddine, O. W. Gnilke, and S. El Rouayheb, "Private information retrieval from MDS coded data in distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7081–7093, Nov. 2018.

[36] M. Grass and T. A. Gulliver, "On self-dual MDS codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1954–1957.

[37] D. Mirandola and G. Zémor, "Critical pairs for the product singleton bound," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4928–4937, Sep. 2015.

[38] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, pp. 767–793, Jul. 1996.

[39] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.
[40] 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. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.69.2881
[41] K. Wang and M. Hayashi, "Permutation enhances classical communication assisted by entangled states," *IEEE Trans. Inf. Theory*, vol. 67, no. 6, pp. 3905–3925, Jun. 2021.

Matteo Allaix (Student Member, IEEE) received the B.Sc. and M.Sc. degrees from the University of Genoa, Italy, in 2017 and 2020, respectively. He is currently pursuing the Ph.D. degree with Aalto University. In 2019, he visited Aalto University, where he wrote his M.Sc. thesis. His research interests include quantum information theory with application to distributed data storage, security, and communications.

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 has been a Research Fellow of the Japan Society of the Promotion of Science (JSPS) since 2020. He is currently a JSPS Post-Doctoral Fellow with the Graduate School of Mathematics, Nagoya University. His research interest includes 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.

Lukas Holzbaur (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from the Technical University of Munich (TUM), Germany, in 2014 and 2017, respectively, and the Ph.D. degree from the Institute for Communications Engineering, TUM, in 2021. His research interest includes coding theory and its applications, in particular to problems related to distributed data storage.

Tefjol Pllaha received the B.Sc. and M.Sc. degrees in mathematics from the University of Tirana, Albania, in 2009 and 2011, respectively, and the Ph.D. degree in mathematics from the University of Kentucky, Lexington, KY, USA, in 2019. He was a Post-Doctoral Researcher at the Department of Communications and Networking, Aalto University, Finland. He is currently a Post-Doctoral Faculty with the Department of Mathematics, University of Nebraska-Lincoln, USA. His current research interests are in aspects of wireless communication and quantum computation.

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 worked with Kyoto University as a Research Fellow of the Japan Society of the Promotion of Science (JSPS) from 1998 to 2000. He worked at the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN, from 2000 to 2003, and the Research Head at the ERATO Quantum Computation and Information Project, Japan Science and Technology Agency (JST), from 2000 to 2006. He also worked as an Adjunct Associate Professor at 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, from 2004 to 2007. He worked as an Associate Professor at the Graduate School of Information Sciences, Tohoku University, from 2007 to 2012. In 2012, he joined as a Professor at the Graduate School of Mathematics, Nagoya University. In 2020, he joined as the Chief Research Scientist at the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China. Also, he worked as a Visiting Research Associate Professor at the Centre for Quantum Technologies, National University of Singapore, from 2009 to 2012, and as a Visiting Research Professor since 2012. He worked as a Visiting Scientist at the Center for Advanced Intelligence Project, RIKEN, from 2017 to 2020. He worked as a Visiting Professor at the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, from 2018 to 2020, and as a Visiting Professor at the Peng Cheng Laboratory, Center for Quantum Computing, Shenzhen, from 2019 to 2020. He has published the book *Quantum Information: An Introduction* (Springer, 2006) whose revised version was published as *Quantum Information Theory: Mathematical Foundation* from Graduate Texts in Physics, (Springer, 2016). He has published other two books *Group Representation for Quantum Theory* and *A Group Theoretic Approach to Quantum Information* (Springer, 2016). His research interests include classical and quantum information theory and classical and quantum statistical inference.

Dr. Hayashi received the Information Theory Society Paper Award in 2011 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 Japan Society for the Promotion of Science. He is on the Editorial Board of *International Journal of Quantum Information* and *International Journal on Advances in Security*.

Camilla Hollanti (Member, IEEE) received the M.Sc. and Ph.D. degrees in pure mathematics from the University of Turku, Finland, in 2003 and 2009, respectively.

From 2004 to 2011, she was with the University of Turku. She was a Lecturer at the University of Tampere from 2009 to 2010. Since 2011, she has been with the Department of Mathematics and Systems Analysis with Aalto University, Finland, where she currently works as a Full Professor and the Vice Head, and leads a Research Group in Algebra, Number Theory, and Applications. From 2017 to 2020, she was affiliated with the Institute of Advanced Studies, Technical University of Munich, where she held a three-year Hans Fischer Fellowship, funded by the German Excellence Initiative and the EU 7th Framework Programme. Her research interests lie within applications of algebraic number theory to wireless communications and physical layer security, as well as in combinatorial and coding theoretic methods related to distributed storage systems and private information retrieval.

Dr. Hollanti serves as a Member of the Board of Governors of the IEEE Information Theory Society from 2020 to 2022. She is one of the General Chairs of IEEE ISIT 2022. She was a recipient of several grants, including six Academy of Finland Grants. In 2014, she received the World Cultural Council Special Recognition Award for young researchers. In 2017, the Finnish Academy of Science and Letters awarded her the Väisälä Prize in Mathematics. She is currently an Editor of the *AIMS Journal on Advances in Mathematics of Communications, SIAM Journal on Applied Algebra and Geometry*, and IEEE TRANSACTIONS ON INFORMATION THEORY.