Capacity of Quantum Private Information Retrieval With Multiple Servers

Seunghoan Song, *Graduate Student Member, IEEE*, and Masahito Hayashi, *Fellow, IEEE*

Abstract—We study the capacity of quantum private information retrieval (QPIR) with multiple servers. In the QPIR problem with multiple servers, a user retrieves a classical file by downloading quantum systems from multiple servers each of which contains the copy of a classical file set while the identity of the downloaded file is not leaked to each server. The QPIR capacity is defined as the maximum rate of the file size over the whole dimension of the downloaded quantum systems. When the servers are assumed to share prior entanglement, we prove that the QPIR capacity with multiple servers is 1 regardless of the number of servers and files. We construct a rate-one protocol only with two servers. This capacity-achieving protocol outperforms its classical counterpart in the sense of the capacity, server secrecy, and upload cost. The strong converse bound is derived concisely without using any secrecy condition. We also prove that the capacity of multi-round QPIR is 1.

Index Terms—Private information retrieval, capacity, quantum cryptography, malicious adversary, oblivious transfer (OT).

I. INTRODUCTION

INTRODUCED by the seminal paper [1], Private Information Retrieval (PIR) finds efficient methods to download a file from non-communicating servers each of which contains the copy of a classical file set while the identity of the downloaded file is not leaked to each server. This problem is trivially solved by requesting all files to one of the servers, but this method is inefficient. Finding an efficient method is the goal of this problem and it has been extensively studied

in many papers [2]–[5]. Moreover, the papers [6]–[12] have studied the Quantum PIR (QPIR) problem where the user downloads quantum systems instead of classical bits to retrieve a classical file from the servers.

In classical PIR studies, the paper [13] started the discussion of the PIR capacity. The PIR capacity is defined by the maximum rate of the file size over the download size when the numbers of the servers and the files are fixed. In the definition of the PIR capacity, the upload cost, i.e., the total size of the queries, is neglected since it does not scale with the file size which is allowed to go infinity. When each of the n servers contains a copy of the f files, the paper [13] showed that the PIR capacity is $(1 - n^{-1})/(1 - n^{-f})$. Moreover, the paper [14] proposed a capacity-achieving protocol with the minimum upload cost and minimum file size in a class of PIR protocols. Furthermore, after [13], several PIR capacities have been studied under different problem settings. Symmetric PIR is the PIR with server secrecy that the user obtains no more information than the target file, and the capacity of the symmetric PIR is $1 - n^{-1}$ [15]. Another extension is the PIR with coded databases [16]–[21], where the files are coded and distributed to the servers. When the files are coded by an (n, k) Maximum Distance Separable (MDS) code, the PIR capacity is $(1 - k/n)/(1 - (k/n)^f)$ [18]. Multi-round PIR has also been studied in [22] and the capacity was proved to be the same as the PIR capacity derived in [13].

On the other hand, the QPIR problem is rarely treated with multiple servers and there is no study on the capacity of the QPIR problem. Though the papers [6], [7] treated the QPIR problem with multiple servers, they evaluated the communication complexity which is the sum of upload and download costs required to retrieve a one-bit file instead of the capacity.

In this paper, as quantum extensions of the classical PIR capacities [13], [15], [22], we show that the capacities of QPIR, symmetric QPIR, and multi-round QPIR are 1. We derive the QPIR capacity when a user retrieves a file secretly from non-communicating n servers each of which contains the whole set of f files by downloading quantum states under the assumption that an entangled state is shared previously among all servers. We evaluate the security of a QPIR protocol with three parameters: the retrieval error probability, the user secrecy that the identity of the queried file is unknown to any individual server, and the server secrecy that the user obtains no more information than the target file. As a main result, we show that the QPIR capacity is 1 regardless of whether it is

TABLE I
CAPACITIES OF CLASSICAL AND QUANTUM PIRs

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\dfrac{1 - n^{-1}}{1 - n^{-f}}$ [13]	1 ‡
Symmetric PIR	$1 - n^{-1}$ [15]	1 ‡
Multi-round PIR	$\dfrac{1 - n^{-1}}{1 - n^{-f}}$ [22]	1

∗ n, f: the numbers of servers and files, respectively.
† Shared randomness among servers is necessary.
‡ Capacities are derived with the strong converse bounds.

TABLE II
COMPARISON OF PROTOCOLS IN THIS PAPER AND [14]

	This paper	Paper [14]
Server secrecy	Yes	No
Capacity	1	$\dfrac{1 - n^{-1}}{1 - n^{-f}}$
Condition for capacity 1	$n \geq 2$	$n \to \infty$
Upload cost	2f bits	$n(f - 1) \log n$ bits
Possible file sizes	$\{\ell^2\}_{\ell=2}^{\infty}$	$\{\ell^{n-1}\}_{\ell=2}^{\infty}$

∗ Server secrecy is the property that the user obtains no information other than the target file.
† n, f: the numbers of servers and files, respectively.
‡ Upload cost is the total bits which are sent to the servers.

of exact/asymptotic security and with/without the restriction that the upload cost is negligible to the download cost. We propose a rate-one QPIR protocol with perfect security and finite upload cost. We prove the converse bound that the rate of any QPIR protocol is less than 1 even with no secrecy, no upload constraint, and any error probability. Moreover, we show that the capacity of multi-round QPIR is 1. We prove the weak converse bound of the multi-round QPIR capacity, i.e., the upper bound when the error probability is asymptotically zero.

Our capacity-achieving protocol has several remarkable advantages compared to the protocol [14] with the minimum upload cost and the minimum file size (see Table II). First, our protocol is a symmetric QPIR protocol, i.e., the user obtains no information of files other than the retrieved one. This contrasts with the protocol in [14] that retrieves some information of the other files. Secondly, our protocol keeps the secrecy against the malicious user and servers. That is, the user cannot obtain more information than the target file even if the user sends malicious queries to the servers, and the servers cannot obtain the identity of the user's target file even if the servers answer malicious file information. Thirdly, the rate of our protocol is greater than the rate $(1 - n^{-1})/(1 - n^{-f})$ of the protocol in [14]. Fourthly, our protocol achieves the capacity 1 only with two servers. That is, in the sense of the QPIR capacity, there is no benefit to using more than two servers. On the other hand, in the protocol in [14], the capacity is strictly increasing in

the number of servers and strictly decreasing in the number of files, and an infinite number of servers are needed to achieve the capacity 1. Fifthly, our protocol needs the upload of 2f bits whereas the protocol in [14] needs $(n(f - 1) \log n)$-bit upload. Lastly, our protocol is defined when the file size m is the square of any integer, but the protocol in [14] requires the file size m to be the $(n - 1)$-th power of any integer.

The converse proofs of the QPIR capacities are much simpler than those of the PIR capacities [13], [15], [22]. Whereas the papers [13], [15], [22] used several entropic inequalities based on the assumptions on the PIR problem, our converse bounds are concisely derived without using any secrecy conditions but only by focusing on the download step of QPIR protocol.

It should be noted that our QPIR protocol can be considered as a distributed version of Oblivious Transfer (OT) [23], [24]. OT is equivalent to the symmetric PIR with one server and therefore, the symmetric PIR with multiple servers can be considered as a distributed version of OT. OT is an important cryptographic protocol because the free uses of an OT protocol construct an arbitrary secure multiparty computation [25], [26]. Unfortunately, the symmetric classical PIR cannot be constructed without shared randomness among servers [27]. On the other hand, the paper [7] showed that the two-way quantum communication between the user and the servers enables the symmetric PIR without shared randomness. Our result extends the result [7] so that the symmetric PIR can also be constructed without shared randomness even for the case of classical upload, quantum download, and prior entanglement among the servers. Note that if the quantum upload is allowed to our model, we do not need the assumption of the prior entanglement because the user can upload an entangled state to all servers.

We assume that the servers share an entangled state before the protocol starts, but do not communicate. Similarly, the prior entanglement by non-communicating multiple parties has been assumed in another quantum protocol, called Multi-prover Quantum Interactive Proof (MQIP) [28]–[30]. In MQIP, to solve a computational problem, a computationally-limited verifier sends queries to multiple provers who do not communicate with each other and have quantum computers, receives answers from them, and then verifies whether the answers from the provers give a correct solution of the problem. Similarly to our assumption, the MQIP studies [28]–[30] assumed that the provers share an entangled state before the protocol starts, but do not communicate with each other. However, even if the assumption of shared entanglement is similar, our communication model is different from those in [28]–[30]: the papers [28], [30] treated the quantum queries and quantum answers, and the paper [29] treated the classical queries and classical answers, but our paper treats classical queries and quantum answers.

The remaining of this paper is organized as follows. Section II presents the formal definition of the QPIR protocol and the QPIR capacity and proposes the QPIR capacity theorem. Section III constructs the rate-one QPIR protocol and analyzes the security of our protocol against the malicious user and servers. Section IV proves the converse bound.
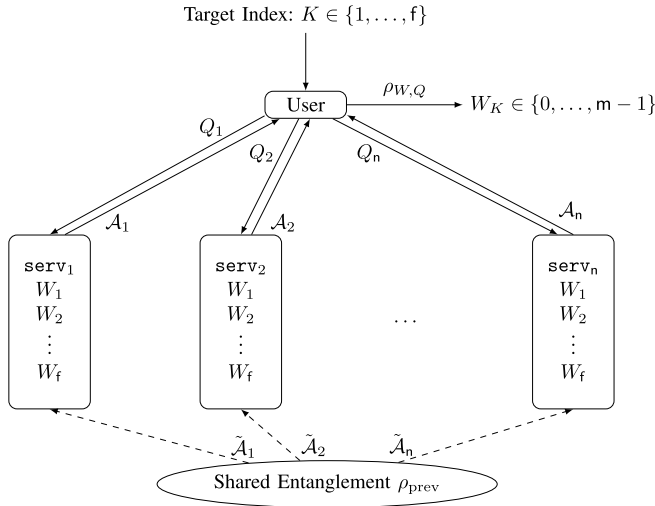
Fig. 1. Quantum private information retrieval protocol with multiple servers. The composite system of the servers is initialized to an entangled state ρ_{perv}.

Section V extends the result to the capacity of multi-round QPIR. Section VI is the conclusion of this paper.

Notations: For any set $\mathcal{T}$, we denote by $|\mathcal{T}|$ the cardinality of the set $\mathcal{T}$ and by $\mathsf{I}_{\mathcal{T}}$ (or I) the identity operator on $\mathcal{T}$. For any matrix B, we denote by $\bar{\mathsf{B}}$ the complex conjugate of B and $\mathsf{B}^{\dagger}$: $= \bar{\mathsf{B}}^{\top}$. The set of integers is denoted by $\mathbb{Z}$, and $\mathbb{Z}_d := \mathbb{Z}/d\mathbb{Z}$ for any integer d. $\Pr_X[A]$ denotes the probability that the variable X satisfies the condition A. For any quantum system $\mathcal{A}$, we denote the set of all quantum states on $\mathcal{A}$ by $\mathcal{S}(\mathcal{A})$.

II. QPIR PROTOCOL AND MAIN THEOREM

In this section, we formally define the QPIR protocol and its capacity and presents the main theorem of the paper. For preliminaries on quantum information theory, see Appendix A.

A. Formal Definition of QPIR Protocol

In this paper, we consider the QPIR with multiple servers described as follows. Let n, f, m be integers greater than 1. The participants of the protocol are one user and n servers. The servers do not communicate with each other and each server contains the whole set of uniformly and independently distributed f files $W_1, \ldots, W_f \in \{0, \ldots, m-1\}$. Each server serv_t possesses a quantum system $\tilde{\mathcal{A}}_t$ and the n servers share an entangled state $\rho_{\text{prev}} \in \mathcal{S}(\bigotimes_{t=1}^{n} \tilde{\mathcal{A}}_t)$. The user chooses the target file index K to retrieve the K-th file W_K, where the distribution of K is uniform and independent of the files $W_1, \ldots, W_f$.

To retrieve the W_K, the user chooses a random variable R_{user} in a set $\mathcal{R}_{\text{user}}$ and encodes the queries by user encoder $\mathsf{Enc}_{\text{user}}$:

$$\mathsf{Enc}_{\text{user}}(K, R_{\text{user}}) = (Q_1, \ldots, Q_n) \in \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_n,$$

where $\mathcal{Q}_t$ is the set of query symbols to the t-th server for any $t \in \{1, \ldots, n\}$. The n queries $Q_1, \ldots, Q_n$ are sent to the servers $\mathsf{serv}_1, \ldots, \mathsf{serv}_n$, respectively. After receiving the t-th query Q_t, each server serv_t applies a Completely Positive Trace-Preserving (CPTP) map Λ_t from $\tilde{\mathcal{A}}_t$ to $\mathcal{A}_t$ depending

on $Q_t, W_1, \ldots, W_f$ and sends the quantum system $\mathcal{A}_t$ to the user. With the server encoder $\mathsf{Enc}_{\mathsf{serv}_t}$, the map Λ_t is written as

$$\Lambda_t = \mathsf{Enc}_{\mathsf{serv}_t}(Q_t, W_1, \ldots, W_f),$$

and the received state of the user is written as

$$\rho_{W,Q} := \Lambda_1 \otimes \cdots \otimes \Lambda_n(\rho_{\text{prev}}) \in \mathcal{S}\left(\bigotimes_{t=1}^{n} \mathcal{A}_t\right), \quad (1)$$

where $W := (W_1, \ldots, W_f)$ and $Q := (Q_1, \ldots, Q_n)$. Next, the user retrieves the file W_K by a decoder which is defined depending on K, Q as a Positive Operator-Valued Measure (POVM) $\mathsf{Dec}(K, Q) := \{\mathsf{Y}_M\}_{M=0}^{\mathsf{m}}$. The protocol outputs the measurement outcome $M \in \{0, \ldots, \mathsf{m}\}$ and if $M = \mathsf{m}$, it is considered as the retrieval failure.

1) Protocol: When the numbers n and f of servers and files are fixed, a QPIR protocol of file size m is formulated by the 4-tuple $\Psi_{\text{QPIR}}^{(\mathsf{m})} := (\rho_{\text{prev}}, \mathsf{Enc}_{\text{user}}, \mathsf{Enc}_{\text{serv}}, \mathsf{Dec})$ of the shared entangled state ρ_{prev} in the servers, the user encoder $\mathsf{Enc}_{\text{user}}$, the collection of the server encoders $\mathsf{Enc}_{\text{serv}} := (\mathsf{Enc}_{\text{serv}_1}, \ldots, \mathsf{Enc}_{\text{serv}_n})$, and the decoder Dec.

2) Security: For any $t \in \{1, \ldots, n\}$, let $\mathfrak{user}(\Psi_{\text{QPIR}}^{(\mathsf{m})})$ and $\mathfrak{serv}_t(\Psi_{\text{QPIR}}^{(\mathsf{m})})$ be the information of the user and the server serv_t at the end of the protocol $\Psi_{\text{QPIR}}^{(\mathsf{m})}$, respectively. The security of a QPIR protocol $\Psi_{\text{QPIR}}^{(\mathsf{m})}$ is evaluated by the error probability, the server secrecy, and the user secrecy defined as

$$P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) := \Pr_{W,K,Q}[M \neq W_K], \quad (2)$$

$$S_{\text{serv}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) := I(W_{K^c}; \mathfrak{user}(\Psi_{\text{QPIR}}^{(\mathsf{m})})|K), \quad (3)$$

$$S_{\text{user}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) := \max_{t \in \{1, \ldots, n\}} I(K; \mathfrak{serv}_t(\Psi_{\text{QPIR}}^{(\mathsf{m})})), \quad (4)$$

where $I(\cdot; \cdot|\cdot)$ denotes the conditional mutual information and $W_{K^c} := (W_1, \ldots, W_{K-1}, W_{K+1}, \ldots, W_f)$. If $S_{\text{serv}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) = 0$, the non-targeted files W_{K^c} are independent of the user information. Similarly, if $S_{\text{user}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) = 0$, the target file index K is independent of any individual server information.

3) Costs, Rate, and Capacity: Given a QPIR protocol $\Psi_{\text{QPIR}}^{(\mathsf{m})}$, we define the upload cost, the download cost, and the QPIR rate by

$$U(\Psi_{\text{QPIR}}^{(\mathsf{m})}) := \sum_{t=1}^{n} \log |\mathcal{Q}_t|, \quad (5)$$

$$D(\Psi_{\text{QPIR}}^{(\mathsf{m})}) := \sum_{t=1}^{n} \log \dim \mathcal{A}_t, \quad (6)$$

$$R(\Psi_{\text{QPIR}}^{(\mathsf{m})}) := \frac{\log \mathsf{m}}{D(\Psi_{\text{QPIR}}^{(\mathsf{m})})}. \quad (7)$$

The upload cost, the download cost, and the QPIR rate evaluate respectively the size of the whole query set $\mathcal{Q}_1 \times \cdots \times \mathcal{Q}_n$, the dimension of the downloaded quantum systems $\mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n$, and the efficnecy of the protocol. When the base of the logarithm is two, the QPIR rate means the number of retrieved bits per one qubit download.

The QPIR capacity is the optimal QPIR rate when the numbers of servers and files are fixed, and we define it with constraints on the security parameters and upload cost. The *asymptotic security-constrained capacity* and the *exact security-constrained capacity* are defined with $\alpha \in [0, 1)$ and $\beta, \gamma, \theta \in [0, \infty]$ by

$$C_{\text{asymp}}^{\alpha,\beta,\gamma,\theta} := \sup_{(8)} \liminf_{\ell \to \infty} R(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}),$$

$$C_{\text{exact}}^{\alpha,\beta,\gamma,\theta} := \sup_{(9)} \liminf_{\ell \to \infty} R(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}),$$

where the supremum is taken for sequences $\{\mathsf{m}_\ell\}_{\ell=1}^{\infty}$ such that $\lim_{\ell \to \infty} \mathsf{m}_\ell = \infty$ and for sequences $\{\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ of QPIR protocols to satisfy either (8) or (9) given by

$$\limsup_{\ell \to \infty} P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \alpha, \quad \limsup_{\ell \to \infty} S_{\text{serv}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \beta,$$

$$\limsup_{\ell \to \infty} S_{\text{user}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \gamma, \quad \limsup_{\ell \to \infty} \frac{U(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})}{D(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})} \leq \theta, \quad (8)$$

and

$$P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \alpha, \quad S_{\text{serv}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \beta,$$

$$S_{\text{user}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \gamma, \quad \limsup_{\ell \to \infty} \frac{U(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})}{D(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})} \leq \theta. \quad (9)$$

It is trivial from the definition that for any $\alpha \in [0, 1)$ and $\beta, \gamma, \theta \in [0, \infty]$,

$$C_{\text{exact}}^{0,0,0,0} \leq C_{\text{exact}}^{\alpha,\beta,\gamma,\theta} \leq C_{\text{asymp}}^{\alpha,\beta,\gamma,\theta} \leq C_{\text{asymp}}^{\alpha,\infty,\infty,\infty}. \quad (10)$$

B. Main Result

The main theorem of this paper is given as follows.

Theorem II.1: When servers can share prior entanglement, the capacity of the quantum private information retrieval for $\mathsf{f} \geq 2$ files and $\mathsf{n} \geq 2$ servers is

$$C_{\text{exact}}^{\alpha,\beta,\gamma,\theta} = C_{\text{asymp}}^{\alpha,\beta,\gamma,\theta} = 1,$$

for any $\alpha \in [0, 1)$ and $\beta, \gamma, \theta \in [0, \infty]$.

Proof: In Sections III and IV, we will prove $C_{\text{exact}}^{0,0,0,0} \geq 1$ and $C_{\text{asymp}}^{\alpha,\infty,\infty,\infty} \leq 1$ for any $\alpha \in [0, 1)$, respectively. Then, the inequality (10) implies the theorem. $\square$

Note that the capacity does not depend on the number of files f and the number of servers n. This contrasts with the classical PIR capacity [13], which is strictly decreasing for f and strictly increasing for n. Moreover, the capacity does not depend on the security constraints, i.e., there is no trade-off between the capacity and the constraints $\alpha, \beta, \gamma, \theta$. Furthermore, the theorem implies that the symmetric QPIR capacity is 1.

Remark II.1: In our QPIR model, we assumed that the files $W_1, \ldots, W_\mathsf{n}$ are uniformly random and mutually independent. However, the assumption is necessary only for proving the converse bounds. Without the assumption, our QPIR protocol has no error and achieves the perfect server and user secrecies.

III. CONSTRUCTION OF PROTOCOL

In this section, we construct a rate-one two-server QPIR protocol with the perfect security and negligible upload cost. Our protocol is constructed if the file size m is the square of an arbitrary integer ℓ. Then, by taking $\mathsf{m}_\ell = \ell^2$, the sequence $\{\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ of our protocols achieves the rate 1 with the perfect security and negligible upload cost, which implies

$$C_{\text{exact}}^{0,0,0,0} \geq 1. \quad (11)$$

In the following, we give preliminaries on quantum operations and states in Section III-A and construct the QPIR protocol in Section III-B.

A. Preliminaries

For an arbitrary integer $\ell \geq 2$, let $\mathcal{A}$ be an ℓ-dimensional Hilbert space spanned by an orthonormal basis $\{|0\rangle, \ldots, |\ell-1\rangle\}$. Define a maximally entangled state $|\Phi\rangle$ on $\mathcal{A} \otimes \mathcal{A}$ by

$$|\Phi\rangle := \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle.$$

For $a, b \in \mathbb{Z}_\ell$, the generalized Pauli operators on $\mathcal{A}$ are defined as

$$\mathsf{X} := \sum_{i=0}^{\ell-1} |i+1\rangle\langle i|, \quad \mathsf{Z} := \sum_{i=0}^{\ell-1} \omega^i |i\rangle\langle i|,$$

where $\omega = \exp(2\pi\sqrt{-1}/\ell)$, and the discrete Weyl operators are defined as

$$\mathsf{W}(a, b) := \mathsf{X}^a \mathsf{Z}^b = \sum_{i=0}^{\ell-1} \omega^{ib} |i+a\rangle\langle i|.$$

These operators satisfy the relations

$$\mathsf{Z}^b \mathsf{X}^a = \omega^{ba} \mathsf{X}^a \mathsf{Z}^b,$$

$$\mathsf{W}(a_1, b_1)\mathsf{W}(a_2, b_2) = \omega^{b_1 a_2} \mathsf{W}(a_1 + a_2, b_1 + b_2),$$

$$\mathsf{W}(a, b)^\dagger = \omega^{ba} \mathsf{W}(-a, -b).$$

For any matrix $\mathsf{T} := \sum_{i,j=0}^{\ell-1} t_{ij} |i\rangle\langle j|$ on $\mathcal{A}$, we define the state $|\mathsf{T}\rangle$ in $\mathcal{A} \otimes \mathcal{A}$ by

$$|\mathsf{T}\rangle := \sum_{i,j=0}^{\ell-1} t_{ij} |i\rangle \otimes |j\rangle.$$

With this notation, the maximally entangled state is written as $|\Phi\rangle = (1/\sqrt{\ell})|\mathsf{I}\rangle$. Since $\mathsf{T}^\top = \sum_{i,j=0}^{\ell-1} t_{ij} |j\rangle\langle i|$, it holds $|\mathsf{T}\rangle = (\mathsf{T} \otimes \mathsf{I})|\mathsf{I}\rangle = (\mathsf{I} \otimes \mathsf{T}^\top)|\mathsf{I}\rangle$. Moreover, for any unitaries U, V on $\mathcal{A}$, we have

$$(\mathsf{U} \otimes \mathsf{V})|\mathsf{T}\rangle = |\mathsf{UTV}^\top\rangle,$$

$$(\mathsf{U} \otimes \overline{\mathsf{U}})|\mathsf{I}\rangle = |\mathsf{UU}^\dagger\rangle = |\mathsf{I}\rangle. \quad (12)$$

With the basis given in the following proposition, we construct the measurement in our QPIR protocol.

Proposition III.1: The set

$$\mathcal{B} := \{(\mathsf{W}(a, b) \otimes \mathsf{I})|\Phi\rangle \mid a, b \in \mathbb{Z}_\ell\}$$

is an orthonormal basis of $\mathcal{A} \otimes \mathcal{A}$.

Proof: Since $\mathsf{W}(a,b) \otimes \mathsf{I}$ is a unitary matrix for any $a, b \in \mathbb{Z}_\ell$, all elements in $\mathcal{B}$ are unit vectors. Then, it is sufficient to show that every different two vectors in $\mathcal{B}$ are mutually orthogonal: for any different $(a,b), (c,d) \in \mathbb{Z}_\ell^2$,

$$((\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle)^\dagger (\mathsf{W}(c,d) \otimes \mathsf{I})|\Phi\rangle = 0. \qquad (13)$$

Since $\mathsf{W}(a,b)^\dagger \mathsf{W}(c,d) = \omega^{b(a-c)} \mathsf{W}(c-a, d-b)$, the left-hand side of (13) is written as

$$\omega^{b(c-a)} \langle \Phi | (\mathsf{W}(c-a, d-b) \otimes \mathsf{I})|\Phi\rangle.$$

Moreover, for any $x, z \in \mathbb{Z}_\ell$, we have

$$\langle \Phi | (\mathsf{W}(x,z) \otimes \mathsf{I})|\Phi\rangle = \frac{1}{\ell} \sum_{i=0}^{\ell-1} \langle i | \mathsf{W}(x,z) | i \rangle \qquad (14)$$

$$= \frac{1}{\ell} \sum_{i=0}^{\ell-1} \omega^{iz} \langle i | i + x \rangle \qquad (15)$$

$$= \delta_{(x,z),(0,0)} \qquad (16)$$

Thus, Eq. (13) holds for any $(a,b) \neq (c,d)$, which implies the desired statement. $\qquad \square$

B. Rate-One QPIR Protocol

In this section, we propose a rate-one two-server QPIR protocol with the perfect security and negligible upload cost. This protocol is constructed from the idea of the classical two-server PIR protocol in [1, Section 3.1].

In this protocol, a user retrieves a file W_K from two servers $\mathtt{serv}_1$ and $\mathtt{serv}_2$. Each server contains a copy of the files $W_1, \ldots, W_\mathsf{f} \in \{0, \ldots, \ell^2 - 1 =: \mathsf{m}_\ell - 1\}$ for an arbitrary integer ℓ. By identifying the set $\{0, \ldots, \ell^2 - 1\}$ with $\mathbb{Z}_\ell^2$, the files $W_1, \ldots, W_\mathsf{f}$ are considered to be elements of $\mathbb{Z}_\ell^2$. We assume that $\mathtt{serv}_1$ and $\mathtt{serv}_2$ possess the ℓ-dimensional quantum systems $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively, and the maximally entangled state $|\Phi\rangle$ in $\mathcal{A}_1 \otimes \mathcal{A}_2$ is shared at the beginning of the protocol.

1) Protocol: The QPIR protocol for retrieving W_K is described as follows.

Step 1. Depending on the target file index K, the user chooses a subset R_{user} of $\{1, \ldots, \mathsf{f}\}$ uniformly. Let $Q_1 := R_{\text{user}}$ and

$$Q_2 := \begin{cases} Q_1 \setminus \{K\} & \text{if } K \in Q_1, \\ Q_1 \cup \{K\} & \text{otherwise.} \end{cases}$$

Step 2. The user sends the queries Q_1 and Q_2 to $\mathtt{serv}_1$ and $\mathtt{serv}_2$, respectively.

Step 3. $\mathtt{serv}_1$ calculates $H_1 := \sum_{i \in Q_1} W_i \in \mathbb{Z}_\ell^2$ and applies $\mathsf{W}(H_1)$ on the quantum system $\mathcal{A}_1$. Similarly, $\mathtt{serv}_2$ calculates $H_2 := \sum_{i \in Q_2} W_i$ and applies $\overline{\mathsf{W}(H_2)}$ to the quantum system $\mathcal{A}_2$. The state on $\mathcal{A}_1 \otimes \mathcal{A}_2$ is $(\mathsf{W}(H_1) \otimes \overline{\mathsf{W}(H_2)})|\Phi\rangle$.

Step 4. $\mathtt{serv}_1$ and $\mathtt{serv}_2$ send the quantum systems $\mathcal{A}_1$ and $\mathcal{A}_2$ to the user, respectively.

Step 5. The user performs a POVM

$$\text{Dec}(K, Q) = \{\mathsf{Y}_{(a,b)} \mid a, b \in \mathbb{Z}_\ell\}$$

on the received state $\rho_{W,Q}$, where each POVM element $\mathsf{Y}_{(a,b)}$ for the outcome (a,b) is defined by

$$\mathsf{Y}_{(a,b)} := (\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle\langle\Phi|(\mathsf{W}(a,b)^\dagger \otimes \mathsf{I})$$

if $K \in Q_1$, and

$$\mathsf{Y}_{(a,b)} := (\mathsf{W}(-a,-b) \otimes \mathsf{I})|\Phi\rangle\langle\Phi|(\mathsf{W}(-a,-b)^\dagger \otimes \mathsf{I})$$

otherwise. The user obtains the measurement outcome (a,b) as the retrieval result.

2) Security: We analyze the security of the protocol, i.e., the error probability, the server secrecy, and the user secrecy.

The protocol has no error as follows. Note that $H_1 = H_2 + W_K$ if $K \in Q_1$, and $H_1 = H_2 - W_K$ otherwise. After Step 3, the state on $\mathcal{A}_1 \otimes \mathcal{A}_2$ is

$$\mathsf{W}(H_1) \otimes \overline{\mathsf{W}(H_2)}|\Phi\rangle$$

$$= \frac{\omega^{\mp b_{W_K} a_{H_2}}}{\sqrt{\ell}} (\mathsf{W}(\pm W_K) \otimes \mathsf{I})(\mathsf{W}(H_2) \otimes \overline{\mathsf{W}(H_2)})|\mathsf{I}\rangle \quad (17)$$

$$= \frac{\omega^{\mp b_{W_K} a_{H_2}}}{\sqrt{\ell}} (\mathsf{W}(\pm W_K) \otimes \mathsf{I})|\mathsf{I}\rangle \qquad (18)$$

$$= \omega^{\mp b_{W_K} a_{H_2}} (\mathsf{W}(\pm W_K) \otimes \mathsf{I})|\Phi\rangle,$$

where $H_2 = (a_{H_2}, b_{H_2})$ and $W_K = (a_{W_K}, b_{W_K}) \in \mathbb{Z}_\ell^2$. The equality (17) is derived from $\mathsf{W}(H_1) = \mathsf{W}(\pm W_K + H_2) = \omega^{\mp b_{W_K} a_{H_2}} \mathsf{W}(\pm W_K) \mathsf{W}(H_2)$ and the equality (18) is from (12). Therefore, in Step 5, the measurement outcome is $W_K \in \mathbb{Z}_\ell^2$ with probability 1.

The perfect server secrecy is obtained because the received state $(\mathsf{W}(\pm W_K) \otimes \mathsf{I})|\Phi\rangle$ of the user is independent of the files $W_1, \ldots, W_{K-1}, W_{K+1}, \ldots, W_\mathsf{f}$.

The perfect user secrecy follows from that of the protocol [1, Section 3.1]. Note that even if the collection of Q_1 and Q_2 depends on K, each of Q_1 and Q_2 is individually independent of the index K. Thus, the perfect user secrecy is obtained.

3) Upload Cost, Download Cost, and Rate: The upload cost is $U(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) = 2\mathsf{f} \log 2$ since two subsets Q_1 and Q_2 of $\{1, \ldots, \mathsf{f}\}$ are uploaded and each subset of $\{1, \ldots, \mathsf{f}\}$ is expressed by f bits. The download cost is $D(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) = \log \dim \mathcal{A}_1 \otimes \mathcal{A}_2 = \log \ell^2 = \log \mathsf{m}_\ell$. Therefore, the rate is

$$R(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) = \frac{\log \mathsf{m}_\ell}{D(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})} = 1,$$

and $U(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})/D(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})$ goes to zero as $\mathsf{m}_\ell \to \infty$.

C. Security Against Malicious Operations

In the previous subsection, we showed that the protocol in Section III-B has the perfect security when the user and the servers follow the protocol. In this subsection, we prove that the protocol in Section III-B also guarantees the server and user secrecies even if the servers or the user apply malicious operations. Namely, we consider two malicious models: the malicious server model and the malicious user model.

The malicious server model considers the case that the servers apply malicious operations to obtain the target file index K but the user follows the protocol, i.e., the query generation and the recovery by the user are the same as the

protocol in Section III-B. Our protocol is secure against this model since each of Q_1 and Q_2 is individually independent of the index K and the servers obtain no more information from the user except for Q_1 and Q_2. Therefore the servers cannot obtain any information of K by malicious operations.

The second security model is the malicious user model, where the user sends malicious queries to the servers to obtain the non-targeted file information in addition to the target file W_K. That is, the user sends malicious queries $Q = (Q_1, Q_2)$ to retrieve both of the file W_K and some information of $W_{K^c} = (W_1, \ldots, W_{K-1}, W_{K+1}, \ldots, W_f)$. Similarly to the malicious server model, we assume that the servers do not deviate from the protocol. Our protocol is also secure against this model since the user downloads the m_ℓ-dimensional quantum system and the user is assumed to obtain $W_K \in \{0, \ldots, \mathsf{m}_\ell - 1\}$. That is, the user cannot obtain more information than W_K. This security is precisely proved by the following relation:

$$I(\mathcal{A}; W_{K^c} | W_K, K, Q)_{\rho_{W,Q}} = 0, \tag{19}$$

where $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ and $I(\cdot; \cdot | \cdot)_\rho$ is the quantum conditional mutual information defined in Appendix B.

Proof of Eq. (19): Since the user obtains the file W_K, we have

$$H(W_K | \mathcal{A}, K, Q)_{\rho_{W,Q}} = 0, \tag{20}$$

where $H(\cdot | \cdot)_\rho$ is the quantum conditional entropy defined in Appendix B. Eq. (20) is equivalent to

$$H(\mathcal{A}, W_K | K, Q)_{\rho_{W,Q}} = H(\mathcal{A} | K, Q)_{\rho_{W,Q}}. \tag{21}$$

The relation (21) implies the following relations:

$$0 \leq H(\mathcal{A} | W_K, K, Q)_{\rho_{W,Q}} \tag{22}$$
$$= H(\mathcal{A}, W_K | K, Q)_{\rho_{W,Q}} - H(W_K | K, Q) \tag{23}$$
$$= H(\mathcal{A} | K, Q)_{\rho_{W,Q}} - \log \mathsf{m}_\ell \leq 0. \tag{24}$$

The equality in (24) follows from the condition (21), the independence between W_K and (K, Q), and the uniform distribution of W_K. The last inequality in (24) follows from $\dim \mathcal{A} = \log \mathsf{m}_\ell$. Therefore, we have

$$H(\mathcal{A} | W_K, K, Q)_{\rho_{W,Q}} = 0 \tag{25}$$

which implies (19). $\qquad\square$

IV. CONVERSE

In this section, we prove the converse bound

$$C_{\text{asymp}}^{\alpha, \infty, \infty, \infty} \leq 1 \tag{26}$$

for any $\alpha \in [0, 1)$. By replacing the notation of $\rho_{W,Q}$ defined in (1), let $\rho_{w,z}$ be the quantum state on the composite system $\bigotimes_{t=1}^{\mathsf{n}} \mathcal{A}_t$, where w is the file to be retrieved and $z := (w^c, q)$ for the collection w^c of other $\mathsf{m} - 1$ files and the collection q of queries.

Applying [31, (4.66)] to the choice $\sigma_z = (1/\mathsf{m}) \sum_{w=0}^{\mathsf{m}-1} \rho_{w,z}$, for any $s \in (0, 1)$, we have

$$(1 - P_{\text{err},z}(\Psi_{\text{QPIR}}^{(\mathsf{m})}))^{1+s} \mathsf{m}^s \leq \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \text{Tr} \, \rho_{w,z}^{1+s} \sigma_z^{-s}, \tag{27}$$

where $P_{\text{err},z}(\Psi_{\text{QPIR}}^{(\mathsf{m})})$ is the error probability when z is fixed. For the completeness of the proof, we give the derivation of (27) in Appendix C. Furthermore, we can bound the RHS of (27) as

$$\frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \text{Tr} \, \rho_{w,z}^{1+s} \sigma_z^{-s} \leq \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \text{Tr} \, \rho_{w,z} \sigma_z^{-s} = \text{Tr} \, \sigma_z^{1-s}$$
$$\leq \max_\sigma \text{Tr} \, \sigma^{1-s} = \max_p \sum_{i=1}^{d} p_i^{1-s} \overset{(a)}{=} \left(\prod_{t=1}^{\mathsf{n}} \dim \mathcal{A}_t \right)^s \tag{28}$$

for $d = \prod_{t=1}^{\mathsf{n}} \dim \mathcal{A}_t$. Here, since $x \mapsto x^{1-s}$ is concave, the maximum $\max_p \sum_{i=1}^{d} p_i^{1-s}$ is realized by the uniform distribution, which shows the equation (a). Combining (27) and (28), the error probability is upper bounded as

$$1 - P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) = 1 - \mathbb{E}_Z P_{\text{err},Z}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) \tag{29}$$
$$\leq \left(\frac{\prod_{t=1}^{\mathsf{n}} \dim \mathcal{A}_t}{\mathsf{m}} \right)^{\frac{s}{1+s}}. \tag{30}$$

For any sequence of QPIR protocols $\{\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$, if $\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}$ satisfies

$$R(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) = \frac{\log \mathsf{m}_\ell}{\log \prod_{t=1}^{\mathsf{n}} \dim \mathcal{A}_t} \geq 1 \tag{31}$$

for any sufficiently large ℓ, we have

$$\frac{\prod_{t=1}^{\mathsf{n}} \dim \mathcal{A}_t}{\mathsf{m}_\ell} \to 0.$$

Hence, by (30), $1 - P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})$ approaches zero, which implies (26).

V. CAPACITY OF MULTI-ROUND QPIR

In this section, we prove that the multi-round QPIR capacity is 1. First, as a generalization of the protocol description in Section II-A, we formally define the multi-round QPIR. Then, we propose the capacity theorem and the proof of the weak converse bound. Since the protocol in Section III-B has the QPIR rate 1, this protocol also achieves the multi-round QPIR capacity. The result in this section includes the result in the previous sections as the one-round QPIR.

A. Formal Definition of Multi-Round QPIR Protocol

For any positive integer r, we give the formal description of the r-round QPIR protocol $\Psi_{\text{QPIR}}^{(\mathsf{m}, \mathsf{r})}$. The information flow of the quantum systems is depicted in Fig. 2. When $\mathsf{r} = 1$, the protocol description is equivalent to the protocol defined in Section II-A.

Let $\mathsf{n}, \mathsf{f}, \mathsf{m}$ be integers greater than 1. Each of the servers $\mathtt{serv}_1, \ldots, \mathtt{serv}_{\mathsf{n}}$ contains the whole copy of the uniformly and independently distributed f files $W = (W_1, \ldots, W_{\mathsf{f}}) \in \{0, \ldots, \mathsf{m} - 1\}^{\mathsf{f}}$. The t-th server $\mathtt{serv}_t$ possesses a quantum system $\mathcal{B}_t$ as local quantum register and the n servers share an entangled state ρ_{prev} on the quantum system $\mathcal{B} := \mathcal{B}_1 \otimes \cdots \otimes \mathcal{B}_{\mathsf{n}}$.

The user chooses the target file index $K \in \{1, \ldots, \mathsf{f}\}$ uniformly and independently of the files $W_1, \ldots, W_{\mathsf{f}}$. The user prepares the query $Q^1 = (Q_1^1, Q_2^1, \ldots, Q_{\mathsf{n}}^1)$ depending on K.
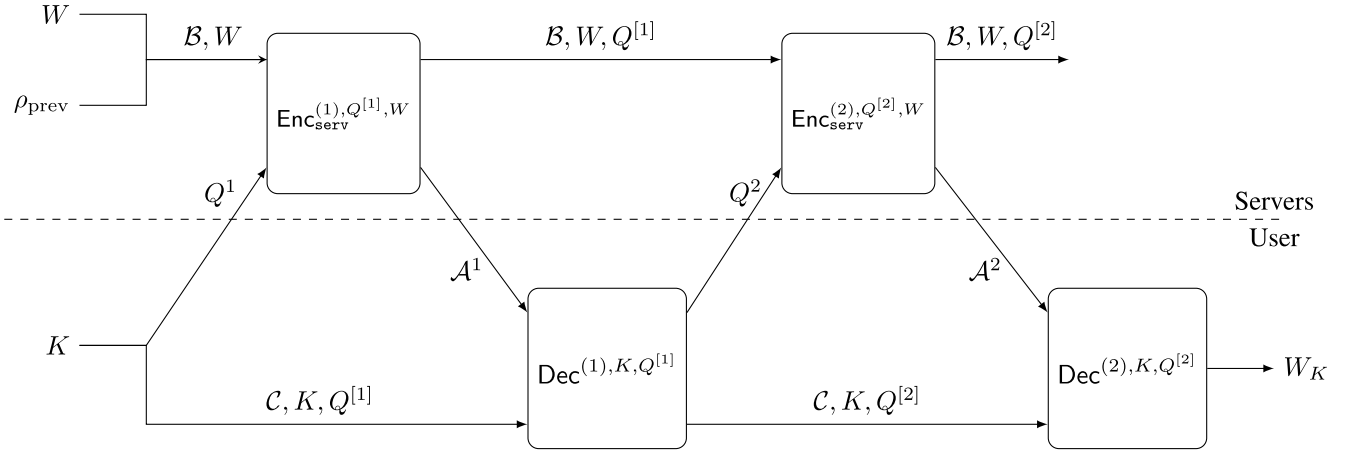
Fig. 2. Information flow in 2-round QPIR protocol. The servers have all files $W = (W_1, \ldots, W_f)$ and the user retrieves the K-th file W_K.

The user has a local quantum register $\mathcal{C}$ where the state is initialized depending on K and Q^1.

For $i \in \{1, \ldots, r\}$, the i-th round is described as follows. Let Q_t^i be the query to $\mathtt{serv}_t$ at round i, and we denote $Q^i := (Q_1^i, \ldots, Q_n^i)$ and $Q_t^{[i]} := (Q_t^1, \ldots, Q_t^i)$. The query Q^i for round i is determined at round $i-1$. The user sends Q_t^i to the t-th server $\mathtt{serv}_t$. Depending on $Q_t^{[i]}$ and W, each server $\mathtt{serv}_t$ applies a CPTP map $\mathsf{Enc}_{\mathtt{serv}_t}^{(i), Q_t^{[i]}, W}$ from $\mathcal{B}_t$ to $\mathcal{A}_t^i \otimes \mathcal{B}_t$. That is, when the collection of the encoders is written as

$$\mathsf{Enc}_{\mathtt{serv}}^{(i), Q^{[i]}, W} := \bigotimes_{t=1}^n \mathsf{Enc}_{\mathtt{serv}_t}^{(i), Q_t^{[i]}, W},$$

the state $\rho_W^{\mathcal{B}}$ on $\mathcal{B}$ is encoded as

$$\rho_W^{\mathcal{A}^i \mathcal{B}} := \mathsf{Enc}_{\mathtt{serv}}^{(i), Q^{[i]}, W}(\rho_W^{\mathcal{B}}),$$

where $\mathcal{A}^i := \mathcal{A}_1^i \otimes \cdots \otimes \mathcal{A}_n^i$. Each server transmits the system $\mathcal{A}_t^i$ to the user and the received state of the user is the reduced state

$$\rho_W^{\mathcal{A}^i} := \mathrm{Tr}_{\mathcal{B}} \, \rho_W^{\mathcal{A}^i \mathcal{B}}. \tag{32}$$

If $i < r$, the user applies a quantum instrument $\mathsf{Dec}^{(i), K, Q^{[i]}} = \{Y_{Q^{i+1}}\}_{Q^{i+1} \in \mathcal{Q}^{i+1}}$ from $\mathcal{A}^i \otimes \mathcal{C}$ to $\mathcal{C}$ depending on K and $Q^{[i]} := (Q^1, \ldots, Q^i)$, where $\mathcal{Q}_1^{i+1} \times \cdots \times \mathcal{Q}_n^{i+1}$ is the set of queries at round $i+1$ and Q^{i+1} is the measurement outcome. Then round i ends and round $i+1$ starts. If $i = r$, i.e., at the final round, the user applies a POVM $\mathsf{Dec}^{(r), K, Q^{[r]}} = \{Y_M\}_{M=0}^m$ on $\mathcal{A}^r \otimes \mathcal{C}$ depending on K and $Q^{[r]}$ and outputs the measurement outcome $M \in \{0, \ldots, m\}$. If $M = m$, it is considered as the retrieval failure.

Similarly to Section II-A, the security of the protocol is evaluated by the the error probability, the server secrecy, and the user secrecy defined by

$$P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(m,r)}) := \Pr_{W, K, Q^1}[M \neq W_K],$$

$$S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(m,r)}) := I(W_{K^c}; \mathfrak{user}(\Psi_{\mathrm{QPIR}}^{(m,r)}) | K),$$

$$S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(m,r)}) := \max_{t \in \{1, \ldots, n\}} I(K; \mathfrak{serv}_t(\Psi_{\mathrm{QPIR}}^{(m,r)})).$$

Given the QPIR protocol $\Psi_{\mathrm{QPIR}}^{(m,r)}$, we define the upload cost, the download cost, and the QPIR rate by

$$U(\Psi_{\mathrm{QPIR}}^{(m,r)}) := \sum_{i=1}^r \log |\mathcal{Q}^i|, \tag{33}$$

$$D(\Psi_{\mathrm{QPIR}}^{(m,r)}) := \sum_{i=1}^r \log \dim \mathcal{A}^i, \tag{34}$$

$$R(\Psi_{\mathrm{QPIR}}^{(m,r)}) := \frac{\log m}{D(\Psi_{\mathrm{QPIR}}^{(m,r)})}. \tag{35}$$

Now, we define the r-round QPIR capacities with four parameters as follows. For an error constraint $\alpha \in [0, 1)$, server secrecy constraint $\beta \in [0, \infty]$, user secrecy constraint $\gamma \in [0, \infty]$, and upload constraint $\theta \in [0, \infty]$, the *asymptotic security-constrained* r-*round capacity* and the *exact security-constrained* r-*round capacity* are defined as

$$C_{\mathrm{asymp}}^{\alpha, \beta, \gamma, \theta} := \sup_{(36)} \liminf_{\ell \to \infty} R(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}),$$

$$C_{\mathrm{exact}}^{\alpha, \beta, \gamma, \theta} := \sup_{(37)} \liminf_{\ell \to \infty} R(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}),$$

where the supremum is taken for sequences $\{m_\ell\}_{\ell=1}^\infty$ such that $\lim_{\ell \to \infty} m_\ell = \infty$ and for sequences $\{\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}\}_{\ell=1}^\infty$ of r-round QPIR protocols to satisfy either (36) or (37) given by

$$\limsup_{\ell \to \infty} P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}) \leq \alpha, \quad \limsup_{\ell \to \infty} S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}) \leq \beta,$$

$$\limsup_{\ell \to \infty} S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}) \leq \gamma, \quad \limsup_{\ell \to \infty} \frac{U(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)})}{D(\Psi_{\mathrm{QPIR}}^{(m_\ell)})} \leq \theta, \quad (36)$$

and

$$P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}) \leq \alpha, \quad S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}) \leq \beta,$$

$$S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)}) \leq \gamma, \quad \limsup_{\ell \to \infty} \frac{U(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)})}{D(\Psi_{\mathrm{QPIR}}^{(m_\ell, r)})} \leq \theta. \quad (37)$$

The multi-round QPIR capacity is derived as follows.

Theorem V.1 (Multi-Round QPIR Capacity): Let r be any positive integer. When servers can share prior entanglement,

the r-round QPIR capacity for $f \geq 2$ files and $n \geq 2$ servers is

$$C_{\text{exact}}^{0,\beta,\gamma,\theta,r} = C_{\text{asymp}}^{0,\beta,\gamma,\theta,r} = 1 \qquad (38)$$

for any $\beta, \gamma, \theta \in [0, \infty]$.

Proof: Eq. (38) is proved by the following inequalities:

$$1 \leq C_{\text{exact}}^{0,0,0,0,r} \leq C_{\text{exact}}^{0,\beta,\gamma,\theta,r} \leq C_{\text{asymp}}^{0,\beta,\gamma,\theta,r} \leq C_{\text{asymp}}^{0,\infty,\infty,\infty,r} \leq 1.$$

The first inequality holds by applying the rate-one QPIR protocol in Section III-B repetitively r times. The second, third, and fourth inequalities follow from the definition of the capacities. The last inequality is proved in Section V-B. Therefore, we obtain the theorem. □

B. Weak Converse Bound of Multi-Round QPIR Capacity

We prove the converse bound

$$C_{\text{asymp}}^{0,\infty,\infty,\infty,r} \leq 1. \qquad (39)$$

Our proof comes from the fact that the multi-round QPIR protocol can be considered as a case of the Classical-Quantum (CQ) channel coding with classical feedback [32]. In the CQ channel coding with classical feedback, the sender encodes a classical message W as a quantum state and sends the state over a fixed channel $\mathcal{N}$. The receiver performs a decoding measurement on the received state and returns the measurement outcome to the sender. The sender and the receiver iterate this process r times while using the previous measurement outcomes for encoding and decoding. At the end of the protocol, the receiver receives the classical message W. The paper [32] proved that the capacity of this problem when the sender and the receiver have their local quantum registers, respectively. More specifically, the paper [32] also considered the energy constraint E that for a given Hamiltonian H on the input system of $\mathcal{N}$, the input states $\rho_1, \ldots, \rho_r$ to $\mathcal{N}$ should satisfy $\sum_{i=1}^{r} \text{Tr} \, \rho_i H \leq E$. The CQ channel capacity is characterized by the following proposition.

Proposition V.1 ([32, Theorem 4]): Let $\mathcal{N}$ be a quantum channel, r be the number of communication rounds, m be the size of the message set, H be the Hamiltonian on the input system of $\mathcal{N}$, E be the energy constraint, and ε be the error probability. Suppose the sender and the receiver have local quantum registers, respectively. Then, for the CQ channel coding with classical feedback and energy constraint, we have the following inequality:

$$(1 - \varepsilon) \log m \leq \sup_{\rho : \text{Tr} \, \rho H \leq E} r H(\mathcal{N}(\rho)) + h_2(\varepsilon). \qquad (40)$$

The multi-round QPIR protocol can be considered as a case of this problem where the channel $\mathcal{N}$ is the identity channel and there is no energy constraint. To see this fact, we consider the the collection of the servers as the sender and the user as the receiver of the CQ channel coding, and focus on the communication of a classical message from the collection of the servers to the user. The servers sends to the user the systems $\mathcal{A}^i$ over the identity channel and the user sends queries Q^i to the servers as the measurement outcome on $\mathcal{A}^i$. The servers and the user have $\mathcal{B}$ and $\mathcal{C}$ as local quantum registers,

respectively. At the end of the protocol, the user obtains the classical target file W_K. Therefore, we can consider the multi-round QPIR protocol as a CQ channel coding with classical feedback.

By the similar proof of [32, Theorem 4], we have the following proposition.

Proposition V.2: Consider the CQ channel coding of a classical message $W \in \{0, \ldots, m-1\}$ from the sender to the receiver by sending quantum systems $\mathcal{A}^1, \ldots, \mathcal{A}^r$ sequentially over the identity channel and assisted by classical feedback. We assume that the sender and the receiver have local quantum registers, respectively. Let $\rho_W^{\mathcal{A}^i}$ be the state on $\mathcal{A}^i$. For the uniformly chosen message W and the decoding output M, we define the error probability $\varepsilon := \Pr[M \neq W]$. Then we have the following inequality

$$(1 - \varepsilon) \log m \leq \sum_{i=1}^{r} H(\rho_W^{\mathcal{A}^i}) + h_2(\varepsilon) \qquad (41)$$

$$\leq \sum_{i=1}^{r} \log \dim \mathcal{A}^i + h_2(\varepsilon), \qquad (42)$$

where $h_2(\cdot)$ is the binary entropy function.

For the completeness of our paper, we give a proof of Proposition V.2 in Appendix D.

Remark V.1: Proposition V.2 is slightly different from [32, Theorem 4]. First, whereas [32, Theorem 4] considers an energy constraint on the quantum channel, Proposition V.2 assumes no energy constraint. Second, whereas [32, Theorem 4] considers the repetitive uses of a fixed quantum channel $\mathcal{N}$, Proposition V.2 considers each use of the identity quantum channels over $\mathcal{A}^1, \ldots, \mathcal{A}^r$. Even with these differences, we can apply the same proof steps of [32, Theorem 4] and the first inequality of [32, Eq. (35)] is the inequality (41).

Now we prove the weak converse bound. We choose an arbitrary sequence $\{\Psi_{\text{QPIR}}^{(m_\ell, r)}\}_{\ell=1}^{\infty}$ of r-round QPIR protocols to satisfy $\varepsilon_\ell := P_{\text{err}}(\Psi_{\text{QPIR}}^{(m_\ell, r)}) \to 0$ as $\ell \to \infty$. Considering the collection of the n servers as the sender and the user as the receiver of Proposition V.2, we can apply Proposition V.2 to the r-round QPIR protocol $\Psi_{\text{QPIR}}^{(m_\ell, r)}$ with the classical message $W_K \in \{0, \ldots, m_\ell - 1\}$, the transmitted quantum systems $\mathcal{A}^1, \ldots, \mathcal{A}^r$, and the classical feedbacks $Q^1, \ldots, Q^r$. In this case, ε and m of Proposition V.2 is substituted by ε_ℓ and m_ℓ, i.e., Eq. (42) is written as

$$(1 - \varepsilon_\ell) \log m_\ell \leq \sum_{i=1}^{r} \log \dim \mathcal{A}^i + h_2(\varepsilon_\ell). \qquad (43)$$

Therefore, we have

$$\lim_{\ell \to \infty} R(\Psi_{\text{QPIR}}^{(m_\ell, r)}) = \lim_{\ell \to \infty} \frac{\log m_\ell}{\sum_{i=1}^{r} \log \dim \mathcal{A}^i} \leq 1, \qquad (44)$$

which implies (39).

VI. CONCLUSION

We have studied the capacity of QPIR with multiple servers when the servers share prior entanglement. Considering the user secrecy and the server secrecy, we defined two kinds of QPIR capacities: asymptotic and exact security-constrained

capacities with upload constraint. We proved that both QPIR capacities are 1 for any security constraints and any upload constraint. We have constructed a capacity-achieving rate-one protocol only with two servers when the file size is the square of an arbitrary integer. The converse has been proved by focusing on the download step of QPIR protocols. Furthermore, we have proved that the capacity of multi-round QPIR is also 1 by the weak converse bound.

It is an interesting open question whether the QPIR without shared entanglement also has an advantage over the classical PIR counterparts. This paper has considered the QPIR under the assumption of the prior entanglement and the quantum capacity of this case is strictly greater than the classical PIR capacity. The QPIR capacity without shared entanglement lies between the QPIR capacity of this paper and the classical PIR capacity. Therefore, it should be studied whether the quantum PIR capacity is strictly higher than the classical PIR capacity even without shared entanglement.

In this paper, we have assumed that the maximally entangled state can be shared by several servers. That is, we have made no restriction for shared entanglement. This setting is similar to the original studies [35], [36] for the entanglement-assisted classical capacity for a noisy quantum channel because they have no restriction for shared entanglement. The recent paper [37] derived the entanglement-assisted classical capacity for a noisy quantum channel when shared entanglement is limited. For the extension, the study [37] invented several new methods, which are essential for this restriction. Therefore, it is remained as a future problem to extend our result to the case when the shared entangled state is restricted.

As another problem, we can consider the QPIR capacity when the channel from servers to user are noisy quantum channels. It is natural to apply quantum error corrections to each noisy quantum channels and apply our QPIR protocol over the virtually implemented noiseless channels by error correction. In this case, the transmission rate is given by the quantum capacity of the noisy quantum channel. For the converse part, we can easily extend the discussion of Section IV. In this extension, the obtained upper bound of the transmission rate is the classical capacity of the noisy quantum channel. Hence, this simple method does not yield the QPIR capacity with noisy quantum channels. Therefore, it is another challenging problem to calculate the QPIR capacity with noisy quantum channels.

APPENDIX A
PRELIMINARIES ON QUANTUM INFORMATION THEORY

In this section, we briefly introduce the fundamental framework of quantum information theory. For more detail, see [31], [33], [34].

In classical information theory, the information is defined by an element x of a finite set $\mathcal{X}$, and the information x is changed by a function $f : \mathcal{X} \to \mathcal{Y}$, where $\mathcal{Y}$ is a finite set. Similarly, in quantum information theory, the quantum information is defined by a quantum state ρ on a quantum system $\mathcal{A}$, and the quantum states ρ on $\mathcal{A}$ is modified by quantum operations κ from the states on $\mathcal{A}$ to the states on a quantum system

$\mathcal{B}$. Another difference between the two information theories is the measurement of information. If there is no error on the measuring apparatus, the measurement of classical information x is deterministic and does not change the information, i.e., measurement outcome is x and the information x is not changed after the measurement. However, the measurement of a quantum state outputs its outcome probabilistically and changes the state. In the following, we define the quantum system, quantum state, quantum operation, and quantum measurement.

A quantum system is defined by a finite-dimensional Hilbert space $\mathcal{A}$. A vector x in $\mathcal{A}$ is denoted by $|x\rangle$, and $\bar{x}^\top$ is denoted by $\langle x|$. A quantum state is defined by a *density matrix* which is a positive semidefinite matrix ρ on $\mathcal{A}$ such that $\operatorname{Tr} \rho = 1$. We denote the set of density matrices on $\mathcal{A}$ by $\mathcal{S}(\mathcal{A})$. When a state ρ is rank-one, i.e., $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle$, the state is called a *pure state* and is identified with the vector $|\psi\rangle \in \mathcal{A}$. If a state ρ is not a pure state, it is called a *mixed state*. The composite system of $\mathcal{A}$ and $\mathcal{B}$ is defined by $\mathcal{A} \otimes \mathcal{B}$. For any quantum state $\rho \in \mathcal{S}(\mathcal{A} \otimes \mathcal{B})$, the *reduced state* on $\mathcal{A}$ is described by $\operatorname{Tr}_\mathcal{B} \rho$, where $\operatorname{Tr}_\mathcal{B}$ is the partial trace on the system $\mathcal{B}$. A state $\rho \in \mathcal{S}(\mathcal{A} \otimes \mathcal{B})$ is called a *separable state* if ρ is written as $\rho = \sum_i p_i \sigma_i \otimes \tau_i$ for states $\sigma_i \in \mathcal{S}(\mathcal{A})$, $\tau_i \in \mathcal{S}(\mathcal{B})$, and a probability distribution $\{p_i\}_i$. A state $\rho \in \mathcal{S}(\mathcal{A} \otimes \mathcal{B})$ is called an *entangled state* if ρ is not separable.

A quantum operation is defined by a *Completely Positive Trace-Preserving (CPTP) linear map* from $\mathcal{S}(\mathcal{A})$ to $\mathcal{S}(\mathcal{B})$. A linear map κ is called a *positive map* if κ maps a positive semidefinite matrix to a positive semidefinite matrix, and is called a *Completely-Positive (CP) map* if the linear map $\kappa \otimes \iota_{\mathbb{C}^n}$ is a positive map for any positive integer n, where $\iota_{\mathbb{C}^n}$ is the identity map on $\mathcal{S}(\mathbb{C}^n)$. An example of quantum operations is $\kappa_U(\rho) \coloneqq U\rho U^\dagger$ for a unitary matrix U on $\mathcal{A}$. By the operation κ_U, a pure state $|\psi\rangle \in \mathcal{A}$ is mapped to the pure state $U|\psi\rangle \in \mathcal{A}$.

A quantum measurement is defined by an *instrument*. A set $\{\kappa_\omega\}_{\omega \in \Omega}$ of CP maps from $\mathcal{S}(\mathcal{A})$ to $\mathcal{S}(\mathcal{B})$ is called an *instrument* if for any quantum state $\rho \in \mathcal{S}(\mathcal{A})$,

$$\sum_{\omega \in \Omega} \operatorname{Tr} \kappa_\omega(\rho) = 1.$$

With probability $\operatorname{Tr} \kappa_\omega(\rho)$, the measurement outcome is ω and the state after the measurement is $\kappa_\omega(\rho)/\operatorname{Tr} \kappa_\omega(\rho)$. When one is interested only in the measurement probability and the outcome, the measurement is described by a *Positive Operator-Valued Measure (POVM)*. A set $\{M_\omega\}_{\omega \in \Omega}$ of positive semi-definite matrices is called an *POVM* if $\sum_{\omega \in \Omega} M_\omega = I$. With probability $\operatorname{Tr} \rho M_\omega$, the measurement outcome is ω.

APPENDIX B
QUANTUM INFORMATION MEASURES

In this section, we introduce quantum information measures necessary for the analysis of QPIR protocols.

Any quantum state ρ is diagonalized as $\rho = \sum_i p_i |i\rangle\langle i|$ for a probability distribution $\{p_i\}_i$. For a state $\rho = \sum_i p_i |i\rangle\langle i|$, *von Neumann entropy* is defined by

$$H(\rho) \coloneqq H(\{p_i\}), \qquad (45)$$

where $H(\cdot)$ in the right-hand side of (45) is Shannon entropy $H(\{p_i\}) := -\sum_i p_i \log p_i$. For any state $\rho \in \mathcal{S}(\mathcal{A} \otimes \mathcal{B})$, we use the notation

$$H(\mathcal{A})_\rho := H(\mathrm{Tr}_\mathcal{B}\,\rho), \quad H(\mathcal{B})_\rho := H(\mathrm{Tr}_\mathcal{A}\,\rho),$$
$$H(\mathcal{A},\mathcal{B})_\rho := H(\rho).$$

For any state $\rho \in \mathcal{S}(\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C})$, the *quantum conditional entropy*, *quantum mutual information*, and *quantum conditional mutual information* are defined as

$$H(\mathcal{A}|\mathcal{B})_\rho := H(\mathcal{A},\mathcal{B})_\rho - H(\mathcal{B})_\rho, \tag{46}$$
$$I(\mathcal{A};\mathcal{B})_\rho := H(\mathcal{A})_\rho + H(\mathcal{B})_\rho - H(\mathcal{A},\mathcal{B})_\rho, \tag{47}$$
$$I(\mathcal{A};\mathcal{B}|\mathcal{C})_\rho := I(\mathcal{A};\mathcal{B},\mathcal{C})_\rho - I(\mathcal{A};\mathcal{C})_\rho. \tag{48}$$

When a quantum state $\rho_X \in \mathcal{S}(\mathcal{A})$ is prepared depending on the random variable $X \in \mathcal{X}$, the state on the composite system of $\mathcal{A}$ and X is defined by

$$\tilde{\rho} = \sum_{x \in \mathcal{X}} \Pr[X = x] \cdot \rho_x \otimes |x\rangle\langle x|.$$

For convenience, we denote $H(\cdot)_{\rho_X} := H(\cdot)_{\tilde{\rho}}$ and $I(\cdot)_{\rho_X} := I(\cdot)_{\tilde{\rho}}$.

APPENDIX C
DERIVATION OF (27)

For the derivation of (27), we use the data-processing inequality of quantum relative Rényi entropy. When $s \in (0, 1)$, quantum relative Rényi entropy is defined as

$$D_{1+s}(\rho\|\sigma) := \frac{1}{s}\,\mathrm{Tr}\,\rho^{1+s}\sigma^{-s} \tag{49}$$

for any states ρ and σ such that $\mathrm{supp}(\rho) \subset \mathrm{supp}(\sigma)$, and D_{1+s} satisfies the data-processing inequality with respect to measurements:

$$D_{1+s}(\rho\|\sigma) \geq D_{1+s}(P_\rho^\mathcal{M}\|P_\sigma^\mathcal{M}), \tag{50}$$

where $P_\rho^\mathcal{M}$ and $P_\rho^\mathcal{M}$ are probability distributions after the measurement $\mathcal{M} = \{M_i\}_i$ on ρ and σ, respectively, i.e.,

$$P_\rho^\mathcal{M} = \sum_i (\mathrm{Tr}\,\rho M_i) \cdot |i\rangle\langle i|, \quad P_\sigma^\mathcal{M} = \sum_i (\mathrm{Tr}\,\sigma M_i) \cdot |i\rangle\langle i|.$$

Next, we prepare the following notations:

$$\sigma_z := \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \rho_{w,z},$$
$$\tilde{\rho}_z := \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} |w\rangle\langle w| \otimes \rho_{w,z},$$
$$\tilde{\sigma}_z := \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} |w\rangle\langle w| \otimes \sigma_z,$$
$$\tilde{\mathsf{Y}} := \sum_{w=0}^{\mathsf{m}-1} |w\rangle\langle w| \otimes \mathsf{Y}_w,$$
$$\mathcal{M} = \{\tilde{\mathsf{Y}}, \mathsf{I} - \tilde{\mathsf{Y}}\},$$

where $\{\mathsf{Y}_w\}_{w=0}^{\mathsf{m}}$ is the decoding measurement defined in Section II. With these notations, we have

$$\mathrm{Tr}\,\tilde{\rho}_z\tilde{\mathsf{Y}} = \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \mathrm{Tr}\,\rho_{w,z}\mathsf{Y}_w = 1 - P_{\mathrm{err},z}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}), \tag{51}$$

$$\mathrm{Tr}\,\tilde{\sigma}_z\tilde{\mathsf{Y}} = \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \mathrm{Tr}\,\sigma_z\mathsf{Y}_w \leq \frac{1}{\mathsf{m}}\,\mathrm{Tr}\,\sigma_z \sum_{w=0}^{\mathsf{m}} \mathsf{Y}_w = \frac{1}{\mathsf{m}}. \tag{52}$$

Combining (50), (51), and (52), we can derive Eq. (27) similarly as [31, (4.66)]:

$$(1 - P_{\mathrm{err},z}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}))^{1+s}\mathsf{m}^s$$
$$\overset{(a)}{\leq} (\mathrm{Tr}\,\tilde{\rho}_z\tilde{\mathsf{Y}})^{1+s}(\mathrm{Tr}\,\tilde{\sigma}_z\tilde{\mathsf{Y}})^{-s}$$
$$\leq (\mathrm{Tr}\,\tilde{\rho}_z\tilde{\mathsf{Y}})^{1+s}(\mathrm{Tr}\,\tilde{\sigma}_z\tilde{\mathsf{Y}})^{-s}$$
$$\quad + (1 - \mathrm{Tr}\,\tilde{\rho}_z\tilde{\mathsf{Y}})^{1+s}(1 - \mathrm{Tr}\,\tilde{\sigma}_z\tilde{\mathsf{Y}})^{-s}$$
$$= \exp\left(sD_{1+s}(P_{\tilde{\rho}_z}^\mathcal{M}\|P_{\tilde{\sigma}_z}^\mathcal{M})\right)$$
$$\overset{(b)}{\leq} \exp\left(sD_{1+s}(\tilde{\rho}_z\|\tilde{\sigma}_z)\right)$$
$$= \mathrm{Tr}\,\tilde{\rho}_z^{1+s}\tilde{\sigma}_z^{-s} = \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \mathrm{Tr}\,\rho_{w,z}^{1+s}\sigma_z^{-s},$$

where (a) is from (51) and (52) and (b) is from (50).

APPENDIX D
PROOF OF PROPOSITION V.2

For the proof of Proposition V.2, we follow the proof of [32, Theorem 4]. Before the proof, we prepare two lemmas from [32].

Lemma D.1 ([32, Lemma 2]): Let τ_{WFAB} be a classical-quantum state such that

$$\tau_{WFAB} = \sum_{w,f} p(w,f)|w,f\rangle\langle w,f| \otimes \tau_{AB|wf}, \tag{53}$$

where $\tau_{AB|wf}$ are pure states. Let $\mathcal{M}$ be one-way Local Operations and Classical Communication (LOCC) map from $A \otimes B$ to $A' \otimes B' \otimes X$, where X is a classical system which is sent from B to A. Then, we have

$$I(W; B'FX) + H(B'|WFX) \tag{54}$$
$$\leq I(W; BF) + H(B|WF). \tag{55}$$

Lemma D.2 ([32, Lemma 3]): Let τ_{WFAB} be a classical-quantum state defined in (53). Then

$$I(W; ABF) + H(AB|WF) \tag{56}$$
$$\leq H(A) + I(W; BF) + H(B|WF). \tag{57}$$

For the proof, we formally describe the communication protocol as follows. We denote the local registers of the sender and the receiver before the communication by $\mathcal{B}^0$ and $\mathcal{C}^0$. Let $\mathcal{A}^0 = \mathbb{C}$. At round $i \in \{1, \ldots, \mathsf{r}\}$, the receiver applies a quantum instrument from $\mathcal{A}^{i-1} \otimes \mathcal{C}^{i-1}$ to $\mathcal{C}^i$ depending on $Q^{[i-1]}$ and sends the measurement outcome Q^i to the sender. Then, the sender applies a quantum operation from $\mathcal{B}^{i-1}$ to $\mathcal{A}^i \otimes \mathcal{B}^i$ depending on W and $Q^{[i]} := (Q^1, \ldots, Q^i)$, and sends $\mathcal{A}^i$ to the receiver. After the final rth-round, the sender applies

a POVM on $\mathcal{A}^r \otimes \mathcal{C}^r$ depending on $Q^{[r]}$ and the measurement outcome M is the decoding output.

Now, we prove Proposition V.2. First, we have

$$(1-\varepsilon)\log \mathsf{m} \overset{(a)}{\le} I(W; M) + h_2(\varepsilon) \tag{58}$$

$$\overset{(b)}{\le} I(W; \mathcal{A}^r \mathcal{C}^r Q^{[r]}) + h_2(\varepsilon), \tag{59}$$

where (a) is from Fano's inequality

$$H(W|M) \le \varepsilon \log \mathsf{m} + h_2(\varepsilon) \tag{60}$$

and the uniform distribution of W, and (b) is from the data-processing inequality for the decoding POVM. Then, it is enough to derive the inequality

$$I(W; \mathcal{A}^r \mathcal{C}^r Q^{[r]}) \le \sum_{i=1}^{r} H(\rho_W^{\mathcal{A}^i}) \tag{61}$$

for the proof of Proposition V.2.

To derive (61), we apply Lemma D.1 and Lemma D.2 as follows. Note that there is no constraint in the size of local registers. Thus, without losing generality, we assume that the sender's and the receiver's local registers are sufficiently large that the joint state on the entire protocol is always written as pure states. Since the operations at each round can be considered as a one-way LOCC map, we can apply Lemma D.1 for $(W, F, A, B, A', B', X) :=$ $(W, Q^{[i-1]}, \mathcal{B}^{i-1}, \mathcal{A}^{i-1} \otimes \mathcal{C}^{i-1}, \mathcal{A}^i \otimes \mathcal{B}^i, \mathcal{C}^i, Q^i)$:

$$I(W; \mathcal{C}^i Q^{[i]}) + H(\mathcal{C}^i | W Q^{[i]})$$
$$\le I(W; \mathcal{A}^{i-1} \mathcal{C}^{i-1} Q^{[i-1]}) + H(\mathcal{A}^{i-1} \mathcal{C}^{i-1} | W Q^{[i-1]}).$$

Furthermore, applying Lemma D.2 with $(W, F, A, B) :=$ $(W, Q^{[i]}, \mathcal{A}^i, \mathcal{C}^i)$. we have

$$I(W; \mathcal{A}^i \mathcal{C}^i Q^{[i]}) + H(\mathcal{A}^i \mathcal{C}^i | W Q^{[i]})$$
$$\le H(\mathcal{A}^i) + I(W; \mathcal{C}^i Q^{[i]}) + H(\mathcal{C}^i | W Q^{[i]}). \tag{62}$$

Combining the above two inequalities, we have

$$I(W; \mathcal{A}^i \mathcal{C}^i Q^{[i]}) + H(\mathcal{A}^i \mathcal{C}^i | W Q^{[i]})$$
$$\le H(\mathcal{A}^i) + I(W; \mathcal{A}^{i-1} \mathcal{C}^{i-1} Q^{[i-1]})$$
$$+ H(\mathcal{A}^{i-1} \mathcal{C}^{i-1} | W Q^{[i-1]}) \tag{63}$$

Applying the inequality (63) recursively, we obtain the desired inequality (61) as

$$I(W; \mathcal{A}^r \mathcal{C}^r Q^{[r]})$$
$$\le I(W; \mathcal{A}^r \mathcal{C}^r Q^{[r]}) + H(\mathcal{A}^r \mathcal{C}^r | W Q^{[r]})$$
$$\overset{(c)}{\le} \sum_{i=2}^{r} H(\mathcal{A}^i) + I(W; \mathcal{A}^1 \mathcal{C}^1 Q^1) + H(\mathcal{A}^1 \mathcal{C}^1 | W Q^1)$$
$$\overset{(d)}{\le} \sum_{i=1}^{r} H(\mathcal{A}^i) + I(W; \mathcal{C}^1 Q^1) + H(\mathcal{C}^1 | W Q^1)$$
$$\overset{(e)}{=} \sum_{i=1}^{r} H(\mathcal{A}^i),$$

where (c) is derived by applying (63) recursively for $i = r, r-1, \ldots, 2$, (d) is from (62), and (e) is obtained as follows: $I(W; \mathcal{C}^1 Q^1) = 0$ because the receiver prepares the state

of $\mathcal{C}^1 \otimes Q^1$ independently of the sender's message W, and $H(\mathcal{C}^1 | W Q^1) = 0$ since the initial state of the local register $\mathcal{C}^1$ is a pure state.

REFERENCES

[1] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[2] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 1592, J. Stern, Ed. Berlin, Germany: Springer, 1999, doi: 10.1007/3-540-48910-X_28.

[3] H. Lipmaa, "First CPIR protocol with data-dependent computation," in *Proc. 12th Int. Conf. Inf. Secur. Cryptol.*, 2010, pp. 193–210.

[4] A. Beimel and Y. Stahl, "Robust information-theoretic private information retrieval," in *Proc. 3rd Int. Conf. Secur. Commun. Netw. (SCN)*, 2003, pp. 326–341.

[5] C. Devet, I. Goldberg, and N. Heninger, "Optimally robust private information retrieval," in *Proc. 21st USENIX Secur. Symp.*, Aug. 2012, pp. 269–283.

[6] I. Kerenidis and R. de Wolf, "Exponential lower bound for 2-query locally decodable codes via a quantum argument," in *Proc. 35th ACM Symp. Theory Comput. (STOC)*, 2003, pp. 106–115.

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

[8] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, Aug. 2011, Art. no. 022313.

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

[10] 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.

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

[12] D. Aharonov, Z. Brakerski, K.-M. Chung, A. Green, C.-Y. Lai, and O. Sattath, "On quantum advantage in information theoretic single-server PIR," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 11478, Y. Ishai and V. Rijmen, Eds. Cham, Switzerland: Springer, 2019, pp. 219–246.

[13] 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.

[14] C. Tian, H. Sun, and J. Chen, "Capacity-achieving private information retrieval codes with optimal message size and upload cost," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 7613–7627, Nov. 2019.

[15] H. Sun and S. A. Jafar, "The capacity of symmetric private information retrieval," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Washington, DC, USA, Dec. 2016, pp. 1–5.

[16] T. H. Chan, S.-W. Ho, and H. Yamamoto, "Private information retrieval for coded storage," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 2842–2846.

[17] 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, Jan. 2017.

[18] 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.

[19] S. Kumar, H.-Y. Lin, E. Rosnes, and A. G. i Amat, "Achieving maximum distance separable private information retrieval capacity with linear codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4243–4273, Jul. 2019.

[20] H.-Y. Lin, S. Kumar, E. Rosnes, and A. G. i Amat, "An MDS-PIR capacity-achieving protocol for distributed storage using non-MDS linear codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 966–970.

[21] 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.

[22] H. Sun and S. A. Jafar, "Multiround private information retrieval: Capacity and storage overhead," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5743–5754, Aug. 2018.

[23] M. O. Rabin, "How to exchange secrets with oblivious transfer," Harvard Univ., Cambridge, MA, USA, Tech. Rep. TR-81, 1981.

[24] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Commun. ACM*, vol. 28, no. 6, pp. 637–647, Jun. 1985.

[25] J. Kilian, "Founding crytpography on oblivious transfer," in *Proc. 20th Annu. ACM Symp. Theory Comput. (STOC)*, 1988, p. 20.

[26] Y. Ishai, M. Prabhakaran, and A. Sahai, "Founding cryptography on oblivious transfer—Efficiently," in *Proc. CRYPTO*, 2008, pp. 572–591.

[27] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 592–629, Jun. 2000.

[28] H. Kobayashi and K. Matsumoto, "Quantum multi-prover interactive proof systems with limited prior entanglement," *J. Comput. Syst. Sci.*, vol. 66, no. 3, pp. 429–450, May 2003.

[29] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies," in *Proc. 19th IEEE Annu. Conf. Comput. Complex.*, Jun. 2004, pp. 236–249.

[30] B. W. Reichardt, F. Unger, and U. Vazirani, "A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games," in *Proc. 4th Conf. Innov. Theor. Comput. Sci. (ITCS)*, New York, NY, USA, 2013, pp. 321–322.

[31] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Graduate Texts in Physics), 2nd ed. Cham, Switzerland: Springer, 2017.

[32] D. Ding, Y. Quek, P. W. Shor, and M. M. Wilde, "Entropy bound for the classical capacity of a quantum channel assisted by classical feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 250–254.

[33] M. M. Wilde, *Quantum Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[34] M. Tomamichel, *Quantum Information Processing With Finite Resources: Mathematical Foundations* (Springer Briefs in Mathematical Physics). Cham, Switzerland: Springer, 2016.

[35] 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, p. 3081, 1999.

[36] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, Oct. 2002.

[37] K. Wang and M. Hayashi, "Permutation enhances classical communication assisted by entangled states," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 1–26.

[38] S. Song and M. Hayashi, "Capacity of quantum private information retrieval with multiple servers," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1727–1731.

Seunghoan Song (Graduate Student Member, IEEE) received the B.E. degree from Osaka University in 2017 and the master's degree in mathematical science from Nagoya University in 2019. He is currently pursuing the Ph.D. degree with the Graduate School of Mathematics, Nagoya University. He has been a Research Fellow of the Japan Society of the Promotion of Science (JSPS) since 2020. His research interests include classical and quantum information theory and its applications to secure communication protocols. He was awarded the School of Engineering Science Outstanding Student Award in 2017 and the Graduate School of Mathematics Award for Outstanding Master's Thesis in 2019.

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 as a Research Fellow with the Japan Society of the Promotion of Science (JSPS), Kyoto University, from 1998 to 2000, and with the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN, from 2000 to 2003, and as the Research Head with 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 with the Superrobust Computation Project Information Science and Technology Strategic Core (21st Century COE by MEXT) Graduate School of Information Science and Technology, The University of Tokyo, from 2004 to 2007. He worked as an Associate Professor with the Graduate School of Information Sciences, Tohoku University, from 2007 to 2012. In 2012, he joined as a Professor with the Graduate School of Mathematics, Nagoya University. Also, he was appointed as a Visiting Research Associate Professor with 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 with the Center for Advanced Intelligence Project, RIKEN, from 2017 to 2020. He worked as a Visiting Professor with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China, from 2018 to 2020, and as a Visiting Professor with the Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen, from 2019 to 2020. In 2020, he joined as a Chief Research Scientist with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology. In 2006, he published the book *Quantum Information: An Introduction* (Springer), whose revised version was published as *Quantum Information Theory: Mathematical Foundation* (Graduate Texts in Physics, Springer) in 2016. In 2016, he published the other two books *Group Representation for Quantum Theory* and *A Group Theoretic Approach to Quantum Information* (Springer). His research interests include classical and quantum information theory and classical and quantum statistical inference. He 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 the Japan Society for the Promotion of Science. He is on the Editorial Board of the *International Journal of Quantum Information* and the *International Journal on Advances in Security*.