Information-Theoretic Aspects of Quantum Private Information Retrieval

A dissertation for the degree of
Doctor of Philosophy (Mathematical Science)

Seunghoan Song

Graduate School of Mathematics
Nagoya University

2020

Abstract

When a user retrieves information from databases, it is often required to protect the privacy of the user. Quantum private information retrieval (QPIR) is a protocol in which a user retrieves one of multiple messages from non-communicating multiple servers by downloading quantum systems without revealing which message is retrieved to any individual server. Symmetric QPIR is QPIR with server secrecy in which the user only obtains the retrieved message but no other information of other messages.

This thesis investigates the fundamental communication limit of symmetric and non-symmetric QPIR and constructs the optimal QPIR protocols achieving the communication limit. The communication cost of a QPIR protocol is evaluated by the *QPIR rate* defined as the ratio of the size of one message to the whole dimension of the downloaded quantum systems. The supremum of the QPIR rate, called the *QPIR capacity*, characterizes the communication limit of QPIR.

Assuming that the servers share prior entanglement, we prove that the symmetric and non-symmetric QPIR capacities are 1 regardless of the number of servers and messages. We construct a rate-one protocol with only 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.

As a variant of QPIR with stronger security requirements, t-private QPIR is a protocol in which the identity of the retrieved message is kept secret even if at most t servers may collude to reveal the identity. We prove that the symmetric and non-symmetric t-private n-server QPIR capacities are $\min\{1, 2(\mathsf{n}-\mathsf{t})/\mathsf{n}\}$ for any $1 \leq \mathsf{t} < \mathsf{n}$. We construct a capacity-achieving QPIR protocol by the stabilizer formalism and prove the optimality of our

protocol. The proposed capacity is also greater than the classical counterpart.

Finally, we give a symmetric $(\mathsf{n}-1)$-private QPIR protocol with bipartite entangled states. The protocol has the QPIR rate $\lceil \mathsf{n}/2 \rceil^{-1}$, which implies that it is capacity-achieving for an even number of servers n. The protocol is practical since the bipartite entangled states are reliably generated with current quantum technology compared to multipartite entangled states.

List of Publications

The thesis is based on the following publications. Chapter 3 and Chapter 4 are based on Sections II–IV and Section V of [1], respectively. Chapter 5 and Chapter 6 are based on [3] and [2], respectively.

[1] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, DOI:10.1109/TIT.2020.3022515, accepted.

[2] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019 (submitted to *Journal on Selected Areas in Information Theory*).

[3] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1077–1082, 2020 (submitted to *IEEE Transactions on Information Theory*).

Most of the contents in Section 2.1 *"Mathematical framework of quantum information theory"* have appeared in Chapter 2 of my master's thesis.

[4] S. Song, "Secure quantum network code," Master's thesis, Nagoya University, 2019.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my advisor Masahito Hayashi. I appreciate his willingness to discuss all of my topics and share his valuable insights throughout my entire graduate career. I also thank another advisor François Le Gall for generously answering many questions and giving valuable advice. I thank my colleagues in Graduate school of mathematics, Nagoya University. I would especially thank Yuuya Yoshida for sharing his deep and stimulating insight on mathematics and having many scientific and non-scientific discussions. I also thank Hayato Arai, Ziyu Liu, and Daiki Suruga for many stimulating conversations. I would like to thank Hsuan-Yin Lin for introducing to me the private information retrieval and thank Eirik Rosnes, Camilla Hollanti, Lukas Holzbaur, Matteo Allaix, and Tefjol Pllaha for fruitful discussions on private information retrieval. I also thank Jaewan Kim for accepting my visit to KIAS and Youngrong Lim for many helpful discussions during the visit. My graduate career is supported by Rotary Yoneyama Memorial Scholarship, Lotte Foundation Scholarship, and JSPS Grant-in-Aid for JSPS Fellows No. JP20J11484.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Private information retrieval

Information security is one of the main concerns in the modern information era. Especially, with the advancing technology of the big data analysis and the recommendation systems, the importance of user's privacy is increasing when the user access to databases. For example, the recommendation systems such as for the videos, the products, and the social network contents are based on the access information of users and the collected information often results in some unintentional leakage of users' privacy. For such cases, it is required to protect the privacy of the user who retrieves information from databases.

Introduced by Chor, Goldreich, Kushilevitz, and Sudan [5], Private Information Retrieval (PIR) is a cryptographic protocol in which a user retrieves a message from server(s) without revealing which message is retrieved to any individual server. In addition to its direct application, PIR is related to other cryptographic protocols such as the oblivious transfer [6, 7], the secure multiparty computation [8,9], and the secret sharing [10,11]. Furthermore, PIR is also related to an error-correcting code, called locally decodable codes [12–15].

As depicted in Figure 1.1, a PIR protocol is described as follows. Suppose that a server contains a classical message set $M_1, \ldots, M_{\mathsf{f}}$. A user wants to retrieve one of the messages from the server. Let K be the index of the targeted message, i.e., the user wants to retrieve M_K. The user uploads queries $Q^{(1)}, \ldots, Q^{(\mathsf{r})}$ and downloads answer $A^{(1)}, \ldots, A^{(\mathsf{r})}$ from the server

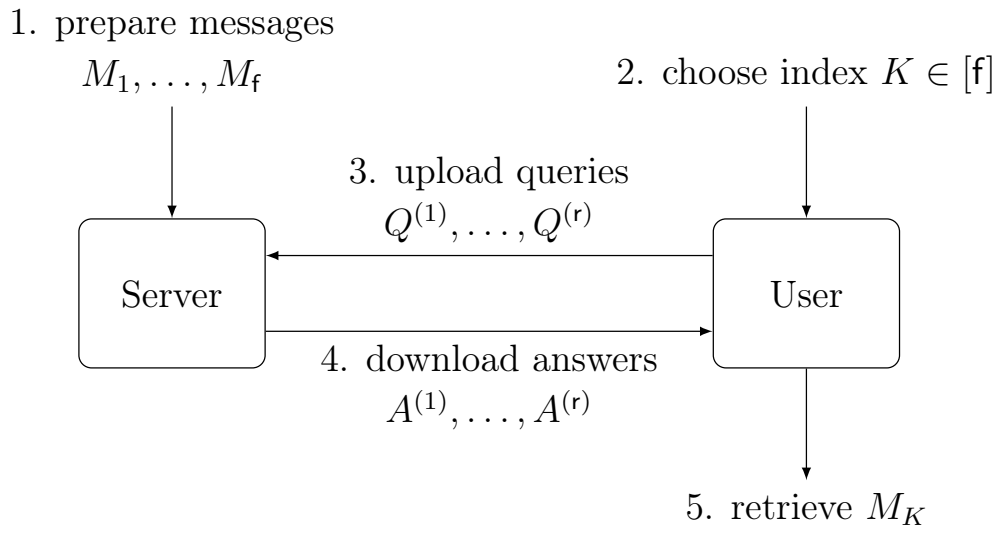


Figure 1.1: One-server PIR protocol.

interactively. The user finally decodes M_K. For the secrecy of the user's request, it is required that the server obtains no information of the target index K. Though this problem seems impossible at first glance, there is a trivial solution: if the user downloads all messages from the server, the user obtains the targeted message M_K and the server cannot know which message is requested. This trivial solution lacks practicality since it is inefficient. Unfortunately, Chor et al. [5] proved that this trivial solution is optimal for communication efficiency. To be precise, they evaluated the communication efficiency by the communication complexity, which is the sum of information bits transmitted between the user and the servers, and showed that the optimal communication complexity is linear to the size of all messages.

Despite this negative result, there have been mainly two approaches to reduce the communication efficiency: PIR with computational assumptions [16–18] and PIR with multiple servers [15, 19–22]. In the first approach, PIR has been considered with the computational assumptions such as the difficulty of quadratic residuosity problem [16] and the phi-hiding assumption [17]. On the other hand, this thesis focuses on PIR with multiple servers. Multi-server PIR considers the case where each of multiple servers contains a copy of all messages with it is assumed that the servers do not communicate with each other. It has been discussed from the first paper of PIR by Chor et

al. [5] and they proposed the following one-round protocol with two servers, which improves the communication complexity significantly.

Protocol 1.1. *Suppose that each of two servers, namely Server 1 and Server 2, contains a copy of all messages* $M_1, \dots, M_{\mathsf{f}} \in \{0, \dots, \mathsf{m}-1\}$*, and the two servers are forbidden to communicate with each other. For retrieving* M_K*, the user prepares two queries* Q_1 *and* Q_2 *as subsets of* $\{1, \dots, \mathsf{f}\}$ *such that* $(Q_1 - Q_2) \cup (Q_2 - Q_1) = \{K\}$ *and sends* Q_i *to Server* i*. Each of Server* i *returns the answer* $A_i = \sum_{j \in Q_i} M_j$ *to the user, where the summation is with respect to the addition modulo* m*. Finally, the user can obtain* $\pm M_K = A_1 - A_2$*, where the sign is determined by whether* $K \in Q_1$ *or* $K \in Q_2$*.*

Since any subset of $\{1, \dots, \mathsf{f}\}$ is described by an f-bit sequence, the upload cost of the above protocol is $2\mathsf{f}$ bits in total and the download cost is $2 \log \mathsf{m}$ bits in total. Thus, Protocol 1.1 has the communication complexity $2\mathsf{f} + 2 \log \mathsf{m}$, which is significant improvement from $\mathsf{f} \log \mathsf{m}$ bits of the trivial solution. The paper [5] and the following works [15,19,20] have also improved the communication complexity with more servers. Similar to Protocol 1.1, most of the multi-server PIR protocols have been constructed with one-round communication. Thus, if it is not specified, we consider the multi-server PIR as the multi-server one-round PIR throughout the thesis.

In PIR, the user may obtain some information on the $\mathsf{n}-1$ non-targeted messages. For example, in Protocol 1.1, the user obtains partial sums of non-targeted messages from the answers A_1 and A_2. Therefore, it is preferable to consider the *server secrecy* in which the user obtains no information other than the targeted message. PIR with the server secrecy is called *symmetric PIR*, which is also called *Oblivious Transfer (OT)* [6,7] in the one-server case. In other words, 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 multi-party computation [8,9]. The one-server symmetric PIR is impossible from the impossibility of OT with information-theoretic security and Gertner et al. [23] proved that the symmetric PIR does not exist even with multiple servers. However, Gertner et al. [23] constructed a symmetric PIR protocol with the assumption of shared randomness among multiple servers.

Furthermore, one critical weakness of the multi-server PIR is the assumption of no communication between servers. In the practical application of the

PIR protocols, some of the servers may communicate and collude to identify the user's request. The t-*private PIR* [5, 14, 21, 22] is PIR with stronger user secrecy, called *user* t-*secrecy* or t-*privacy*, in which the identity of the targeted message is unknown to any collection of t servers. In t-private PIR, it is assumed that the user does not know which servers are colluding but only knows the number of colluding servers t.

1.2 Information-theoretic approach to PIR

With its origin by Claude Shannon [24], one of the main goals of the information theory is to survey the asymptotic behavior of information-processing tasks when information resources are available asymptotically many times. For instance, the source coding considers the asymptotic compression rate for arbitrarily large sequences of i.i.d. random variables, and the channel coding considers the asymptotic transmission rate when a given channel can be used arbitrarily many times.

In a similar sense, Chan, Ho, and Yamamoto [25] started to consider the multi-server one-round PIR when the message size can be arbitrarily large. For the measure of communication efficiency, they only considered the download cost because any one-round PIR protocol can be modified so that the query cost is negligible to the message size. To see this, suppose that the queries are prepared originally for a $\log \mathsf{m}$-bit message. Then, the user can reuse the same query k times for retrieving a $(k \log \mathsf{m})$-bit message for arbitrary natural number k. Thus, the upload (query) cost can be made negligible by increasing the message size arbitrarily large for the fixed query.

Furthermore, to characterize the asymptotic communication limit of PIR, Sun and Jafar [26] defined the *PIR rate* of a protocol as the ratio of the size of one message to the number of total downloaded bits and the *PIR capacity* as the supremum of the PIR rate for fixed numbers of servers and messages. They derived the PIR capacity for n servers and f messages as

$$C = \frac{1 - 1/\mathsf{n}}{1 - (1/\mathsf{n})^{\mathsf{f}}}, \tag{1.1}$$

which is greater than the PIR rate $1/\mathsf{f}$ of the trivial solution of downloading all messages. The PIR capacity approaches 1 as the number of servers n goes

to infinity. The paper [27] proposed a capacity-achieving PIR protocol with the minimum upload cost and message size in a class of PIR protocols.

PIR capacities have also been derived in many other settings [28–40]. The symmetric PIR capacity is $1-\mathsf{n}^{-1}$ [28], the t-private PIR capacity is $(1-\mathsf{t}/\mathsf{n})/(1-(\mathsf{t}/\mathsf{n})^{\mathsf{f}})$ [29], and the symmetric t-private PIR capacity is $1-\mathsf{t}/\mathsf{n}$ [30]. The papers [31–37] have considered PIR with coded databases, where each server contains coded symbols of the messages instead of a copy of all messages. When the messages are coded by an (n,k) Maximum Distance Separable (MDS) code, the PIR capacity is $(1-\mathsf{k}/\mathsf{n})/(1-(\mathsf{k}/\mathsf{n})^{\mathsf{f}})$ [31]. Multi-round PIR has also been studied in [38] and the capacity was proved to be the same as the PIR capacity derived in [26].

1.3 Quantum private information retrieval

There has been growing interest in quantum information theory as a mean to overcome the limitations of existing communication technologies. Above all, there has been a great deal of interest in enhancing security such as quantum key distribution [41, 42], quantum zero-knowledge proof [43], quantum fingerprinting [44], quantum secret sharing [45], quantum bit commitment [46].

As one direction of quantum secure protocols, Quantum PIR (QPIR) has been studied [47–55]. The papers [47–54] have considered the case where two-way quantum communication is allowed, i.e., the queries and the answers are quantum information. Let s be the number of bits in the database, i.e., the total size of all messages. When the server does not deviate from the protocol, Le Gall [48] proposed a one-server QPIR protocol whose communication complexity is $O(\sqrt{\mathsf{s}})$, and Kerenidis et al. [49] improved this result to $O(\operatorname{poly}\log \mathsf{s})$. However, Baumeler and Broadbent [50] showed that for a stronger adversarial model, called *specious server model*, the trivial solution of downloading all messages is again optimal for one-server QPIR. To be specific, in the specious server model, the server can perform any malicious operations as far as they are not noticed by users, and they showed that the communication complexity is at least $O(\mathsf{s})$ in this model. For multi-server QPIR, Kerenidis and de Wolf [51] proposed a two-server QPIR protocol with communication complexity $O(\mathsf{s}^{3/10})$, and they [52] proved that quantum symmetric QPIR can be constructed without shared randomness among servers.

The key resource to make the advantages of quantum communication

is quantum entanglement. The quantum enhancements in one-server QPIR [48,49] and multi-server symmetric QPIR [52] are achieved by generating and using entanglement between the user and the servers. For better advantages, the papers [49, 53] considered one-server QPIR with prior entanglement between the user and the server. With the prior entanglement, Kerenidis et al. [49] constructed a QPIR protocol for honest server with communication complexity $O(\log \mathsf{s})$, and Aharonov et al. [53] proved that the trivial solution is also optimal for the specious adversary.

1.4 Contributions and organization

The main contribution of the thesis is to give an information-theoretic approach to QPIR for the first time. This thesis considers the QPIR problem in the communication model in which the queries are classical, the answers are quantum, and the prior quantum entanglement is shared among the servers. On this communication model, this thesis derives various QPIR capacities and construct capacity-achieving QPIR protocols. In Chapter 3, we derive that the symmetric and non-symmetric one-round QPIR capacities are 1 and construct a capacity-achieving symmetric QPIR protocol with two servers. In Chapter 4, we prove that the symmetric and non-symmetric multi-round QPIR capacities are also 1, which implies that the multi-round communication does not help QPIR. In Chapter 5, we extend the result of Chapter 3 to the t-private QPIR capacities. We prove that the symmetric and non-symmetric t-private QPIR capacities are 1 if less than half of the servers collude and $2(\mathsf{n}-\mathsf{t})/\mathsf{n}$ if more than half collude. We also construct a capacity-achieving symmetric t-private QPIR protocol by stabilizer formalism, which requires multipartite entanglement as prior entanglement. In Chapter 6, we construct another capacity-achieving symmetric $(\mathsf{n}-1)$-private QPIR protocol only with bipartite entanglement.

Table 1.1 summarizes and compares the derived QPIR capacities with classical counterparts. As in Table 1.1, the derived QPIR capacities are greater than the PIR capacities. Furthermore, the QPIR protocols proposed in this thesis also have advantages over the classical PIR protocols, which will be explained in each chapter.

Throughout this thesis, the communication model of QPIR is classical queries, the quantum answers, and the prior quantum entanglement among

the servers. Our model has an advantage over to that of the previous QPIR studies, which considered two-way quantum communication. Our model assumes weaker conditions since if the quantum upload is allowed, the user can upload an entangled state to all servers. In our model, the user only needs to have the measurement apparatus but does not need to create and manipulate the quantum states.

This thesis also discusses the strong converse bounds for the first time in the PIR studies. The proofs of both classical and quantum PIR capacities consist of the achievability proof, which gives the existence of a capacity-achieving protocol, and the converse bound, which gives a tight upper bound of the PIR rate. In existing classical PIR studies, the converse bounds have been proved for the case where the error probability approaches zero. The converse bounds of this type are called *weak converse bounds*. However, the weak converse bounds do not preclude the trade-off between the capacity and the error probability, i.e., the capacity may increase if we allow some level of errors. Thus, only with the weak converse bound, it is an open problem if there is such trade-off. The *strong converse bound* proves that there is no such trade-off between the capacity and the error. To be precise, the strong converse bound is the tight upper bound of the rate when any error probability less than 1 is allowed. This thesis gives the first approach to the strong converse bounds on PIR.

The remainder of the thesis is organized as follows. Chapter 2 is the preliminary chapter. Chapter 2 introduces the mathematical framework of quantum information theory, the quantum information measures, and the stabilizer formalism.

In Chapter 3, as quantum extensions of the classical PIR capacities [26, 28], we show that the symmetric and non-symmetric capacities of QPIR are 1. For the achievability of the capacity, we propose a rate-one QPIR protocol with perfect security and finite upload cost. As the converse part, we show the strong converse bound that the rate of any QPIR protocol is less than 1 even with no secrecy, no upload constraint, and any error probability.

In Chapter 4, we show that the capacities of symmetric and non-symmetric multi-round QPIR are 1. Since the rate-one protocol in Chapter 3 achieves the multi-round QPIR capacity, Chapter 4 only proves the weak converse bound on the multi-round QPIR capacity, i.e., the upper bound when the error probability is asymptotically zero.

Table 1.1: Capacities of classical and quantum PIRs

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$ [26]	1 ‡ [Chapter 3]
Symmetric PIR	$1-\frac{1}{\mathsf{n}}$ [28] †	
Multi-round PIR	$\frac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$ [38]	1 [Chapter 4]
Symmetric multi-round PIR	-	
t-Private PIR	$\frac{1-\mathsf{t}/\mathsf{n}}{1-(\mathsf{t}/\mathsf{n})^{\mathsf{f}}}$ [29]	$\min\left\{1, \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}\right\}$ ‡ [Chapter 5]
Symmetric t-private PIR	$1-\frac{\mathsf{t}}{\mathsf{n}}$ [30] †	

$*$ $\mathsf{n}, \mathsf{f} \geq 2$: the numbers of servers and messages, respectively.

† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

In Chapter 5, we derive the symmetric and non-symmetric t-private QPIR capacities for any t less than the number of servers n. As a main result, we prove that the t-private QPIR capacity is $\min\{1, 2(\mathsf{n}-\mathsf{t})/\mathsf{n}\}$ for $1 \leq \mathsf{t} < \mathsf{n}$. Especially, when at most half of the servers collude, i.e., $1 \leq \mathsf{t} \leq \mathsf{n}/2$, the capacity is 1 even if we require the strongest security condition in which the protocol has zero-error, perfect user t-secrecy, and perfect server secrecy. For the proof, we construct the capacity-achieving protocol by the stabilizer formalism and present the converse bounds for $1 \leq \mathsf{t} \leq \mathsf{n}/2$ and $\mathsf{n}/2 < \mathsf{t} < \mathsf{n}$, respectively.

In Chapter 6, we propose a symmetric $(\mathsf{n}-1)$-private QPIR protocol with bipartite entangled states. Whereas the protocol of Chapter 5 requires multipartite entanglement among all servers as prior entanglement, this protocol only requires multiple copies of bipartite entangled states instead of a large entangled state.

Chapter 7 summarizes the results of this thesis and discusses open problems.

Chapter 2

Preliminaries

2.1 Mathematical framework of quantum information theory

In this section, we introduce the mathematical framework of quantum information theory from the four postulate of quantum systems, quantum states, quantum operation, and measurement. Most of the contents in this section have appeared in my master thesis [4] and more detailed introduction including the physical motivations of the postulates can be found in [65], [66], and [67].

2.1.1 Quantum system and quantum state

A quantum system is described by a Hilbert space $\mathcal{H}$, which is a complex vector space with standard inner product $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$. Throughout this thesis, we only consider the quantum systems as finite-dimensional Hilbert spaces $\mathcal{H}$ which is isomorphic to $\mathbb{C}^d$ for some positive integer d.

Postulate 1 (Quantum system)**.** *Any quantum system is described by a finite-dimensional Hilbert space.*

We use the bra-ket notation to describe vectors in $\mathcal{H}$ and vectors in the dual space $\mathcal{H}^*$. From one-to-one correspondence between $\mathcal{H}$ and $\mathcal{H}^*$, for any vector $|x\rangle \coloneqq (x_1, \ldots, x_d)^\top$ in $\mathcal{H}$, there is a unique vector $\langle x| \in \mathcal{H}^*$ defined by

$$\langle x|y\rangle \coloneqq \sum_{i=1}^{d} \bar{x}_i y_i \quad \forall y \in \mathcal{H}.$$

For a square matrix X on $\mathcal{H}$, the Hermitian transpose is denoted by $X^* = \bar{X}^\top$. A matrix X on $\mathcal{H}$ is called a *Hermitian matrix* if $X = X^*$. A Hermitian matrix X is called positive definite if

$$\langle x|X|x\rangle > 0 \quad \text{for any } |x\rangle \in \mathcal{H},$$

and it is denoted by $X > 0$. Similarly, a Hermitian matrix X is called positive semidefinite if

$$\langle x|X|x\rangle \geq 0 \quad \text{for any } |x\rangle \in \mathcal{H},$$

and it is denoted by $X \geq 0$.

Quantum states are defined by density matrices.

Definition 2.1 (Density matrix on $\mathcal{H}$)**.** *A square matrix ρ on $\mathcal{H}$ is called a density matrix on $\mathcal{H}$ if*

$$\operatorname{Tr}\rho = 1 \quad \textit{and} \quad \rho \geq 0.$$

Postulate 2 (Quantum state)**.** *Any state of a quantum system $\mathcal{H}$ is described by a density matrix on $\mathcal{H}$.*

A quantum state is called *pure state* if its rank is 1 and a state which is not pure is called a *mixed state*. We sometimes treat a pure state as a unit vector since rank-one density matrices $\rho = |\psi\rangle\langle\psi|$ on $\mathcal{H}$ has a one-to-one correspondence with unit vectors $|\psi\rangle$ in $\mathcal{H}$. Since a quantum state is a Hermitian matrix, it can be diagonalized and therefore, any mixed state can be represented by a probabilistic mixture of pure states. We denote by $\mathcal{S}(\mathcal{H})$ the set of states on a quantum system $\mathcal{H}$ and by $\mathcal{M}(\mathcal{H})$ the set of square matrices on $\mathcal{H}$. Since $\mathcal{S}(\mathcal{H})$ is a convex set, pure states are the extreme points of $\mathcal{S}(\mathcal{H})$.

2.1.2 Composite system and state

Consider the case where we treat multiple quantum systems simultaneously. A composite system is given as a tensor product of the quantum systems, e.g., the composite system of $\mathcal{H}_A$ and $\mathcal{H}_B$ is given as $\mathcal{H}_A \otimes \mathcal{H}_B$.

Throughout this thesis, we use single lettered subscripts to differentiate quantum systems, e.g. $\mathcal{H}_A, \mathcal{H}_B, \ldots$ and multi-lettered subscript to denote

composite systems, e.g. $\mathcal{H}_{AB} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B$. Furthermore, we use the notation $|x_A, x_B\rangle \coloneqq |x_A\rangle \otimes |x_B\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.

States on a composite system are defined in the same way as states on a single system. Note that the states are not necessarily the tensor product of those in each subsystems. When a state is written as tensor products of states on subsystems, it is called *seperable states*, i.e., a state ρ is called separable if

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i, \quad \sum_i p_i = 1, \quad p_i \geq 1,$$

where ρ_A^i and ρ_B^i are states on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. States which are not seperable are called *entangled states*.

For any state ρ in $\mathcal{H}_{AB}$, the states $\rho_A \coloneqq \mathrm{Tr}_B \rho$ and $\rho_B \coloneqq \mathrm{Tr}_A \rho$ are called *reduced states*, where the partial trace Tr_B (Tr_A) is defined as follows.

Definition 2.2 (Partial trace)**.** *Let $\{|e_i^B\rangle\}$ be a basis of the system $\mathcal{H}_B$. For any $X \in \mathcal{M}(\mathcal{H}_{AB})$,*

$$\operatorname*{Tr}_B X \coloneqq \sum_i (I \otimes \langle e_i^B|) X (I \otimes |e_i^B\rangle),$$

or alternatively, $\mathrm{Tr}_B : \mathcal{H}_{AB} \to \mathcal{H}_A$ is a linear operator such that

$$\operatorname*{Tr}_B X \otimes Y \coloneqq X \operatorname{Tr} Y, \quad \forall X \in \mathcal{M}(\mathcal{H}_A),\ Y \in \mathcal{M}(\mathcal{H}_B).$$

Given any $\rho \in \mathcal{S}(\mathcal{H}_A)$, a state $\tilde{\rho} \in \mathcal{S}(\mathcal{H}_{AR})$ is called an *extension* of ρ if

$$\operatorname*{Tr}_R \tilde{\rho} = \rho.$$

Especially, if an extension $\tilde{\rho}$ of ρ is a pure state, the state $\tilde{\rho}$ is called a *purification* of ρ.

The *completely mixed state* and *maximally entangled states* are commonly used states in quantum information theory. The completely mixed state of a d-dimensional space $\mathcal{H}$ is defined by

$$\rho_{\mathrm{mix}} \coloneqq \frac{1}{d} I \in \mathcal{S}(\mathcal{H}).$$

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ are d-dimensional quantum systems. Pure states on $\mathcal{H}_A \otimes \mathcal{H}_B$ are called maximally entangled states if the reduced states on $\mathcal{H}_A$ and $\mathcal{H}_B$ are the completely mixed states. The completely mixed states are written as

$$\sum_{i=1}^{d} \frac{1}{\sqrt{d}} |e_i, f_i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

where $\{|e_i\rangle \mid i = 1, \ldots, d\}$ and $\{|f_i\rangle \mid i = 1, \ldots, d\}$ are bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The maximally entangled state is a purification of ρ_{mix} and conversely, the completely mixed state ρ_{mix} is the reduced state of maximally entangled states.

2.1.3 Quantum operation

Quantum operations describe dynamics of quantum systems. In this subsection, we will define quantum operations by completely positive and trace-preserving maps based on natural conditions that quantum operations should satisfy.

In the following, we consider quantum operations as maps κ from $\mathcal{S}(\mathcal{H}_A)$ to $\mathcal{S}(\mathcal{H}_B)$ and characterize three natural conditions that κ should satisfy. First, we consider the condition of affinity and linearity. A map f is called an *affine map* if

$$f(px_1 + (1-p)x_2) = pf(x_1) + (1-p)f(x_2), \quad p \in [0,1].$$

Since a mixed state is a probabilistic mixture of other states, it is natural that a quantum operation acts in the same way on the states composing the mixed state. That is, when ρ_1 and ρ_2 are states on $\mathcal{H}_A$, the quantum operation κ should satisfy the following condition of affine maps:

$$\kappa(p\rho_1 + (1-p)\rho_2) = p\kappa(\rho_1) + (1-p)\kappa(\rho_2), \quad p \in [0,1].$$

Condition 1 Quantum operations are affine maps.

We further assume a similar but stronger condition, linearity.

Condition 1' Quantum operations are linear maps.

Next, we consider the condition of positivity. A positive map is a map that maps a positive semidefinite matrix to a positive semidefinite matrix. Since quantum states are positive semidefinite matrices, the quantum operations should be positive maps.

Condition 2 Quantum operations are positive maps.

Let $\iota_{\mathbb{C}^n}$ be the identity operation on $\mathcal{S}(\mathbb{C}^n)$. We can consider $\kappa \otimes \iota_{\mathbb{C}^n}$ as a quantum operation from $\mathcal{S}(\mathcal{H}_A \otimes \mathbb{C}^n)$ to $\mathcal{S}(\mathcal{H}_B \otimes \mathbb{C}^n)$ and $\kappa \otimes \iota_{\mathbb{C}^n}$ should be

positive from Condition 2. When $\kappa \otimes \iota_{\mathbb{C}^n}$ is a positive map, the operation κ is called n-positive map. When κ is n-positive for any dimension n, the operation κ is called a completely positive map. Therefore, quantum operations should be completely positive maps.

Condition 2' Quantum operations are completely positive maps.

The last condition is the trace-preserving property. The resultant state $\kappa(\rho)$ should be traced to 1 since it is a density matrix.

Condition 3 Quantum operations are trace-preserving maps.

To summarize, quantum operations should satisfy the above Conditions 1', 2', 3. The maps satisfying these three conditions are called *Completely Positive and Trace-Preserving (CPTP) maps*. Quantum information theory postulates that the set of CPTP maps is the same as the set of quantum operations.

Postulate 3. *Any quantum operations are described by CPTP maps.*

An example of quantum operations is $\kappa_U(\rho) \coloneqq U\rho U^*$ for a unitary matrix U. By the operation κ_U, a pure state $|\psi\rangle$ is mapped to the pure state $U|\psi\rangle$.

The CPTP maps are characterized by the following theorem.

Theorem 2.1 (Equivalent conditions of CPTP maps)**.** *For a map $\kappa : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$, the following conditions are equivalent. The dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ are denoted by d_A and d_B, respectively.*

1. *κ is a CPTP map.*
2. *κ is a trace-preserving and $(\min\{d_A, d_B\})$-positive map.*
3. *(Stinespring representation) Let $\mathcal{H}_B$ be a d_B-dimensional quantum system. There exist a pure state $\rho_0 \in \mathcal{H}_{BC}$ and a unitary matrix U on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ such that*
$$\kappa(\rho) = \operatorname*{Tr}_{AC} U(\rho \otimes \rho_0)U^*.$$
4. *(Choi-Kraus representation) There exists a set $\{F_i\}_{i=1}^{d_A d_B}$ of linear maps from $\mathcal{H}_A$ to $\mathcal{H}_B$ satisfying $\sum_i F_i F_i^* = I_A$ such that*
$$\kappa(\rho) = \sum_i F_i \rho F_i^*.$$

The Stinespring representation implies that quantum operations are the same as applying a unitary operation and reducing to the subsystem.

2.1.4 Measurement

Measurement on a quantum system is an essential tool to extract information from the quantum state. If a measurement is performed on a system, the measurement outcome is obtained probabilistically and it also disturbs the state of the system. Therefore, to model a measurement, it needs to describe both of probabilistic behavior of outcomes and change of states.

Given a set Ω of measurement outcomes, we describe a measurement by a set of maps $\kappa_\Omega \coloneqq \{\kappa_\omega \mid \omega \in \Omega\}$ such that the probability to obtain $\omega \in \Omega$ is $\operatorname{Tr} \kappa_\omega(\rho)$ and the resultant state is

$$\frac{1}{\operatorname{Tr} \kappa_\omega(\rho)} \kappa_\omega(\rho).$$

Similar to the conditions for quantum operations, the maps $\{\kappa_\omega \mid \omega \in \Omega\}$ should satisfy the following conditions.

Condition 1 κ_ω are linear maps.

Condition 2 κ_ω are completely positive (CP) maps.

Condition 3 $\sum_{\omega \in \Omega} \operatorname{Tr} \kappa_\omega(\rho) = 1$.

The set of maps κ_ω that satisfies the Conditions 1, 2, 3 are called an *instrument*.

Definition 2.3 (Instrument κ_Ω)**.** *A set $\kappa_\Omega = \{\kappa_\omega \mid \omega \in \Omega\}$ of linear CP maps is called an instrument if $\sum_\omega \kappa_\omega$ is a CPTP map.*

The last postulate of quantum information theory is given as follows.

Postulate 4 (Measurement)**.** *Any measurement is described by an instrument $\kappa_\Omega \coloneqq \{\kappa_\omega \mid \omega \in \Omega\}$. When a measurement κ_Ω is performed, the probability to obtain $\omega \in \Omega$ is $\operatorname{Tr} \kappa_\omega(\rho)$ and when the outcome is ω, the resultant state is $(1/\operatorname{Tr} \kappa_\omega(\rho))\kappa_\omega(\rho)$.*

When we are only interested in the outcome of the measurement, we consider the measurement as a Positive Operator-Valued Measure (POVM).

Definition 2.4 (Positive operator-valued measure (POVM) $\mathbf{M}_\Omega$)**.** *A set of matrices* $\mathbf{M}_\Omega \coloneqq \{M_\omega \in \mathcal{M}(\mathcal{H}) \mid \omega \in \Omega\}$ *is called a POVM on the quantum system* $\mathcal{H}$ *if*

$$\sum_\omega M_\omega = I_\mathcal{H} \quad \textit{and} \quad M_\omega \geq 0 \quad \textit{for any } \omega \in \Omega.$$

Given a state ρ and a POVM $\mathbf{M}_\Omega = \{M_\omega \mid \omega \in \Omega\}$ on $\mathcal{H}$, the probability for obtaining ω is $\operatorname{Tr} \rho M_\omega$. When all POVM elements are orthogonal projections, i.e., $M_\omega^2 = M_\omega$ and $M_\omega^* = M_\omega$, the POVM is called a Projection-Valued Measure (PVM). We sometimes regard an orthonormal basis $\{|e_i\rangle\}$ of $\mathcal{H}$ as a PVM since it has a one-to-one correspondence with the PVM $\{|e_i\rangle\langle e_i|\}$. We call the PVM of a basis the *basis measurement*.

For more details of measurement processes and state reduction, we refer to [68–70].

2.1.5 Classical resources in quantum information theory

Given a fixed basis of a quantum system, we call a quantum state *classical* if it is diagonal with respect to the basis. A discrete random variable X with values $\mathcal{X}$ and a distribution p_X are described by a classical state

$$\sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x|. \tag{2.1}$$

Sampling of X corresponds to the basis measurement of $\{|x\rangle \mid x \in \mathcal{X}\}$. For a function f, the random variable $f(X)$ is described by

$$\sum_{x \in \mathcal{X}} p_X(x) |f(x)\rangle\langle f(x)| = \sum_{y \in f(\mathcal{X})} p_{f(X)}(y) |y\rangle\langle y|, \tag{2.2}$$

where $p_{f(X)}(y) = \sum_{x:f(x)=y} p_X(x)$. The change of random variable $X \mapsto f(X)$ can be described by the following CPTP map which maps (2.1) to (2.2): Stinespring representation with $\rho_0 = |f(x_0)\rangle\langle f(x_0)|$ and $U = \sum_{x,y} |x\rangle\langle x| \otimes |g(x,y)\rangle\langle y|$ for some $x_0 \in \mathcal{X}$ and some function g such that $g(x, f(x_0)) = f(x)$ and $f(\mathcal{X}) = \{g(x,y) \mid y \in f(\mathcal{X})\}$ for any x.

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

$$\rho_{\mathcal{H}X} = \sum_{x \in \mathcal{X}} p_X(x) \rho_x \otimes |x\rangle\langle x|. \tag{2.3}$$

The state (2.3) is often called a *Classical-Quantum (CQ) state*. The reduced state on $\mathcal{H}$ is the averaged state $\sum_{x\in\mathcal{X}} p_X(x)\rho_x$ and the reduced state on X is (2.1). Thus, the probability to sample $X = x$ is $p_X(x)$ and the resultant state after sampling of $X = x$ is ρ_x.

2.2 Information measures and inequalities

In this section, we introduce quantum information measures and inequalities. We will use these measures and inequalities in the later chapters for the evaluation of the security for QPIR protocols and the converse proofs of QPIR capacities.

2.2.1 Classical information measures and inequalities

Entropic measures

Let X be a discrete random variable with values in $\mathcal{X}$ and the distribution $p = \{p_x\}_{x\in\mathcal{X}}$. The *Shannon entropy* is defined as

$$H(X) = H(p) \coloneqq -\sum_{x\in\mathcal{X}} p_x \log p_x. \tag{2.4}$$

When p is a two-valued distribution $\{p_1, 1-p_1\}$, $H(p)$ is characterized by p_1 and thus we define the binary entropy function as

$$h_2(p_1) \coloneqq H(p) = -p_1 \log p_1 - (1-p_1)\log(1-p_1). \tag{2.5}$$

For random variables X and Y, the *conditional entropy* is defined as

$$H(X|Y) \coloneqq H(XY) - H(Y) \tag{2.6}$$

and the *mutual information* is defined as

$$I(X;Y) \coloneqq H(X) - H(X|Y) \tag{2.7}$$

For random variables X, Y with possible values in $\{0,\dots,n-1\}$, the *Fano's inequality* is given as [56]

$$H(X|Y) \le \varepsilon \log(n-1) + h_2(\varepsilon), \tag{2.8}$$

where $\varepsilon \coloneqq \Pr[X \neq Y]$.

Distance measures

Given two probability distributions $p = \{p_x\}_{x\in\mathcal{X}}$ and $q = \{q_x\}_{x\in\mathcal{X}}$, the *variational distance* is defined as

$$d(p,q) \coloneqq \frac{1}{2}\sum_{x\in\mathcal{X}} |p_x - q_x| \tag{2.9}$$

and the *relative entropy* is defined as

$$D(p\|q) \coloneqq \begin{cases} \sum_{x\in\mathcal{X}} p_x(\log p_x - \log q_x) & \text{if } \operatorname{supp}(p) \subset \operatorname{supp}(q) \\ \infty & \text{otherwise,} \end{cases} \tag{2.10}$$

where $\operatorname{supp}(p) \coloneqq \{x \in \mathcal{X} \mid p_x \neq 0\}$. The variational distance is a metric on the set of quantum states but the relative entropy does not satisfy the axioms of a metric because $D(p\|q) \neq D(q\|p)$, in general. However, the variational distance and the relative entropy are related by the *Pinsker's inequality* [57]

$$2d^2(p,q) \leq D(p\|q). \tag{2.11}$$

With the relative entropy, the mutual information is written as

$$I(X;Y) = D(p_{XY}\|p_X \times p_Y). \tag{2.12}$$

2.2.2 Quantum information measures and inequalities

Quantum entropic measures

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 $\rho = \sum_i p_i|i\rangle\langle i|$, the *von Neumann entropy* is defined by

$$H(\rho) \coloneqq \operatorname{Tr}\rho\log\rho = H(\{p_i\}), \tag{2.13}$$

where $H(\cdot)$ in the last term denotes is the Shannon entropy defined in (2.4). For any state $\rho \in \mathcal{S}(\mathcal{A}\otimes\mathcal{B})$, we use the notation

$$H(\mathcal{A})_\rho \coloneqq H(\operatorname*{Tr}_{\mathcal{B}}\rho), \quad H(\mathcal{B})_\rho \coloneqq H(\operatorname*{Tr}_{\mathcal{A}}\rho),$$
$$H(\mathcal{AB})_\rho \coloneqq H(\rho).$$

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

$$H(\mathcal{A}|\mathcal{B})_\rho \coloneqq H(\mathcal{AB})_\rho - H(\mathcal{B})_\rho, \tag{2.14}$$

$$I(\mathcal{A};\mathcal{B})_\rho \coloneqq H(\mathcal{A})_\rho + H(\mathcal{B})_\rho - H(\mathcal{AB})_\rho, \tag{2.15}$$

$$I(\mathcal{A};\mathcal{B}|\mathcal{C})_\rho \coloneqq I(\mathcal{A};\mathcal{BC})_\rho - I(\mathcal{A};\mathcal{C})_\rho. \tag{2.16}$$

If there is no confusion, we denote $H(\cdot)_{\rho_X} \coloneqq H(\cdot)_{\rho_{\mathcal{H}X}}$ and $I(\cdot)_{\rho_X} \coloneqq I(\cdot)_{\rho_{\mathcal{H}X}}$ for classical-quantum states defined in (2.3).

Distance measures

The *trace distance* of ρ and σ on $\mathcal{H}$ is defined as

$$d(\rho,\sigma) \coloneqq \frac{1}{2}\operatorname{Tr}|\rho - \sigma| \tag{2.17}$$

and the *quantum relative entropy* is defined as

$$D(\rho\|\sigma) \coloneqq \begin{cases} \operatorname{Tr}\rho(\log\rho - \log\sigma) & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma), \\ \infty & \text{otherwise,} \end{cases} \tag{2.18}$$

where $\operatorname{supp}(\rho) \coloneqq \{|x\rangle \in \mathcal{H} \mid \rho|x\rangle \neq 0\}$. Similar to the classical case, the trace distance is a metric on the set of quantum states but the quantum relative entropy does not satisfy the axioms of a metric. Moreover, the *quantum Pinsker inequality* [65, Eq. (3.53)] relates the trace distance and the quantum relative entropy as

$$2d^2(\rho,\sigma) \leq D(\rho\|\sigma). \tag{2.19}$$

With the quantum relative entropy, the quantum mutual information is written as

$$I(\mathcal{A};\mathcal{B})_\rho = D(\rho\|\rho_\mathcal{A} \otimes \rho_\mathcal{B}), \tag{2.20}$$

where $\rho_\mathcal{A}$ and $\rho_\mathcal{B}$ are reduced states of ρ on $\mathcal{A}$ and $\mathcal{B}$, respectively.

Quantum relative Rényi entropy and data-processing inequalities

For $s \in (-1,0) \cup (0,\infty)$, the *quantum relative Rényi entropy* [60] is defined as

$$D_{1+s}(\rho\|\sigma) := \begin{cases} \frac{1}{s}\log \operatorname{Tr} \rho^{1+s}\sigma^{-s} & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma) \text{ or } s \in (-1,0), \\ \infty & \text{otherwise.} \end{cases}$$

By limiting s to 0, we obtain the quantum relative entropy as

$$\lim_{s\to 0} D_{1+s}(\rho\|\sigma) = \frac{d}{ds}\log \operatorname{Tr} \rho^{1+s}\sigma^{-s}|_{s=0} = D(\rho\|\sigma) \tag{2.21}$$

Thus, we consider the quantum relative entropy as the quantum relative Rényi entropy for $s = 1$.

The quantum relative Rényi entropy satisfies the data-processing inequality with respect to CPTP maps κ [65, Eq. (5.56)] and measurements $\mathcal{M}$ [65, Eq. (3.23)]:

$$D_{1+s}(\rho\|\sigma) \geq D_{1+s}(\kappa(\rho)\|\kappa(\sigma)) \qquad \text{for } s \in [-1,1], \tag{2.22}$$

$$D_{1+s}(\rho\|\sigma) \geq D_{1+s}(P_\rho^{\mathcal{M}}\|P_\sigma^{\mathcal{M}}) \qquad \text{for } s \geq -1, \tag{2.23}$$

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.,

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

When the state on $\mathcal{A}\otimes\mathcal{B}$ is $\rho_{\mathcal{AB}}$, a measurement is performed on the system $\mathcal{B}$, and the measurement outcome is described by the random variable X, we have

$$I(\mathcal{A};\mathcal{B})_{\rho_{\mathcal{AB}}} \geq I(\mathcal{A};X)_{\rho_{\mathcal{A}X}} \tag{2.24}$$

from (2.20) and (2.23).

Fannes-type inequalities

Fannes-type inequalities evaluate the difference of the entropy, the conditional entropy, and the mutual information by the trace distance. Let

$$\eta_0(x) := \begin{cases} 1/e & \text{if } 1/e < x, \\ -x\log x & \text{if } 0 < x < 1/e, \end{cases} \tag{2.25}$$

and $\varepsilon \coloneqq 2d(\rho, \sigma)$. When ρ and σ are the states on d-dimensional space $\mathcal{A}$, the *Fannes inequality* [58] is

$$|H(\mathcal{A})_\rho - H(\mathcal{A})_\sigma| \leq \varepsilon \log d + \eta_0(\varepsilon). \tag{2.26}$$

When ρ and σ are the states on $\mathcal{A} \otimes \mathcal{B}$, the *Alicki-Fannes inequality* [59] is

$$|H(\mathcal{A}|\mathcal{B})_\rho - H(\mathcal{A}|\mathcal{B})_\sigma| \leq 4\varepsilon \log d + 2h_2(\varepsilon). \tag{2.27}$$

Combining (2.26) and (2.27), we have [65, Eq. (5.105)]

$$\begin{aligned} |I(\mathcal{A};\mathcal{B})_\rho - I(\mathcal{A};\mathcal{B})_\sigma| &\leq |H(\rho) - H(\sigma)| + |H(\mathcal{A}|\mathcal{B})_\rho - H(\mathcal{A}|\mathcal{B})_\sigma| && (2.28) \\ &\leq 5\varepsilon \log d + \eta_0(\varepsilon) + 2h_2(\varepsilon). && (2.29) \end{aligned}$$

2.3 Notation

For any set $\mathcal{T}$, we denote by $|\mathcal{T}|$ the cardinality of the set $\mathcal{T}$. For any quantum system $\mathcal{H}$, $\dim \mathcal{H}$ denotes the dimension of $\mathcal{H}$. The matrix I_n denotes the $n \times n$ identity matrix and $I_\mathcal{H}$ denotes the identity matrix on $\mathcal{H}$. $\Pr_X[f(X)]$ is the probability that X satisfies the condition $f(X)$. The set of integers is denoted by $\mathbb{Z}$ and $\mathbb{Z}_d \coloneqq \mathbb{Z}/d\mathbb{Z}$ for any integer d.

Chapter 3

Capacity of Quantum Private Information Retrieval

This chapter investigates the fundamental communication limit of symmetric and non-symmetric multi-server QPIR and constructed an optimal protocol achieving the communication limit. We considered the communication model in which the user sends classical query and the servers return quantum answers but the servers share prior entanglement before the protocol starts. The communication efficiency of a QPIR protocol is evaluated by the *QPIR rate* defined as the ratio of the size of one message to the total dimension of the downloaded quantum systems. Higher QPIR rate implies higher communication efficiency and an upper bound of QPIR rates is 1 from definition. The maximum of QPIR rates, called the *QPIR capacity*, characterizes the optimal communication efficiency of QPIR. In this chapter, we prove that the symmetric and non-symmetric QPIR capacities are 1. Capacity 1 implies that symmetric QPIR can be achieved with the same efficiency as retrieval without secrecy.

To be precise, we evaluate the security of a QPIR protocol with three parameters: the retrieval error probability, the user secrecy in which the identity of the queried message is unknown to any individual server, and the server secrecy in which the user obtains no more information than the targeted message. The main theorem of this chapter is that the QPIR capacity is 1 regardless of whether it is of exact/asymptotic security and with/without the restriction that the upload cost is negligible to the download cost. For the achievability of the capacity, we propose a rate-one QPIR protocol with

Table 3.1: Comparison of protocols in Chapter 3 and [27]

	QPIR protocol	PIR protocol [27]
Server secrecy	Yes	No
Capacity	1	$\frac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$
Condition for capacity 1	$\mathsf{n} \geq 2$	$\mathsf{n} \to \infty$
Upload cost	$2\mathsf{f}$ bits	$\mathsf{n}(\mathsf{f}-1)\log \mathsf{n}$ bits
Possible message sizes	$\{\ell^2\}_{\ell=2}^{\infty}$	$\{\ell^{\mathsf{n}-1}\}_{\ell=2}^{\infty}$

∗ Server secrecy is the property that the user obtains no information other than the targeted message.

† n, f: the numbers of servers and messages, respectively.

‡ Upload cost is the total bits which are sent to the servers.

perfect security and finite upload cost. The proposed QPIR protocol can be considered as a quantum version of Protocol 1.1. For the converse bound, we give the strong converse bound, which proves that the rate 1 is optimal even if any error probability is allowed and no security is guaranteed.

The capacity-achieving protocol has several remarkable advantages compared to the classical PIR protocol in [27] whose upload cost and message size are minimized (see Table 3.1). First, our protocol is a symmetric QPIR protocol, i.e., the user obtains no information from messages other than the retrieved one. This contrasts with the protocol in [27] that retrieves some information of the other messages. Second, our protocol keeps the secrecy against the malicious user and servers. That is, the user cannot obtain more information than the targeted message even if the user sends malicious queries to the servers, and the servers cannot obtain the identity of the user's targeted message even if the servers return malicious answers. Third, the rate 1 of our protocol is greater than the rate $(1-\mathsf{n}^{-1})/(1-\mathsf{n}^{-\mathsf{f}})$ of the protocol

in [27]. Fourth, our protocol achieves the capacity with only 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 [27], the capacity is strictly increasing in the number of servers and strictly decreasing in the number of messages, and an infinite number of servers are needed to achieve the capacity 1. Fifth, our protocol needs the upload of $2\mathsf{f}$ bits whereas the protocol in [27] needs $(\mathsf{n}(\mathsf{f}-1)\log\mathsf{n})$-bit upload. Last, our protocol exists if the message size m is the square of any integer, but the protocol in [27] requires the message size m to be the $(\mathsf{n}-1)$-th power of any integer.

The converse proofs of the QPIR capacities are much simpler than those of the PIR capacities [26, 28]. Whereas the papers [26, 28] used several entropy inequalities based on the assumptions on the PIR problem, our converse bounds are concisely derived without using any secrecy conditions but by focusing on the download step of QPIR protocol.

The remaining of this chapter is organized as follows. Section 3.1 presents the formal definition of the QPIR protocol and capacity and proposes the QPIR capacity theorem. Section 3.2 constructs the rate-one QPIR protocol and analyzes the security of our protocol against the malicious user and servers. Section 3.3 proves the converse bound.

3.1 QPIR protocol and capacity theorem

In this section, we formally define the QPIR protocol and its capacity and presents the capacity theorem.

3.1.1 Formal definition of QPIR protocol

In this thesis, we consider QPIR with multiple servers described as follows (Figure 3.1). Let $\mathsf{n}, \mathsf{f}, \mathsf{m}$ 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 messages $M = (M_1, \ldots, M_{\mathsf{f}}) \in \{1, \ldots, \mathsf{m}\}^{\mathsf{f}}$. Let $\mathcal{A}'_1, \ldots, \mathcal{A}'_{\mathsf{n}}$ be d'-dimensional Hilbert spaces. The state of $\mathcal{A}'_1 \otimes \cdots \otimes \mathcal{A}'_{\mathsf{n}}$ is initialized as ρ_{prev}, and is distributed such that the j-th server $\mathtt{serv}_j$ contains $\mathcal{A}'_j$. The user chooses the index of the targeted message K to retrieve the K-th message M_K, where the distribution of K is uniform and independent

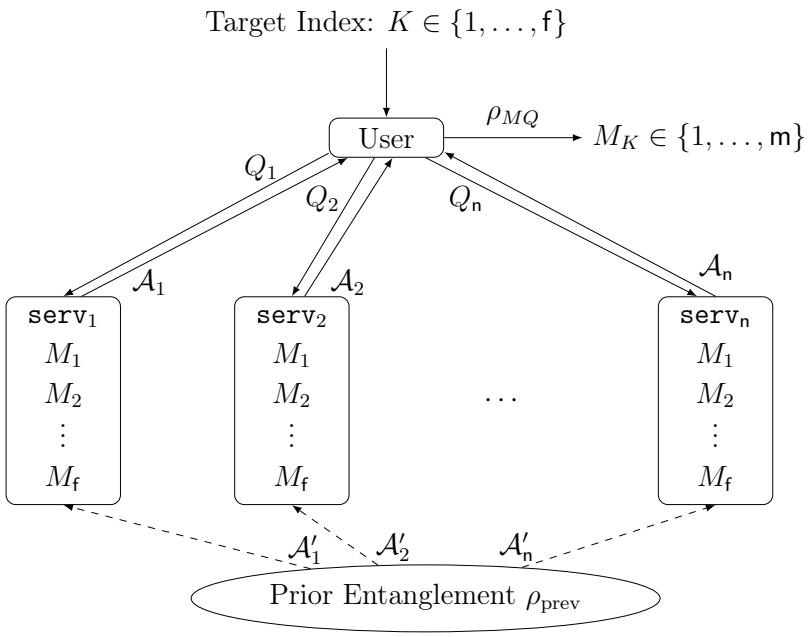


Figure 3.1: Quantum private information retrieval protocol with multiple servers. The composite system of the servers is initialized to an entangled state ρ_{perv}.

of the message $M_1, \ldots, M_{\mathsf{f}}$.

To retrieve the K-th message M_K, the user chooses a random variable R_{user} in a set $\mathcal{R}_{\mathrm{user}}$ and encodes the queries for retrieving M_K by user encoder $\mathsf{Enc}_{\mathrm{user}}$:

$$\mathsf{Enc}_{\mathrm{user}}(K, R_{\mathrm{user}}) = Q = (Q_1, \ldots, Q_{\mathsf{n}}) \in \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_{\mathsf{n}},$$

where $\mathcal{Q}_j$ is the set of query symbols to the j-th server for any $j \in \{1, \ldots, \mathsf{n}\}$. The n queries $Q_1, \ldots, Q_{\mathsf{n}}$ are sent to the servers $\mathtt{serv}_1, \ldots, \mathtt{serv}_{\mathsf{n}}$, respectively. Let $\mathcal{A}_1, \ldots, \mathcal{A}_{\mathsf{n}}$ be d-dimensional Hilbert spaces and $\mathcal{A} \coloneqq \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_{\mathsf{n}}$. After receiving the j-th query Q_j, each server $\mathtt{serv}_j$ applies a CPTP map Λ_j from $\mathcal{A}'_j$ to $\mathcal{A}_j$ depending on $Q_j, M_1, \ldots, M_{\mathsf{f}}$ and sends the quantum system $\mathcal{A}_j$ to the user. With the server encoder $\mathsf{Enc}_{\mathrm{serv}_j}$, the map Λ_j is written as

$$\Lambda_j = \mathsf{Enc}_{\mathrm{serv}_j}(Q_j, M_1, \ldots, M_{\mathsf{f}}),$$

and the received state of the user is written as

$$\rho_{MQ} \coloneqq \Lambda_1 \otimes \cdots \otimes \Lambda_{\mathsf{n}}(\rho_{\mathrm{prev}}) \in \mathcal{S}\left(\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j\right). \tag{3.1}$$

the user decodes the received state by a decoder, which is given as a POVM $\mathsf{Dec}(K,Q) \coloneqq \{Y_{K,Q}(w) \mid w \in \{1,\ldots,\mathsf{m}\}\}$ on $\mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_{\mathsf{n}}$ dependently of the variables K and Q. The protocol outputs the measurement outcome $W \in \{1,\ldots,\mathsf{m}\}$.

Given the numbers of servers n and messages f, the above QPIR protocol of message size m is described by the four-tuple

$$\Psi_{\mathrm{QPIR}}^{(\mathsf{m})} \coloneqq (\rho_{\mathrm{prev}}, \mathsf{Enc}_{\mathrm{user}}, \mathsf{Enc}_{\mathrm{serv}}, \mathsf{Dec})$$

of the prior entanglement, user encoder, server encoder, and decoder, where $\mathsf{Enc}_{\mathrm{serv}} \coloneqq (\mathsf{Enc}_{\mathrm{serv}_1}, \ldots, \mathsf{Enc}_{\mathrm{serv}_{\mathsf{n}}})$.

3.1.2 Security measures

For any $j \in \{1,\ldots,\mathsf{n}\}$, we denote $\mathfrak{user}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ and $\mathfrak{serv}_j(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ by the information of the user and the server $\mathtt{serv}_j$ at the end of the protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$, respectively. The security of a QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$ is evaluated by the error probability, the server secrecy, and the user secrecy, which are defined as

$$P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \Pr_{W,K,Q}[W \neq M_K], \tag{3.2}$$

$$S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq I(M_K^c; \mathfrak{user}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})|K), \tag{3.3}$$

$$S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \max_{j\in\{1,\ldots,\mathsf{n}\}} I(K; \mathfrak{serv}_j(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})), \tag{3.4}$$

where $M_K^c \coloneqq (M_1,\ldots,M_{K-1},M_{K+1},\ldots,M_{\mathsf{f}})$. If $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 0$, the non-targeted messages M_K^c are independent of the user information. Similarly, if $S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 0$, the index of the targeted message K is independent of any individual server's information.

Remark 3.1. We evaluate the error of a protocol by the error probability $P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$. This is because the messages M and the index of the targeted message K are randomly chosen, and even if M and K are fixed, the protocol is defined in Section 3.1.1 outputs the outcome W probabilistically. Notice that even if M and K are fixed, the queries Q are randomly chosen and the decoder $\mathsf{Dec}(K,Q)$ is a quantum measurement, which gives the output randomly.

3.1.3 Costs and QPIR rate

We define the upload cost, the download cost, and the QPIR rate of a protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$ by

$$U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \sum_{j=1}^{\mathsf{n}} \log |\mathcal{Q}_j|, \tag{3.5}$$

$$D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \sum_{j=1}^{\mathsf{n}} \log \dim \mathcal{A}_j, \tag{3.6}$$

$$R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \frac{\log \mathsf{m}}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})}. \tag{3.7}$$

The upload cost, the download cost, and the QPIR rate defined respectively as the size of the whole query set $\mathcal{Q}_1 \times \cdots \times \mathcal{Q}_{\mathsf{n}}$, the total dimension of the downloaded quantum systems $\mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_{\mathsf{n}}$, and the ratio of the size of the retrieved message M_K over the download cost. When the base of the logarithm is two, the QPIR rate means the number of retrieved bits per download of one qubit (i.e., a 2-dimensional Hilbert space) and it evaluates the communication efficiency of the protocol. From definition, the QPIR rate $R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ is upper bounded by 1. Since the QPIR rate of the trivial solution is $1/\mathsf{f}$, QPIR protocols are expected to have QPIR rates greater than $1/\mathsf{f}$.

3.1.4 QPIR capacity

The QPIR capacity is the optimal QPIR rate when the numbers of servers and messages are fixed. We define the QPIR capacity with constraints on the security measures 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

$$C_{\mathrm{asymp}}^{\alpha,\beta,\gamma,\theta} \coloneqq \sup_{(3.8)} \liminf_{\ell\to\infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}),$$

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta} \coloneqq \sup_{(3.9)} \liminf_{\ell\to\infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}),$$

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 $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ of QPIR protocols to satisfy either (3.8) or (3.9)

given by

$$\begin{aligned} \limsup_{\ell\to\infty} P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \alpha, \ \limsup_{\ell\to\infty} S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \beta, \\ \limsup_{\ell\to\infty} S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \gamma, \ \limsup_{\ell\to\infty} \frac{U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})} \le \theta, \end{aligned} \tag{3.8}$$

and

$$\begin{aligned} P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \alpha, \ S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \beta, \\ S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \gamma, \ \limsup_{\ell\to\infty} \frac{U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})} \le \theta. \end{aligned} \tag{3.9}$$

The parameters $\alpha, \beta, \gamma, \theta$ are the upper bounds of the error probability, server secrecy, user secrecy, and upload cost, respectively. The two capacities $C_{\mathrm{asymp}}^{\alpha,\beta,\gamma,\theta}$, $C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta}$ are defined as the supremum of QPIR rates for all QPIR protocols satisfying the upper bounds asymptotically and exactly, respectively. Since any protocols satisfying the upper bounds $\alpha, \beta, \gamma, \theta$ exactly also satisfy the bounds asymptotically, for any $\alpha \in [0, 1)$ and $\beta, \gamma, \theta \in [0, \infty]$, we have the inequality

$$C_{\mathrm{exact}}^{0,0,0,0} \le C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta} \le C_{\mathrm{asymp}}^{\alpha,\beta,\gamma,\theta} \le C_{\mathrm{asymp}}^{\alpha,\infty,\infty,\infty}. \tag{3.10}$$

By the definition with these four parameters $\alpha, \beta, \gamma, \theta$, we consider both symmetric and non-symmetric QPIR capacities at the same time. If $(\alpha, \gamma) = (0, 0)$, the capacities $C_{\mathrm{exact}}^{0,\beta,0,\theta}$ and $C_{\mathrm{asymp}}^{0,\beta,0,\theta}$ are the QPIR capacities with perfect security and if $(\alpha, \beta, \gamma) = (0, 0, 0)$, the capacities $C_{\mathrm{exact}}^{0,0,0,\theta}$ and $C_{\mathrm{asymp}}^{0,0,0,\theta}$ are the symmetric QPIR capacities with perfect security.

3.1.5 Capacity theorem

The main theorem of this chapter is given as follows.

Theorem 3.1 (QPIR capacity)**.** *The capacity of the quantum private information retrieval for* $\mathsf{f} \ge 2$ *messages and* $\mathsf{n} \ge 2$ *servers is*

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

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

Proof. In Section 3.2, we will prove $C_{\text{exact}}^{0,0,0,0} \geq 1$ by constructing a rate-one symmetric QPIR protocol. On the other hand, $C_{\text{asymp}}^{\alpha,\infty,\infty,\infty} \leq 1$ for any $\alpha \in [0,1)$ is trivial upper bound but we give a formal proof of this bound in Section 3.3. Then, the inequality (3.10) implies the theorem. □

Note that the capacity does not depend on the number of messages f and the number of servers n. This contrasts with the classical PIR capacity [26], 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 3.2. In our QPIR model, we assumed that the messages $M_1, \ldots, M_{\mathsf{f}}$ are uniformly at random. However, the assumption is necessary only for proving the converse bounds. Without the assumption, our QPIR protocol has no error and achieves perfect server and user secrecies.

Remark 3.3. We also assumed that the systems $\mathcal{A}'_1, \ldots, \mathcal{A}'_{\mathsf{n}}$ are same dimensional and the same for $\mathcal{A}_1, \ldots, \mathcal{A}_{\mathsf{n}}$. Indeed, we can prove Theorem 3.1 without this assumption. However, we give this assumption for simplicity and since it is necessary for the converse proof of t-private QPIR capacity (Chapter 5), which uses the same formal definition of the protocol.

3.2 Construction of QPIR protocol

In this section, we construct a rate-one two-server QPIR protocol with perfect security and negligible upload cost. Our protocol is constructed if the message 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 perfect security and negligible upload cost, which implies

$$C_{\text{exact}}^{0,0,0,0} \geq 1. \tag{3.11}$$

In the following, we give preliminaries on quantum operations and states in Section 3.2.1 and construct the QPIR protocol in Section 3.2.2.

3.2.1 Preliminaries for protocol construction

For an arbitrary integer $\ell \geq 2$, let $\mathcal{H}$ be an ℓ-dimensional Hilbert space spanned by an orthonormal basis $\{|i\rangle \mid i \in \mathbb{Z}_\ell\}$. Define a maximally entangled state $|\Phi\rangle$ on $\mathcal{H} \otimes \mathcal{H}$ by

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

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

$$\mathsf{X} \coloneqq \sum_{i=0}^{\ell-1} |i+1\rangle\langle i|, \quad \mathsf{Z} \coloneqq \sum_{i=0}^{\ell-1} \omega^i |i\rangle\langle i|, \tag{3.12}$$

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

$$\mathsf{W}(a,b) \coloneqq \mathsf{X}^a\mathsf{Z}^b = \sum_{i=0}^{\ell-1} \omega^{ib} |i+a\rangle\langle i|. \tag{3.13}$$

These operators satisfy the relations

$$\mathsf{Z}^b\mathsf{X}^a = \omega^{ba}\mathsf{X}^a\mathsf{Z}^b, \tag{3.14}$$

$$\mathsf{W}(a_1,b_1)\mathsf{W}(a_2,b_2) = \omega^{b_1a_2}\mathsf{W}(a_1+a_2, b_1+b_2), \tag{3.15}$$

$$\mathsf{W}(a,b)^* = \omega^{ba}\mathsf{W}(-a,-b). \tag{3.16}$$

We use the following double-ket notation [61] for denoting pure states by matrices: For any matrix $T \coloneqq \sum_{i,j=0}^{\ell-1} t_{ij}|i\rangle\langle j|$ on $\mathcal{H}$,

$$|T\rangle\!\rangle \coloneqq \sum_{i,j=0}^{\ell-1} t_{ij}|i\rangle \otimes |j\rangle \in \mathcal{H} \otimes \mathcal{H}. \tag{3.17}$$

With this notation, the maximally entangled state is written as

$$|\Phi\rangle = \frac{1}{\sqrt{\ell}}|I\rangle\!\rangle.$$

Since $T^\top = \sum_{i,j=0}^{\ell-1} t_{ij}|j\rangle\langle i|$, it holds $|T\rangle\!\rangle = (T \otimes I)|I\rangle\!\rangle = (I \otimes T^\top)|I\rangle\!\rangle$. Moreover, for any unitaries U, V on $\mathcal{H}$, we have

$$(U \otimes V)|T\rangle\!\rangle = |UTV^\top\rangle\!\rangle, \tag{3.18}$$

$$(U \otimes \overline{U})|I\rangle\!\rangle = |UU^*\rangle\!\rangle = |I\rangle\!\rangle. \tag{3.19}$$

For the maximally entangled state $|\Phi\rangle$ on $\mathcal{H}\otimes\mathcal{H}$, the Pauli operation $\mathsf{W}(a,b)$ on the first (second) quantum system $\mathcal{H}$ can be translated to the operation $\overline{\mathsf{W}(-a,-b)}$ on the second (first) quantum system $\mathcal{H}$ by

$$\begin{aligned}&(I\otimes\mathsf{W}(a,b))|\Phi\rangle = (\mathsf{W}(a,b)^\top\otimes I)|\Phi\rangle\\ &= ((\overline{\mathsf{W}(a,b)^*}\otimes I)|\Phi\rangle = \omega^{ab}(\overline{\mathsf{W}(-a,-b)}\otimes I)|\Phi\rangle.\end{aligned} \tag{3.20}$$

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

Proposition 3.1. *The set*

$$\mathbf{M}_{\mathbb{Z}_\ell^2} \coloneqq \{(\mathsf{W}(a,b)\otimes I)|\Phi\rangle \mid a,b\in\mathbb{Z}_\ell\}$$

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

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

$$((\mathsf{W}(a,b)\otimes I)|\Phi\rangle)^*(\mathsf{W}(c,d)\otimes I)|\Phi\rangle = 0. \tag{3.21}$$

Since $\mathsf{W}(a,b)^*\mathsf{W}(c,d) = \omega^{b(a-c)}\mathsf{W}(c-a,d-b)$, the left-hand side of (3.21) is written as

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

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

$$\langle\Phi|(\mathsf{W}(x,z)\otimes I)|\Phi\rangle = \frac{1}{\ell}\sum_{i=0}^{\ell-1}\langle i|\mathsf{W}(x,z)|i\rangle \tag{3.22}$$

$$= \frac{1}{\ell}\sum_{i=0}^{\ell-1}\omega^{iz}\langle i|i+x\rangle \tag{3.23}$$

$$= \delta_{(x,z),(0,0)} \tag{3.24}$$

Thus, Eq. (3.21) holds for any $(a,b)\neq(c,d)$, which implies the desired statement. □

3.2.2 Construction of QPIR protocol

In this section, we propose a rate-one two-server QPIR protocol with perfect security and negligible upload cost. This protocol is constructed from the idea of the classical two-server PIR protocol in [5, Section 3.1].

In this protocol, a user retrieves a message M_K from two servers $\mathtt{serv}_1$ and $\mathtt{serv}_2$. Each server contains a copy of the messages $M_1, \dots, M_{\mathsf{f}} \in \{0, \dots, \ell^2 - 1 =: \mathsf{m}_\ell - 1\}$ for an arbitrary integer ℓ. By identifying the set $\{0, \dots, \ell^2 - 1\}$ with $\mathbb{Z}_\ell^2$, the messages $M_1, \dots, M_{\mathsf{f}}$ 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.

Protocol 3.1. *The QPIR protocol for retrieving M_K is described as follows.*

Step 1. ***[Preparation]*** *Depending on the index of the targeted message K, the user chooses a subset R_{user} of $\{1, \dots, \mathsf{f}\}$ uniformly. Let $Q_1 \coloneqq R_{\text{user}}$ and*

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

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

Step 3. ***[Download]*** *$\mathtt{serv}_1$ calculates $H_1 \coloneqq \sum_{i \in Q_1} M_i \in \mathbb{Z}_\ell^2$ and applies $\mathsf{W}(H_1)$ on the quantum system $\mathcal{A}_1$. Similarly, $\mathtt{serv}_2$ calculates $H_2 \coloneqq \sum_{i \in Q_2} M_i$ 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 $(\mathsf{W}(H_1) \otimes \overline{\mathsf{W}(H_2)})|\Phi\rangle$.*

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

Step 4. ***[Retrieval]*** *The user performs a POVM*

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

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

$$Y_{K,Q}(a, b) \coloneqq (\mathsf{W}(a, b) \otimes I)|\Phi\rangle\langle\Phi|(\mathsf{W}(a, b)^* \otimes I)$$

if $K \in Q_1$, *and*

$$Y_{K,Q}(a,b) \coloneqq (\mathsf{W}(-a,-b) \otimes I)|\Phi\rangle\langle\Phi|(\mathsf{W}(-a,-b)^* \otimes I)$$

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

Protocol 3.1 is analyzed as follows.

Error probability

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

$$\begin{aligned}
&\mathsf{W}(H_1) \otimes \overline{\mathsf{W}(H_2)}|\Phi\rangle \\
&= \frac{\omega^{\mp b_{M_K} a_{H_2}}}{\sqrt{\ell}} (\mathsf{W}(\pm M_K) \otimes I)(\mathsf{W}(H_2) \otimes \overline{\mathsf{W}(H_2)})|I\rangle\!\rangle \qquad (3.25) \\
&= \frac{\omega^{\mp b_{M_K} a_{H_2}}}{\sqrt{\ell}} (\mathsf{W}(\pm M_K) \otimes I)|I\rangle\!\rangle \qquad (3.26) \\
&= \omega^{\mp b_{M_K} a_{H_2}} (\mathsf{W}(\pm M_K) \otimes I)|\Phi\rangle,
\end{aligned}$$

where $H_2 = (a_{H_2}, b_{H_2})$ and $M_K = (a_{M_K}, b_{M_K}) \in \mathbb{Z}_\ell^2$. The equality (3.25) is derived from $\mathsf{W}(H_1) = \mathsf{W}(\pm M_K + H_2) = \omega^{\mp b_{M_K} a_{H_2}} \mathsf{W}(\pm M_K)\mathsf{W}(H_2)$ and the equality (3.26) is from (3.19). Therefore, in Step 5, the measurement outcome is $M_K \in \mathbb{Z}_\ell^2$ with probability 1.

User secrecy and server secrecy

Perfect user secrecy follows from that of the protocol [5, 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, perfect user secrecy is obtained.

Perfect server secrecy is obtained because the received state of the user is $(\mathsf{W}(\pm M_K) \otimes I)|\Phi\rangle$, which is independent of the messages except for M_K.

Costs and QPIR rate

The upload cost is $U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) = 2\mathsf{f} \log 2$ 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 $D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) = \log \dim \mathcal{A}_1 \otimes \mathcal{A}_2 = \log \ell^2 = \log \mathsf{m}_\ell$. Therefore, the rate is

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

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

3.2.3 Security against malicious operations

In the previous subsection, we showed that the protocol in Section 3.2.2 has perfect security when the user and the servers follow the protocol. In this subsection, we prove that the protocol in Section 3.2.2 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 where the servers apply malicious operations to obtain the index of the targeted message 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 3.2.2. 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 message in addition to the targeted message M_K. That is, the user sends malicious queries $Q = (Q_1, Q_2)$ to retrieve the message M_K and some information of $M_K^c = (M_1, \ldots, M_{K-1}, M_{K+1}, \ldots, M_{\mathsf{f}})$. Similar to the malicious server model, we assume that the servers follow 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 $M_K \in \{0, \ldots, \mathsf{m}_\ell - 1\}$. That is, the user cannot obtain more information than M_K. This security is precisely proved by the following relation:

$$I(\mathcal{A}; M_K^c | M_K, K, Q)_{\rho_{MQ}} = 0, \tag{3.27}$$

where $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$.

Proof of Eq. (3.27). Since the user obtains the message M_K, we have

$$H(M_K|\mathcal{A}, K, Q)_{\rho_{MQ}} = 0. \tag{3.28}$$

Eq. (3.28) is equivalent to

$$H(\mathcal{A}, M_K|K, Q)_{\rho_{MQ}} = H(\mathcal{A}|K, Q)_{\rho_{MQ}}. \tag{3.29}$$

The relation (3.29) implies the following relations:

$$\begin{aligned} 0 &\le H(\mathcal{A}|M_K, K, Q)_{\rho_{MQ}} && (3.30)\\ &= H(\mathcal{A}, M_K|K, Q)_{\rho_{MQ}} - H(M_K|K, Q) && (3.31)\\ &= H(\mathcal{A}|K, Q)_{\rho_{MQ}} - \log \mathsf{m}_\ell \le 0. && (3.32) \end{aligned}$$

The equality in (3.32) follows from the condition (3.29), the independence between M_K and (K, Q), and the uniform distribution of M_K. The last inequality in (3.32) follows from $\dim \mathcal{A} = \log \mathsf{m}_\ell$. Therefore, we have

$$H(\mathcal{A}|M_K, K, Q)_{\rho_{MQ}} = 0 \tag{3.33}$$

which implies (3.27). □

3.3 Strong converse bound

In this section, we prove the converse bound

$$C_{\mathrm{asymp}}^{\alpha,\infty,\infty,\infty} \le 1 \tag{3.34}$$

for any $\alpha \in [0, 1)$.

For the proof, we prepare the following proposition from [65, Eq. (4.66)]. The proof of Proposition 3.2 is reorganized in Appendix A.

Proposition 3.2 ([65, Eq. (4.66)]). *Consider the scenario that a classical message $w \in \{0, \dots, \mathsf{m} - 1\}$ is encoded as ρ_w and it is decoded by the the decoding measurement $\{Y(w)\}_{w=1}^{\mathsf{m}}$. Define the average error probability by $P_{\mathrm{err}} = (1/\mathsf{m}) \sum_{i=1}^{\mathsf{m}} \operatorname{Tr} \rho_w Y(w)$. Then, for any $s \in [0, 1]$ and any state σ such that $\operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma)$, we have*

$$(1 - P_{\mathrm{err}})^{1+s} \mathsf{m}^s \le \frac{1}{\mathsf{m}} \sum_{w=1}^{\mathsf{m}} \operatorname{Tr} \rho_w^{1+s} \sigma^{-s}. \tag{3.35}$$

We introduce the following notation. By replacing the notation of ρ_{MQ} defined in (3.1), let $\rho_{m_k,z}$ be the quantum state on the composite system $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j$, where m_k is the message to be retrieved and $z \coloneqq (m_k^c, q)$ for the collection m_k^c of other $\mathsf{m}-1$ messages and the collection q of queries. Let $\sigma_z \coloneqq (1/\mathsf{m}) \sum_{m_k=1}^{\mathsf{m}} \rho_{m_k,z}$.

Applying Proposition 3.2 with $(s, \rho_w, Y(w), \sigma) \coloneqq (1, \rho_{m_k,z}, Y_{k,q}(w), \sigma_z)$, we have

$$(1 - P_{\mathrm{err},z}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}))^2 \mathsf{m} \le \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \rho_{m_k,z}^2 \sigma_z^{-1}, \tag{3.36}$$

where $P_{\mathrm{err},z}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ is the error probability when z is fixed. Furthermore, we can bound the RHS of (3.36) as

$$\begin{aligned} &\frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \rho_{m_k,z}^2 \sigma_z^{-1} \le \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \rho_{m_k,z} \sigma_z^{-1} \\ &= \operatorname{Tr} \sigma_z \sigma_z^{-1} = \operatorname{Tr} I = \prod_{j=1}^{\mathsf{n}} \dim \mathcal{A}_j \end{aligned} \tag{3.37}$$

Combining (3.36) and (3.37), the error probability is upper bounded as

$$1 - P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 1 - \mathbb{E}_Z P_{\mathrm{err},Z}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \tag{3.38}$$

$$\le \sqrt{\frac{\prod_{j=1}^{\mathsf{n}} \dim \mathcal{A}_j}{\mathsf{m}}}. \tag{3.39}$$

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

$$R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) = \frac{\log \mathsf{m}_\ell}{\log \prod_{j=1}^{\mathsf{n}} \dim \mathcal{A}_j} \ge 1 \tag{3.40}$$

for any sufficiently large ℓ, we have

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

Hence, by (3.39), $1 - P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})$ approaches zero, which implies (3.34).

Chapter 4

Capacity of Multi-Round Quantum Private Information Retrieval

In Chapter 3, we considered the case where the user and the servers communicate only one round. In this chapter, we consider the QPIR problem when the user and the servers communicate multiple times. When multi-round interaction is allowed, the user and the servers may choose their encoders and decoder depending on the information obtained in the previous rounds. Thus, multi-round QPIR is not reduced to one-round QPIR and it is expected to achieve higher QPIR rate in general.

The strength of the models of multi-round protocols differs depending on whether the user's and servers' memories are classical memory or quantum memory. With classical memories, the user and the servers record only classical information. On the other hand, when quantum memories are available, they can regard their quantum memories as the environment systems of quantum operations and measurements, and thus a kind of quantum side information becomes available. Since the classical information can be recorded in the quantum memory, the model with quantum memories includes the model with classical memories. To survey the model with stronger resources as possible, in this chapter, we consider that the user and the servers have quantum memories.

The main question in this chapter is as follows.

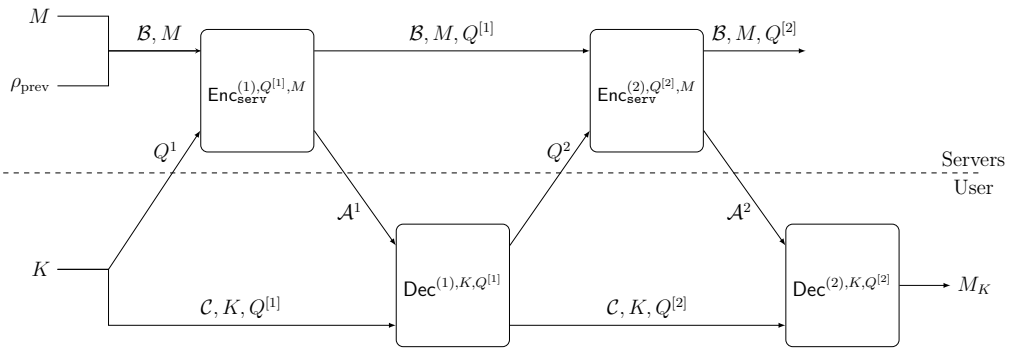


Figure 4.1: Information flow in 2-round QPIR protocol. The servers have all messages $M = (M_1, \ldots, M_{\mathsf{f}})$ and the user retrieves the K-th message M_K.

Question 1. *Is the multi-round QPIR capacity with local quantum memories strictly higher than the one-round QPIR capacity derived in Chapter 3?*

Since multi-round QPIR with quantum memories generalizes the model in Chapter 3, one may expect a positive answer to the question. Furthermore, there exists a one-server multi-round QPIR protocol which has better communication complexity than any one-server one-round QPIR protocols [48]. On the other hand, one may also conjecture the answer negatively because there have been many negative results in similar scenarios: The classical multi-round PIR capacity is the same as the one-round capacity [38]; In classical one-sender one-receiver multi-round communication protocols, the feedback does not increase the capacity [62].

In this chapter, we answer Question 1 negatively: the multi-round QPIR capacity is 1. The proof idea is to use the trivial upper bound 1 of the QPIR rate as we remarked in Section 3.1.3. This chapter essentially gives the formal proof of this trivial upper bound for the multi-round case. Section 4.1 formally defines the multi-round QPIR protocol as a generalization of the protocol description in Section 3.1.1 and proposes the capacity theorem. Section 4.2 proves the weak converse bound that any multi-round QPIR protocol has rate at most 1. Then the achievability of the capacity is guaranteed by the protocol in Section 3.2.2, which has the QPIR rate 1. The weak converse bound in Section 4.2 also applies to the one-round QPIR in Chapter 3.

4.1 Multi-round QPIR protocol and capacity theorem

4.1.1 Formal definition of multi-round QPIR protocol

For any positive integer r, we give the formal description of the r-round QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m},\mathsf{r})}$. The information flow of the quantum systems is depicted in Figure 4.1. When $\mathsf{r}=1$, the protocol description is equivalent to the protocol defined in Section 3.1.1.

Let $\mathsf{n},\mathsf{f},\mathsf{m}$ be integers greater than 1. Each of the servers $\mathtt{serv}_1,\dots,\mathtt{serv}_{\mathsf{n}}$ contains the whole copy of the uniformly and independently distributed f messages $M=(M_1,\dots,M_{\mathsf{f}})\in\{1,\dots,\mathsf{m}\}^{\mathsf{f}}$. The j-th server $\mathtt{serv}_j$ possesses a quantum system $\mathcal{B}_j$ as local quantum register and the n servers share an entangled state ρ_{prev} on the quantum system $\mathcal{B}\coloneqq\mathcal{B}_1\otimes\cdots\otimes\mathcal{B}_{\mathsf{n}}$.

The user chooses the index of the targeted message $K\in\{1,\dots,\mathsf{f}\}$ uniformly and independently of the messages $M_1,\dots,M_{\mathsf{f}}$. The user prepares the query $Q^1=(Q_1^1,Q_2^1,\dots,Q_{\mathsf{n}}^1)$ depending on K. The user has a local quantum register $\mathcal{C}$ where the state is initialized depending on K and Q^1.

For $i\in\{1,\dots,\mathsf{r}\}$, the i-th round is described as follows. Let Q_j^i be the query to $\mathtt{serv}_j$ at round i, and we denote $Q^i\coloneqq(Q_1^i,\dots,Q_{\mathsf{n}}^i)$ and $Q_j^{[i]}\coloneqq(Q_j^1,\dots,Q_j^i)$. The query Q^i for round i is determined at round $i-1$. The user sends Q_j^i to the j-th server $\mathtt{serv}_j$. Depending on $Q_j^{[i]}$ and M, each server $\mathtt{serv}_j$ applies a CPTP map $\mathsf{Enc}_{\mathtt{serv}_j}^{(i),Q_j^{[i]},M}$ from $\mathcal{B}_j$ to $\mathcal{A}_j^i\otimes\mathcal{B}_j$. That is, when the collection of the encoders is written as

$$\mathsf{Enc}_{\mathtt{serv}}^{(i),Q^{[i]},M}\coloneqq\bigotimes_{j=1}^{\mathsf{n}}\mathsf{Enc}_{\mathtt{serv}_j}^{(i),Q_j^{[i]},M},$$

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

$$\rho_M^{\mathcal{A}^i\mathcal{B}}\coloneqq\mathsf{Enc}_{\mathtt{serv}}^{(i),Q^{[i]},M}(\rho_M^{\mathcal{B}}),$$

where $\mathcal{A}^i\coloneqq\mathcal{A}_1^i\otimes\cdots\otimes\mathcal{A}_{\mathsf{n}}^i$. Each server transmits the system $\mathcal{A}_j^i$ to the user and the received state of the user is the reduced state

$$\rho_M^{\mathcal{A}^i}\coloneqq\operatorname*{Tr}_{\mathcal{B}}\rho_M^{\mathcal{A}^i\mathcal{B}}. \tag{4.1}$$

If $i < \mathsf{r}$, the user applies a quantum instrument $\mathsf{Dec}^{(i),K,Q^{[i]}} = \{Y^i_{Q^{i+1}}\}_{Q^{i+1}\in\mathcal{Q}^{i+1}}$ from $\mathcal{A}^i\otimes\mathcal{C}$ to $\mathcal{C}$ depending on K and $Q^{[i]} := (Q^1,\dots,Q^i)$, where $\mathcal{Q}_1^{i+1}\times\cdots\times\mathcal{Q}_{\mathsf{n}}^{i+1}$ 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 $i=\mathsf{r}$, i.e., at the final round, the user applies a POVM $\mathsf{Dec}^{(\mathsf{r}),K,Q^{[\mathsf{r}]}} = \{Y_{K,Q}(w)\}_{w=1}^{\mathsf{m}}$ on $\mathcal{A}^{\mathsf{r}}\otimes\mathcal{C}$ depending on K and $Q^{[\mathsf{r}]}$ and outputs the measurement outcome $W\in\{1,\dots,\mathsf{m}\}$.

Similar to Section 3.1.1, the security of the protocol is evaluated by the the error probability, the server secrecy, and the user secrecy defined by

$$\begin{aligned}
P_{\mathrm{err}}(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}) &:= \Pr_{W,K,Q^1}[W\neq M_K],\\
S_{\mathrm{serv}}(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}) &:= I(M_K^c;\mathfrak{user}(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}})|K),\\
S_{\mathrm{user}}(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}) &:= \max_{j\in\{1,\dots,\mathsf{n}\}} I(K;\mathfrak{serv}_j(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}})),
\end{aligned}$$

where $\mathfrak{user}(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}})$ and $\mathfrak{serv}_j(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}})$ are the information of the user and the server $\mathtt{serv}_j$ at the end of the protocol $\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}$, respectively. Given the QPIR protocol $\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}$, we define the upload cost, the download cost, and the QPIR rate by

$$U(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}) := \sum_{i=1}^{\mathsf{r}}\log|\mathcal{Q}^i|, \tag{4.2}$$

$$D(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}) := \sum_{i=1}^{\mathsf{r}}\log\dim\mathcal{A}^i, \tag{4.3}$$

$$R(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}}) := \frac{\log\mathsf{m}}{D(\Psi^{(\mathsf{m},\mathsf{r})}_{\mathrm{QPIR}})}. \tag{4.4}$$

Now, we define the r-round QPIR capacities with four parameters. The capacities are defined in the same way as Section 3.1.4 but we use the superscript r to denote that they are the r-round capacities. 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

$$\begin{aligned}
C^{\alpha,\beta,\gamma,\theta,\mathsf{r}}_{\mathrm{asymp}} &:= \sup_{(4.5)}\liminf_{\ell\to\infty} R(\Psi^{(\mathsf{m}_\ell,\mathsf{r})}_{\mathrm{QPIR}}),\\
C^{\alpha,\beta,\gamma,\theta,\mathsf{r}}_{\mathrm{exact}} &:= \sup_{(4.6)}\liminf_{\ell\to\infty} R(\Psi^{(\mathsf{m}_\ell,\mathsf{r})}_{\mathrm{QPIR}}),
\end{aligned}$$

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 $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})}\}_{\ell=1}^{\infty}$ of r-round QPIR protocols to satisfy either (4.5) or (4.6) given by

$$\begin{aligned}&\limsup_{\ell\to\infty} P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})\le\alpha,\ \ \limsup_{\ell\to\infty} S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})\le\beta,\\ &\limsup_{\ell\to\infty} S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})\le\gamma,\ \ \limsup_{\ell\to\infty}\frac{U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})}\le\theta,\end{aligned}\tag{4.5}$$

and

$$\begin{aligned}&P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})\le\alpha,\ \ S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})\le\beta,\\ &S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})\le\gamma,\ \ \limsup_{\ell\to\infty}\frac{U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})})}\le\theta.\end{aligned}\tag{4.6}$$

Since multi-round model allows more options for the QPIR task, we have the following inequality from definition: for any $\mathsf{r}\le\mathsf{r}'$,

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta,\mathsf{r}}\le C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta,\mathsf{r}'},\tag{4.7}$$

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta,\mathsf{r}}\le C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta,\mathsf{r}'}.\tag{4.8}$$

However, it is not trivial from definition whether the inequalities (4.7), (4.8) are strict or not.

4.1.2 Capacity theorem

The multi-round QPIR capacity is derived as follows.

Theorem 4.1 (Multi-round QPIR capacity)**.** *Let* r *be any positive integer. The* r*-round QPIR capacity for* $\mathsf{f}\ge 2$ *messages and* $\mathsf{n}\ge 2$ *servers is*

$$C_{\mathrm{exact}}^{0,\beta,\gamma,\theta,\mathsf{r}}=C_{\mathrm{asymp}}^{0,\beta,\gamma,\theta,\mathsf{r}}=1\tag{4.9}$$

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

Proof. Eq. (4.9) is proved by the following inequalities:

$$1\le C_{\mathrm{exact}}^{0,0,0,0,\mathsf{r}}\le C_{\mathrm{exact}}^{0,\beta,\gamma,\theta,\mathsf{r}}\le C_{\mathrm{asymp}}^{0,\beta,\gamma,\theta,\mathsf{r}}\le C_{\mathrm{asymp}}^{0,\infty,\infty,\infty,\mathsf{r}}\le 1.$$

The first inequality holds by applying the rate-one QPIR protocol in Section 3.2.2 repetitively r times. The second, third, and fourth inequalities follow from the definition of the capacities. The last inequality is proved in Section 4.2. Therefore, we obtain the theorem. □

For one-round case ($\mathsf{r} = 1$), the capacity result also applies to the QPIR model of in Section 3.1.1. Differently from Theorem 3.1, Theorem 4.1 proves only for the case where error probability goes to 0 (i.e., $\alpha = 0$). Theorems 3.1 and 4.1 prove that the inequalities (4.7), (4.8) are indeed equalities when error probability is asymptotically 0.

4.2 Weak converse bound

We prove the converse bound

$$C_{\text{asymp}}^{0,\infty,\infty,\infty,\mathsf{r}} \leq 1. \tag{4.10}$$

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 [63]. In the CQ channel coding with classical feedback, the sender encodes a classical message M 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 M. The paper [63] proved the capacity of this problem when the sender and the receiver have their local quantum registers, respectively. The paper [63] also considered the energy constraint E that for a given Hamiltonian H on the input system of $\mathcal{N}$, the input states $\rho_1, \ldots, \rho_{\mathsf{r}}$ to the channel $\mathcal{N}$ should satisfy $\sum_{i=1}^{\mathsf{r}} \operatorname{Tr} \rho_i \mathsf{H} \leq E$. The CQ channel capacity is characterized by the following proposition.

Proposition 4.1 ([63, 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 acting 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:*

$$(1-\varepsilon)\log \mathsf{m} \leq \sup_{\rho:\operatorname{Tr}\rho\mathsf{H}\leq E} \mathsf{r} H(\mathcal{N}(\rho)) + h_2(\varepsilon). \tag{4.11}$$

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 targeted message M_K. Therefore, we can consider the multi-round QPIR protocol as a CQ channel coding with classical feedback.

By the similar proof of [63, Theorem 4], we have the following proposition.

Proposition 4.2. *Consider the CQ channel coding of a classical message $M \in \{1, \ldots, \mathsf{m}\}$ from the sender to the receiver by sending quantum systems $\mathcal{A}^1, \ldots, \mathcal{A}^{\mathsf{r}}$ sequentially over the identity channel and assisted by classical feedback. We assume that the sender and the receiver have local quantum registers, respectively. Let $\rho_M^{\mathcal{A}^i}$ be the state on $\mathcal{A}^i$. For the uniformly chosen message M and the decoding output W, we define the error probability $\varepsilon := \Pr[M \neq W]$. Then we have the following inequality*

$$(1-\varepsilon)\log \mathsf{m} \leq \sum_{i=1}^{\mathsf{r}} H(\rho_M^{\mathcal{A}^i}) + h_2(\varepsilon) \tag{4.12}$$

$$\leq \sum_{i=1}^{\mathsf{r}} \log \dim \mathcal{A}^i + h_2(\varepsilon), \tag{4.13}$$

where $h_2(\cdot)$ is the binary entropy function defined in (2.5).

For completeness of our thesis, we give a proof of Proposition 4.2 in Appendix B.

Remark 4.1. Proposition 4.2 is slightly different from [63, Theorem 4]. First, whereas [63, Theorem 4] considers an energy constraint on the quantum channel, Proposition 4.2 assumes no energy constraint. Second, whereas [63, Theorem 4] considers the repetitive uses of a fixed quantum channel $\mathcal{N}$, Proposition 4.2 considers each use of the identity quantum channels over $\mathcal{A}^1, \ldots, \mathcal{A}^{\mathsf{r}}$. Even with these differences, we can apply the same proof steps of [63, Theorem 4] and the first inequality of [63, Eq. (35)] is the inequality (4.12).

Now we prove the weak converse bound. We choose an arbitrary sequence $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})}\}_{\ell=1}^{\infty}$ of r-round QPIR protocols to satisfy $\varepsilon_\ell := P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})}) \to 0$ as $\ell \to \infty$. Considering the collection of the n servers as the sender and the user as the receiver of Proposition 4.2, we can apply Proposition 4.2 to the r-round QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})}$ with the classical message $M_K \in \{1,\dots,\mathsf{m}_\ell\}$, transmitted quantum systems $\mathcal{A}^1,\dots,\mathcal{A}^{\mathsf{r}}$, and classical feedback $Q^1,\dots,Q^{\mathsf{r}}$. In this case, ε and m of Proposition 4.2 is substituted by ε_ℓ and m_ℓ, i.e., Eq. (4.13) is written as

$$(1-\varepsilon_\ell)\log \mathsf{m}_\ell \le \sum_{i=1}^{\mathsf{r}} \log\dim \mathcal{A}^i + h_2(\varepsilon_\ell). \tag{4.14}$$

Therefore, we have

$$\lim_{\ell\to\infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell,\mathsf{r})}) = \lim_{\ell\to\infty} \frac{\log \mathsf{m}_\ell}{\sum_{i=1}^{\mathsf{r}} \log\dim \mathcal{A}^i} \le 1, \tag{4.15}$$

which implies (4.10).

Chapter 5

Capacity of Quantum Private Information Retrieval with Colluding Servers

The multi-server QPIR model considered in Chapter 3 has a critical weakness that the assumption of no communication among servers is too restrictive. By relieving this assumption, this chapter considers t-private QPIR in which the identity of the retrieved message is kept secret even if at most t servers may communicate and collude. We derive the t-private QPIR capacity for any t less than the number of servers n. The formal definition of QPIR protocol is the same way as Chapter 3. The t-private QPIR capacity is defined with three security parameters: error probability, server secrecy, user t-secrecy. As a main result, we prove that the symmetric and non-symmetric t-private QPIR capacity is $\min\{1, 2(\mathsf{n}-\mathsf{t})/\mathsf{n}\}$ for $1 \leq \mathsf{t} < \mathsf{n}$. Our result implies that even if some servers collude, as far as the number of colluding servers is less than half ($\mathsf{t} \leq \mathsf{n}/2$), the remarkable result of QPIR capacity 1 still applies to the t-private case.

The derived quantum capacity is strictly greater than the classical symmetric t-private PIR capacity $(\mathsf{n}-\mathsf{t})/\mathsf{n}$ in [30], and when more than half of the servers collude (i.e., $\mathsf{n}/2 \leq \mathsf{t}$), the derived quantum capacity is exactly twice the classical capacity. In addition, compared to the classical t-private PIR capacity $(1-\mathsf{t}/\mathsf{n})(1-(\mathsf{t}/\mathsf{n})^{\mathsf{f}})$ [29], our quantum capacity is greater when $\mathsf{t} < \mathsf{n}/2$ or $(\mathsf{n}/\mathsf{t})^{\mathsf{f}} > 2$, where the latter inequality satisfied when the number of messages f are large enough.

Our result implies that symmetric $\lfloor \mathsf{n}/2 \rfloor$-private QPIR can be constructed without sacrificing any communication efficiency since the capacity is 1 for $1 \leq \mathsf{t} \leq \mathsf{n}/2$. Moreover, QPIR with more servers may obtain the stronger secrecy against collusion. This result contrasts with Chapter 3 that the symmetric (1-private) QPIR has no advantage to increase the number of servers since a two-server protocol achieves the capacity. The proposed protocol includes the protocol in Chapter 3 as an example of symmetric 1-private QPIR protocols.

The outline of our protocol is described as follows by the stabilizer formalism. Given a subspace V of an even dimensional vector space, let $\mathrm{V}^{\perp_J}$ be its orthogonal space with respect to the symplectic bilinear form. In the stabilizer formalism, the stabilizer is described by a subspace V such that $\mathrm{V} \subset \mathrm{V}^{\perp_J}$ and the state is prepared on the stabilized subspace. When the Weyl operator $\tilde{\mathbf{W}}(\mathbf{s}, \mathbf{t}) \coloneqq \mathbf{X}(\mathbf{s})\mathbf{Z}(\mathbf{t})$ is applied, in the decoding process, an appropriate quantum measurement outputs the outcome $(\mathbf{s}, \mathbf{t}) + \mathrm{V}^{\perp_J}$, which is a partial information of the Weyl operator. With this fact, we design our QPIR protocol so that the servers share an entangled state on the stabilized subspace, the servers apply Weyl operators depending on the queries and messages, and the user performs the measurement to obtain the targeted message. Here, for guaranteeing the security, we choose the subspace V and the queries to satisfy the following three conditions. 1) The queries to any t servers are independent of the user's request (for user secrecy). 2) When the Weyl operator applied by the servers is $\tilde{\mathbf{W}}(\mathbf{s}, \mathbf{t})$ on the whole composite system, the targeted message has one-to-one correspondence with the value $(\mathbf{s}, \mathbf{t}) + \mathrm{V}^{\perp_J}$ (for correctness). 3) The information of other messages is in $\mathrm{V}^{\perp_J}$ (for server secrecy). The main difficulty of the protocol construction is to find an appropriate vector space V which generates the properties 1), 2), and 3). The problem reduces to the search of a symplectic matrix with a linear independence condition in row vectors and a symplectic orthogonality condition in column vectors. We concretely constructs the symplectic matrix satisfying those conditions.

The remainder of this chapter is organized as follows. Section 5.1 defines the security and the QPIR capacity and presents the t-private QPIR capacity theorem. Section 5.2 is the preliminary section for protocol construction. With the stabilizer formalism defined in Section 5.2.1, we present a communication protocol for classical messages by stabilizer formalism and give

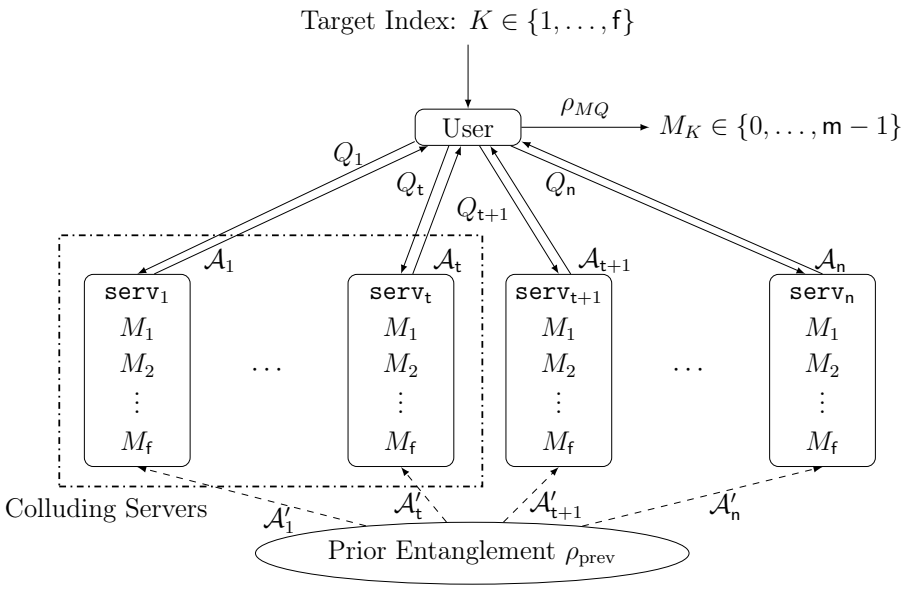


Figure 5.1: Quantum private information retrieval protocol, where t servers collude to know the target index K. The user does not know which t servers collude. The only difference from Figure 3.1 is that at most t servers may collude.

a fundamental lemma for protocol construction. Section 5.3 constructs the capacity-achieving symmetric t-private QPIR protocol. The proposed protocol has no error, perfect user secrecy, and perfect server secrecy. Section 5.4 presents the converse bounds of the capacity result. We present three upper bounds of the capacity depending on the number of colluding servers and the security parameters.

5.1 QPIR protocol and capacity theorem

For t-private QPIR, the protocol is identically defined as the QPIR protocol Section 3.1.1, but the security and the capacity are defined differently. Therefore, throughout this chapter, we use the protocol description in Section 3.1.1, and in this section, we define the security measures and present the t-private QPIR capacity theorem. The t-private QPIR protocol is depicted in Figure 5.1.

5.1.1 Security measures

Given the number of colluding servers $\mathsf{t} \in \{1, \dots, \mathsf{n}-1\}$, the security measures are defined as follows. In this chapter, we assume that all servers and the user follow the protocol and do not deviate from the protocol. Under this assumption, we consider the security of the QPIR protocol as follows. Let $W \in \{1, \dots, \mathsf{m}\}$ be the protocol output, M_k^c be the collection of all messages except for M_k, S_n be the symmetric group of $\{1, \dots, \mathsf{n}\}$, i.e., the set of all permutations on $\{1, \dots, \mathsf{n}\}$, and $Q_{\pi,\mathsf{t}} \coloneqq (Q_{\pi(1)}, \dots, Q_{\pi(\mathsf{t})})$ for $\pi \in \mathsf{S}_\mathsf{n}$. The security of a QPIR protocol is evaluated by the error probability, server secrecy, and user t-secrecy defined as

$$P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \max_{(*)} \Pr_W[W \neq m_k | M = m, Q = q, K = k] \tag{5.1}$$

$$S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \max_{(*)} I(M_k^c; \mathcal{A} | Q = q, K = k)_{\rho_{Mq}} \tag{5.2}$$

$$S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \max_{\pi \in \mathsf{S}_\mathsf{n}} I(K; Q_{\pi,\mathsf{t}}), \tag{5.3}$$

where the maximum $(*)$ is taken for all $m = (m_1, \dots, m_\mathsf{n}), q \in \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_\mathsf{n}, k \in \{1, \dots, \mathsf{f}\}$ such that $\Pr[K = k, Q = q] \neq 0$.

The error probability $P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ is the worst-case probability that the protocol output W is the targeted message of the user. The server secrecy is the property that the servers' information of the non-targeted messages are kept secret from the user. That is, the server secrecy $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ measures the independence between the non-targeted messages and the quantum systems $\mathcal{A}$ that the user obtains. Since we assumed that the servers do not deviate from the protocol, $\mathtt{serv}_j$ only obtains Q_j but not the other information. Therefore, the user t-secrecy $S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ is defined as the mutual information between the target index K and the queries $Q_{\pi,\mathsf{t}}$ to any t servers. We define these security measures for the worst-case of all messages m, queries q, and the target index k.

Remark 5.1. The server secrecy is also written as

$$S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = \max_{(*)} I(M_k^c; \mathcal{A} | Q = q)_{\rho_{Mq}}. \tag{5.4}$$

This equation follows from $I(M_k^c; \mathcal{A} | Q = q)_{\rho_{Mq}} = I(M_k^c; \mathcal{A} | Q = q, K = k)_{\rho_{Mq}}$ which is derived from the independence between K and $M_k^c \mathcal{A}$ when $Q = q$ is fixed.

Remark 5.2. When a QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$ satisfies $P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \alpha$ and $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \beta$ for sufficiently small $\alpha, \beta \geq 0$, the condition $\Pr[K = k, Q = q] \neq 0$ implies $\Pr[K = i, Q = q] = 0$ for any $k \neq i \in \{1, \ldots, \mathsf{f}\}$. Otherwise, we derive a contradiction as follows. If $\Pr[K = k, Q = q] \cdot \Pr[K = i, Q = q] \neq 0$ for some $k \neq i$, the server secrecy $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \beta$ implies $I(M_i^c; \mathcal{A}|Q = q, K = i)_{\rho_{Mq}}, I(M_k^c; \mathcal{A}|Q = q, K = k)_{\rho_{Mq}} \leq \beta$. However, we have the following contradiction

$$
\begin{aligned}
&(1-\alpha)\log \mathsf{m} - h_2(\alpha) \overset{(a)}{\leq} I(M_k; \mathcal{A}|Q = q, K = k)_{\rho_{Mq}} \overset{(b)}{=} I(M_k; \mathcal{A}|Q = q)_{\rho_{Mq}} \\
&\leq I(M_i^c; \mathcal{A}|Q = q)_{\rho_{Mq}} \overset{(b)}{=} I(M_i^c; \mathcal{A}|Q = q, K = i)_{\rho_{Mq}} \leq \beta,
\end{aligned}
$$

from Fano's inequality and two equalities with (b) is from the independence of K and $(M_1, \ldots, M_{\mathsf{f}}, \mathcal{A})$ when $Q = q$ is fixed. Since β can be chosen to be an arbitrary small number, these inequalities imply that the message size m is also sufficiently close to zero, which is a contradiction.

5.1.2 t-Private QPIR capacity

For fixed numbers of servers n and messages f, we define the t-private QPIR capacity. The capacities are defined similar to Section 3.1.4 but we use the subscript t to denote that they are the t-private capacities. For any $\alpha \in [0, 1)$ and any β, γ, $\theta \in [0, \infty]$, the *asymptotic* and *exact security-constrained* t-*private QPIR capacities* are defined by

$$
C_{\mathrm{asymp},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} := \sup_{(5.7)} \liminf_{\ell \to \infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}), \tag{5.5}
$$

$$
C_{\mathrm{exact},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} := \sup_{(5.8)} \liminf_{\ell \to \infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}), \tag{5.6}
$$

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 $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ of QPIR protocols to satisfy either (5.7) or (5.8) given by

$$
\begin{aligned}
&\limsup_{\ell\to\infty} P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \leq \alpha, \quad \limsup_{\ell\to\infty} S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \leq \beta, \\
&\limsup_{\ell\to\infty} S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \leq \gamma, \quad \limsup_{\ell\to\infty} \frac{U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})} \leq \theta,
\end{aligned} \tag{5.7}
$$

and

$$P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \alpha,\ S_{\text{serv}}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \beta,$$
$$S_{\text{user}}^{(\mathsf{t})}(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}) \leq \gamma,\ \limsup_{\ell\to\infty} \frac{U(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})}{D(\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)})} \leq \theta. \tag{5.8}$$

5.1.3 Capacity theorem

The following theorem is the main result of this chapter.

Theorem 5.1 (t-private QPIR capacity)**.** *The capacity of t-private QPIR with $\mathsf{n} \geq 2$ servers and $\mathsf{f} \geq 2$ messages is derived for any $\alpha \in [0,1)$ and any $\beta, \gamma, \theta \in [0,\infty)$ as follows:*

$$C_{\text{asymp},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} = C_{\text{exact},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} = 1 \qquad \text{if } 1 \leq \mathsf{t} \leq \frac{\mathsf{n}}{2}, \tag{5.9}$$
$$C_{\text{asymp},\mathsf{t}}^{0,\beta,0,\theta} = C_{\text{exact},\mathsf{t}}^{\alpha,0,0,\theta} = \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \qquad \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} < \mathsf{n}. \tag{5.10}$$

The capacity-achieving QPIR protocol is constructed in Section 5.3 for $\mathsf{n}/2 \leq \mathsf{t} < \mathsf{n}$. The protocol obtains zero-error ($P_{\text{err}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) = 0$), perfect server secrecy ($S_{\text{serv}}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) = 0$), and perfect user t-secrecy ($S_{\text{user}}^{(\mathsf{t})}(\Psi_{\text{QPIR}}^{(\mathsf{m})}) = 0$). Since the user $(\mathsf{n}/2)$-secrecy guarantees the user t-secrecy for $1 \leq \mathsf{t} < \mathsf{n}/2$, the constructed protocol for $\mathsf{t} = \mathsf{n}/2$ is also the capacity-achieving protocol for $1 \leq \mathsf{t} < \mathsf{n}/2$. The converse bounds are given in Section 5.4.

Note that if $\mathsf{t} \leq \mathsf{n}/2$, the capacity is 1 and independent of n and f, which is similar result as the QPIR capacity without colluding servers in Chapter 3. When $\mathsf{t} > \mathsf{n}/2$, the capacity is twice the symmetric PIR capacity $(\mathsf{n}-\mathsf{t})/\mathsf{n}$ and is still independent of the number of messages f. As discussed in the introduction and Table 1.1, the t-private QPIR capacity is greater than the classical counterparts. Furthermore, we prove in Appendix C that the capacity result is the same even if we change the definition of the security measures as the average measures for all files m, queries q, and target indexes k.

Remark 5.3. In the definition of the protocol, we assumed the condition that the target index K and the messages $M_1, \ldots, M_{\mathsf{f}}$ are chosen uniformly. Indeed, this condition is necessary only for the proof of converse bounds. Even if the distributions are arbitrary, the protocol in Section 5.3 guarantees

that any t-servers obtains no information about K and the user obtains no information of non-targeted messages, except for the information obtained from the underlying distributions of K and $M_1, \ldots, M_{\mathsf{f}}$.

Remark 5.4. In Chapter 3, we defined the error probability (3.2) as the average error probability. On the other hand, this chapter defines the error probability (5.1) as the worst-case error probability. From the definitions, the QPIR capacity with the worst-case error is less than the QPIR capacity with the average error. However, this chapter extends the result of Chapter 3 by proving that the 1-private QPIR capacity with worst-case error is also 1.

Remark 5.5. The capacity (5.10) is derived for the case where any server secrecy $\beta \in [0, \infty)$ is allowed. However, one may notice that for some parameters $(\mathsf{n}, \mathsf{t}, \mathsf{f})$, the capacity (5.10) is smaller than the capacity $(1-(\mathsf{t}/\mathsf{n}))/(1-(\mathsf{t}/\mathsf{n})^{\mathsf{f}})$ [29] of classical t-private PIR without server secrecy. For instance, when $(\mathsf{n}, \mathsf{t}, \mathsf{f}) = (4, 3, 2)$, the capacity (5.10) is 0.5 and the capacity in [29] is 0.57. This follows from the fact that the capacity (5.10) is derived for finite β but the capacity in [29] is derived for the case where the β is allowed to be infinite.

5.2 Preliminaries for protocol construction

In this section, we give preliminaries for our protocol construction in Section 5.3. Section 5.2.1 introduces the stabilizer formalism and Section 5.2.2 presents a protocol for classical messages constructed defined from the stabilizer formalism. Section 5.2.3 gives a fundamental lemma for th and e construction of our QPIR protocol.

5.2.1 Stabilizer formalism over finite field

In this subsection, we introduce the stabilizer formalism for finite field. Stabilizer formalism gives an algebraic structure for the quantum information processing. We use this formalism for the construction of the QPIR protocol. Stabilizer formalism is often used for quantum error-correction. At the end of this subsection (Remark 5.6), we give a brief review of quantum stabilizer error-correcting code with the notation introduced in this subsection. More

detailed introduction of the stabilizer formalism and stabilizer codes can be found at [71–74].

Let $\mathbb{F}_q$ be a finite field whose order is a prime power $q = p^r$ and $\mathcal{H}$ be a q-dimensional Hilbert space with a basis $\{|i\rangle \mid i \in \mathbb{F}_q\}$. We define $\operatorname{tr} x \coloneqq \operatorname{Tr} T_x \in \mathbb{F}_p$ for $x \in \mathbb{F}_q$, where $T_x \in \mathbb{F}_p^{r\times r}$ denotes the matrix representation of the map $y \in \mathbb{F}_q \mapsto xy \in \mathbb{F}_q$ by identifying the finite field $\mathbb{F}_q$ with the vector space $\mathbb{F}_p^r$. For $a, b \in \mathbb{F}_q$, we define two unitary matrices on $\mathcal{H}$

$$\mathsf{X}_q(a) \coloneqq \sum_{i\in\mathbb{F}_q} |i+a\rangle\langle i|, \quad \mathsf{Z}_q(b) \coloneqq \sum_{i\in\mathbb{F}_q} \omega^{\operatorname{tr} bi}|i\rangle\langle i|,$$

where $\omega \coloneqq \exp(2\pi\sqrt{-1}/p)$. For $\mathbf{a} = (a_1, \dots, a_n), \mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$, and $\mathbf{w} = [\mathbf{a}, \mathbf{b}] \in \mathbb{F}_q^{2n}$, we define a unitary matrix on $\mathcal{H}^{\otimes n}$

$$\tilde{\mathbf{W}}(\mathbf{w}) = \tilde{\mathbf{W}}(\mathbf{a}, \mathbf{b}) \coloneqq \mathsf{X}_q(a_1)\mathsf{Z}_q(b_1) \otimes \mathsf{X}_q(a_2)\mathsf{Z}_q(b_2) \otimes \cdots \otimes \mathsf{X}_q(a_n)\mathsf{Z}_q(b_n).$$

The Heisenberg-Weyl group is defined as

$$\mathrm{HW}_q^n \coloneqq \left\{c\tilde{\mathbf{W}}(\mathbf{w}) \mid \mathbf{w} \in \mathbb{F}_q^n,\ c \in \mathbb{C}\right\}. \tag{5.11}$$

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, we denote $\langle \mathbf{x}, \mathbf{y}\rangle \coloneqq \operatorname{tr}\sum_{i=1}^n x_i y_i \in \mathbb{F}_p$ and define a skew-symmetric matrix J on $\mathbb{F}_q^{2n}$ by

$$J = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

Since $\mathsf{X}_q(a)\mathsf{Z}_q(b) = \omega^{-\operatorname{tr} ab}\mathsf{Z}_q(b)\mathsf{X}_q(a)$, for any $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in \mathbb{F}_q^{2n}$, we have

$$\tilde{\mathbf{W}}(\mathbf{a}, \mathbf{b})\tilde{\mathbf{W}}(\mathbf{c}, \mathbf{d}) = \omega^{\langle(\mathbf{a},\mathbf{b}),J(\mathbf{c},\mathbf{d})\rangle}\tilde{\mathbf{W}}(\mathbf{c}, \mathbf{d})\tilde{\mathbf{W}}(\mathbf{a}, \mathbf{b}), \tag{5.12}$$

$$\tilde{\mathbf{W}}(\mathbf{a}, \mathbf{b})\tilde{\mathbf{W}}(\mathbf{c}, \mathbf{d}) = \omega^{\langle\mathbf{b},\mathbf{c}\rangle}\tilde{\mathbf{W}}(\mathbf{a}+\mathbf{c}, \mathbf{b}+\mathbf{d}). \tag{5.13}$$

A commutative subgroup of HW_q^n not containing cI for any $c \neq 0$ is called a *stabilizer*. A subspace V of $\mathbb{F}_q^{2n}$ is called *self-orthogonal* with respect to the bilinear form $\langle\cdot, J\cdot\rangle$ if

$$\mathrm{V} \subset \mathrm{V}^{\perp_J} \coloneqq \{\mathbf{w} \in \mathbb{F}_q^{2n} \mid \langle\mathbf{v}, J\mathbf{w}\rangle = 0 \text{ for any } \mathbf{v} \in \mathrm{V}\}.$$

We can define a stabilizer from any self-orthogonal subspace of $\mathbb{F}_q^{2n}$ by the following proposition.

Proposition 5.1. *Let* V *be a self-orthogonal subspace of* $\mathbb{F}_q^{2n}$*. There exists* $\{c_{\mathbf{v}} \in \mathbb{C} \mid \mathbf{v} \in \mathrm{V}\}$ *such that*

$$S(\mathrm{V}) \coloneqq \{\mathbf{W}(\mathbf{v}) \coloneqq c_{\mathbf{v}} \tilde{\mathbf{W}}(\mathbf{v}) \mid \mathbf{v} \in \mathrm{V}\} \subset \mathrm{HW}_q^n \tag{5.14}$$

is a stabilizer.

For completeness, we give the proof of Proposition 5.1 in Appendix D.

Proposition 5.2. *Let* V *be a self-orthogonal* d*-dimensional subspace of* $\mathbb{F}_q^{2n}$ *and* $S(\mathrm{V})$ *be a stabilizer defined from* V*. For the quotient space* $\mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}$*, we denote the elements by* $[\mathbf{w}] = \mathbf{w} + \mathrm{V}^{\perp_J} \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}$*.*

1. *All elements* $\mathbf{W}(\mathbf{v}) \in S(\mathrm{V})$ *are simultaneously and uniquely decomposed as*

$$\mathbf{W}(\mathbf{v}) = \sum_{[\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}} \omega^{\langle \mathbf{v}, J\mathbf{w} \rangle} P_{[\mathbf{w}]}^{\mathrm{V}} \qquad (\forall \mathbf{v} \in \mathrm{V}), \tag{5.15}$$

   where $\{P_{[\mathbf{w}]}^{\mathrm{V}}\}$ *are orthogonal projections such that*

$$P_{[\mathbf{w}]}^{\mathrm{V}} P_{[\mathbf{w}']}^{\mathrm{V}} = 0 \text{ for any } [\mathbf{w}] \neq [\mathbf{w}'], \tag{5.16}$$

$$\sum_{[\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}} P_{[\mathbf{w}]}^{\mathrm{V}} = I_{\mathcal{H}^{\otimes n}}. \tag{5.17}$$

2. *Let* $\mathcal{H}_{[\mathbf{w}]}^{\mathrm{V}} \coloneqq \operatorname{Im} P_{[\mathbf{w}]}^{\mathrm{V}}$*. For any* $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_q^{2n}$*, we have the relation*

$$\mathbf{W}(\mathbf{w}) \mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} = \mathcal{H}_{[\mathbf{w}+\mathbf{w}']}^{\mathrm{V}}. \tag{5.18}$$

3. *For any* $[\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}$*,*

$$\dim \mathcal{H}_{[\mathbf{w}]}^{\mathrm{V}} = q^{n-d}. \tag{5.19}$$

For completeness, we give the proof of Proposition 5.2 in Appendix E.

We use the decomposition in the following corollary in our protocol construction.

Corollary 5.1. *By* (5.17) *and* (5.19)*, the quantum system* $\mathcal{H}^{\otimes n}$ *is decomposed as*

$$\mathcal{H}^{\otimes n} = \bigotimes_{[\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}} \mathcal{H}_{[\mathbf{w}]}^{\mathrm{V}} = \mathcal{W} \otimes \mathbb{C}^{q^{n-d}}, \tag{5.20}$$

where $\mathcal{W}$ *is the* q^d*-dimensional subspace with the basis* $\{|[\mathbf{w}]\rangle \mid [\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}\}$ *such that* $\mathcal{H}^{\mathrm{V}}_{[\mathbf{w}]} = |[\mathbf{w}]\rangle \otimes \mathbb{C}^{q^{n-d}} := \{|[\mathbf{w}]\rangle \otimes |v\rangle \mid |v\rangle \in \mathbb{C}^{q^{n-d}}\}$*. With this decomposition, the relation* (5.18) *is written as*

$$\mathbf{W}(\mathbf{w})|[\mathbf{w}']\rangle \otimes \mathbb{C}^{q^{n-d}} = |[\mathbf{w}+\mathbf{w}']\rangle \otimes \mathbb{C}^{q^{n-d}}. \tag{5.21}$$

Proof. Eq. (5.20) follows from (5.17) and (5.19) and Eq. (5.21) follows directly from the relation (5.18). □

We also have the following lemma.

Lemma 5.1. *For any* $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_q^{2n}$*, we have*

$$\mathbf{W}(\mathbf{w}')\big(|[\mathbf{w}]\rangle\langle[\mathbf{w}]| \otimes I_{q^{n-d}}\big)\mathbf{W}(\mathbf{w}')^* = |[\mathbf{w}+\mathbf{w}']\rangle\langle[\mathbf{w}+\mathbf{w}']| \otimes I_{q^{n-d}}.$$

Proof. Let $X := \mathbf{W}(\mathbf{w}')\big(|[\mathbf{w}]\rangle\langle[\mathbf{w}]| \otimes I_{q^{n-d}}\big)\mathbf{W}(\mathbf{w}')^*$. Since $X^2 = X$ and $X^* = X$, the matrix X is an orthogonal projection. Since $|[\mathbf{w}+\mathbf{w}']\rangle \otimes \mathbb{C}^{q^{n-d}}$ is an invariant subspace of X and $\operatorname{rank} X = \dim |[\mathbf{w}+\mathbf{w}']\rangle \otimes \mathbb{C}^{q^{n-d}} = q^{n-d}$, the matrix X is the orthogonal projection onto $|[\mathbf{w}+\mathbf{w}']\rangle \otimes \mathbb{C}^{q^{n-d}}$, which implies the lemma. □

Remark 5.6. In terms of quantum stabilizer code, the space $\mathcal{H}^{\mathrm{V}}_{[\mathbf{0}]} = |[\mathbf{0}]\rangle \otimes \mathbb{C}^{q^{n-d}}$ is called the *code space*, which is the stabilized space by the action of the group $S(\mathrm{V})$. In other words, from (5.15), the code space $\mathcal{H}^{\mathrm{V}}_{[\mathbf{0}]}$ is the intersection of eigenspaces of $S(\mathrm{V})$ with eigenvalue 1. In quantum stabilizer code, a message state is prepared in the code space $\mathcal{H}^{\mathrm{V}}_{[\mathbf{0}]}$. If an error $\mathbf{W}(\mathbf{e})$ is applied, the encoded state on $\mathcal{H}^{\mathrm{V}}_{[\mathbf{0}]}$ is changed to a state on $\mathcal{H}^{\mathrm{V}}_{[\mathbf{e}]}$ by (5.18). Then, the error correction is preformed by obtaining the identity of the subspace $\mathcal{H}^{\mathrm{V}}_{[\mathbf{e}]}$ by the measurement $\{P^{\mathrm{V}}_{[\mathbf{e}]} \mid [\mathbf{e}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}\}$ on $\mathcal{H}^{\otimes n}$ and performing the recovery operation $\mathbf{W}(-\mathbf{r})$ for some $\mathbf{r} \in [\mathbf{e}]$, which maps from $\mathcal{H}^{\mathrm{V}}_{[\mathbf{e}]}$ to $\mathcal{H}^{\mathrm{V}}_{[\mathbf{0}]}$. This error correction is performed correctly if $\mathbf{e}-\mathbf{r} \in \mathrm{V}$ since the combined operation of the error and the correction is $\mathbf{W}(-\mathbf{r})\mathbf{W}(\mathbf{e}) = \mathbf{W}(\mathbf{e}-\mathbf{r})$ and the code space $\mathcal{H}^{\mathrm{V}}_{[\mathbf{0}]}$ is invariant with respect to the operation $\mathbf{W}(\mathbf{e}-\mathbf{r})$ if $\mathbf{e}-\mathbf{r} \in \mathrm{V}$. However, if $\mathbf{e}-\mathbf{r} \in \mathrm{V}^{\perp_J} \setminus \mathrm{V}$, the error correction is not correct.

Remark 5.7. Lemma 5.1 is equivalent to considering the state on $\mathbb{C}^{q^{n-d}}$ as completely mixed state $\rho_{\mathrm{mix}} = I_{q^{n-d}}/q^{n-d}$. If the state ρ on $\mathbb{C}^{q^{n-d}}$ is not the completely mixed state, there always exists an operation $\mathbf{W}(\mathbf{w}')$ such that ρ is changed to another state $\rho'_{\mathbf{w}'}$ as

$$\mathbf{W}(\mathbf{w}')(|[\mathbf{w}]\rangle\langle[\mathbf{w}]| \otimes \rho)\mathbf{W}(\mathbf{w}')^* = |[\mathbf{w}+\mathbf{w}']\rangle\langle[\mathbf{w}+\mathbf{w}']| \otimes \rho'_{\mathbf{w}'}.$$

For example, we have $\rho \neq \rho'_{\mathbf{w}'}$ for $[\mathbf{w}] = [\mathbf{0}]$ and some $\mathbf{w}' \in \mathrm{V}^{\perp_J} \setminus \mathrm{V}$.

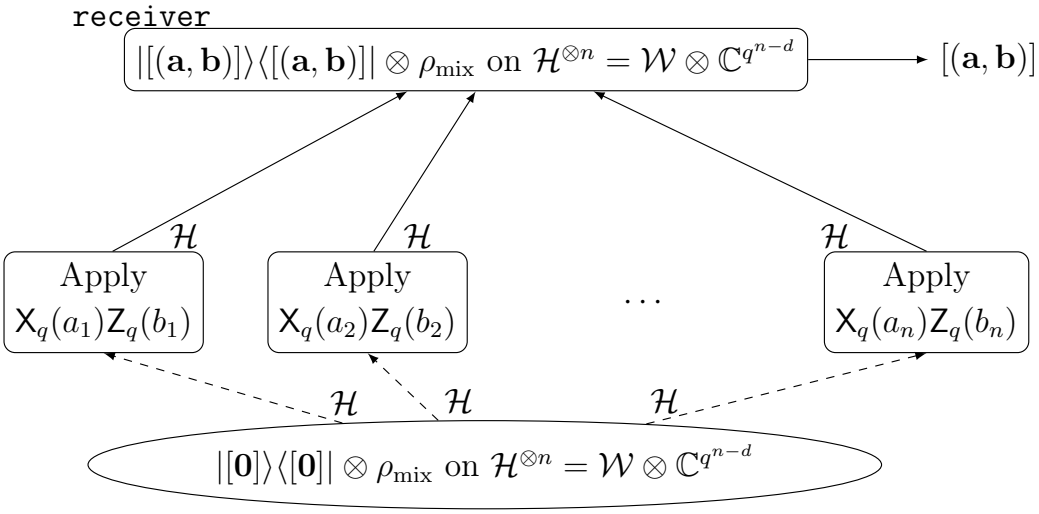


Figure 5.2: Protocol 5.1.

5.2.2 Communication protocol for classical messages by stabilizer formalism

In this section, we propose a communication protocol for classical messages from n players to a receiver. The protocol is constructed by the stabilizer formalism. We will construct our t-private QPIR protocol in Section 5.3 by modifying the protocol in this subsection.

In the following protocol, n players encode $(a_1, b_1), \ldots, (a_n, b_n) \in \mathbb{F}_q^2$ and the receiver decodes

$$[(\mathbf{a},\mathbf{b})] = [(a_1, \ldots, a_n, b_1, \ldots, b_n)] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J},$$

where V is a self-orthogonal subspace of $\mathbb{F}_q^{2n}$. The protocol is depicted in Figure 5.2.

Protocol 5.1. *Let* V *be a self-orthogonal* d*-dimensional subspace of* $\mathbb{F}_q^{2n}$ *and* $S(\mathrm{V})$ *be a stabilizer associated with* V*. By Corollary 5.1, we decompose*

$$\mathcal{H}^{\otimes n} = \bigotimes_{[\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}} \mathcal{H}^{\mathrm{V}}_{[\mathbf{w}]} = \mathcal{W} \otimes \mathbb{C}^{q^{n-d}}. \tag{5.22}$$

The following protocol consists of a receiver and n *players, namely, player 1,* $\ldots$*, player* n*.*

1. ***[Distribution of entangled state]*** *The state of* $\mathcal{H}^{\otimes n} = \mathcal{W} \otimes \mathbb{C}^{q^{n-d}}$ *is initialized as* $|[\mathbf{0}]\rangle\langle[\mathbf{0}]| \otimes \rho_{\mathrm{mix}}$*, where* ρ_{mix} *is the completely mixed state on* $\mathbb{C}^{q^{n-d}}$*, i.e.,* $\rho_{\mathrm{mix}} = (1/q^{n-d}) \cdot I_{q^{n-d}}$*. The* n *subsystems of* $\mathcal{H}^{\otimes n}$ *are distributed to the* n *players, respectively.*

2. ***[Message encoding]*** *For each* $s \in \{1, \dots, \mathsf{n}\}$*, the player* s *applies* $\mathsf{X}_q(a_s)\mathsf{Z}_q(b_s)$ *to the distributed system* $\mathcal{H}$ *and sends the system* $\mathcal{H}$ *to the receiver.*

3. ***[Message decoding]*** *The receiver applies the PVM* $\mathbf{M}^{\mathrm{V}} = \{P^{\mathrm{V}}_{[\mathbf{w}]} \mid [\mathbf{w}] \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_J}\}$ *on* $\mathcal{H}^{\otimes n}$*, where* $[\mathbf{w}]$ *is the measurement outcome associated with* $P^{\mathrm{V}}_{[\mathbf{w}]}$*.* □

In the above protocol, Lemma 5.1 implies that the receiver receives the state $|[(\mathbf{a}, \mathbf{b})]\rangle\langle[(\mathbf{a}, \mathbf{b})]| \otimes \rho_{\mathrm{mix}}$. Thus, the receiver obtains

$$[(\mathbf{a}, \mathbf{b})] = [(a_1, \dots, a_n, b_1, \dots, b_n)] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}$$

as the measurement outcome but no more information than $[(\mathbf{a}, \mathbf{b})]$. Note that if the initial state of $\mathbb{C}^{q^{n-d}}$ is not ρ_{mix}, some more information of $(\mathbf{a}, \mathbf{b})$ can be leaked to the receiver since the final state on $\mathbb{C}^{q^{n-d}}$ may depend on $(\mathbf{a}, \mathbf{b})$. See Remark 5.7 for more detail.

In Section 5.3, we will construct our QPIR protocol by modifying Protocol 5.1. For fulfilling the QPIR task, we will choose a suitable self-orthogonal subspace V and design query structures and server encoders in Section 5.3.

5.2.3 Fundamental lemma for protocol construction

In this subsection, we prepare a lemma for the QPIR protocol construction, which is necessary for guaranteeing the secrecy.

In the statement of the following proposition, we use an algebraic extension of a finite field. When α is a root of some polynomial over a field $\mathbb{F}$, an *algebraic extension* $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α. Any algebraic extension of a finite field $\mathbb{F}_q$ is another finite field. See [75] and [76] for details. We denote $\mathbb{F}(\alpha_1, \dots, \alpha_n) \coloneqq [\mathbb{F}(\alpha_1, \dots, \alpha_{n-1})](\alpha_n)$.

Proposition 5.3. *Let* $\mathbb{F}_{q'}$ *be the finite field of order* q' *and* $\mathbb{F}_q$ *be the algebraic extension* $\mathbb{F}_{q'}(\alpha_1, \dots, \alpha_{k-2})$*, where* $\alpha_i \notin \mathbb{F}_{q'}(\alpha_1, \dots, \alpha_{i-1})$ *for any* i*. Given*

two positive integers $r < k$, define a matrix $A = (a_{ij}) \in \mathbb{F}_q^{(k-r)\times r}$ such that

$$a_{11} = 1, \tag{5.23}$$
$$a_{ij} \in \mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{i+j-2}) \setminus \mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{i+j-3}) \qquad \text{if } (i,j) \neq (1,1). \tag{5.24}$$

Then, any r row vectors of

$$\bar{A} \coloneqq \begin{pmatrix} A \\ I_r \end{pmatrix} \in \mathbb{F}_q^{k\times r} \tag{5.25}$$

are linearly independent. In particular, when $k = 2r$, the square matrix $A \in \mathbb{F}_q^{r\times r}$ is invertible.

Proof. Before we give the proof, we introduce the following notation: For an $n \times m$ matrix $M = (m_{ij})$, $S \subset \{1, \ldots, n\}$ and $T \subset \{1, \ldots, m\}$, define a submatrix $M(S,T) \coloneqq (m_{ij})_{i\in S, j\in T}$.

Let $S \subset \{1, \ldots, k-r\}$ and $T \subset \{1, \ldots, r\}$ be subsets such that $|S|+|T| = r$. Choose r row vectors of $\bar{A}$ as

$$\bar{A}(S \cup (k-r+T), \{1, \ldots, r\}) = \begin{pmatrix} A(S, \{1, \ldots, r\}) \\ I_r(T, \{1, \ldots, r\}) \end{pmatrix}. \tag{5.26}$$

The row vectors of $\bar{A}(S \cup (k-r+T), \{1, \ldots, r\})$ are linearly independent if and only if $A(S, T^c) \in \mathbb{F}_q^{|S|\times|S|}$ is invertible, where $T^c \coloneqq \{1, \ldots, r\} \setminus T$. Therefore, we show in the following that the determinant of $A(S, T^c)$ is nonzero.

From the definition of A in (5.24), the $(|S|, |S|)$ element $a_{\max S, \max T^c}$ of $A(S, T^c)$ is in $\mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{\max S + \max T^c - 2}) \setminus \mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{\max S + \max T^c - 3})$ but the other $|S|^2 - 1$ elements are in $\mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{\max S + \max T^c - 3})$. Thus, by the cofactor expansion of the determinant, i.e., $\det M = \sum_j (-1)^{i+j} m_{i,j} M_{i,j}$ for a matrix $M = (m_{ij})$ and its i, j minor $M_{i,j}$, we have

$$\det A(S, T^c) = a_{\max S, \max T^c} \cdot \det A(S \setminus \{\max S\}, T^c \setminus \{\max T^c\}) + x \tag{5.27}$$

with some $x \in \mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{\max S + \max T^c - 3})$. If

$$\det A(S \setminus \{\max S\}, T^c \setminus \{\max T^c\}) \neq 0,$$

then $\det A(S, T^c) \neq 0$. Thus, by induction, we have $\det A(S, T^c) \neq 0$ since $\det A(\{\min S\}, \{\min T^c\}) = a_{\min S, \min T^c} \neq 0$. □

Remark 5.8. Proposition 5.3 is a slight generalization of the construction [64, Appendix A], which proposed the same construction only for $a_{ij} = \alpha_{i+j-2}$ in (5.24).

The following lemma is fundamental to guarantee the secrecy in our QPIR protocol.

Lemma 5.2. *Let n, t be positive integers such that $n/2 \leq t < n$. Let $\mathbb{F}_{q'}$ be the finite field of order q' and $\mathbb{F}_q$ be the algebraic extension $\mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{n+2t-2})$, where $\alpha_i \notin \mathbb{F}_{q'}(\alpha_1, \ldots, \alpha_{i-1})$ for any i. There exist $2t$ linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{2t} \in \mathbb{F}_q^{2n}$ satisfying the following conditions.*

(a) *Let $\mathbf{w}_1, \ldots, \mathbf{w}_{2n}$ be the row vectors of the matrix $D = (\mathbf{v}_1, \ldots, \mathbf{v}_{2t}) \in \mathbb{F}_q^{2n \times 2t}$. Then, $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(t)}, \mathbf{w}_{\pi(1)+n}, \ldots, \mathbf{w}_{\pi(t)+n}$ are linearly independent for any permutation π in S_n.*

(b) *$\langle \mathbf{v}_i, J\mathbf{v}_j \rangle = 0$ for any $i \in \{1, \ldots, 2n-2t\}$ and any $j \in \{1, \ldots, 2t\}$.*

Proof. Let $S \in \mathbb{F}_q^{2n \times 2n}$ be a symplectic matrix, i.e., $S^\top J S = J$, and $\mathbf{s}_i \in \mathbb{F}_q^{2n}$ be the i-th column vector of S. Then, the following $\mathbf{v}_1, \ldots, \mathbf{v}_{2t} \in \mathbb{F}_q^{2n}$ satisfy condition (b):

$$(\mathbf{v}_1, \ldots, \mathbf{v}_{2n-2t}) \coloneqq (\mathbf{s}_{2t-n+1}, \ldots, \mathbf{s}_n) \tag{5.28}$$

$$(\mathbf{v}_{2n-2t+1}, \ldots, \mathbf{v}_{2t}) \coloneqq (\mathbf{s}_1, \ldots, \mathbf{s}_{2t-n}, \mathbf{s}_{n+1}, \ldots, \mathbf{s}_{2t}). \tag{5.29}$$

Therefore, in the following, we prove that there exists a symplectic matrix $S = (\mathbf{s}_1, \ldots, \mathbf{s}_{2n})$ such that the row vectors of $S' \coloneqq (\mathbf{s}_1, \ldots, \mathbf{s}_{2t})$ satisfy condition (a).

First, we construct a symplectic matrix as follows. For convenience, let $\alpha_0 \coloneqq 1$. Define two square symmetric matrices $A = (a_{ij}), B = (b_{ij}) \in \mathbb{F}_q^{n \times n}$ as

$$a_{ij} = \alpha_{i+j-2}, \quad b_{ij} = \alpha_{i+j-2+(2t-n)}, \tag{5.30}$$

i.e.,

$$A = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_n & \cdots & \alpha_{2n-2} \end{pmatrix}, \quad B = \begin{pmatrix} \alpha_{2t-n} & \alpha_{2t-n+1} & \cdots & \alpha_{2t-1} \\ \alpha_{2t-n+1} & \alpha_{2t-n+2} & \cdots & \alpha_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{2t-1} & \alpha_{2t} & \cdots & \alpha_{n+2t-2} \end{pmatrix}.$$

Since the matrices

$$\begin{pmatrix} I_n & X \\ 0 & I_n \end{pmatrix}, \begin{pmatrix} I_n & 0 \\ X & I_n \end{pmatrix} \tag{5.31}$$

are symplectic matrices for any symmetric matrix X, and the multiple of two symplectic matrices is a symplectic matrix [74, Section 8.2.2], the matrix

$$S = \begin{pmatrix} I_n + BA^{-1} & B \\ A^{-1} & I_n \end{pmatrix} = \begin{pmatrix} I_n & B \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ A^{-1} & I_n \end{pmatrix} \tag{5.32}$$

is a symplectic matrix, where the inverse A^{-1} exists from Proposition 5.3. With the notation $B = (B_1, B_2) \in \mathbb{F}_q^{n\times(2t-n)} \times \mathbb{F}_q^{n\times(2n-2t)}$, we have

$$S' \coloneqq (\mathbf{s}_1, \ldots, \mathbf{s}_{2t}) = \left(\begin{array}{c|c} I_n + BA^{-1} & B_1 \\ \hline A^{-1} & \begin{matrix} I_{2t-n} \\ 0 \end{matrix} \end{array}\right). \tag{5.33}$$

Now, we prove that the row vectors of S' satisfy condition (a). Since (i) the right multiplication of invertible matrices and (ii) elementary column operations do not change the linear independence of the row vectors, we manipulate the matrix S' in the following way:

$$S' = \left(\begin{array}{c|c} I_n + BA^{-1} & B_1 \\ \hline A^{-1} & \begin{matrix} I_{2t-n} \\ 0 \end{matrix} \end{array}\right) \xrightarrow{\text{(i)}} \left(\begin{array}{c|c} I_n + BA^{-1} & B_1 \\ \hline A^{-1} & \begin{matrix} I_{2t-n} \\ 0 \end{matrix} \end{array}\right) \begin{pmatrix} A & 0 \\ 0 & I_{2t-n} \end{pmatrix}$$

$$= \left(\begin{array}{c|c} A + B & B_1 \\ \hline I_n & \begin{matrix} I_{2t-n} \\ 0 \end{matrix} \end{array}\right) = \left(\begin{array}{cc|c} A_1 + B_1 & A_2 + B_2 & B_1 \\ \hline I_{2t-n} & 0 & I_{2t-n} \\ 0 & I_{2n-2t} & 0 \end{array}\right)$$

$$\xrightarrow{\text{(ii)}} \left(\begin{array}{cc|c} A_1 & A_2 + B_2 & B_1 \\ \hline 0 & 0 & I_{2t-n} \\ 0 & I_{2n-2t} & 0 \end{array}\right) \xrightarrow{\text{(ii)}} \left(\begin{array}{ccc} A_1 & B_1 & A_2 + B_2 \\ \hline 0 & I_{2t-n} & 0 \\ 0 & 0 & I_{2n-2t} \end{array}\right) =: S'',$$

where $A = (A_1, A_2) \in \mathbb{F}_q^{n\times(2t-n)} \times \mathbb{F}_q^{n\times(2n-2t)}$. By the above transformation, the linear independence of the row vectors of S' is equivalent to that of S''. Let

$$S''' := \left(\begin{array}{ccc} A_1 & B_1 & A_2+B_2 \\ \hline I_{2t-n} & 0 & 0 \\ 0 & I_{2t-n} & 0 \\ 0 & 0 & I_{2n-2t} \end{array}\right) \tag{5.34}$$

by adding the row vectors $(I_{2t-n}, 0, 0)$ to S''. If any $2t$ row vectors of S''' are linearly independent, then S'' and S' also satisfy the same property. Since A_1, B_1, A_2+B_2 are written as

$$A_1 = \begin{pmatrix} \alpha_0 & \cdots & \alpha_{2t-n-1} \\ \vdots & \ddots & \vdots \\ \alpha_{n-1} & \cdots & \alpha_{2t-2} \end{pmatrix},$$

$$B_1 = \begin{pmatrix} \alpha_{2t-n} & \cdots & \alpha_{4t-2n-1} \\ \vdots & \ddots & \vdots \\ \alpha_{2t-1} & \cdots & \alpha_{4t-n-2} \end{pmatrix},$$

$$A_2+B_2 = \begin{pmatrix} \alpha_{4t-2n}+\alpha_{2t-n} & \cdots & \alpha_{2t-1}+\alpha_{n-1} \\ \vdots & \ddots & \vdots \\ \alpha_{4t-n-1}+\alpha_{2t-1} & \cdots & \alpha_{n+2t-2}+\alpha_{2n-2} \end{pmatrix},$$

the matrix $(A_1 \mid B_1 \mid A_2+B_2)$ satisfies the conditions of Proposition 5.3. The application of Proposition 5.3 to S''' shows that any $2t$ row vectors of S''' are linearly independent. Thus, the matrix S' also satisfies the same property as S''', which implies condition (a). □

Many studies in classical information theory have already studied the matrices $D \in \mathbb{F}_q^{n\times t}$ whose arbitrary t ($\leq n$) row vectors are linearly independent, which is similar to condition (a) of Lemma 5.2. For instance, matrices of this kind have been studied as a generator matrix of the maximum distance separable (MDS) codes [77] and have been widely used in the construction of secure communication protocols, e.g., classical private information retrievals [31,32,36], wiretap channel II [78], and secure network coding [64,79].

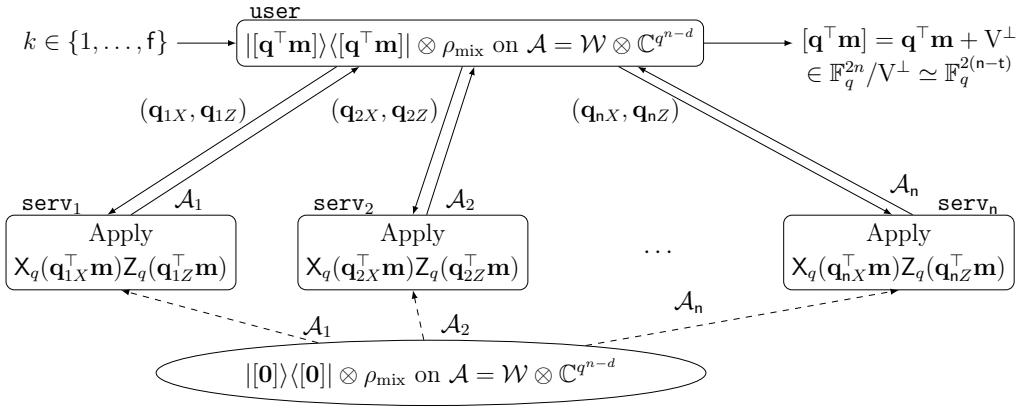


Figure 5.3: Optimal t-Private QPIR protocol. $\mathbf{m} = (\mathbf{m}_1^\top, \ldots, \mathbf{m}_k^\top)^\top$ and $\mathbf{q} = (\mathbf{q}_{1X}^\top, \ldots, \mathbf{q}_{\mathsf{n}X}^\top, \mathbf{q}_{1Z}^\top, \ldots, \mathbf{q}_{\mathsf{n}Z}^\top)^\top$ are the collections of messages and queries, respectively.

5.3 Construction of QPIR protocol with colluding servers

In this section, by combining Protocol 5.1 and Lemma 5.2, we construct the capacity-achieving QPIR protocol for $\mathsf{n} \geq 2$ servers, $\mathsf{f} \geq 2$ messages, and $\mathsf{n}/2 \leq \mathsf{t} < \mathsf{n}$ colluding servers. The protocol is depicted in Figure 5.3. For collusion of $1 \leq \mathsf{t} < \mathsf{n}/2$ servers, the protocol for $\mathsf{t} = \mathsf{n}/2$ is the capacity-achieving protocol.

Let $\mathsf{n} \geq 2$, $\mathsf{f} \geq 2$, and $\mathsf{n}/2 \leq \mathsf{t} < \mathsf{n}$. For the construction of the protocol, we choose a prime power q and a basis $\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}}$ of $\mathbb{F}_q^{2\mathsf{n}}$ such that the first $2\mathsf{t}$ vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}$ satisfy the conditions of Lemma 5.2. Let

$$\mathrm{V} \coloneqq \mathrm{span}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\} \subset \mathbb{F}_q^{2\mathsf{n}}.$$

Then, from condition (b) of Lemma 5.2, the subspace V is self-orthogonal with respect to $\langle \cdot, J \cdot \rangle$, $\mathrm{V}^{\perp_J} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and

$$\mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J} = \{[\mathbf{w}] \coloneqq \mathbf{w} + \mathrm{V}^{\perp_J} \mid \mathbf{w} \in \mathrm{span}\{\mathbf{v}_{2\mathsf{t}+1}, \ldots, \mathbf{v}_{2\mathsf{n}}\}\}.$$

Let

$$D_1 \coloneqq \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_{2\mathsf{t}} \end{pmatrix} \in \mathbb{F}_q^{2\mathsf{n} \times 2\mathsf{t}}, \tag{5.35}$$

$$D_2 \coloneqq \begin{pmatrix} \mathbf{v}_{2\mathsf{t}+1} & \mathbf{v}_{2\mathsf{t}+2} & \cdots & \mathbf{v}_{2\mathsf{n}} \end{pmatrix} \in \mathbb{F}_q^{2\mathsf{n} \times 2(\mathsf{n}-\mathsf{t})}. \tag{5.36}$$

We assume that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_{2\mathsf{n}}$ are publicly known to the user and all servers. Each server contains all messages $\mathbf{m}_1, \dots, \mathbf{m}_{\mathsf{f}} \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})}$. We denote $\mathbf{m} \coloneqq (\mathbf{m}_1^\top, \dots, \mathbf{m}_k^\top)^\top \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\mathsf{f}}$.

Protocol 5.2. *The* t*-private QPIR protocol for retrieving* $\mathbf{m}_k$ *is constructed as follows.*

Step 1. ***[Preparation]*** *Let* $\mathcal{A}_1, \dots, \mathcal{A}_{\mathsf{n}}$ *be* q*-dimensional Hilbert spaces. From Corollary 5.1, the quantum system* $\mathcal{A} \coloneqq \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_{\mathsf{n}}$ *is decomposed as* $\mathcal{A} = \mathcal{W} \otimes \mathbb{C}^{q^{2\mathsf{t}-\mathsf{n}}}$*, where* $\mathcal{W} = \operatorname{span}\{|[\mathbf{w}]\rangle \mid [\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}\}$*. The state of* $\mathcal{A}$ *is initialized as*

$$|[\mathbf{0}]\rangle\langle[\mathbf{0}]| \otimes \rho_{\mathrm{mix}},$$

where $\rho_{\mathrm{mix}} \coloneqq (1/q^{2\mathsf{t}-\mathsf{n}}) \cdot I_{q^{2\mathsf{t}-\mathsf{n}}}$*, and is distributed so that the* j*-th server has* $\mathcal{A}_j$ *for* $j = 1, 2, \dots, \mathsf{n}$*.*

Step 2. ***[Query]*** *The user randomly chooses a matrix* $R \in \mathbb{F}_q^{2\mathsf{t}\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}$ *with the uniform distribution. Let* $E_k \coloneqq (\delta_{i,j-2(\mathsf{n}-\mathsf{t})(k-1)})_{i,j} \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}$*, where* $\delta_{x,y} = 1$ *if* $x = y$ *and* $\delta_{x,y} = 0$ *if* $x \neq y$*. That is,* E_k *is the block matrix whose* k*-th block is* $I \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\times 2(\mathsf{n}-\mathsf{t})}$ *and all other blocks are zero. Let*

$$\begin{aligned}\mathbf{q} &= (\mathbf{q}_{1X}^\top, \dots, \mathbf{q}_{\mathsf{n}X}^\top, \mathbf{q}_{1Z}^\top, \dots, \mathbf{q}_{\mathsf{n}Z}^\top)^\top \\ &\coloneqq (D_1, D_2)\begin{pmatrix} R \\ E_k \end{pmatrix} \\ &= D_1 R + D_2 E_k \in \mathbb{F}_q^{2\mathsf{n}\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}.\end{aligned}$$

The user sends the query $(\mathbf{q}_{jX}, \mathbf{q}_{jZ}) \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\mathsf{f}} \times \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\mathsf{f}}$ *to the* j*-th server for* $j = 1, 2, \dots, \mathsf{n}$*.*

Step 3. ***[Download]*** *For each* $j = 1, 2, \dots, \mathsf{n}$*, the* j*-th server applies*

$$\mathsf{X}_q(\mathbf{q}_{jX}^\top \mathbf{m})\mathsf{Z}_q(\mathbf{q}_{jZ}^\top \mathbf{m})$$

to $\mathcal{A}_j$ *and sends* $\mathcal{A}_j$ *to the user.*

Step 4. ***[Retrieval]*** *The user applies the PVM* $\mathbf{M}^{\mathrm{V}} = \{P_{[\mathbf{w}]}^{\mathrm{V}} \mid [\mathbf{w}] \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_J}\}$ *on* $\mathcal{A}$*, where* $[\mathbf{w}]$ *is the measurement outcome associated with* $P_{[\mathbf{w}]}^{\mathrm{V}}$*. The measurement outcome of the user is denoted by* $[\mathbf{w}_{\mathrm{out}}]$*. In the expansion* $\mathbf{w}_{\mathrm{out}} = \sum_{i=1}^{2\mathsf{n}} c_i \mathbf{v}_i$*, the user outputs* $(c_{2\mathsf{t}+1}, c_{2\mathsf{t}+2}, \dots, c_{2\mathsf{n}}) \in \mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})}$*.*

The performance of Protocol 5.2 is analyzed as follows.

Error probability

We show that the user obtains $\mathbf{m}_k$ without error. Let

$$\mathbf{w}' \coloneqq \mathbf{q}^\top \mathbf{m} \tag{5.37}$$

$$= (\mathbf{q}_{1X}^\top \mathbf{m}, \dots, \mathbf{q}_{\mathsf{n}X}^\top \mathbf{m}, \mathbf{q}_{1Z}^\top \mathbf{m}, \dots, \mathbf{q}_{\mathsf{n}Z}^\top \mathbf{m})^\top \in \mathbb{F}_q^{2\mathsf{n}}. \tag{5.38}$$

The state after the servers' encoding is

$$\mathbf{W}(\mathbf{w}')(|[\mathbf{0}]\rangle\langle[\mathbf{0}]| \otimes \rho_{\mathrm{mix}})\mathbf{W}(\mathbf{w}')^* = |[\mathbf{w}']\rangle\langle[\mathbf{w}']| \otimes \rho_{\mathrm{mix}}, \tag{5.39}$$

where the equality follows from Lemma 5.1. Thus, the measurement outcome $[\mathbf{w}_{\mathrm{out}}]$ is $[\mathbf{w}']$. Note that we have

$$\mathbb{F}_q^{2\mathsf{n}} \ni \mathbf{w}' = \mathbf{q}^\top \mathbf{m} \tag{5.40}$$

$$= D_1 R\mathbf{m} + D_2 E_k \mathbf{m} \tag{5.41}$$

$$= D_1 R\mathbf{m} + \sum_{i=1}^{2\mathsf{n}-2\mathsf{t}} m_{k,i}\mathbf{v}_{2\mathsf{t}+i} \tag{5.42}$$

and the first term $D_1 R\mathbf{m}$ of (5.42) is a vector in $\mathrm{V}^{\perp_J}$, which implies

$$[\mathbf{w}_{\mathrm{out}}] = [\mathbf{w}'] = \mathbf{w}' + \mathrm{V}^\perp = \sum_{i=1}^{2\mathsf{n}-2\mathsf{t}} m_{k,i}\mathbf{v}_{2\mathsf{t}+i} + \mathrm{V}^\perp = \left[\sum_{i=1}^{2\mathsf{n}-2\mathsf{t}} m_{k,i}\mathbf{v}_{2\mathsf{t}+i}\right].$$

Thus, the user obtains $(c_{2\mathsf{t}+1}, c_{2\mathsf{t}+2}, \dots, c_{2\mathsf{n}}) = (m_{k,1}, \dots, m_{k,2(\mathsf{n}-\mathsf{t})}) = \mathbf{m}_k$ without error.

Server secrecy

The protocol has perfect server secrecy because from (5.39), the state after the servers' encoding is $|[\mathbf{w}']\rangle\langle[\mathbf{w}']| \otimes \rho_{\mathrm{mix}}$, which is independent of the non-retrieved messages.

Remark 5.9. The server secrecy is not perfect if the prior entangled state is $|[\mathbf{0}]\rangle\langle[\mathbf{0}]| \otimes \rho$ for some non completely mixed state ρ. As remarked in Remark 5.7, if $|[\mathbf{0}]\rangle\langle[\mathbf{0}]| \otimes \rho$ is the initial entangled state, the state ρ may be changed depending on the servers' operation $\mathbf{W}(\mathbf{w}')$, i.e.,

$$\mathbf{W}(\mathbf{w}')(|[\mathbf{0}]\rangle\langle[\mathbf{0}]| \otimes \rho)\mathbf{W}(\mathbf{w}')^* = |[\mathbf{w}']\rangle\langle[\mathbf{w}']| \otimes \rho'_{\mathbf{w}'} \tag{5.43}$$

for some state $\rho'_{\mathbf{w}'}$. Thus, the user may obtain some information of $\mathbf{w}'$ from the state $\rho'_{\mathbf{w}'}$, i.e., some information of the non-targeted messages is leaked.

User secrecy

To discuss the user secrecy of Protocol 5.2, we introduce the following notations. We denote $\mathbf{v}_i = (v_{1,i}, \ldots, v_{2\mathsf{n},i})^\top \in \mathbb{F}_q^{2\mathsf{n}}$ for $i = 1, \ldots, 2\mathsf{n}$. For any permutation π in S_n, we denote

$$\mathbf{v}_{i,\pi} \coloneqq \begin{pmatrix} v_{\pi(1),i} \\ \vdots \\ v_{\pi(\mathsf{t}),i} \\ v_{\mathsf{n}+\pi(1),i} \\ \vdots \\ v_{\mathsf{n}+\pi(\mathsf{t}),i} \end{pmatrix} \in \mathbb{F}_q^{2\mathsf{t}},$$

$$D_{1,\pi} \coloneqq (\mathbf{v}_{1,\pi}, \ldots, \mathbf{v}_{2\mathsf{t},\pi}) \in \mathbb{F}_q^{2\mathsf{t}\times 2\mathsf{t}},$$
$$D_{2,\pi} \coloneqq (\mathbf{v}_{2\mathsf{t}+1,\pi}, \ldots, \mathbf{v}_{2\mathsf{n},\pi}) \in \mathbb{F}_q^{2\mathsf{t}\times 2(\mathsf{n}-\mathsf{t})}.$$

The user t-secrecy is proved as follows. Let π be an arbitrary permutation in S_n. The queries to the $\pi(1)$-th server, $\ldots$, $\pi(\mathsf{t})$-th server are written as

$$(\mathbf{q}_{\pi(1)X}, \ldots, \mathbf{q}_{\pi(\mathsf{t})X}, \mathbf{q}_{\pi(1)Z}, \ldots, \mathbf{q}_{\pi(\mathsf{t})Z})^\top = D_{1,\pi}R + D_{2,\pi}E_k \in \mathbb{F}_q^{2\mathsf{t}\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}.$$

Since condition (a) of Lemma 5.2 implies $\operatorname{rank} D_{1,\pi} = 2\mathsf{t}$, i.e., $D_{1,\pi}$ is invertible, when R is uniformly at random in $\mathbb{F}_q^{2\mathsf{t}\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}$, the distribution of

$$(\mathbf{q}_{\pi(1)X}, \ldots, \mathbf{q}_{\pi(\mathsf{t})X}, \mathbf{q}_{\pi(1)Z}, \ldots, \mathbf{q}_{\pi(\mathsf{t})Z})^\top$$

is the uniform distribution on $\mathbb{F}_q^{2\mathsf{t}\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}$. Therefore, the colluding servers obtain no information of the index of the targeted message k since the matrix R is unknown to the colluding servers and is uniformly at random in $\mathbb{F}_q^{2\mathsf{t}\times 2(\mathsf{n}-\mathsf{t})\mathsf{f}}$.

Costs and QPIR rate

The message size is $\mathsf{m} = |\mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})}| = q^{2(\mathsf{n}-\mathsf{t})}$. The download cost and upload cost are

$$D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = \log \dim \bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j = \mathsf{n} \log q,$$
$$U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = \log |\mathbb{F}_q^{2(\mathsf{n}-\mathsf{t})\mathsf{f}\times 2\mathsf{n}}| = 4\mathsf{n}\mathsf{f}(\mathsf{n}-\mathsf{t}) \log q.$$

The QPIR rate is

$$R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = \frac{\log \mathsf{m}}{D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})} = \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}},$$

which achieves the QPIR capacity in Theorem 5.1.

5.4 Converse bounds

The converse bounds of Theorem 5.1 are written for any $\alpha \in [0,1)$ and any $\beta, \gamma, \theta \in [0, \infty)$ as

$$C_{\mathrm{asymp},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} \leq 1 \qquad \text{if } 1 \leq \mathsf{t} \leq \frac{\mathsf{n}}{2}, \tag{5.44}$$

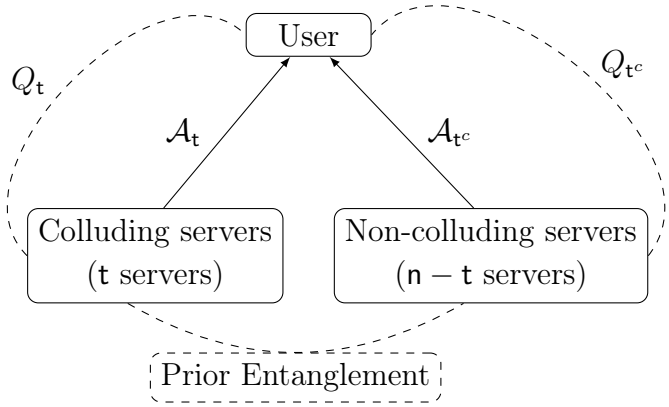
$$C_{\mathrm{exact},\mathsf{t}}^{\alpha,0,0,\theta} \leq \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \qquad \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} < \mathsf{n}, \tag{5.45}$$

$$C_{\mathrm{asymp},\mathsf{t}}^{0,\beta,0,\theta} \leq \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \qquad \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} < \mathsf{n}. \tag{5.46}$$

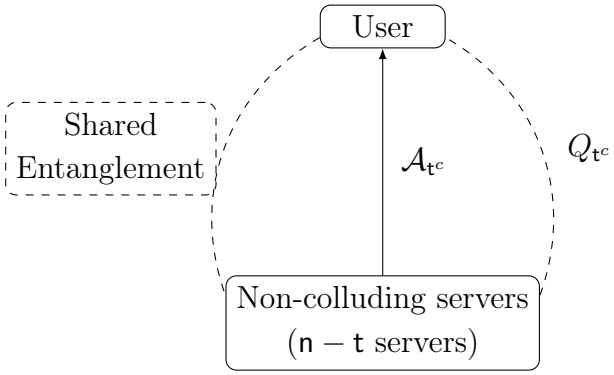
The proof idea of the converse bounds (5.45), (5.46) is explained intuitively with Figure 5.4 as follows. By the secrecy conditions, the state on $\bigotimes_{j=1}^{\mathsf{t}} \mathcal{A}_{\pi(j)}$ from the colluding servers is independent of the message information, which will be precisely stated in Lemma 5.4. With this fact, the state on $\bigotimes_{j=1}^{\mathsf{t}} \mathcal{A}_{\pi(j)}$ can be considered as a shared entanglement between the user and the non-colluding servers. That is, the downloading step of the protocol (Figure 5.4-(a)) can be considered as the entanglement-assisted communication of a classical message (Figure 5.4-(b)). Since the capacity of the entanglement-assisted classical communication for the identity channel is two times the dimension of the transmitted quantum systems, the PIR capacity is upper bounded by $2(\mathsf{n}-\mathsf{t})/\mathsf{n}$ and the tightness of this bound is guaranteed by the QPIR protocol in Section 5.3. The bound (5.44) is proved by noting that the retrieved message size cannot exceed the dimension of downloaded quantum systems.

The remainder of this section is organized as follows. In Section 5.4.1, we prepare lemmas necessary for the converse proofs. In Sections 5.4.2, 5.4.3, and 5.4.4, we present the proofs of (5.46), (5.45), (5.44), respectively.

Throughout this section, we fix an arbitrary $\pi \in \mathsf{S}_{\mathsf{n}}$ without losing gen-



(a) Downloading step of QPIR protocol. The user shares Q_{t} with colluding servers and Q_{t^c} with non-colluding servers.



(b) Entanglement-assisted communication of classical message with shared randomness Q_{t^c}. Note that the user know Q but not which query Q_{t^c} the non-colluding servers contain.

Figure 5.4: Proof idea of converse bounds. By the secrecy conditions, the downloading step (a) can be considered as (b). Here, we denote $\mathcal{A}_{\mathsf{t}} \coloneqq \bigotimes_{j=1}^{\mathsf{t}} \mathcal{A}_j$, $\mathcal{A}_{\mathsf{t}^c} \coloneqq \bigotimes_{j=\mathsf{t}+1}^{\mathsf{n}} \mathcal{A}_j$, $Q_{\mathsf{t}} \coloneqq (Q_1, \ldots, Q_{\mathsf{t}})$, and $Q_{\mathsf{t}^c} \coloneqq (Q_{\mathsf{t}+1}, \ldots, Q_{\mathsf{n}})$.

erality and use the notation

$$Q_{\mathsf{t}} \coloneqq (Q_{\pi(1)}, \dots, Q_{\pi(\mathsf{t})}), \tag{5.47}$$

$$Q_{\mathsf{t}^c} \coloneqq (Q_{\pi(\mathsf{t}+1)}, \dots, Q_{\pi(\mathsf{n})}), \tag{5.48}$$

$$\mathcal{A}_{\mathsf{t}} \coloneqq \bigotimes_{j=1}^{\mathsf{t}} \mathcal{A}_{\pi(j)}, \tag{5.49}$$

$$\mathcal{A}_{\mathsf{t}^c} \coloneqq \bigotimes_{j=\mathsf{t}+1}^{\mathsf{n}} \mathcal{A}_{\pi(j)}. \tag{5.50}$$

We also denote by $\rho_{MQ_{\mathsf{t}}}$ the state on $\mathcal{A}_{\mathsf{t}}$ of the t-colluding servers after the servers' encoding. For random variables X and Y, we denote by p_X the probability distribution of X, by $p_{X|Y}$ the distribution of X conditioned by Y, by $p_{X|Y=y}$ the distribution of X conditioned by $Y = y$. We sometimes denote $p_{X=x} = \Pr[X = x]$ and $p_{X=x|Y=y} = \Pr[X = x|Y = y]$ for simplicity.

5.4.1 Lemmas for converse bounds

We prepare two lemmas. The security conditions (5.1), (5.2), and (5.3) give the following bounds.

Lemma 5.3. *The server secrecy* $S_{\mathrm{serv}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) \le \beta$ *implies*

$$I(M_k^c; \mathcal{A}Q|K = k)_{\rho_{MQ}} \le \beta. \tag{5.51}$$

The user t*-secrecy* $S^{(\mathsf{t})}_{\mathrm{user}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) \le \gamma$ *implies*

$$\max_{i \neq k \in \{1,\dots,\mathsf{f}\}, \pi \in \mathsf{S}_{\mathsf{n}}} d(p_{Q_{\mathsf{t}}|K=k}, p_{Q_{\mathsf{t}}|K=i}) \le \sqrt{2\mathsf{f}\gamma}, \tag{5.52}$$

where $d(\cdot,\cdot)$ *is the variational distance* $d(p,q) \coloneqq (1/2) \cdot \sum_j |p_j - q_j|$ *for probability distributions* p, q.

Proof. The relation (5.51) is proved as follows:

$$\begin{aligned} I(M_k^c; \mathcal{A}Q|K = k)_{\rho_{MQ}} &= I(M_k^c; \mathcal{A}|Q, K = k)_{\rho_{MQ}} + I(M_k^c; Q|K = k)_{\rho_{MQ}} \\ &= I(M_k^c; \mathcal{A}|Q, K = k)_{\rho_{MQ}} \\ &= \sum_q p_{Q=q|K=k} \cdot I(M_k^c; \mathcal{A}|Q = q, K = k)_{\rho_{MQ}} \\ &\le \beta, \end{aligned} \tag{5.53}$$

where the equality (5.53) holds because Q is independent of M_k^c.

The relation (5.52) is proved as follows. For any $\pi \in \mathsf{S}_\mathsf{n}$ and any $k \in \{1, \ldots, \mathsf{f}\}$, we have

$$\gamma \geq I(K; Q_\mathsf{t}) = D(p_{KQ_\mathsf{t}} \| p_K \times p_{Q_\mathsf{t}}) = \frac{1}{\mathsf{f}} \sum_{k'} D(p_{Q_\mathsf{t}|K=k'} \| p_{Q_\mathsf{t}})$$

$$\overset{(a)}{\geq} \frac{2}{\mathsf{f}} \sum_{k'} d^2(p_{Q_\mathsf{t}|K=k'}, p_Q) \geq \frac{2}{\mathsf{f}} d^2(p_{Q_\mathsf{t}|K=k}, p_{Q_\mathsf{t}}),$$

where the inequality (a) follows from Pinsker's inequality (2.11). Thus, for any $i, k \in \{1, \ldots, \mathsf{f}\}$, we have

$$\sqrt{2\mathsf{f}\gamma} \geq d(p_{Q_\mathsf{t}|K=k}, p_{Q_\mathsf{t}}) + d(p_{Q_\mathsf{t}}, p_{Q_\mathsf{t}|K=i}) \tag{5.54}$$

$$\geq d(p_{Q_\mathsf{t}|K=k}, p_{Q_\mathsf{t}|K=i}), \tag{5.55}$$

which implies (5.52). □

In the converse proofs, we will only use the evaluation given in Lemma 5.3 instead of the conditions $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \beta$ and $S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \gamma$. We also prepare the following lemma.

Lemma 5.4. *If a QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$ satisfies $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \beta$ and $S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \leq \gamma$, then for any $k \in \{1, \ldots, \mathsf{f}\}$, we have the relation*

$$I(M_k; \mathcal{A}_\mathsf{t} | Q_\mathsf{t}, K = k)_{\rho_{MQ_\mathsf{t}}} \leq \beta + g(\mathsf{m}, \gamma) \tag{5.56}$$

after the servers' encoding, where

$$g(\mathsf{m}, \gamma) := 10\sqrt{2\mathsf{f}\gamma} \log \mathsf{m} + \eta_0(2\sqrt{2\mathsf{f}\gamma}) + 2h_2(2\sqrt{2\mathsf{f}\gamma}). \tag{5.57}$$

Here, $\eta_0(\cdot)$ and $h_2(\cdot)$ are defined in (2.25). In particular, when $\gamma = 0$, we have

$$I(M_k; \mathcal{A}_\mathsf{t} | Q_\mathsf{t}, K = k)_{\rho_{MQ_\mathsf{t}}} \leq \beta$$

for any $k \in \{1, \ldots, \mathsf{f}\}$.

Proof. Let $k \neq i \in \{1, \ldots, \mathsf{f}\}$. We obtain the lemma as follows.

$$I(M_k; \mathcal{A}_\mathsf{t} | Q_\mathsf{t}, K = k)_{\rho_{MQ_\mathsf{t}}} \tag{5.58}$$

$$\leq I(M_k; \mathcal{A}_\mathsf{t} Q_\mathsf{t} | K = k)_{\rho_{MQ_\mathsf{t}}} \tag{5.59}$$

$$\overset{(a)}{\leq} I(M_k; \mathcal{A}_\mathsf{t} Q_\mathsf{t} | K = i)_{\rho_{MQ_\mathsf{t}}} + g(\mathsf{m}, \gamma) \tag{5.60}$$

$$\leq I(M_i^c; \mathcal{A} Q | K = i)_{\rho_{MQ}} + g(\mathsf{m}, \gamma) \tag{5.61}$$

$$\overset{(b)}{\leq} \beta + g(\mathsf{m}, \gamma). \tag{5.62}$$

The inequality (b) follows from (5.51).

The inequality (a) is derived as follows. When we define

$$\tilde{\rho}_{MQ_{\mathsf{t}}|k} \coloneqq \sum_{m,q_{\mathsf{t}}} (1/\mathsf{m}^{\mathsf{f}}) \cdot p_{Q_{\mathsf{t}}=q_{\mathsf{t}}|K=k} \cdot |m, q_{\mathsf{t}}\rangle\langle m, q_{\mathsf{t}}| \otimes \rho_{mq_{\mathsf{t}}}$$

for $k \in \{1, \dots, \mathsf{f}\}$, the inequality (5.52) implies that

$$d(\tilde{\rho}_{MQ_{\mathsf{t}}|k}, \tilde{\rho}_{MQ_{\mathsf{t}}|i}) \leq \sqrt{2\mathsf{f}\gamma} \tag{5.63}$$

for any $i \neq k \in \{1, \dots, \mathsf{f}\}$, where $d(\cdot, \cdot)$ is the trace distance $d(\rho, \sigma) \coloneqq (1/2) \cdot \mathrm{Tr}\,|\rho - \sigma|$ for quantum states ρ, σ defined in (2.17). Thus, Fannes inequality for mutual information (2.29) implies that

$$|I(M_k; \mathcal{A}_{\mathsf{t}} Q_{\mathsf{t}} | K = k)_{\rho_{MQ_{\mathsf{t}}}} - I(M_k; \mathcal{A}_{\mathsf{t}} Q_{\mathsf{t}} | K = i)_{\rho_{MQ_{\mathsf{t}}}}| \leq g(\mathsf{m}, \gamma),$$

which yields the inequality (a). □

Lastly, we prepare the following lemma, which is fundamental for the proof of the weak converse bound (5.46).

Lemma 5.5. *Let $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$ be a t-private QPIR protocol such that*

$$S_{\mathrm{serv}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) \leq \beta, \tag{5.64}$$

$$S^{(\mathsf{t})}_{\mathrm{user}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) \leq \gamma, \tag{5.65}$$

$$P_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) \leq \min\{1/2, 1 - 10\sqrt{2\mathsf{f}\gamma}\}. \tag{5.66}$$

Then, the protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$ satisfies

$$\log \mathsf{m} \leq \frac{2(\mathsf{n} - \mathsf{t}) \log \mathsf{d} + \beta + \eta_0(2\sqrt{2\mathsf{f}\gamma}) + 2h_2(2\sqrt{2\mathsf{f}\gamma}) + h_2\Big(P_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big)}{1 - P_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) - 10\sqrt{2\mathsf{f}\gamma}},$$

where $\eta_0(\cdot)$ and $h_2(\cdot)$ are defined in (2.25).

Proof. We prove the lemma by four steps.

Step 1: First, we prepare the following notation. Fix $K = k$ arbitrarily. Let $\rho_{m_k, m_k^c, q}$ be the quantum state on the composite system $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j$, where m_k is the message to be retrieved, m_k^c is the collection of non-retrieved $\mathsf{f} - 1$ messages, and q is the collection of queries. Note that in view of Figure 5.4-(b), the targeted message m_k corresponds to the classical message

and the query q determines the decoding algorithm, but the non-targeted messages m_k^c are independent of m_k and q. Therefore, we only consider, in the following, the averaged states

$$\tau_{m_k,q} \coloneqq \frac{1}{\mathsf{m}^{\mathsf{f}-1}} \sum_{m_k^c} \rho_{m_k,m_k^c,q}, \quad \sigma_q \coloneqq \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \tau_{m_k,q}. \tag{5.67}$$

Considering the entire system $\mathcal{A}$ as a bipartite system $\mathcal{A}_{\mathsf{t}} \otimes \mathcal{A}_{\mathsf{t}^c}$, let $\tau'_{m_k,q_{\mathsf{t}}}$ and $\sigma'_{q_{\mathsf{t}}}$ be the reduced density matrices of $\tau_{m_k,q}$ and σ_q on $\mathcal{A}_{\mathsf{t}}$, respectively. Depending on k and q, we denote the decoding POVM by $\{Y_{k,q}(w)\}_{w\in\{1,\ldots,\mathsf{m}\}}$. Then, we define

$$R_q \coloneqq \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} |m_k\rangle\langle m_k| \otimes \tau_{m_k,q}, \tag{5.68}$$

$$S_q \coloneqq \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} |m_k\rangle\langle m_k| \otimes \sigma'_{q_{\mathsf{t}}} \otimes I/\mathsf{d}^{\mathsf{n}-\mathsf{t}}, \tag{5.69}$$

$$Y_{k,q} \coloneqq \sum_{m_k=1}^{\mathsf{m}} |m_k\rangle\langle m_k| \otimes Y_{k,q}(m_k). \tag{5.70}$$

Step 2: In this step, we derive the inequality

$$(1 - P_{\mathrm{err},k}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})) \log \mathsf{m} \le \mathbb{E}_Q D(R_Q \| S_Q) + h_2\Big(P_{\mathrm{err},k}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})\Big), \tag{5.71}$$

where $P_{\mathrm{err},k}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \Pr_{W,M_k}[W \neq M_k | K = k]$.

The data-processing inequality for quantum relative entropy (2.23) with respect to the two-valued measurement $\{Y_{k,q}, I - Y_{k,q}\}$ is written as

$$\begin{aligned} D(\rho||\sigma) &\ge D(P_\rho||P_\sigma) \\ &= -h_2(P_\rho(1)) - P_\rho(1)\log P_\sigma(1) - P_\rho(2)\log P_\sigma(2), \end{aligned} \tag{5.72}$$

where

$$P_\rho = \{P_\rho(1), P_\rho(2)\} = \{\operatorname{Tr}\rho Y_{k,q}, \operatorname{Tr}\rho(I - Y_{k,q})\}, \tag{5.73}$$

$$P_\sigma = \{P_\sigma(1), P_\sigma(2)\} = \{\operatorname{Tr}\sigma Y_{k,q}, \operatorname{Tr}\sigma(I - Y_{k,q})\}. \tag{5.74}$$

For the states R_q and S_q, we have

$$\begin{aligned} P_{R_q} &= \{P_{R_q}(1), P_{R_q}(2)\} = \{P_{\mathrm{err},k,q}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}), 1 - P_{\mathrm{err},k,q}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})\}, \\ P_{S_q} &= \{P_{S_q}(1), P_{S_q}(2)\} = \left\{\frac{1}{\mathsf{m}}, 1 - \frac{1}{\mathsf{m}}\right\}, \end{aligned}$$

where $P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) := \Pr_{W,M_k}[W \neq M_k | K = k, Q = q]$. Here, P_{S_q} is independent of k and q. Applying (5.72) to the states R_q and S_q, we have

$$(1 - P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})) \log \mathsf{m} = P_{R_q}(2) \log P_{S_q}(2)^{-1} \tag{5.75}$$
$$\le D(R_q \| S_q) + h_2(P_{R_q}(1)) \tag{5.76}$$
$$= D(R_q \| S_q) + h_2\Big(P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big). \tag{5.77}$$

Taking expectation with respect to Q and using the concavity of h_2, we have

$$(1 - P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})) \log \mathsf{m} = \mathbb{E}_Q (1 - P_{\mathrm{err},k,Q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})) \log \mathsf{m} \tag{5.78}$$
$$\le \mathbb{E}_Q D(R_Q \| S_Q) + h_2\Big(P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big), \tag{5.79}$$

which is the desired inequality (5.71).

Step 3: Next, we derive the inequality

$$\mathbb{E}_Q D(R_Q \| S_Q) \le 2(\mathsf{n} - \mathsf{t}) \log \mathsf{d} + I(M_k; \mathcal{A}_{\mathsf{t}} | Q_{\mathsf{t}}, K = k)_{\rho_{MQ_{\mathsf{t}}}}. \tag{5.80}$$

The inequality (5.80) is derived by

$$\mathbb{E}_Q D(R_Q \| S_Q) = \mathbb{E}_Q \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} D\left(\tau_{m_k,Q} \middle\| \sigma'_{Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right)$$
$$\overset{(a)}{=} \mathbb{E}_Q \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \left(D\left(\tau_{m_k,Q} \middle\| \tau'_{m_k,Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right) + D(\tau'_{m_k,Q_{\mathsf{t}}} \| \sigma'_{Q_{\mathsf{t}}}) \right)$$
$$= \mathbb{E}_Q \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} D\left(\tau_{m_k,Q} \middle\| \tau'_{m_k,Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right) + I(M_k; \mathcal{A}_{\mathsf{t}} | Q_{\mathsf{t}}, K = k)_{\rho_{MQ_{\mathsf{t}}}}$$
$$\overset{(b)}{\le} 2(\mathsf{n} - \mathsf{t}) \log \mathsf{d} + I(M_k; \mathcal{A}_{\mathsf{t}} | Q_{\mathsf{t}}, K = k)_{\rho_{MQ_{\mathsf{t}}}}.$$

The equation (a) can be shown as follows.

$$D\left(\tau_{m_k,Q} \middle\| \sigma'_{Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right)$$
$$= \operatorname{Tr} \tau_{m_k,Q} \left(\log \tau_{m_k,Q} - \log \left(\sigma'_{Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}} \right) \right)$$
$$= \operatorname{Tr} \tau_{m_k,Q} \Bigg\{ \log \tau_{m_k,Q} - \log \left(\tau'_{m_k,Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}} \right)$$
$$+ \log \left(\tau'_{m_k,Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}} \right) - \log \left(\sigma'_{Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}} \right) \Bigg\}$$
$$= D\left(\tau_{m_k,Q} \middle\| \tau'_{m_k,Q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right) + D(\tau'_{m_k,Q_{\mathsf{t}}} \| \sigma'_{Q_{\mathsf{t}}}).$$

The inequality (b) can be shown as follows. We diagonalize the state $\tau_{m_k,Q} = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ and denote by ρ_i the reduced density matrix of $|\phi_i\rangle\langle\phi_i|$ on $\mathcal{A}_{\mathsf{t}}$. Then,

$$\begin{aligned} &D\left(\tau_{m_k,Q}\middle\|\tau'_{m_k,Q_{\mathsf{t}}}\otimes\frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right) \le \sum_i p_i D\left(|\phi_i\rangle\langle\phi_i|\middle\|\rho_i\otimes\frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right) \\ &= \log \mathsf{d}^{\mathsf{n}-\mathsf{t}} + \sum_i p_i H(\rho_i) \le 2\log \mathsf{d}^{\mathsf{n}-\mathsf{t}}, \end{aligned}$$

where the last inequality is proved from $H(\rho_i) = H(\rho'_i) \le \log \mathsf{d}^{\mathsf{n}-\mathsf{t}}$ for the reduced density matrix ρ'_i of $|\phi_i\rangle\langle\phi_i|$ on $\mathcal{A}_{\mathsf{t}^c}$.

Step 4: Lastly, we prove Lemma 5.5. Combining Eq. (5.71), Eq. (5.80), and Lemma 5.4, we have

$$\begin{aligned} &(1-P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}))\log \mathsf{m} \\ &\le 2(\mathsf{n}-\mathsf{t})\log \mathsf{d} + I(M_k;\mathcal{A}_{\mathsf{t}}|Q,K=k)_{\rho_{MQ,\mathsf{t}}} + h_2\Big(P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big) \\ &\le 2(\mathsf{n}-\mathsf{t})\log \mathsf{d} + \beta + g(\mathsf{m},\gamma) + h_2\Big(P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big) \\ &= 2(\mathsf{n}-\mathsf{t})\log \mathsf{d} + \beta + 10\sqrt{2\mathsf{f}\gamma}\log \mathsf{m} + \eta_0(2\sqrt{2\mathsf{f}\gamma}) + 2h_2(2\sqrt{2\mathsf{f}\gamma}) \\ &\quad + h_2\Big(P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big) \end{aligned}$$

Then, rewriting the above inequality, we obtain Lemma 5.5 as

$$\begin{aligned} \log \mathsf{m} &\le \frac{2(\mathsf{n}-\mathsf{t})\log \mathsf{d} + \beta + \eta_0(2\sqrt{2\mathsf{f}\gamma}) + 2h_2(2\sqrt{2\mathsf{f}\gamma}) + h_2\Big(P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big)}{1-P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) - 10\sqrt{2\mathsf{f}\gamma}} \\ &\overset{(c)}{\le} \frac{2(\mathsf{n}-\mathsf{t})\log \mathsf{d} + \beta + \eta_0(2\sqrt{2\mathsf{f}\gamma}) + 2h_2(2\sqrt{2\mathsf{f}\gamma}) + h_2\Big(P_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big)}{1-P_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) - 10\sqrt{2\mathsf{f}\gamma}}, \end{aligned}$$

where (c) follows from $P_{\mathrm{err},k}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) \le P_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) < 1/2$. □

Remark 5.10. In Step 2, we condition on $Q = q$ and then take expectation with respect to Q. The reason why we condition on $Q = q$ is that the states and the decoder are determined depending on the value of Q. Thus, to derive (5.75) which relates the error probability and quantum relative entropy, we need to condition on $Q = q$. On the other hand, we need to take expectation on Q in (5.79) because we need to recover Q_{t} as a random variable to apply the user secrecy condition $I(K;Q_{\mathsf{t}}) \le \gamma$. To be precise, we use the user secrecy condition $I(K;Q_{\mathsf{t}}) \le \gamma$ in the proof of Lemma 5.4 and we apply Lemma 5.4 in Step 4.

5.4.2 Weak converse bound for $\mathsf{t} > \mathsf{n}/2$ with user secrecy

In this subsection, we prove the converse bound (5.46). We choose a sequence of QPIR protocols $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ such that

$$(\alpha_\ell, \beta_\ell, \gamma_\ell) \coloneqq (P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}), S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}), S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}))$$

satisfies

$$\begin{aligned}\limsup_{\ell\to\infty} \alpha_\ell &= 0,\\ \limsup_{\ell\to\infty} \gamma_\ell &= 0,\\ \limsup_{\ell\to\infty} \beta_\ell &= \beta.\end{aligned}$$

Let d_ℓ be the dimension of $\mathcal{A}_j$ $(\forall j \in [\mathsf{n}])$ for the protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}$. Then, for any sufficiently large ℓ such that $\alpha_\ell \le \min\{1/2, 1 - 10\sqrt{2\mathsf{f}\gamma_\ell}\}$, Lemma 5.5 gives

$$\log \mathsf{m}_\ell \le \frac{2(\mathsf{n}-\mathsf{t})\log \mathsf{d}_\ell + \beta_\ell + \eta_0(2\sqrt{2\mathsf{f}\gamma_\ell}) + 2h_2(2\sqrt{2\mathsf{f}\gamma_\ell}) + h_2(\alpha_\ell)}{1 - \alpha_\ell - 10\sqrt{2\mathsf{f}\gamma_\ell}}.$$

Hence, the asymptotic QPIR rate satisfies

$$\begin{aligned}&\lim_{\ell\to\infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})\\ &= \lim_{\ell\to\infty} \frac{\log \mathsf{m}_\ell}{\mathsf{n}\log \mathsf{d}_\ell}\\ &\le \lim_{\ell\to\infty} \frac{2(\mathsf{n}-\mathsf{t})\log \mathsf{d}_\ell + \beta_\ell + \eta_0(2\sqrt{2\mathsf{f}\gamma_\ell}) + 2h_2(2\sqrt{2\mathsf{f}\gamma_\ell}) + h_2(\alpha_\ell)}{(1 - \alpha_\ell - 10\sqrt{2\mathsf{f}\gamma_\ell})\mathsf{n}\log \mathsf{d}_\ell}\\ &= \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}},\end{aligned}$$

where the last equality follows from the relation $(\alpha_\ell, \beta_\ell, \gamma_\ell, \mathsf{d}_\ell) \to (0, \beta, 0, \infty)$ as $\ell \to \infty$. Thus we obtain the converse bound (5.46).

5.4.3 Strong converse bound for $\mathsf{t} > \mathsf{n}/2$ with perfect secrecy

In this subsection, we prove the strong converse bound (5.45) for $\mathsf{t} > \mathsf{n}/2$ with perfect secrecy Throughout this subsection, we use the notation given in Step 1 of the proof of Lemma 5.5.

The converse bound (5.45) is the bound with the assumption of perfect secrecy, i.e., $S_{\mathrm{serv}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) = 0$ and $S^{(\mathsf{t})}_{\mathrm{user}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) = 0$. With perfect secrecy, we have the following corollary of Lemma 5.4.

Corollary 5.2. *Suppose* $S_{\mathrm{serv}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) = 0$ *and* $S^{(\mathsf{t})}_{\mathrm{user}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) = 0$. *Then, the relation*

$$I(M_k; \mathcal{A}_{\pi(\mathsf{t})} | Q_{\mathsf{t}}, K = k)_{\rho_{MQ_{\mathsf{t}}}} = 0$$

holds for any $k \in \{1, \ldots, \mathsf{f}\}$ *after the application of the server encoder. That is, the state on the system* $\mathcal{A}_{\pi(\mathsf{t})}$ *does not depend on the message* M_k.

We give a simple direct proof for this corollary in Appendix F.

Now, we prove Eq. (5.45). Let $S_{\mathrm{serv}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) = 0$ and $S^{(\mathsf{t})}_{\mathrm{user}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}) = 0$. We consider the case where arbitrary $K = k$, $Q = q$, and $\pi \in \mathsf{S}_{\mathsf{n}}$ are fixed. Since Corollary 5.2 guarantees that the reduced density matrix $\tau'_{m_k,q_{\mathsf{t}}}$ on $\mathcal{A}_{\mathsf{t}}$ does not depend on m_k, we denote it by $\tau'_{q_{\mathsf{t}}}$. Applying Proposition 3.2 with

$$(s, \rho_w, Y(w), \sigma) := \left(1, \tau_{m_k,q}, Y_{k,q}(w), \tau'_{q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right),$$

we have

$$(1 - P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}))^2 \mathsf{m} \le \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \tau^2_{m_k,q} \left(\tau'_{q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right)^{-1}. \tag{5.81}$$

Given m_k and q, consider the decomposition $\tau_{m_k,q} = \sum_x p_x |\psi_{m_k,q,x}\rangle\langle\psi_{m_k,q,x}|$. Let $\rho'_{q_{\mathsf{t}},x}$ be the reduced density matrix of $|\psi_{m_k,q,x}\rangle\langle\psi_{m_k,q,x}|$ on $\mathcal{A}_{\mathsf{t}}$, i.e., $\tau'_{q_{\mathsf{t}}} = \sum_x p_x \rho'_{q_{\mathsf{t}},x}$. Then,

$$\begin{aligned}
&\operatorname{Tr} \tau^2_{m_k,q} \left(\tau'_{q_{\mathsf{t}}} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right)^{-1} \\
&\overset{(a)}{\le} \sum_x p_x \operatorname{Tr}(|\psi_{m_k,q,x}\rangle\langle\psi_{m_k,q,x}|)^2 \left(\rho'_{q_{\mathsf{t}},x} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right)^{-1} \\
&= \sum_x p_x \operatorname{Tr} |\psi_{m_k,q,x}\rangle\langle\psi_{m_k,q,x}| \left(\rho'_{q_{\mathsf{t}},x} \otimes \frac{I}{\mathsf{d}^{\mathsf{n}-\mathsf{t}}}\right)^{-1} \\
&= \mathsf{d}^{\mathsf{n}-\mathsf{t}} \sum_x p_x \operatorname{Tr} \rho'_{q_{\mathsf{t}},x} (\rho'_{q_{\mathsf{t}},x})^{-1} = \mathsf{d}^{\mathsf{n}-\mathsf{t}} \sum_x p_x \operatorname{Tr} I = \mathsf{d}^{2(\mathsf{n}-\mathsf{t})},
\end{aligned} \tag{5.82}$$

where (a) follows from the application of the data-processing inequality (2.22) to the choice

$$\begin{aligned} s &:= 1, \\ \rho &:= \sum_x p_x |x\rangle\langle x| \otimes |\psi_{m_k,q,x}\rangle\langle\psi_{m_k,q,x}| \in \mathcal{S}(X \otimes \mathcal{A}), \\ \sigma &:= \sum_x p_x |x\rangle\langle x| \otimes (\rho'_{q_{\mathsf{t}},x} \otimes I/\mathsf{d}^{\mathsf{n}-\mathsf{t}}) \in \mathcal{S}(X \otimes \mathcal{A}), \\ \kappa &:= \operatorname*{Tr}_X . \end{aligned}$$

Combining (5.81) and (5.82), we have

$$(1 - P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}))^2 \le \frac{\mathsf{d}^{2(\mathsf{n}-\mathsf{t})}}{\mathsf{m}}. \tag{5.83}$$

Let $\{\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}\}_{\ell=1}^{\infty}$ be an arbitrary sequence of QPIR protocols such that the QPIR rate greater than $2(\mathsf{n}-\mathsf{t})/\mathsf{n}$ for any sufficiently large ℓ, i.e.,

$$R(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}) = \frac{\log \mathsf{m}_\ell}{\log \mathsf{d}_\ell^{\mathsf{n}}} > \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}, \tag{5.84}$$

which is equivalent to

$$\frac{\log \mathsf{m}_\ell}{\log \mathsf{d}_\ell^{2(\mathsf{n}-\mathsf{t})}} > 1. \tag{5.85}$$

Here, d_ℓ is the dimension of $\mathcal{A}_j$ $(\forall j \in [\mathsf{n}])$ for the protocol $\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}$. From (5.85), $\mathsf{d}_\ell^{2(\mathsf{n}-\mathsf{t})}/\mathsf{m}_\ell$ goes to 0, and then from (5.83), the probability $1 - P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}})$ approaches 0. Since

$$1 - P_{\mathrm{err}}(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}) \le 1 - P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}), \tag{5.86}$$

we have $1 - P_{\mathrm{err}}(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}) \to 0$, which implies (5.45).

5.4.4 Strong converse bound for $\mathsf{t} \le \mathsf{n}/2$

In this subsection, we prove the strong converse bound (5.44) for $\mathsf{t} \le \mathsf{n}/2$. Throughout this subsection, we also use the notation given in Step 1 of the proof of Lemma 5.5.

The bound (5.44) is proved similar to Chapter 3 as follows. Fix $K = k$ and $Q = q$. Let $\sigma_q \coloneqq (1/\mathsf{m}) \sum_{m_k=1}^{\mathsf{m}} \tau_{m_k,q}$. Applying Proposition 3.2 with

$$(s, \rho_w, Y(w), \sigma) \coloneqq (1, \tau_{m_k,q}, Y_{k,q}(w), \sigma_q),$$

we have

$$(1 - P_{\mathrm{err},k,q}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}))^2 \mathsf{m} \leq \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \tau_{m_k,q}^2 \sigma_q^{-1}. \tag{5.87}$$

Then,

$$\frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \tau_{m_k,q}^2 \sigma_q^{-1} \leq \frac{1}{\mathsf{m}} \sum_{m_k=1}^{\mathsf{m}} \operatorname{Tr} \tau_{m_k,q} \sigma_q^{-1} = \operatorname{Tr} I = \prod_{j=1}^{\mathsf{n}} \dim \mathcal{A}_j. \tag{5.88}$$

Combining (5.87) and (5.88), we have

$$(1 - P_{\mathrm{err},k,q}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}))^2 \leq \frac{\prod_{j=1}^{\mathsf{n}} \dim \mathcal{A}_j}{\mathsf{m}}. \tag{5.89}$$

Let $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ be an arbitrary sequence of QPIR protocols such that the QPIR rate of $\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}$ is strictly greater than 1 for any sufficiently large ℓ, i.e.,

$$R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) = \frac{\log \mathsf{m}_\ell}{\log \mathsf{d}_\ell^{\mathsf{n}}} > 1, \tag{5.90}$$

where d_ℓ is the dimension of $\mathcal{A}_j$ ($\forall j \in [\mathsf{n}]$) for the protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}$. Then, Eq. (5.90) implies that

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

Hence, from (5.89), for any k and q, $1 - P_{\mathrm{err},k,q}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})$ approaches zero. Since

$$1 - P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \leq 1 - P_{\mathrm{err},k,q}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}), \tag{5.91}$$

we have $1 - P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \to 0$, which implies (5.44).

Chapter 6

Quantum Private Information Retrieval with Colluding Servers by Bipartite Entangled States

The t-private symmetric QPIR protocol in Section 5.3 required a multipartite entangled state as prior entanglement. However, because of limitation in current quantum technology, it is hard to generate and control multipartite entangled states compared to bipartite entangled states. Thus, it is desirable to construct a protocol with bipartite entangled states instead of multipartite entangled states.

In this chapter, we construct the $(\mathsf{n}-1)$-private QPIR protocol with bipartite entangled states. The protocol in this chapter achieves $(\mathsf{n}-1)$-private QPIR capacity derived in Theorem 5.1 and has the following advantages compared to the protocol in Section 5.3. First, our protocol only requires multiple copies of bipartite entangled states whereas the protocol in Section 5.3 requires multipartite entanglement as prior entanglement. Since the bipartite entanglement is more reliably generated with current technology, our construction is more suitable for the implementation on quantum devices than the protocol in Section 5.3. Second, our protocol is more constructive than the protocol in Section 5.3. Our protocol is a combination of two simple protocols: quantum teleportation [80] and superdense coding [81], which have been experimentally realized in [82,83] and [84,85], respectively. On the other hand, the protocol in Section 5.3 is constructed with more sophisticated method of stabilizer formalism. Thus, our protocol is more accessible to the

experimentalists and the theorists who are not familiar with the stabilizer formalism.

The protocol in this chapter is a generalization of the QPIR protocol in Chapter 3. The protocol in Chapter 3 extended the classical two-server PIR protocol [5] by the idea of superdense coding [81]. Similarly, our protocol extends an $(\mathsf{n}-1)$-private PIR protocol explained below by the idea of superdense coding [81] and quantum teleportation [80]. The classical $(\mathsf{n}-1)$-private PIR protocol we extend is described as follows. Let $(\log \mathsf{m})$-bit messages $M_1, \dots, M_{\mathsf{f}}$ be contained in each of n servers and the queries $Q_1, \dots, Q_{\mathsf{n}-1}$ be independently and uniformly chosen subsets of $\{1, \dots, \mathsf{f}\}$. To retrieve the K-th message, the user chooses Q_{n} which satisfies $\bigoplus_{j=1}^{\mathsf{n}} Q_j = \{K\}$, where $\bigoplus$ is the symmetric difference, and sends the queries $Q_1, \dots, Q_{\mathsf{n}}$ to each server. For each $j \in \{1, \dots, \mathsf{n}\}$, the j-th server returns $H_j := \sum_{i \in Q_j} M_i$ to the user and then the user can retrieve $M_K = \sum_{j=1}^{\mathsf{n}} H_j$, where both summations are with respect to the addition modulo 2. The protocol is private because the collection of any $\mathsf{n}-1$ variables in $Q_1, \dots, Q_{\mathsf{n}}$ is independent of the target index K.

The protocol in this chapter has several remarkable properties. First, our protocol is a symmetric QPIR protocol. Second, the upload cost of our protocol is nf bits, which is linear for the number of servers n and the number of messages f but independent of the message size m. Third, our protocol requires the message size $\mathsf{m} = 2^{2\ell}$, i.e., 2ℓ bits, for any positive integer ℓ, whereas the $(\mathsf{n}-1)$-private classical PIR protocol in [29] requires the message size $\mathsf{m} = q^{\mathsf{n}^{\mathsf{f}}}$ depending on n and f for a sufficiently large prime power q.

Following the conference paper of this chapter [2], the paper [55] proposed a QPIR protocol for coded and colluding servers which works for any $[\mathsf{n}, k]$-MDS code and secure against t-collusion with $\mathsf{t} = \mathsf{n} - k$. Their protocol is an extension of the QPIR protocol of this paper by the combination with the classical PIR protocol [32] and it achieves better rates than the classical counterparts [32, 36].

The rest of the paper is organized as follows. Section 6.1 presents the main theorem. Section 6.2 is preliminaries for the protocol construction and Section 6.3 constructs the QPIR protocol with $\mathsf{n}-1$ colluding servers.

6.1 Main theorem

Let $|\Phi\rangle \coloneqq (1/2)(|00\rangle + |11\rangle)$ and one copy of the state $|\Phi\rangle$ is counted as an *ebit*. The main theorem of this chapter is as follows.

Theorem 6.1 ($(\mathsf{n}-1)$-private symmetric QPIR protocol with bipartite entanglement)**.** *For $(\mathsf{n}-1)$-private symmetric QPIR with any $\mathsf{n} \geq 2$ servers and $\mathsf{f} \geq 2$ messages, there exists a QPIR protocol with the rate $\lceil \mathsf{n}/2 \rceil^{-1}$, perfect security, nf-bit upload cost, 2ℓ-bit messages for any integer $\ell \geq 1$, and $(\lfloor 3\mathsf{n}/2 \rfloor - 2)$ ebits as prior entanglement.*

Note that the protocol in this section achieves $(\mathsf{n}-1)$-private QPIR capacity derived in Theorem 5.1 when the number of server n is any even number. Compared to the capacity-achieving protocol in Section 5.3, which requires one n-partite entangled state, the protocol in this section needs only many copies of bipartite entangled state (ebits) as prior entanglement. Section 6.3 constructs the protocol that achieves the performance given in Theorem 6.1. When $\mathsf{n} = 2$, the protocol in Section 6.3 corresponds to the protocol in Chapter 3.

6.2 Preliminaries for protocol construction

In this section, we prepare two simple protocols to describe our QPIR protocol. Throughout this chapter, we consider the unit quantum system $\mathcal{H}$ as a *qubit*, i.e., a two-dimensional Hilbert space spanned by an orthonormal basis $\{|0\rangle, |1\rangle\}$. Thus, we use the notations $\mathsf{X}, \mathsf{Z}, \mathsf{W}(a,b), |T\rangle\!\rangle, \mathbf{M}_{\mathbb{Z}_2^2}$ of Section 3.2.1. Note in the following that $\mathsf{W}(a,b)$ on a qubit is a real matrix and therefore $\overline{\mathsf{W}(a,b)} = \mathsf{W}(a,b)$ and $\mathsf{W}(a,b)^* = \mathsf{W}(a,b)^\top$.

6.2.1 Quantum teleportation with an operation

First, we give a modified version of the quantum teleportation protocol [80], where an operation $\mathsf{W}(c,d)$ is performed on $\mathcal{H}_3$ before the quantum teleportation protocol starts.

Protocol 6.1. *Suppose that Alice possesses two qubits $\mathcal{H}_1$ and $\mathcal{H}_2$, Bob possesses a qubit $\mathcal{H}_3$. The state on $\mathcal{H}_1$ is ρ and Alice and Bob share $|\Phi\rangle \in$*

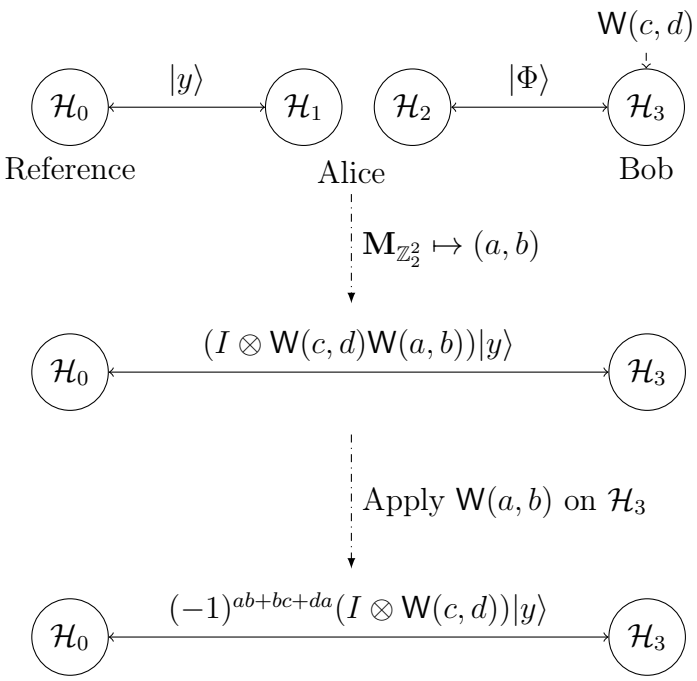


Figure 6.1: Change of states in quantum teleportation protocol with an operation $\mathsf{W}(c,d)$ on $\mathcal{H}_3$ (Protocol 6.1). The symbol $\mathbf{M}_{\mathbb{Z}_2^2} \mapsto (a,b)$ implies that the PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ is applied on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and the measurement outcome is $(a,b) \in \mathbb{Z}_2^2$.

$\mathcal{H}_2 \otimes \mathcal{H}_3$. *Quantum teleportation protocol with an operation is given as follows.*

Step 1. Bob applies the unitary operation $\mathsf{W}(c,d)$ *on* $\mathcal{H}_3$.

Step 2. Alice applies PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ *on* $\mathcal{H}_1 \otimes \mathcal{H}_2$ *and sends the measurement outcome* (a,b) *to Bob.*

Step 3. Bob applies the unitary $\mathsf{W}(a,b)$ *on* $\mathcal{H}_3$.

The resultant state on $\mathcal{H}_3$ is $\mathsf{W}(c,d)\rho\mathsf{W}(c,d)^*$ and it preserves the entanglement. Note that Protocol 6.1 requires two-bit transmission from Alice to Bob. The protocol without Step 1 in Protocol 6.1 is the quantum teleportation protocol [80].

Analysis of Protocol 6.1

We show that the resultant state on $\mathcal{H}_3$ is $\mathsf{W}(c,d)\rho\mathsf{W}(c,d)^*$ and it preserves the entanglement (see Figure 6.1).

Let $\mathcal{H}_0$ be a qubit and $|y\rangle = \sum_{i,j=0}^{1} y_{ij}|i,j\rangle \in \mathcal{H}_0 \otimes \mathcal{H}_1$ be a purification of the state ρ. Before the protocol starts, the state on $\mathcal{H}_0 \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ is

$$|z\rangle \coloneqq \frac{1}{\sqrt{2}} \sum_{i,j,r=0}^{1} y_{ij}|i,j,r,r\rangle. \tag{6.1}$$

If the measurement outcome is (a,b) in Step 2, the state on $\mathcal{H}_0 \otimes \mathcal{H}_3$ at the end of Step 2 is

$$\begin{aligned}
&2 \cdot (I_{\mathcal{H}_0} \otimes \langle\Phi|(I_{\mathcal{H}_1} \otimes \mathsf{W}(a,b))^* \otimes \mathsf{W}(c,d))|z\rangle &(6.2)\\
&= \sum_{i,j=0}^{1} y_{ij}(-1)^{jb+jd+ad}|i, j+a+c\rangle \\
&= (-1)^{ad} \sum_{i,j=0}^{1} y_{ij}(-1)^{j(b+d)}|i, j+a+c\rangle \\
&= (-1)^{ad}(I_{\mathcal{H}_0} \otimes \mathsf{W}(a+c, b+d))|y\rangle \\
&= (I_{\mathcal{H}_0} \otimes \mathsf{W}(c,d)\mathsf{W}(a,b))|y\rangle, &(6.3)
\end{aligned}$$

where the multiplicand 2 in (6.2) is the normalizing multiplicand. At the end of Step 3, the state on $\mathcal{H}_0 \otimes \mathcal{H}_3$ is

$$(-1)^{ab+bc+da}(I_{\mathcal{H}_0} \otimes \mathsf{W}(c,d))|y\rangle, \tag{6.4}$$

which is an identical state to $(I_{\mathcal{H}_0} \otimes \mathsf{W}(c,d))|y\rangle$. Therefore, the resultant state on $\mathcal{H}_3$ is $\mathsf{W}(c,d)\rho\mathsf{W}(c,d)^*$ and it preserves the entanglement.

Remark 6.1. Even in case that the order of Step 1 and Step 2 is reversed, the state before and after the operation $\mathsf{W}(a,b)$ is identical to (6.3) and (6.4).

6.2.2 Two-sum transmission protocol

Consider there are three parties Alice, Bob, and Carol. By the following protocol, Carol receives the sum of Alice's information $(a,b) \in \mathbb{Z}_2^2$ and Bob's information $(c,d) \in \mathbb{Z}_2^2$.

Protocol 6.2. *Suppose that the joint state of two qubits $\mathcal{H}_1$ and $\mathcal{H}_2$ is the maximally entangled state $|\Phi\rangle$ and Alice and Bob possess $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. The two-sum transmission protocol is given as follows.*

Step 1. Alice and Bob apply $\mathsf{W}(a,b)$ on $\mathcal{H}_1$ and $\mathsf{W}(c,d)$ on $\mathcal{H}_2$, respectively.

Step 2. Alice and Bob send the quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$ to Carol, respectively.

Step 3. Carol performs the PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ and obtains the measurement outcome (e,f) as the protocol output.

In Protocol 6.2, the output (e,f) is $(a+c, b+d)$, which can be proved trivially from (3.15) and (3.20). The protocol requires two-qubit transmission each from Alice and Bob.

6.3 QPIR protocol with $\mathsf{n}-1$ colluding servers

In this section, we propose a QPIR protocol that achieves the performance given in Theorem 6.1 for any $\mathsf{n} \geq 2$ servers. In our protocol, we consider each server contains the following message set. Given two arbitrary integers $\ell \geq 1$ and $\mathsf{f} \geq 2$, the message set is given by the collection of 2ℓ-bit messages $M_1, \ldots, M_{\mathsf{f}} \in \mathbb{Z}_2^{2\ell}$ and M_i for any $i \in \{1, \ldots, \mathsf{f}\}$ is denoted by

$$M_i = (M_i^{(1)}, \ldots, M_i^{(\ell)}) \in (\mathbb{Z}_2^2)^{\times \ell}.$$

Section 6.3.1 presents our $(\mathsf{n}-1)$-private QPIR protocol with three servers $(\mathsf{n}=3)$ and $\ell = 1$ as the simplest case. Then, by using Protocol 6.2 and the idea of the protocol in Section 6.3.1, Section 6.3.2 presents our protocol for any n servers and any ℓ.

6.3.1 Construction of protocol for $\mathsf{n}=3$ and $\ell=1$

Protocol 6.3. *Our QPIR protocol for 3 servers with messages $M_1, \ldots, M_{\mathsf{f}} \in \mathbb{Z}_2^2$ is described as follows (see Figure 6.2).*

Step 1. ***[Preparation]*** *The servers $\mathtt{serv}_1$, $\mathtt{serv}_2$, $\mathtt{serv}_3$ possess one qubit $\mathcal{H}_1$, two qubits $\mathcal{H}_2^{\mathrm{L}}$, $\mathcal{H}_2^{\mathrm{R}}$, and one qubit $\mathcal{H}_3$, respectively. The initial states on both of $\mathcal{H}_1 \otimes \mathcal{H}_2^{\mathrm{L}}$ and $\mathcal{H}_2^{\mathrm{R}} \otimes \mathcal{H}_3$ are the maximally entangled state $|\Phi\rangle$.*

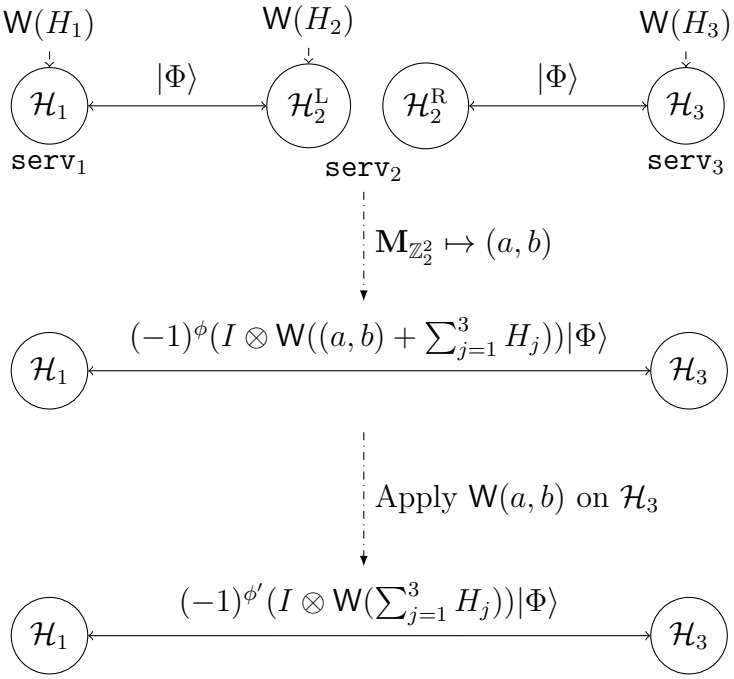


Figure 6.2: Two-private QPIR protocol for three servers and $\ell = 1$. $\mathbf{M}_{\mathbb{Z}_2^2} \mapsto (a,b)$ implies that the PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ is applied on $\mathcal{H}_2^{\mathrm{L}} \otimes \mathcal{H}_2^{\mathrm{R}}$ and the measurement outcome is $(a,b) \in \mathbb{Z}_2^2$. The values $\phi, \phi' \in \mathbb{Z}_2$ are determined by (a,b), H_1, H_2, and H_3.

Step 2. ***[Query]*** *Let K be the index of the message to be retrieved. Choose two subsets Q_1 and Q_2 of $\{1,\ldots,\mathsf{f}\}$ independently and uniformly at random. Define Q_3 by*

$$Q_3 \coloneqq Q_1 \oplus Q_2 \oplus \{K\}.$$

For each $j \in \{1,2,3\}$, the user sends the query Q_j to $\mathtt{serv}_j$.

Step 3. ***[Download]*** *For each $j \in \{1,2,3\}$, the server $\mathtt{serv}_j$ calculates*

$$H_j \coloneqq \sum_{i \in Q_j} M_i. \tag{6.5}$$

The server $\mathtt{serv}_1$ ($\mathtt{serv}_3$) applies $\mathsf{W}(H_1)$ to $\mathcal{H}_1$ ($\mathsf{W}(H_3)$ to $\mathcal{H}_3$) and transmits $\mathcal{H}_1$ ($\mathcal{H}_3$) to the user. The server $\mathtt{serv}_2$ applies $\mathsf{W}(H_2)$ on $\mathcal{H}_2^{\mathrm{L}}$, performs the PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ on $\mathcal{H}_2^{\mathrm{L}} \otimes \mathcal{H}_2^{\mathrm{R}}$, and transmits the measurement outcome $(a,b) \in \mathbb{Z}_2^2$ to the user.

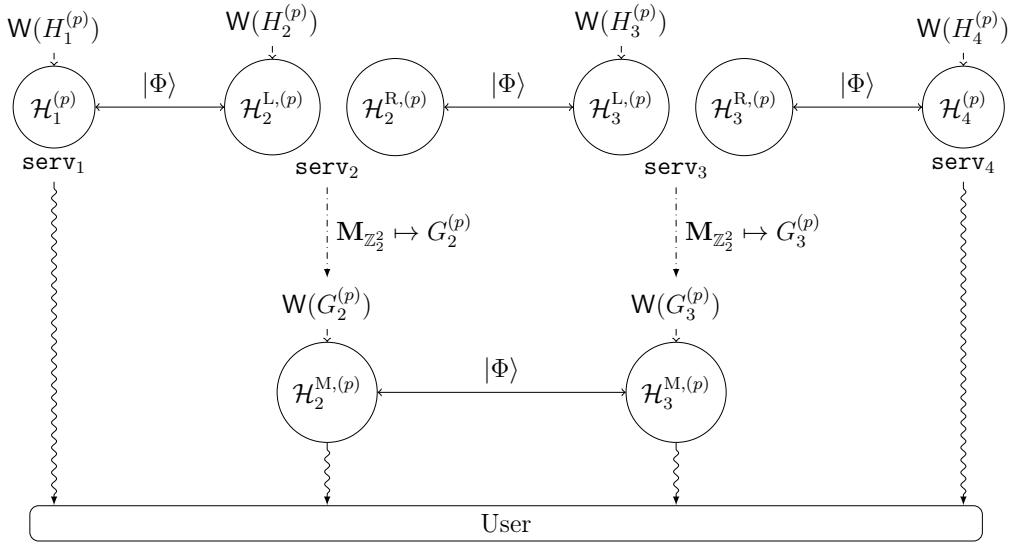


Figure 6.3: Download step of $(\mathsf{n}-1)$-private QPIR protocol for four servers and any integer $1 \le p \le \ell$. For any $j \in \{2,3\}$, $\mathbf{M}_{\mathbb{Z}_2^2} \mapsto G_j^{(p)}$ implies that the PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ is applied on $\mathcal{H}_j^{\mathrm{L},(p)} \otimes \mathcal{H}_j^{\mathrm{R},(p)}$ and the measurement outcome is $G_j^{(p)} \in \mathbb{Z}_2^2$. The snake shape arrow indicates the transmission of a qubit.

Step 4. ***[Retrieval]*** *The user applies* $\mathsf{W}(a,b)$ *on* $\mathcal{H}_3$ *and performs the PVM* $\mathbf{M}_{\mathbb{Z}_2^2}$ *on* $\mathcal{H}_1 \otimes \mathcal{H}_3$*, and the output of the protocol is the measurement outcome* $W \in \mathbb{Z}_2^2$*.*

Analysis of Protocol 6.3

First, we show the correctness of the protocol. The state of $\mathcal{H}_1 \otimes \mathcal{H}_2^{\mathrm{L}} \otimes \mathcal{H}_2^{\mathrm{R}} \otimes \mathcal{H}_3$ before the PVM at Step 3 is

$$(\mathsf{W}(H_1) \otimes \mathsf{W}(H_2))|\Phi\rangle \otimes (I \otimes \mathsf{W}(H_3))|\Phi\rangle \tag{6.6}$$
$$= (-1)^{\phi_0}(\mathsf{W}(H_1+H_2) \otimes I)|\Phi\rangle \otimes (I \otimes \mathsf{W}(H_3))|\Phi\rangle, \tag{6.7}$$

where $\phi_0 \in \mathbb{Z}_2$ is determined depending on H_1 and H_2. After the PVM at Step 3 with the measurement outcome (a,b), the state on $\mathcal{H}_1 \otimes \mathcal{H}_3$ is

$$(\mathsf{W}(H_1+H_2) \otimes \mathsf{W}((a,b)+H_3))|\Phi\rangle \tag{6.8}$$
$$= (-1)^{\phi_0'}(I \otimes \mathsf{W}((a,b)+H_1+H_2+H_3))|\Phi\rangle, \tag{6.9}$$

where $\phi_0' \in \mathbb{Z}_2$ is determined by $(a,b), H_1, H_2, H_3$. Thus, after the user's operation at Step 4, the state on $\mathcal{H}_1 \otimes \mathcal{H}_3$ is

$$(I \otimes \mathsf{W}(H_1 + H_2 + H_3))|\Phi\rangle. \tag{6.10}$$

(Alternatively, we can also obtain the same result (6.10) by considering the servers and the user apply Protocol 6.1 for $(c,d) := H_3$ and $|y\rangle := (\mathsf{W}(H_1) \otimes \mathsf{W}(H_2))|\Phi\rangle = (-1)^{\phi_0}(I \otimes \mathsf{W}(H_1 + H_2))|\Phi\rangle$.) Therefore, the user obtains the measurement outcome $\hat{W}_K = \sum_{t=1}^{3} H_t = W_K$, which implies the correctness of our protocol.

The user secrecy follows from the fact that any two of H_1, H_2, H_3 are independent of the target index K. The server secrecy follows from the fact that the user's information is (M_K, a, b) which is independent of any message except for M_K.

The upload cost is $\mathsf{nf} = 3\mathsf{f}$ bits because each of Q_1, Q_2, Q_3 is written by f bits. In the protocol, the user downloads 2 qubits and 2 bits but we count the download cost as 4 qubits since we only count quantum communication in our QPIR model and one qubit conveys one bit at most. The message size is $2\ell = 2$ bits. Therefore, the QPIR rate is $2/(\mathsf{n}+1) = 2/4$.

6.3.2 Construction of protocol for n servers

In this subsection, we present our protocol for any $\mathsf{n} \geq 2$ servers and any $\ell \geq 1$. The idea of our protocol construction is described as follows. The number of servers n are generalized to be arbitrary by using the idea of the three-server protocol in Section 6.3.1. In this generalization, it is necessary for servers to transmit the sum of measurement outcomes to the user, and it is performed efficiently by using the two-sum transmission protocol (Protocol 6.2). The index ℓ is increased by using the same query repetitively until the protocol retrieves the entire message.

Protocol 6.4. *Our protocol for* n *servers is described as follows (see Figure 6.3).*

Step 1. ***[Preparation]*** *For each* $p \in \{1, \ldots, \ell\}$*, prepare the following quantum systems and states. The servers* $\mathtt{serv}_1$ *and* $\mathtt{serv}_\mathsf{n}$ *have qubits* $\mathcal{H}_1^{(p)}$ *and* $\mathcal{H}_\mathsf{n}^{(p)}$*, respectively. For each* $j \in \{2, \ldots, \mathsf{n}-1\}$*, the server* $\mathtt{serv}_j$ *has three qubits* $\mathcal{H}_j^{\mathrm{L},(p)}$, $\mathcal{H}_j^{\mathrm{R},(p)}$, $\mathcal{H}_j^{\mathrm{M},(p)}$*. If* n *is odd, we consider*

the server $\mathtt{serv}_{\mathsf{n}-1}$ *has only two qubits* $\mathcal{H}_{\mathsf{n}-1}^{\mathrm{L},(p)}$, $\mathcal{H}_{\mathsf{n}-1}^{\mathrm{R},(p)}$. *The maximally entangled state* $|\Phi\rangle$ *is shared between each of the following bipartite systems:*

- $\mathcal{H}_1 \otimes \mathcal{H}_2^{\mathrm{L},(p)}, \mathcal{H}_{\mathsf{n}-1}^{\mathrm{R},(p)} \otimes \mathcal{H}_{\mathsf{n}}$,
- $\mathcal{H}_2^{\mathrm{R},(p)} \otimes \mathcal{H}_3^{\mathrm{L},(p)}, \mathcal{H}_3^{\mathrm{R},(p)} \otimes \mathcal{H}_4^{\mathrm{L},(p)}, \dots, \mathcal{H}_{\mathsf{n}-2}^{\mathrm{R},(p)} \otimes \mathcal{H}_{\mathsf{n}-1}^{\mathrm{L},(p)}$,
- $\mathcal{H}_{2j}^{\mathrm{M},(p)} \otimes \mathcal{H}_{2j+1}^{\mathrm{M},(p)}$ *for any* $j \in \{1, \dots, \lfloor \mathsf{n}/2 \rfloor - 1\}$.

Step 2. ***[Query]*** *Let* K *be the index of the message to be retrieved. Choose subsets* $Q_1, \dots, Q_{\mathsf{n}-1}$ *of* $\{1, \dots, \mathsf{f}\}$ *independently and uniformly at random. Define* Q_{n} *by*

$$Q_{\mathsf{n}} \coloneqq \bigoplus_{j=1}^{\mathsf{n}-1} Q_j \oplus \{K\}.$$

The user sends the query Q_j *to* $\mathtt{serv}_j$ *for each* $j \in \{1, \dots, \mathsf{n}\}$.

Step 3. ***[Download]*** *For each* $j \in \{1, \dots, \mathsf{n}\}$, *depending on the query* Q_j, *the server* $\mathtt{serv}_j$ *calculates*

$$\begin{aligned} H_j &= (H_j^{(1)}, \dots, H_j^{(\ell)}) \\ &\coloneqq \sum_{i \in Q_j} M_i = \left(\sum_{i \in Q_j} M_i^{(1)}, \dots, \sum_{i \in Q_j} M_i^{(\ell)} \right). \end{aligned} \tag{6.11}$$

Then, for each $p \in \{1, \dots, \ell\}$, *the servers perform the following process.*

a) The server $\mathtt{serv}_1$ *(*$\mathtt{serv}_{\mathsf{n}}$*) applies* $\mathsf{W}(H_1^{(p)})$ *to* $\mathcal{H}_1$ *(*$\mathsf{W}(H_{\mathsf{n}}^{(p)})$ *to* $\mathcal{H}_{\mathsf{n}}^{(p)}$*) and transmits* $\mathcal{H}_1^{(p)}$ *(*$\mathcal{H}_{\mathsf{n}}^{(p)}$*) to the user.*

b) For each $j \in \{2, \dots, \mathsf{n}-1\}$, *the server* $\mathtt{serv}_j$ *applies* $\mathsf{W}(H_j^{(p)})$ *on* $\mathcal{H}_j^{\mathrm{L},(p)}$ *and performs the PVM* $\mathbf{M}_{\mathbb{Z}_2^2}$ *on* $\mathcal{H}_j^{\mathrm{L},(p)} \otimes \mathcal{H}_j^{\mathrm{R},(p)}$ *whose measurement outcome is denoted by* $G_j^{(p)} \in \mathbb{Z}_2^2$.

c) For each $j \in \{1, \dots, \lfloor \mathsf{n}/2 \rfloor - 1\}$, *the servers* $\mathtt{serv}_{2j}$ *and* $\mathtt{serv}_{2j+1}$ *transmit the sum* $G_{2j}^{(p)} + G_{2j+1}^{(p)}$ *to the user by the two-sum transmission protocol (Protocol 6.2) with qubits* $\mathcal{H}_{2j}^{\mathrm{M},(p)}$ *and* $\mathcal{H}_{2j+1}^{\mathrm{M},(p)}$.

d) If n *is odd,* $\mathtt{serv}_{\mathsf{n}-1}$ *transmits* $G_{\mathsf{n}-1}^{(p)} \in \mathbb{Z}_2^2$ *to the user.*

Step 4. ***[Retrieval]*** *For each $p \in \{1, \dots, \ell\}$, the user performs the following process.*

a) For any $j \in \{1, \dots, \lfloor \mathsf{n}/2 \rfloor - 1\}$, the user receives the sum $G_{2j}^{(p)} + G_{2j+1}^{(p)}$ by Download Step c). If n is odd, the user obtains $G_{\mathsf{n}-1}^{(p)}$ additionally.

b) The user applies $\mathsf{W}(\sum_{j=2}^{\mathsf{n}-1} G_j^{(p)})$ on $\mathcal{H}_{\mathsf{n}}^{(p)}$.

c) The user performs the PVM $\mathbf{M}_{\mathbb{Z}_2^2}$ on $\mathcal{H}_1^{(p)} \otimes \mathcal{H}_{\mathsf{n}}^{(p)}$ whose measurement outcome is denoted by $W^{(p)} \in \mathbb{Z}_2^2$.

The protocol output is $W = (W^{(1)}, \dots, W^{(\ell)}) \in (\mathbb{Z}_2^2)^{\times \ell}$.

Protocol 6.4 is analyzed as follows.

Error Probability

Let p be any element of $\{1, \dots, \ell\}$.

As shown in the next paragraph, at the end of Download Step, the state on $\mathcal{H}_1^{(p)} \otimes \mathcal{H}_{\mathsf{n}}^{(p)}$ is

$$(-1)^{\phi_{\mathsf{n}}^{(p)}} \left(I \otimes \mathsf{W}\left(\sum_{j=1}^{\mathsf{n}} H_j^{(p)} + \sum_{j=2}^{\mathsf{n}-1} G_j^{(p)} \right) \right) |\Phi\rangle, \tag{6.12}$$

where $\phi_{\mathsf{n}}^{(p)} \in \mathbb{Z}_2$ is determined depending on $H_1^{(p)}, \dots, H_{\mathsf{n}}^{(p)}, G_2^{(p)}, \dots, G_{\mathsf{n}-1}^{(p)}$. Then, at the end of Retrieval Step b), the state on $\mathcal{H}_1^{(p)} \otimes \mathcal{H}_{\mathsf{n}}^{(p)}$ is

$$(-1)^{\widetilde{\phi}_{\mathsf{n}}^{(p)}} \left(I \otimes \mathsf{W}\left(\sum_{j=1}^{\mathsf{n}} H_j^{(p)} \right) \right) |\Phi\rangle, \tag{6.13}$$

where $\widetilde{\phi}_{\mathsf{n}}^{(p)} \in \mathbb{Z}_2$ is determined depending on $H_1^{(p)}, \dots, H_{\mathsf{n}}^{(p)}, G_2^{(p)}, \dots, G_{\mathsf{n}-1}^{(p)}$. Thus, at Retrieval Step c), the measurement outcome is $M^{(p)} = \sum_{j=1}^{\mathsf{n}} H_j^{(p)} = M_K^{(p)} \in \mathbb{Z}_2^2$, which implies that our protocol correctly retrieves $W_K^{(p)}$. Since $W_K^{(p)}$ is retrieved correctly for any p, the targeted message $W_K = (W_K^{(1)}, \dots, W_K^{(\ell)})$ is retrieved correctly.

Now, we prove (6.12). Since the operations of different servers are applied on different quantum systems, the order of the servers' operations can be arbitrary. Therefore, in the following, we consider that the servers

$\mathtt{serv}_1, \ldots, \mathtt{serv}_{\mathsf{n}}$ apply the operations sequentially. At the end of the operation of $\mathtt{serv}_1$, the state on $\mathcal{H}_1^{(p)} \otimes \mathcal{H}_2^{\mathrm{L},(p)}$ is

$$|y_1\rangle \coloneqq (\mathsf{W}(H_1^{(p)}) \otimes I)|\Phi\rangle = (-1)^{\phi_1^{(p)}} (I \otimes \mathsf{W}(H_1^{(p)}))|\Phi\rangle, \tag{6.14}$$

where $\phi_1^{(p)}$ is determined depending on $H_1^{(p)}$. Suppose that at the end of the operations of $\mathtt{serv}_k$ for any $k \in \{1, \ldots, \mathsf{n}-2\}$, the state on $\mathcal{H}_1 \otimes \mathcal{H}_{k+1}^{\mathrm{L},(p)}$ is

$$|y_k\rangle \coloneqq (-1)^{\phi_k^{(p)}} \left(I \otimes \mathsf{W}\left(\sum_{j=1}^{k} H_j^{(p)} + \sum_{j=2}^{k} G_j^{(p)} \right) \right) |\Phi\rangle, \tag{6.15}$$

where $\phi_k^{(p)} \in \mathbb{Z}_2$ is determined depending on $H_1^{(p)}, \ldots, H_k^{(p)}, G_2^{(p)}, \ldots, G_k^{(p)}$. Note that the operations of $\mathtt{serv}_{k+1}$ corresponds to the steps 0 and 1 of Protocol 6.1 for $|y\rangle \coloneqq |y_k\rangle$, $(a, b) \coloneqq G_{k+1}^{(p)}$, and $(c, d) \coloneqq H_{k+1}^{(p)}$. Therefore, after the operations of $\mathtt{serv}_{k+1}$, the state on $\mathcal{H}_1^{(p)} \otimes \mathcal{H}_{k+2}^{\mathrm{L},(p)}$ is

$$|y_{k+1}\rangle \coloneqq (-1)^{\phi_{k+1}^{(p)}} \left(I \otimes \mathsf{W}\left(\sum_{j=1}^{k+1} H_j^{(p)} + \sum_{j=2}^{k+1} G_j^{(p)} \right) \right) |\Phi\rangle, \tag{6.16}$$

where $\phi_{k+1}^{(p)} \in \mathbb{Z}_2$ is determined depending on $H_1^{(p)}, \ldots, H_{k+1}^{(p)}, G_2^{(p)}, \ldots, G_k^{(p)}$ and the system $\mathcal{H}_{k+2}^{\mathrm{L},(p)}$ denotes $\mathcal{H}_{\mathsf{n}}^{(p)}$ for the case $k = \mathsf{n}-2$. By the mathematical induction, the state on $\mathcal{H}_1^{(p)} \otimes \mathcal{H}_{\mathsf{n}}^{(p)}$ after the operations of $\mathtt{serv}_{\mathsf{n}-1}$ is

$$|y_{\mathsf{n}-1}\rangle = (-1)^{\phi_{\mathsf{n}-1}^{(p)}} \left(I \otimes \mathsf{W}\left(\sum_{j=1}^{\mathsf{n}-1} H_j^{(p)} + \sum_{j=2}^{\mathsf{n}-1} G_j^{(p)} \right) \right) |\Phi\rangle, \tag{6.17}$$

and after the operation of $\mathtt{serv}_{\mathsf{n}}$, the state is

$$(-1)^{\phi_{\mathsf{n}}^{(p)}} \left(I \otimes \mathsf{W}\left(\sum_{j=1}^{\mathsf{n}} H_j^{(p)} + \sum_{j=2}^{\mathsf{n}-1} G_j^{(p)} \right) \right) |\Phi\rangle, \tag{6.18}$$

where $\phi_{\mathsf{n}}^{(p)} \in \mathbb{Z}_2$ is determined depending on $H_1^{(p)}, \ldots, H_{\mathsf{n}}^{(p)}, G_2^{(p)}, \ldots, G_{\mathsf{n}-1}^{(p)}$. Thus, we have Eq. (6.12).

User secrecy and server secrecy

The user secrecy is obtained because the collection of any $\mathsf{n}-1$ variables in $Q_1, \ldots, Q_{\mathsf{n}}$ is independent of the target index K. Next, we consider the server

secrecy. The user obtains M_K and $G_{2j}^{(p)} + G_{2j+1}^{(p)}$ for any $j \in \{1, \dots, \lfloor \mathsf{n}/2 \rfloor - 1\}$ and any $p \in \{1, \dots, \ell\}$. If n is odd, the user obtains $G_{\mathsf{n}-1}^{(p)}$ additionally. Note that before the measurement by the server $\mathtt{serv}_j$ for $j \in \{2, \dots, \mathsf{n}-1\}$, the state on $\mathcal{H}_j^{\mathrm{L},(p)} \otimes \mathcal{H}_j^{\mathrm{R},(p)}$ is the completely mixed state, which implies that the measurement outcomes $G_j^{(p)}$ for all j are independent of any message. Therefore, the user obtains no message other than M_K.

Costs and QPIR rate

The upload cost is nf bits because each subset $Q_1, \dots, Q_{\mathsf{n}}$ of $\{1, \dots, \mathsf{f}\}$ is written by f bits. For each $p \in \{1, \dots, \ell\}$, the user downloads n qubits $\mathcal{H}_1^{(p)}$, $\mathcal{H}_2^{\mathrm{M},(p)}$, $\dots$, $\mathcal{H}_{\mathsf{n}-1}^{\mathrm{M},(p)}$, $\mathcal{H}_{\mathsf{n}}^{(p)}$ if n is even, and downloads $\mathsf{n}-1$ qubits $\mathcal{H}_1^{(p)}$, $\mathcal{H}_2^{\mathrm{M},(p)}$, $\dots$, $\mathcal{H}_{\mathsf{n}-2}^{\mathrm{M},(p)}$, $\mathcal{H}_{\mathsf{n}}^{(p)}$ and two bits $G_{\mathsf{n}-1}^{(p)} \in \mathbb{Z}_2^2$ if n is odd. Since we only count quantum communication in our QPIR model and one qubit conveys one bit at most, the total download cost is $\mathsf{n}\ell$ qubits when n is even and $(\mathsf{n}+1)\ell$ qubits when n is odd. The message size is 2ℓ bits, i.e., $\mathsf{m} = 2^{2\ell}$. Therefore, the QPIR rate is

$$R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = \begin{cases} \dfrac{2\ell}{\mathsf{n}\ell} = \dfrac{2}{\mathsf{n}} & \text{if } \mathsf{n} \text{ is even} \\ \dfrac{2\ell}{(\mathsf{n}+1)\ell} = \dfrac{2}{\mathsf{n}+1} & \text{if } \mathsf{n} \text{ is odd.} \end{cases} \tag{6.19}$$

Moreover, the sequence $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}$ of our protocols for $\mathsf{m}_\ell := 2^{2\ell}$ achieves the negligible upload cost with respect to the download cost, i.e.,

$$\lim_{\ell \to \infty} \frac{\mathsf{nf}}{\mathsf{n}\ell} = \lim_{\ell \to \infty} \frac{\mathsf{nf}}{(\mathsf{n}+1)\ell} = 0.$$

Chapter 7

Conclusion

7.1 Summary

We characterized the information-theoretic optimal rate of QPIRs by deriving the symmetric and non-symmetric QPIR capacities for non-colluding and colluding servers. As a model of QPIR protocol, we considered the case where each of the multiple servers contains a copy of all classical messages, the servers share prior entanglement, and the user uploads classical queries to the servers and downloads quantum answers from the servers. For a precise analysis of the capacities, we defined two kinds of QPIR capacities for each model: asymptotic and exact security-constrained capacities with the upload constraints.

Chapter 3 proved that the symmetric and non-symmetric QPIR capacities are 1 for any security constraints and any upload constraint. We constructed a capacity-achieving rate-one protocol with only two servers when the message size is the square of an arbitrary integer. The converse bound is proved by focusing on the download step of QPIR protocols. Furthermore, Chapter 4 also proved the capacity of multi-round QPIR is also 1 by the weak converse bound.

Chapter 5 discussed symmetric and non-symmetric t-private QPIR. In t-private QPIR, the protocol needs to guarantee the user t-secrecy in which any collection of t queries contains no information of the user's request. When the number of colluding servers t is less than or equal to a half of the number of servers n, the capacities are exactly 1 whether considering the security conditions or not and if $\mathsf{t} > \mathsf{n}/2$, the capacities are $2(\mathsf{n}-\mathsf{t})/\mathsf{n}$ with some secu-

rity assumptions. For the proof of the capacities, we constructed a t-private QPIR protocol with perfect security conditions by the stabilizer formalism. We also derived the converse bounds, which complete the optimality of our protocol.

Chapter 6 constructed a symmetric $(\mathsf{n}-1)$-private QPIR protocol with bipartite entangled states. The protocol has the QPIR rate $\lceil \mathsf{n}/2 \rceil^{-1}$, which implies that it is capacity-achieving for an even number of servers n. We constructed the protocol by using quantum teleportation and the two-sum transmission protocol repetitively.

7.2 Open problems

It is an interesting open problem whether QPIR without prior entanglement also has an advantage over the classical PIR counterparts. This thesis has considered QPIR under the assumption of prior entanglement and the QPIR capacities with prior entanglement are strictly greater than the classical PIR capacities. The QPIR capacities without prior entanglement lie between the QPIR capacities of this thesis and the classical PIR capacities. Therefore, it should be studied whether the quantum PIR capacity is strictly higher than the classical PIR capacity even without prior entanglement.

In Chapter 3, we assumed that the maximally entangled state can be shared by several servers. That is, we have made no restriction for prior entanglement. This setting is similar to the original studies [86, 87] for the entanglement-assisted classical capacity for a noisy quantum channel because they have no restriction for prior entanglement. A recent paper [88] derived the entanglement-assisted classical capacity for a noisy quantum channel when prior entanglement is limited. For the extension, the paper [88] 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 the servers to the 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 converse bounds. 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.

In Chapter 5, we only considered t-private QPIR with the most trivial security model that the user and the servers follow the protocol and do not deviate from the protocol. Thus, adversarial models as Section 3.2.3 need to be discussed. t-Private QPIR capacity should also be discussed for the multi-round case.

Following the capacity results [26, 28, 29, 36, 38] of classical PIRs, there have been many extensions of classical PIR studies. PIR with coded storage [31, 32, 89], the single-server PIR with weak privacy [90], and the single-server PIR with side information [91, 92]. There have also been approaches to apply the classical PIR to other problems, e.g., matrix multiplication [93] and private set intersection [94]. The quantum extensions of these results are also interesting open problems.

Bibliography

[5] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *Journal of the ACM*, 45(6):965-981, 1998. Earlier version in FOCS'95.

[6] M. O. Rabin, "How to exchange secrets with oblivious transfer," *Technical Report TR-81*, Harvard University, 1981.

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

[8] J. Kilian, "Founding crytpography on oblivious transfer," *Proc. 1988 ACM Annual Symposium on Theory of Computing*, p. 20.

[9] Y. Ishai, M. Prabhakaran, and A. Sahai, "Founding Cryptography on Oblivious Transfer - Efficiently," CRYPTO, pp. 572–591, 2008.

[10] A. Shamir, "How to share a secret," *Communications of the ACM,* 22:612–613, 1979.

[11] A. Beimel, Y. Ishai, E. Kushilevitz, and I. Orlov, "Share Conversion and Private Information Retrieval," *Proceedings of the 27th Annual Conference on Computational Complexity,* pp. 258–268, 2012.

[12] O. Goldreich, H. Karloff, L. Schulman, and L. Trevisan, "Lower bounds for linear locally decodable codes and private information retrieval," *Proceedings of 17th IEEE Conference on Computational Complexity,* pp. 175–183, 2002.

[13] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," *Proceedings of 32nd ACM STOC,* pp. 80–86, 2000.

[14] O. Barkol, Y. Ishai, and E. Weinreb, "On locally decodable codes, self-correctable codes, and t-private PIR," *Algorithmica,* vol. 58, no. 4, pp. 831–859, 2010.

[15] S. Yekhanin, "Towards 3-query locally decodable codes of subexponential length," 39th STOC, 2007, pp. 266–274.

[16] E. Kushilevitz, R. Ostrovsky "Replication is not needed: single database, computationally-private information retrieval," *Proceedings of the 38th Annual Symposium on Foundations of Computer Science,* Miami Beach, Florida, USA: IEEE Computer Society, pp. 364–373, 1997.

[17] C. Cachin, S. Micali, and M. Stadler, "Computationally Private Information Retrieval with Polylogarithmic Communication," *Stern J. (eds) Advances in Cryptology - EUROCRYPT 1999, Lecture Notes in Computer Science, Springer,* Berlin, Heidelberg, vol 1592, pp. 402–414, 1999.

[18] H. Lipmaa, "First CPIR Protocol with Data-Dependent Computation," *Proceedings of the 12th International Conference on Information Security and Cryptology,* pp. 193–210, 2010.

[19] A. Beimel and Y. Stahl, "Robust information-theoretic private information retrieval," *Proceedings of the 3rd International Conference on Security in Communication Networks (SCN'02)*, pp. 326–341, 2003.

[20] C. Devet, I. Goldberg, and N. Heninger, "Optimally Robust Private Information Retrieval," *21st USENIX Security Symposium*, August 2012.

[21] Y. Ishai and E. Kushilevitz, "Improved upper bounds on information theoretic private information retrieval," *Proc. of the 31th STOC,* pp. 79–88. 1999.

[22] A. Beimel, Y. Ishai "Information-Theoretic Private Information Retrieval: A Unified Construction," *In: Orejas F., Spirakis P.G., van Leeuwen J. (eds) Automata, Languages and Programming. ICALP 2001,* 2001.

[23] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. "Protecting data privacy in private information retrieval schemes," *Journal of Computer and Systems Sciences*, 60(3):592–629, 2000. Earlier version in STOC 98.

[24] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.,* 27, 623–656 (1948).

[25] T. H. Chan, S.-W. Ho, and H. Yamamoto, "Private Information Retrieval for Coded Storage," *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, pp. 2842–2846, 2015.

[26] H. Sun and S. Jafar, "The Capacity of Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, 2017.

[27] C. Tian, H. Sun, and J. Chen, "Capacity-Achieving Private Information Retrieval Codes with Optimal Message Size and Upload Cost," *IEEE Transactions on Information Theory,* vol. 65, no. 11, pp. 7613-7627, 2019.

[28] H. Sun and S. Jafar, "The Capacity of Symmetric Private Information Retrieval," 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1–5.

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

[30] Q. Wang and M. Skoglund, "Secure Symmetric Private Information Retrieval from Colluding Databases with Adversaries," *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1083–1090, 2017.

[31] K. Banawan and S. Ulukus, "The Capacity of Private Information Retrieval from Coded Databases," *IEEE Transactions on Information Theory*, vol. 64, no. 3, 2018.

[32] 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.

[33] S. Kumar, H.-Y. Lin, E. Rosnes, and A. Graell i Amat, "Achieving maximum distance separable private information retrieval capacity with linear codes," *IEEE Transactions on Information Theory*, vol. 65, no. 3, pp. 4243–4273, 2019.

[34] H.-Y. Lin, S. Kumar, E. Rosnes, and A. Graell i Amat, "An MDS-PIR capacity-achieving protocol for distributed storage using non-MDS linear codes," *Proc. IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, Jun. 17-22, 2018.

[35] L. Holzbaur, R. Freij-Hollanti, C. Hollanti "On the Capacity of Private Information Retrieval from Coded, Colluding, and Adversarial Servers," *Proceedings of IEEE Information Theory Workshop*, 2019.

[36] Q. Wang and M. Skoglund, "Symmetric private information retrieval for MDS coded distributed storage," *Proceedings of 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, May 2017.

[37] L. Holzbaur, R. Freij-Hollanti, J. Li, C. Hollanti, "Towards the Capacity of Private Information Retrieval from Coded and Colluding Servers," *arXiv:1903.12552 [cs.IT]*, 2019.

[38] H. Sun and S. A. Jafar, "Multiround Private Information Retrieval: Capacity and Storage Overhead," *IEEE Transactions on Information Theory*, vol. 64, no. 8, pp. 5743–5754, 2018.

[39] R. Tandon, "The capacity of cache aided private information retrieval," *Proceedings of 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1078–1082, 2017.

[40] K. Banawan and S. Ulukus, "The capacity of private information retrieval from byzantine and colluding databases," *IEEE Transactions on Information Theory*, vol. 65, no. 2, pp. 1206–1219, 2019.

[41] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,* vol. 175, pp. 8, 1984.

[42] A. Ekert "Quantum cryptography based on Bell's theorem," *Physical Review Letters,* 67: 661–663, 1991.

[43] J. Watrous, "Zero-Knowledge against Quantum Attacks," *SIAM Journal on Computing,* 39 (1): 25–58, 2009.

[44] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum Fingerprinting." *Physical Review Letters,* 87 (16): 167902, 2001.

[45] C. Crepeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," in Proc. Eurocrypt 2005, pp. 285-301. Springer-Verlag, 2005.

[46] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, "Experimental Bit Commitment Based on Quantum Communication and Special Relativity," *Physical Review Letters,* 111 (18): 180504, 2013.

[47] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Physical Review A* 84, 022313, 2011.

[48] F. Le Gall, "Quantum Private Information Retrieval with Sublinear Communication Complexity," *Theory of Computing*, 8(16):369–374, 2012.

[49] I. Kerenidis, M. Laurière, F. Le Gall, and M. Rennela, "Information cost of quantum communication protocols," *Quantum information & computation,* 16(3-4):181–196, 2016.

[50] Ä. Baumeler and A. Broadbent, "Quantum Private Information Retrieval has linear communication complexity," *Journal of Cryptology*, vol. 28, issue 1, pp. 161–175, 2015.

[51] I. Kerenidis and R. de Wolf. "Exponential lower bound for 2-query locally decodable codes via a quantum argument," Proceedings of 35th ACM STOC, pp. 106–115, 2003.

[52] I. Kerenidis and R. de Wolf, "Quantum symmetrically-private information retrieval," *Information Processing Letters*, vol. 90, pp. 109–114, 2004.

[53] D. Aharonov, Z. Brakerski, K.-M. Chung, A. Green, C.-Y. Lai, O. Sattath, "On Quantum Advantage in Information Theoretic Single-Server PIR," *Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11478. Springer, Cham*, 2019.

[54] W. Kon and C. Lim, "Provably-secure symmetric private information retrieval with quantum cryptography," *arXiv:2004.13921 [quant-ph],* 2020.

[55] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti, "Quantum Private Information Retrieval from MDS-coded and Colluding Servers," *IEEE Journal on Selected Areas in Information Theory,* doi: 10.1109/JSAIT.2020.3015089.

[56] R. M. Fano, Transmission of Information: A Statistical Theory of Communication, the M.I.T. Press and John Wiley and Sons, New York & London, 1961.

[57] M. S. Pinsker, Information and Information Stability of Random Variables and Processes, San Francisco: Holden-Day, CA, 1964. (Originally published in Russian in 1960.)

[58] M. Fannes, "A continuity property of the entropy density for spin lattice systems," *Communications in Mathematical Physics,* 31, 291–294, 1973.

[59] R. Alicki and M. Fannes, "Continuity of quantum mutual information," *J. of Phys. A: Math. and Gen.,* 37(5):L55–L57, 2004.

[60] D. Petz. "Quasi-entropies for finite quantum systems," *Reports on Mathematical Physics,* 23.1, pp. 57–65, 1986.

[61] G.M. D'Ariano and P. Lo Presti and M.F. Sacchi, "Bell Measurements and Observables," *Physics Letters A* 272, 32 (2000).

[62] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory,* vol. 2, no. 3, pp. 8–19, 1956.

[63] D. Ding, Y. Quek, P. W. Shor, M. M. Wilde "Entropy Bound for the Classical Capacity of a Quantum Channel Assisted by Classical Feedback," *Proceedings of the 2019 IEEE International Symposium on Information Theory,* Paris, France, pp. 250–254, 2019.

[64] N. Cai and M. Hayashi, "Secure Network Code for Adaptive and Active Attacks with No-Randomness in Intermediate Nodes," *IEEE Transactions on Information Theory*, vol. 66, 1428–1448, 2020.

[65] M. Hayashi, *Quantum Information Theory: Mathematical Foundation,* Graduate Texts in Physics, Springer, (Second edition of Quantum Information: An Introduction Springer), 2017.

[66] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information,* Cambridge: Cambridge University Press, 2000.

[67] M. M. Wilde, *Quantum Information Theory,* Cambridge: Cambridge University Press, 2013.

[68] M. Ozawa, "Quantum measuring processes of continuous observables," *J. Math. Phys.,* 25: 79–87, 1984.

[69] M. Ozawa, "Uncertainty Relations for Noise and Disturbance in Generalized Quantum Measurements," *Annals of Physics,* 311 (2), 350-416, 2004.

[70] F. Buscemi, M. Hall, M. Ozawa, M. Wilde, "Noise and disturbance in quantum measurements: an information-theoretic approach," *Physical review letters,* 112 (5), 050401

[71] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over gf (4)," *IEEE Transactions on Information Theory,* vol. 44, no. 4, pp. 1369–1387, 1998.

[72] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory,* vol. 47, no. 7, pp. 3065–3072, 2001.

[73] A. Ketkar, A. Klappenecker, S. Kumar and P. Sarvepalli, "Nonbinary stablizer codes over finite fields," *IEEE Transactions on Information Theory,* vol. 52, no. 11, pp. 4892–4914, 2006.

[74] M. Hayashi, *Group Representation for Quantum Theory,* Cham, Switzerland: Springer, 2017.

[75] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam: North-Holland, 1977.

[76] R. Lidl and H. Niederreiter, *Finite Fields (2nd ed., Encyclopedia of Mathematics and its Applications),* Cambridge: Cambridge University Press, 1996.

[77] R. C. Singleton, "Maximum distance q-nary codes," *IEEE Transactions on Information Theory,* 10 (2): 116–118.

[78] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," AT & T Bell Labs. Tech. J., vol. 63, pp. 2135 – 2157, 1984.

[79] N. Cai and R. W. Yeung, "Secure Network Coding on a Wiretap Network," IEEE Trans. Inform. Theory, vol. 57, no. 1, 424–435, 2011.

[80] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, 70(13):1895–1899, 1993.

[81] C. Bennett and S. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, 69 (20): 2881, 1992.

[82] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Physical Review Letters,* 80 (6): 1121–1125, 1998.

[83] H. Krauter, D. Salart, C. A. Muschik, J. M. Petersen, Heng Shen, T. Fernholz, and E. S. Polzik, "Deterministic quantum teleportation between distant atomic objects," *Nature Physics,* vol. 9, issue 7, pp. 400–404, 2013.

[84] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense Coding in Experimental Quantum Communication," *Physical Review Letters,* 76, 4656, 1996.

[85] B. P. Williams, R. J. Sadlier, and T. S. Humble, "Superdense Coding over Optical Fiber Links with Complete Bell-State Measurements," *Physical Review Letters,* 118(5), 2017.

[86] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Physical Review Letters*, vol. 83, no. 15, p. 3081, 1999.

[87] 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 Transactions on Information Theory*, vol. 48, no. 10, pp. 2637–2655, 2002.

[88] K. Wang and M. Hayashi, "Permutation Enhances Classical Communication Assisted by Entangled States," *Proc. 2020 IEEE Int. Symp. Information Theory (ISIT 2020)*, Los Angeles, California, USA, 2020.

[89] K. Banawan, B. Arasli and S. Ulukus, "Improved Storage for Efficient Private Information Retrieval," *2019 IEEE Information Theory Workshop (ITW),* Visby, Sweden, 2019.

[90] H. Lin, S. Kumar, E. Rosnes, A. G. i. Amat and E. Yaakobi, "The Capacity of Single-Server Weakly-Private Information Retrieval," *2020 IEEE International Symposium on Information Theory (ISIT),* Los Angeles, CA, USA, 2020.

[91] F. Kazemi, E. Karimi, A. Heidarzadeh and A. Sprintson, "Single-Server Single-Message Online Private Information Retrieval with Side Information," *2019 IEEE International Symposium on Information Theory (ISIT),* Paris, France, 2019.

[92] S. Li, "Single-server Multi-message Private Information Retrieval with Side Information: the General Cases," *2020 IEEE International Symposium on Information Theory (ISIT),* Los Angeles, CA, USA, 2020.

[93] W. Chang and R. Tandon, "On the Upload versus Download Cost for Secure and Private Matrix Multiplication," *2019 IEEE Information Theory Workshop (ITW),* Visby, Sweden, 2019.

[94] Z. Wang, K. Banawan and S. Ulukus, "Private Set Intersection Using Multi-Message Symmetric Private Information Retrieval," *2020 IEEE International Symposium on Information Theory (ISIT),* Los Angeles, CA, USA, 2020.

Appendix A

Proof of Proposition 3.2

First, we prepare the following notations:

$$\begin{aligned}
\tilde{\rho} &:= \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} |w\rangle\langle w| \otimes \rho_w, \\
\tilde{\sigma} &:= \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} |w\rangle\langle w| \otimes \sigma, \\
\tilde{Y} &:= \sum_{w=0}^{\mathsf{m}-1} |w\rangle\langle w| \otimes Y(w), \\
\mathcal{M} &= \{\tilde{Y}, I - \tilde{Y}\}.
\end{aligned}$$

With these notations, we have

$$\operatorname{Tr} \tilde{\rho}\tilde{Y} = \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \operatorname{Tr} \rho_w Y(w) = 1 - P_{\mathrm{err}}, \tag{A.1}$$

$$\operatorname{Tr} \tilde{\sigma}\tilde{Y} = \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \operatorname{Tr} \sigma Y(w) \le \frac{1}{\mathsf{m}} \operatorname{Tr} \sigma \sum_{w=0}^{\mathsf{m}} Y(w) = \frac{1}{\mathsf{m}}. \tag{A.2}$$

Combining (2.23), (A.1), and (A.2), we derive the desired inequality (3.35) of Proposition 3.2 as

$$\begin{aligned}
&(1 - P_{\mathrm{err}})^{1+s} \mathsf{m}^{-s} \\
&\overset{(a)}{\le} (\operatorname{Tr} \tilde{\rho}\tilde{Y})^{1+s} (\operatorname{Tr} \tilde{\sigma}\tilde{Y})^{-s} \\
&\le (\operatorname{Tr} \tilde{\rho}\tilde{Y})^{1+s} (\operatorname{Tr} \tilde{\sigma}\tilde{Y})^{-s} + (1 - \operatorname{Tr} \tilde{\rho}\tilde{Y})^{1+s} (1 - \operatorname{Tr} \tilde{\sigma}\tilde{Y})^{-s}
\end{aligned}$$

$$
\begin{aligned}
&= \exp\bigl(sD_{1+s}(P_{\tilde{\rho}}^{\mathcal{M}} \| P_{\tilde{\sigma}}^{\mathcal{M}})\bigr) \\
&\overset{(b)}{\leq} \exp(sD_{1+s}(\tilde{\rho} \| \tilde{\sigma})) \\
&= \operatorname{Tr} \tilde{\rho}^{1+s} \tilde{\sigma}^{-s} = \frac{1}{\mathsf{m}} \sum_{w=0}^{\mathsf{m}-1} \operatorname{Tr} \rho_w^{1+s} \sigma^{-s},
\end{aligned}
$$

where (a) is from (A.1) and (A.2) and (b) is from (2.23).

Appendix B

Proof of Proposition 4.2

For the proof of Proposition 4.2, we follow the proof of [63, Theorem 4]. Before the proof, we prepare two lemmas from [63].

Lemma B.1 ([63, Lemma 2]). *Let τ_{WFAB} be a classical-quantum state such that*

$$\tau_{WFAB} = \sum_{w,f} p(w,f)|w,f\rangle\langle w,f| \otimes \tau_{AB|wf}, \tag{B.1}$$

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

$$I(W;B'FX) + H(B'|WFX) \tag{B.2}$$
$$\leq I(W;BF) + H(B|WF). \tag{B.3}$$

Lemma B.2 ([63, Lemma 3]). *Let τ_{WFAB} be a classical-quantum state defined in (B.1). Then*

$$I(W;ABF) + H(AB|WF) \tag{B.4}$$
$$\leq H(A) + I(W;BF) + H(B|WF). \tag{B.5}$$

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

Now, we prove Proposition 4.2. First, we have

$$(1-\varepsilon)\log \mathsf{m} \overset{(a)}{\leq} I(M;W) + h_2(\varepsilon) \tag{B.6}$$

$$\overset{(b)}{\leq} I(M;\mathcal{A}^{\mathsf{r}}\mathcal{C}^{\mathsf{r}}Q^{[\mathsf{r}]}) + h_2(\varepsilon), \tag{B.7}$$

where (a) is from Fano's inequality (2.8)

$$H(M|W) \leq \varepsilon \log \mathsf{m} + h_2(\varepsilon) \tag{B.8}$$

and the uniform distribution of M, and (b) is from the data-processing inequality 2.29 for the decoding POVM. Then, it is enough to derive the inequality

$$I(W;\mathcal{A}^{\mathsf{r}}\mathcal{C}^{\mathsf{r}}Q^{[\mathsf{r}]}) \leq \sum_{i=1}^{\mathsf{r}} H(\rho_W^{\mathcal{A}^i}) \tag{B.9}$$

for the proof of Proposition 4.2.

To derive (B.9), we apply Lemma B.1 and Lemma B.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 B.1 for $(W, F, A, B, A', B', X) := (M, Q^{[i-1]}, \mathcal{B}^{i-1}, \mathcal{A}^{i-1} \otimes \mathcal{C}^{i-1}, \mathcal{A}^i \otimes \mathcal{B}^i, \mathcal{C}^i, Q^i)$:

$$\begin{aligned} &I(M;\mathcal{C}^iQ^{[i]}) + H(\mathcal{C}^i|MQ^{[i]}) \\ &\leq I(M;\mathcal{A}^{i-1}\mathcal{C}^{i-1}Q^{[i-1]}) + H(\mathcal{A}^{i-1}\mathcal{C}^{i-1}|MQ^{[i-1]}). \end{aligned}$$

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

$$\begin{aligned} &I(M;\mathcal{A}^i\mathcal{C}^iQ^{[i]}) + H(\mathcal{A}^i\mathcal{C}^i|MQ^{[i]}) \\ &\leq H(\mathcal{A}^i) + I(M;\mathcal{C}^iQ^{[i]}) + H(\mathcal{C}^i|MQ^{[i]}). \end{aligned} \tag{B.10}$$

Combining the above two inequalities, we have

$$\begin{aligned} &I(M;\mathcal{A}^i\mathcal{C}^iQ^{[i]}) + H(\mathcal{A}^i\mathcal{C}^i|MQ^{[i]}) \\ &\leq H(\mathcal{A}^i) + I(M;\mathcal{A}^{i-1}\mathcal{C}^{i-1}Q^{[i-1]}) + H(\mathcal{A}^{i-1}\mathcal{C}^{i-1}|MQ^{[i-1]}) \end{aligned} \tag{B.11}$$

Applying the inequality (B.11) recursively, we obtain the desired inequality (B.9) of Proposition 4.2 as

$$\begin{aligned} &I(M;\mathcal{A}^{\mathsf{r}}\mathcal{C}^{\mathsf{r}}Q^{[\mathsf{r}]}) \\ &\leq I(M;\mathcal{A}^{\mathsf{r}}\mathcal{C}^{\mathsf{r}}Q^{[\mathsf{r}]}) + H(\mathcal{A}^{\mathsf{r}}\mathcal{C}^{\mathsf{r}}|MQ^{[\mathsf{r}]}) \\ &\overset{(c)}{\leq} \sum_{i=2}^{\mathsf{r}} H(\mathcal{A}^i) + I(M;\mathcal{A}^1\mathcal{C}^1Q^1) + H(\mathcal{A}^1\mathcal{C}^1|MQ^1) \\ &\overset{(d)}{\leq} \sum_{i=1}^{\mathsf{r}} H(\mathcal{A}^i) + I(M;\mathcal{C}^1Q^1) + H(\mathcal{C}^1|MQ^1) \\ &\overset{(e)}{=} \sum_{i=1}^{\mathsf{r}} H(\mathcal{A}^i), \end{aligned}$$

where (c) is derived by applying (B.11) recursively for $i = \mathsf{r}, \mathsf{r}-1, \ldots, 2$, (d) is from (B.10), and (e) is obtained as follows: $I(M;\mathcal{C}^1Q^1) = 0$ because the receiver prepares the state of $\mathcal{C}^1 \otimes Q^1$ independently of the sender's message M, and $H(\mathcal{C}^1|MQ^1) = 0$ since the initial state of the local register $\mathcal{C}^1$ is a pure state.

Appendix C

QPIR capacity with average security measures

In Section 5.1.1, we defined the security measures as the worst-case definition. In this appendix, we show that the capacity does not changes even if we change the definition of the security measures as for the average case.

Define the average security measures as

$$\tilde{P}_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \Pr_W[W \neq M_K | MQK] \tag{C.1}$$

$$\tilde{S}_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq I(M_K^c; \mathcal{A}|QK)_{\rho_{MQ}} \tag{C.2}$$

$$\tilde{S}_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) \coloneqq \mathbb{E}_{\pi \in \mathsf{S}_\mathsf{n}} I(K; Q_{\pi,\mathsf{t}}), \tag{C.3}$$

and QPIR capacities $\tilde{C}_{\mathrm{exact},\mathsf{t}}^{\alpha,\beta,\gamma,\theta}$ and $\tilde{C}_{\mathrm{asymp},\mathsf{t}}^{\alpha,\beta,\gamma,\theta}$ are defined the same as (5.5) and (5.6) except that the security measures $P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$, $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$, $S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ are replaced by $\tilde{P}_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$, $\tilde{S}_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$, $\tilde{S}_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$. Then, similar to Theorem 5.1, the average capacity is derived as

$$\tilde{C}_{\mathrm{asymp},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} = \tilde{C}_{\mathrm{exact},\mathsf{t}}^{\alpha,\beta,\gamma,\theta} = 1 \qquad \text{if } 1 \leq \mathsf{t} \leq \frac{\mathsf{n}}{2}, \tag{C.4}$$

$$\tilde{C}_{\mathrm{asymp},\mathsf{t}}^{0,\beta,0,\theta} = \tilde{C}_{\mathrm{exact},\mathsf{t}}^{\alpha,0,0,\theta} = \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \qquad \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} < \mathsf{n}. \tag{C.5}$$

For the achievability proof of (C.4) and (C.5), the QPIR protocol in Section 5.3 achieves the capacity.

The converse bounds are also proved similar to the case of the worst-case security. The converse bounds are written for any $\alpha \in [0, 1)$ and any

$\beta, \gamma, \theta \in [0, \infty)$ as

$$\tilde{C}^{\alpha,\beta,\gamma,\theta}_{\mathrm{asymp},\mathsf{t}} \le 1 \qquad \text{if } 1 \le \mathsf{t} \le \frac{\mathsf{n}}{2}, \tag{C.6}$$

$$\tilde{C}^{\alpha,0,0,\theta}_{\mathrm{exact},\mathsf{t}} \le \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \qquad \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} < \mathsf{n}, \tag{C.7}$$

$$\tilde{C}^{0,\beta,0,\theta}_{\mathrm{asymp},\mathsf{t}} \le \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} \qquad \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} < \mathsf{n}. \tag{C.8}$$

First, the converse bound (C.8) is proved by the same steps as Section 5.4 except for the following part. In Section 5.4, Eq. (5.77) is written as

$$\begin{aligned}&(1 - P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}))\log \mathsf{m} \\ &\le D(R_q \| S_q) + h_2\Big(P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big).\end{aligned}$$

and by taking the expectation of (5.77) with respect to Q, we obtain (5.79). Similarly, we take the expectation of (5.77) with respect to K, Q and then, we obtain

$$\begin{aligned}&(1 - \tilde{P}_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}))\log \mathsf{m} \\ &\le \mathbb{E}_{K,Q} D(R_q \| S_q | K) + h_2\Big(\tilde{P}_{\mathrm{err}}(\Psi^{(\mathsf{m})}_{\mathrm{QPIR}})\Big).\end{aligned}$$

Then, by the similar steps as Section 5.4, the converse bound (C.8) is proved.

For the converse bounds (C.6) and (C.7), in the last steps of the proofs in Sections 5.4.3 and 5.4.4, we replace (5.86) and (5.91) by

$$1 - \tilde{P}_{\mathrm{err}}(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}) \le 1 - \inf_{k,q} P_{\mathrm{err},k,q}(\Psi^{(\mathsf{m}_\ell)}_{\mathrm{QPIR}}). \tag{C.9}$$

Then, the converse bounds (C.6) and (C.7) are proved in the same way.

Appendix D

Proof of Proposition 5.1

We concretely construct the subgroup $S(\mathrm{V})$ as follows. From (5.12), all elements of $S(\mathrm{V})$ are commutative regardless of the choice of $c_{\mathbf{v}}$. Since $I \in S(\mathrm{V})$, we set $\mathbf{W}(\mathbf{0}) = I$, i.e., $c_{\mathbf{0}} = 1$. Then, it is enough to choose $c_{\mathbf{v}}$ so that $S(\mathrm{V})$ satisfies the closure for the multiplication.

We choose $\{c_{\mathbf{v}} \in \mathbb{C} \mid \mathbf{v} \in \mathrm{V}\}$ as follows. For a fixed basis $\mathbf{v}_1, \ldots, \mathbf{v}_d$ of V, we choose $c_{\mathbf{v}_i}$ as follows: if $p > 2$, choose $c_{\mathbf{v}_i}$ as a p-th root of unity, i.e., $c_{\mathbf{v}_i} = \omega^k$ for some integer k; if $p = 2$, choose $c_{\mathbf{v}_i}$ as

$$c_{\mathbf{v}_i} = \pm\sqrt{-1}^{\langle \mathbf{b}_i, \mathbf{a}_i \rangle} = \begin{cases} \pm 1 & \text{if } \langle \mathbf{b}_i, \mathbf{a}_i \rangle = 0, \\ \pm\sqrt{-1} & \text{if } \langle \mathbf{b}_i, \mathbf{a}_i \rangle = 1, \end{cases}$$

where $\mathbf{a}_i, \mathbf{b}_i$ are vectors in $\mathbb{F}_q^n$ such that $(\mathbf{a}_i, \mathbf{b}_i) = \mathbf{v}_i$. For any $\mathbf{v} = \sum_i a_i \mathbf{v}_i \in \mathrm{V}$, we choose $c_{\mathbf{v}}$ by the relation

$$\mathbf{W}(\mathbf{v}) = \mathbf{W}(\mathbf{v}_1)^{a_1} \cdots \mathbf{W}(\mathbf{v}_d)^{a_d}. \tag{D.1}$$

Next, we prove the closure for the multiplication in $S(\mathrm{V})$ by the above choice of $c_{\mathbf{v}}$. For any basis element $\mathbf{v}_i$, we have

$$\mathbf{W}(\mathbf{v}_i)^p = c_{\mathbf{v}_i}^p \tilde{\mathbf{W}}(\mathbf{v}_i)^p \overset{(a)}{=} c_{\mathbf{v}_i}^p \omega^{p(p-1)\langle \mathbf{b}_i, \mathbf{a}_i \rangle / 2} \tilde{\mathbf{W}}(p\mathbf{v}_i) = c_{\mathbf{v}_i}^p I = I. \tag{D.2}$$

where (a) follows from (5.13). Then, we can confirm the closure for the multiplication as

$$\begin{aligned} \mathbf{W}(\mathbf{v})\mathbf{W}(\mathbf{v}') &= \mathbf{W}(\mathbf{v}_1)^{a_1} \cdots \mathbf{W}(\mathbf{v}_d)^{a_d} \mathbf{W}(\mathbf{v}_1)^{a'_1} \cdots \mathbf{W}(\mathbf{v}_d)^{a'_d} && \text{(D.3)} \\ &= \mathbf{W}(\mathbf{v}_1)^{a_1 + a'_1} \cdots \mathbf{W}(\mathbf{v}_d)^{a_d + a'_d} && \text{(D.4)} \\ &= \mathbf{W}(\mathbf{v}_1)^{a_1 + a'_1 \bmod p} \cdots \mathbf{W}(\mathbf{v}_d)^{a_d + a'_d \bmod p} && \text{(D.5)} \\ &= \mathbf{W}(\mathbf{v} + \mathbf{v}') && \text{(D.6)} \end{aligned}$$

for any $\mathbf{v}, \mathbf{v}' \in \mathrm{V}$, where the equality (D.4) is from the commutative property of $S(\mathrm{V})$ and the equality (D.5) is from (D.2). Thus, $S(\mathrm{V})$ is a commutative subgroup of HW_q^n not containing cI for any $c \neq 0$, i.e., a stabilizer.

Alternatively, if $p > 2$, the set $S(\mathrm{V})$ is a stabilizer by choosing $c_{(\mathbf{a},\mathbf{b})} = (\omega^{(p+1)/2})^{\langle \mathbf{a},\mathbf{b} \rangle}$ since

$$\mathbf{W}(\mathbf{a},\mathbf{b})\mathbf{W}(\mathbf{c},\mathbf{d}) = (\omega^{(p+1)/2})^{\langle (\mathbf{a},\mathbf{b}), J(\mathbf{c},\mathbf{d}) \rangle} \mathbf{W}(\mathbf{a}+\mathbf{c}, \mathbf{b}+\mathbf{d})$$

for any $(\mathbf{a},\mathbf{b}), (\mathbf{c},\mathbf{d}) \in \mathbb{F}_q^n$ and V is self-orthogonal.

Appendix E

Proof of Proposition 5.2

Let V be a self-orthogonal d-dimensional subspace of $\mathbb{F}_q^{2n}$ and $S(\mathrm{V})$ be a stabilizer defined by (5.14). Notice the following facts.

Fact 1) $\mathbf{W}(\mathbf{v})\mathbf{W}(\mathbf{v}') = \mathbf{W}(\mathbf{v}+\mathbf{v}')$ for any $\mathbf{v}, \mathbf{v}' \in \mathrm{V}$ by the closure for the multiplication of $S(\mathrm{V})$,

Fact 2) All eigenvalues of $\mathbf{W}(\mathbf{v})$ are in $\{\omega^k \mid k \in \mathbb{F}_p\}$, since $(\mathbf{W}(\mathbf{v}))^p = \mathbf{W}(p\mathbf{v}) = \mathbf{W}(\mathbf{0}) = I_{q^n}$ for any $\mathbf{v} \in \mathrm{V}$.

Fact 3) All elements of $S(\mathrm{V})$ are simultaneously diagonalized, since $S(\mathrm{V})$ is a commutative group.

First, we prove 1) of the proposition. By Facts 2 and 3, we have the simultaneous decomposition of all elements $\mathbf{W}(\mathbf{v}) \in S(\mathrm{V})$ as

$$\mathbf{W}(\mathbf{v}) = \sum_{f:\mathrm{V}\to\mathbb{F}_p} \omega^{f(\mathbf{v})} P_f^{\mathrm{V}} \qquad (\forall \mathbf{v} \in \mathrm{V}), \tag{E.1}$$

where the summation is taken for all maps f from V to $\mathbb{F}_p$ and $\{P_f^{\mathrm{V}}\}$ are orthogonal projections such that

$$P_f^{\mathrm{V}} P_{f'}^{\mathrm{V}} = 0 \text{ for any } f \neq f', \tag{E.2}$$

$$\sum_{f\in\mathrm{V}^*} = I_{\mathcal{H}^{\otimes n}}. \tag{E.3}$$

Let V^* be the space of linear maps from V to $\mathbb{F}_p$. Since Fact 1 implies $\omega^{f(\mathbf{v})+f(\mathbf{v}')} P_f^{\mathrm{V}} = \omega^{f(\mathbf{v}+\mathbf{v}')} P_f^{\mathrm{V}}$ for any $\mathbf{v} \in \mathrm{V}$ and $f : \mathrm{V} \to \mathbb{F}_p$, we have $P_f^{\mathrm{V}} = 0$

for any $f \notin \mathrm{V}^*$. Thus, (E.1) is written as

$$\mathbf{W}(\mathbf{v}) = \sum_{f \in \mathrm{V}^*} \omega^{f(\mathbf{v})} P_f^{\mathrm{V}} \qquad (\forall \mathbf{v} \in \mathrm{V}). \tag{E.4}$$

Furthermore, the space V^* is isomorphic to $\mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}$ by the following identification: we identify $f \in \mathrm{V}^*$ and $[\mathbf{w}] := \mathbf{w} + \mathrm{V}^{\perp_J} \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}$ if $f(\mathbf{v}) = \langle \mathbf{v}, J\mathbf{w} \rangle$ for any $\mathbf{v} \in \mathrm{V}$. Therefore, we denote $P_{[\mathbf{w}]}^{\mathrm{V}} := P_f^{\mathrm{V}}$ if f and $[\mathbf{w}]$ are identical and Eq. (E.4) is written as

$$\mathbf{W}(\mathbf{v}) = \sum_{[\mathbf{w}] \in \mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}} \omega^{\langle \mathbf{v}, J\mathbf{w} \rangle} P_{[\mathbf{w}]}^{\mathrm{V}} \qquad (\forall \mathbf{v} \in \mathrm{V}), \tag{E.5}$$

which implies 1) of the proposition. The uniqueness of the decomposition (E.5) is from the uniqueness of the eigendecomposition.

Next, we prove 2) of the proposition. Let $\mathcal{H}_{[\mathbf{w}]}^{\mathrm{V}} := \operatorname{Im} P_{[\mathbf{w}]}^{\mathrm{V}}$. For any $\mathbf{v} \in \mathrm{V}$, we have

$$\mathbf{W}(\mathbf{v})\mathbf{W}(\mathbf{w})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} \overset{(a)}{=} \omega^{\langle \mathbf{v}, J\mathbf{w} \rangle} \mathbf{W}(\mathbf{w})\mathbf{W}(\mathbf{v})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} \tag{E.6}$$

$$\overset{(b)}{=} \omega^{\langle \mathbf{v}, J(\mathbf{w}+\mathbf{w}') \rangle} \mathbf{W}(\mathbf{w})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}}, \tag{E.7}$$

where (a) is from

$$\mathbf{W}(\mathbf{v})\mathbf{W}(\mathbf{w}) = \omega^{\langle \mathbf{v}, J\mathbf{w} \rangle} \mathbf{W}(\mathbf{w})\mathbf{W}(\mathbf{v}),$$

which follows from (5.12), and (b) is from

$$\mathbf{W}(\mathbf{v})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} = \omega^{\langle \mathbf{v}, J\mathbf{w}' \rangle} \mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}},$$

which follows from (E.5). Since (E.7) implies that $\mathbf{W}(\mathbf{v})$ maps $\mathbf{W}(\mathbf{w})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}}$ to $\omega^{\langle \mathbf{v}, J(\mathbf{w}+\mathbf{w}') \rangle} \mathbf{W}(\mathbf{w})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}}$, we have $\mathbf{W}(\mathbf{w})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} \subseteq \mathcal{H}_{[\mathbf{w}+\mathbf{w}']}^{\mathrm{V}}$ from (E.5). Conversely, we also have $\mathbf{W}(-\mathbf{w})\mathcal{H}_{[\mathbf{w}+\mathbf{w}']}^{\mathrm{V}} \subseteq \mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}}$. Thus, we have $\dim \mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} = \dim \mathcal{H}_{[\mathbf{w}+\mathbf{w}']}^{\mathrm{V}}$ and therefore, obtain the desired relation $\mathbf{W}(\mathbf{w})\mathcal{H}_{[\mathbf{w}']}^{\mathrm{V}} = \mathcal{H}_{[\mathbf{w}+\mathbf{w}']}^{\mathrm{V}}$.

Lastly, we prove 3) of the proposition. By 2) of the proposition, all spaces $\mathcal{H}_{[\mathbf{w}]}^{\mathrm{V}}$ have the same dimension. Therefore, we have

$$\dim \mathcal{H}_{[\mathbf{w}]}^{\mathrm{V}} = \frac{\dim \mathcal{H}^{\otimes n}}{|\mathbb{F}_q^{2n}/\mathrm{V}^{\perp_J}|} = \frac{\dim \mathcal{H}^{\otimes n}}{|\mathrm{V}|} = q^{n-d}.$$

Appendix F

Simple proof of Lemma 5.4 with perfect security

We give the proof of Corollary 5.2, i.e., Lemma 5.4 with perfect secrecy. Due to the user secrecy $S_{\mathrm{user}}^{(\mathsf{t})}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 0$, the uploaded information Q_{t} is independent of K. Since the $\rho_{MQ_{\mathsf{t}}}$ is determined by Q_{t}, we have

$$I(M_k; \mathcal{A}_{\pi(\mathsf{t})}|Q_{\mathsf{t}}, K = k)_{\rho_{MQ_{\mathsf{t}}}} = I(M_k; \mathcal{A}_{\pi(\mathsf{t})}|Q_{\mathsf{t}}, K = i)_{\rho_{MQ_{\mathsf{t}}}}$$

for any $i \neq k \in \{1, \ldots, \mathsf{f}\}$. Since server secrecy $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 0$ implies

$$I(M_k; \mathcal{A}_{\pi(\mathsf{t})}|Q_{\mathsf{t}}, K = i)_{\rho_{MQ_{\mathsf{t}}}} = 0 \quad \forall i \neq k \in \{1, \ldots, \mathsf{f}\}, \tag{F.1}$$

we have $I(M_k; \mathcal{A}_{\pi(\mathsf{t})}|Q_{\mathsf{t}}, K = k)_{\rho_{MQ_{\mathsf{t}}}} = 0$ for any $k \in \{1, \ldots, \mathsf{f}\}$, which implies Lemma 5.4.