

# Quantum Private Information Retrieval for Quantum Messages

Seunghoan Song<sup>a</sup> and Masahito Hayashi<sup>b,a</sup>

<sup>a</sup>Graduate School of Mathematics, Nagoya University

<sup>b</sup>Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology

Email: m17021a@math.nagoya-u.ac.jp & hayashi@sustech.edu.cn

**Abstract**—Quantum private information retrieval (QPIR) for quantum messages is the protocol in which a user retrieves one of the multiple quantum states from one or multiple servers without revealing which state is retrieved. We consider QPIR in two different settings: the blind setting, in which the servers contain one copy of the message states, and the visible setting, in which the servers contain the description of the message states. One trivial solution in both settings is downloading all states from the servers and the main goal of this paper is to find more efficient QPIR protocols. First, we prove that the trivial solution is optimal for one-server QPIR in the blind setting. In one-round protocols, the same optimality holds even in the visible setting. On the other hand, when the user and the server share entanglement, we prove that there exists an efficient one-server QPIR protocol in the blind setting. Furthermore, in the visible setting, we prove that it is possible to construct *symmetric* QPIR protocols in which the user obtains no information of the non-targeted messages. We construct three two-server symmetric QPIR protocols for pure states. Note that symmetric classical PIR is impossible without shared randomness unknown to the user.

## I. INTRODUCTION

*A. Backgrounds: Private information retrieval (PIR) for classical messages*

1) *Private information retrieval (PIR)*: Private information retrieval is a method to retrieve a message from a server without revealing which message is retrieved. PIR has a simple solution of downloading all messages and this trivial solution is proved to be optimal [1], i.e., the optimal communication complexity is  $O(m)$ , where  $m$  is the total number of bits in the messages. To improve the communication efficiency of PIR, there have been mainly two approaches: PIR with computational assumptions [2], [3] and PIR with multiple servers [4]–[6]. Recently, information-theoretic aspects of PIR has been extensively studied [27]–[41]. In this paper, we only focus on the one-server and multi-server PIRs without computational assumptions.

Symmetric PIR (SPIR) is PIR in which the user obtains only the targeted message but no information of the non-targeted messages. In the one-server case, SPIR is also called oblivious transfer, which is proven to be impossible even in the quantum case [7]. In the multi-server case, Gertner et al. [8] proved that SPIR is impossible, but it becomes possible if the servers share randomness.

2) *One-server quantum PIR for classical messages*: PIR has also been studied when quantum communication is allowed between the user and the server(s) [9]–[20]. Hereinafter,

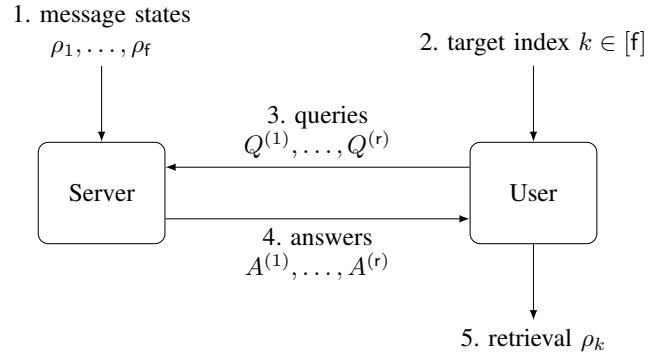


Fig. 1: One-server QPIR protocol with quantum messages. At round  $i$ , the user uploads a query  $Q^{(i)}$  and downloads an answer  $A^{(i)}$ .

we denote quantum PIR for classical messages as C-QPIR. Interestingly, when the server is honest, i.e., the server does not deviate from the protocol, Le Gall [13] proposed a C-QPIR protocol with communication complexity  $O(\sqrt{m})$ , and Kerenidis et al. [14] improved this result by  $O(\text{poly log } m)$ , where the communication in the quantum case is the total number of communicated qubits. However, when the server deviates from the protocol as far as its malicious operations are not revealed to the user, which is called *specious adversary*, Baumeler and Broadbent [12] proved that the communication complexity is at least  $O(m)$ , i.e., the trivial solution of downloading all messages is optimal also for this case. When prior entanglement is allowed between the user and the server, the communication complexity is improved by  $O(\log m)$  for the honest server model [14], but the communication complexity is also lower bounded by  $O(m)$  for the specious attack [15].

3) *Multi-server quantum PIR for classical messages*: For multi-server C-QPIR, Kerenidis and de Wolf [10] proposed a symmetric C-QPIR protocol without shared randomness. Song and Hayashi [16] derived symmetric and non-symmetric C-QPIR capacity, which is defined similar to its classical counterpart [28], [29] as the optimal communication efficiency for arbitrary-long classical messages, and proved that symmetric C-QPIR can be constructed without any communication loss if prior-entanglement among servers is allowed. They [17], [18] and Allaix et al. [19] also considered C-QPIR with colluding

TABLE I: Definition of symbols

Symbol	Definition
$m$	Total size of messages (states)
$f$	Number of messages (states)
$r$	Number of rounds in multi-round models
$n$	Number of servers in multi-server models

servers in which secrecy of the protocol is preserved even if some servers may communicate and collude. Kon and Lim [20] constructed a symmetric C-QPIR protocol with quantum-key distribution.

### B. Contribution: quantum PIR for quantum messages

Even if quantum PIR has been studied for classical messages, there has been no study of PIR for quantum messages, i.e., quantum states. This paper considers quantum PIR for quantum messages. Throughout this paper, we denote quantum PIR for quantum messages as QPIR. Downloading all quantum messages is also a trivial solution for QPIR. Intuitively, it seems reasonable to conjecture this trivial solution is optimal for QPIR. However, since the C-QPIR for the honest server has more efficient solutions than the trivial solution [13], [14], we cannot exclude the possibility of efficient one-server QPIR protocols. Furthermore, whereas the optimality proof of classical PIR [1] uses the communication transcript between the server and the user, we cannot apply the same technique because quantum states cannot be copied because of the no-cloning theorem. Thus, the first goal is to answer whether the trivial solution is also optimal QPIR under several attack models and how we can construct more efficient protocols than the trivial solution. Furthermore, it is not unknown if symmetric QPIR (QSPIR) is possible on the multiple server model.

1) *Two settings in QPIR*: QPIR can be studied in two distinct settings, called the *blind* and *visible* settings, in which quantum state compression has also been extensively studied [21]–[26]. In the blind setting, the server(s) contains quantum systems  $X_1, \dots, X_f$  with the message states  $\rho_1, \dots, \rho_f$ , respectively, but does not know the states of the systems. Due to the no-cloning theorem, the server(s) cannot generate more copies of the message states and the server's operations are independent of the message states. QPIR in the blind setting is suitable for the case where the server(s) generates the message states by some quantum algorithm and performs the QPIR task.

On the other hand, in the visible setting, the server(s) contains the descriptions of the message states. With the descriptions of quantum states, the servers can generate multiple copies of the quantum states, without the limitation of the no-cloning theorem, and apply quantum operations depending on the descriptions of the states. Since any protocol in the blind setting can be considered as a protocol in the visible setting, we can generally expect to achieve lower communication complexity in the visible setting. Even if the description of a quantum state is classical information, it is infinite-length classical information, and therefore we cannot send this

description via QPIR for classical messages. Furthermore, the visible setting is a reasonable setting for the case where the user has no ability to generate quantum states and requires the generation of the targeted state along with the QPIR task.

2) *Optimality of trivial solution for one-server QPIR*: Our first result is that the trivial solution is optimal for one-server QPIR for the honest server model. For the one-server case, the comparison of the our results and previous results are summarized in Table II. We first prove for the one-round case and then extend the result to the multi-round case. In the one-round case, we prove the optimality both for blind and visible settings, but in the multi-round case, we only prove for the blind setting. The entropic inequalities are the key instruments for the proof, and we prove and use a chain rule for the multi-round case. Since the honest server model is the weakest attack model, this result implies that the trivial solution is also optimal for any attack models.

3) *One-server QPIR protocol with prior entanglement in blind setting*: Secondly, with prior entanglement between the user and the server, we prove that there exists an efficient QPIR protocol on the honest server model. To be precise, we propose a method to construct a QPIR protocol of communication complexity  $O(f(m))$  with prior entanglement from C-QPIR protocol of communication complexity  $O(f(m))$  with prior entanglement. We construct the QPIR protocol by the combination of C-QPIR and quantum teleportation [43]. The proposed QPIR protocol inherits the security of C-QPIR. With this property, on the honest server model with prior entanglement, there exists a QPIR protocol of communication complexity  $O(\log m)$  since there exist C-QPIR protocols of communication complexity  $O(\log m)$  by Kerenidis et al. [14].

4) *Two-server QSPIR protocols for pure states in visible setting*: Lastly, we prove that QSPIR is possible in the visible setting. We propose two-server QSPIR protocols for pure states in the visible setting, and the protocols work for the different classes of states. The first protocol is for pure qubit states. This protocol succeeds with probability and requires 8-qubit average communication and 4-e-bit average entanglement between servers (or 16-qubit communication without shared entanglement). The second protocol is for pure *qudit* states, where a qudit means a quantum  $d$ -level system. This protocol also succeeds with probability and requires  $4d^d \log d$ -qubit average communication and  $2d^d \log d$ -e-bit average entanglement between servers (or  $8d^d \log d$ -qubit communication without shared entanglement). The last protocol is for pure states  $|\mathbf{U}\rangle = \sum_{s,t} u_{st} |s\rangle |t\rangle$  described by commutative unitary matrices  $\mathbf{U} = \sum_{s,t} u_{st} |s\rangle \langle t|$  on qudits. This protocol succeeds deterministically with  $4 \log d$ -qubit communication and  $2 \log d$  ebits (or  $8 \log d$ -qubit communication without shared entanglement).

The QSPIR protocols have the following important properties. First, the protocols delegate most of the quantum information processing to the servers. All queries of the user are classical and the only quantum resource required for the user is a measurement apparatus for a fixed basis. Second, the average quantum communication complexities of these

TABLE II: Optimal communication complexity of one-server QPIR

(a) One-server QPIR

Messages	Server Model	Optimal communication complexity	Ref.
Classical	Honest	$O(\text{poly log } m)$	[14]
Classical	Specious	$\Theta(m)$	[12]
Quantum (blind)	Honest	$\Theta(m)$	[This paper]
Quantum (visible)	Honest	$\Theta(m)$ (for one-round)	[This paper]

(b) One-server QPIR with prior entanglement

Messages	Server Model	Optimal communication complexity	Ref.
Classical	Honest	$O(\log m)$	[14]
Classical	Specious	$\Theta(m)$	[15]
Quantum (blind/visible)	Honest	$O(\log m)$	[This paper]

(m: Total size of messages)

protocols do not scale with the number of message states. On the other hand, as a trade-off, the size of the queries scales linearly with the number of message states.

The idea of our QSPIR protocols is explained as follows. In the visible setting, we can prepare the message states  $|\psi_\ell\rangle$  by the state preparation unitaries  $U_\ell$  such that  $U_\ell|0\rangle = |\psi_\ell\rangle$ . We can decompose any state preparation unitaries  $U_\ell$  on qudits by phase-shift operations and rotation operations, which are described classically by  $2(d-1)$  angles. Then, with the query structure of classical PIR, the servers collectively encode the phase-shift operations and the rotation operations composing  $U_k$  into the maximally entangled states, where  $k$  is the index of the targeted message state  $|\psi_k\rangle$ . By the query structure of classical PIR, this encoding process can be accomplished without leaking  $k$  to each server. The user receives the maximally entangled states encoded with the phase-shift operations and the rotation operations, and finally recovers the targeted message state  $|\psi_k\rangle$  by the entanglement-swapping. The QSPIR protocol for qubit states is done more efficiently since only one rotation operation is necessary for decomposing  $U_\ell$ . For qudit states for  $d \geq 3$ , the rotation operations for decomposing  $U_\ell$  are non-commutative and this non-commutativity leads to the increased complexity.

The remainder of the paper is organized as follows. Section II is the preliminaries of the paper. Section III derives the lower bound of the communication complexity for one-server QPIR. In the blind setting, Section IV proposes an efficient one-server QPIR protocol with prior entanglement. Section V proposes an efficient QPIR protocol in the visible setting. Section VI is the conclusion of the paper.

## II. PRELIMINARIES

We define  $[a : b] = \{a, a+1, \dots, b\}$  and  $[a] = \{1, \dots, a\}$ . The dimension of a quantum system  $X$  is denoted by  $|X|$ . The von Neumann entropy is defined as  $H(X) = H(\rho_X) = -\text{Tr} \rho_X \log \rho_X$ , where  $\rho_X$  is the state on the quantum system  $X$ .

**Proposition 1.** *The von Neumann entropy satisfies the following properties.*

- (a)  $H(X) = H(Y)$  if the state on  $X \otimes Y$  is a pure state,
- (b)  $H(XY) = H(X) + H(Y)$  for product states on  $X \otimes Y$ ,

(c) *Entropy does not change by unitary operations,*

(d)  $H(XY) + H(X) \geq H(Y)$ ,

(e)  $H(\sum_s p_s \rho_s) = \sum_s p_s (H(\rho_s) - \log p_s)$  if  $\text{Tr} \rho_s \rho_t = 0$  for any  $s \neq t$ .

The property (d) is proved as follows. Let  $Z$  be the reference system in which the state on  $XYZ$  is pure. Then,  $H(XY) + H(X) = H(Z) + H(X) \geq H(XZ) = H(Y)$ . Throughout the paper, we use the symbols (a), (b), (c), (d), (e) to denote which property is used, e.g.,  $\stackrel{(a)}{=}$  means that the equality holds from the property (a).

**Proposition 2.** *Consider two quantum systems  $A$  and  $B$ . If any pure states  $\rho_{AB}$  and  $\rho'_{AB}$  satisfy  $\rho_A = \rho'_A$ , there exists a unitary  $U_B$  on  $B$  such that  $\rho_{AB} = (I_A \otimes U_B) \rho'_{AB} (I_A \otimes U_B^*)$ .*

*Proof.* Diagonalize  $\rho_A = \sum_s p_s |s\rangle\langle s|$ . When  $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$  and  $\rho'_{AB} = |\psi'_{AB}\rangle\langle\psi'_{AB}|$ , we have  $|\psi_{AB}\rangle = \sum_s p_s |s, f(s)\rangle$  and  $|\psi'_{AB}\rangle = \sum_s p_s |s, g(s)\rangle$ , where  $\{|f(s)\rangle\}$  and  $\{|g(s)\rangle\}$  are sets of orthonormal vectors of  $B$ . Thus,  $U_B = \sum_s |f(s)\rangle\langle g(s)|$  is the desired unitary.  $\square$

For a  $d_1 \times d_2$  matrix

$$M = \sum_{s=0}^{d_1-1} \sum_{t=0}^{d_2-1} m_{st} |s\rangle\langle t| \in \mathbb{C}^{d_1 \times d_2}, \quad (1)$$

we define

$$|M\rangle\rangle = \sum_{s=0}^{d_1-1} \sum_{t=0}^{d_2-1} m_{st} |s\rangle|t\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}. \quad (2)$$

For  $A \in \mathbb{C}^{d_1 \times d_2}$ ,  $B \in \mathbb{C}^{d_1 \times d_1}$ , and  $C \in \mathbb{C}^{d_2 \times d_2}$ , we have the relation

$$(B \otimes C^T) |A\rangle\rangle = |BAC\rangle\rangle. \quad (3)$$

We call a  $d$ -dimensional system  $\mathbb{C}^d$  a *qudit*. Define generalized Pauli matrices and the maximally entangled state on

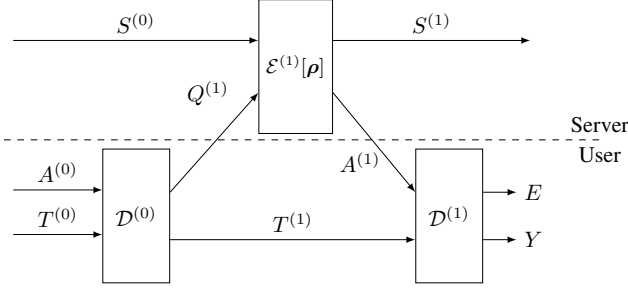


Fig. 2: One-round QPIR protocol in the visible setting.

qudits as

$$X_d = \sum_{s=0}^{d-1} |s+1\rangle\langle s|, \quad (4)$$

$$Z_d = \sum_{s=0}^{d-1} \omega^s |s\rangle\langle s|, \quad (5)$$

$$|I_d\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} |s, s\rangle, \quad (6)$$

where  $\omega = \exp(2\pi i/d)$  and  $\iota = \sqrt{-1}$ . We define the generalized Bell measurements

$$M_{XZ,d} = \{|X^a Z^b\rangle \mid a, b \in [0 : d-1]\}. \quad (7)$$

If there is no confusion, we denote  $X_d, Z_d, I_d, M_{XZ,d}$  by  $X, Z, I, M_{XZ}$ . Let  $A, A', B, B'$  be qudits. If the state on  $A \otimes A' \otimes B \otimes B'$  is  $|A\rangle \otimes |B\rangle$  and the measurement  $M_{XZ}$  is performed on  $A' \otimes B'$  with outcome  $(a, b) \in [0 : d-1]^2$ , the resultant state is

$$|AX^a Z^{-b} B^\top\rangle \in A \otimes B. \quad (8)$$

### III. OPTIMALITY OF TRIVIAL PROTOCOL FOR ONE-SERVER QPIR

In this section, we prove that the trivial solution of downloading all messages is optimal for the one-server QPIR in two cases. We first prove the optimality when the user and the server communicate for one-round in Section III-A, and extends the optimality to the multi-round case in Section III-B. The multi-round case is proved only in the blind setting.

#### A. Optimality of trivial protocol for one-server one-round QPIR

In this subsection, we prove that the optimal communication complexity for one-server one-round QPIR is  $m$ , where  $m$  is the total number of qubits in the message states. The achievability part is proved by the trivial solution, which can be implemented in the blind setting, and we will prove the tight lower bound in the visible setting. Since any protocol in the blind setting can be regarded as a protocol in the visible setting, our tight lower bound in the visible setting proves that the trivial solution is optimal for both blind and visible settings.

We formally describe one-server one-round QPIR protocols in the visible setting with Figure 2 as follows. The message states are given as arbitrary  $f$  states  $\rho = (\rho_1, \dots, \rho_f)$  on quantum systems  $X_1, \dots, X_f$ , respectively. The server has the descriptions of all messages states  $\rho$ . The user chooses the index of the targeted message  $K \in [f]$ , i.e.,  $\rho_k$  is the targeted quantum state when  $K = k$ . We assume that the user and the server contain local quantum registers, respectively, so that all local operations are written as unitary operations. A QPIR protocol  $\Phi$  is described by three unitary maps  $(\mathcal{D}^{(0)}, \mathcal{D}^{(1)}, \mathcal{E}^{(1)})$  in the following steps.

- 1) **Query:** When  $K = k$ , the user prepares the initial state as  $|k\rangle \otimes |0\rangle \in A^{(0)} \otimes T^{(0)}$ , applies a unitary map  $\mathcal{D}^{(0)}$  from  $A^{(0)} \otimes T^{(0)}$  to  $Q^{(1)} \otimes T^{(1)}$ , and sends  $Q^{(1)}$  to the server.
- 2) **Answer:** The server prepares the initial state  $|0\rangle \in S^{(0)}$ , applies a unitary map  $\mathcal{E}^{(1)}[\rho]$  from  $S^{(0)} \otimes Q^{(1)}$  to  $A^{(1)} \otimes S^{(1)}$ , and returns to the user the system  $A^{(1)}$ .
- 3) **Reconstruction:** The user applies a unitary map  $\mathcal{D}^{(1)}$  from  $A^{(1)} \otimes T^{(1)}$  to  $Y \otimes E$ , and outputs the state on  $Y$  as the protocol output.

The input-output relation  $\Lambda_\Phi(k, \rho)$  of the QPIR protocol  $\Phi$  is written with a CPTP  $\Gamma_{\Phi, \rho}$  as

$$\begin{aligned} \Lambda_\Phi(k, \rho) &= \Gamma_{\Phi, \rho}(|k\rangle\langle k|) \\ &= \text{Tr}_{S^{(1)}, E} \mathcal{D}^{(1)} \circ \mathcal{E}^{(1)}[\rho] \circ \mathcal{D}^{(0)}(|k\rangle\langle k| \otimes |0\rangle\langle 0|). \end{aligned}$$

The QPIR protocol  $\Phi$  should satisfy the following conditions.

- **Correctness:** When the output state on  $Y$  with the target index  $K = k$  is denoted by  $\rho_Y^k$ , the correctness is

$$\rho_Y^k = \rho_k \quad (9)$$

for any  $k$  and any message states  $\rho$ .

- **User secrecy:** When the state on  $Q^{(1)}$  with the target index  $K = k$  is denoted by  $\rho_{Q^{(1)}}^k$ , the user secrecy is

$$\rho_{Q^{(1)}}^k = \rho_{Q^{(1)}}^\ell \quad (10)$$

for any  $k, \ell$ .

We evaluate the efficiency of a QPIR protocol  $\Phi$  by the communication complexity  $\text{CC}(\Phi) := \log |Q^{(1)}| + \log |A^{(1)}|$ , which is the whole dimension of uploaded and downloaded systems. The communication complexity of the trivial solution of downloading all states is  $\sum_{\ell=1}^f \log |X_\ell|$ . The following theorem proves the optimality of the trivial solution.

**Theorem 1.** For any one-server one-round QPIR protocol  $\Phi$ , the communication complexity  $\text{CC}(\Phi)$  is lower bounded as

$$\text{CC}(\Phi) \geq \sum_{\ell=1}^f \log |X_\ell|, \quad (11)$$

where  $X_\ell$  is the system of the  $\ell$ -th message  $\rho_\ell$ .

For the proof of Theorem 1, we prepare the following notations and lemma. Given the description of states  $\rho$  and the target index  $k$ , we denote the state on the system  $A^{(1)} \otimes T^{(1)}$  by  $\rho_{A^{(1)}T^{(1)}}^{k, \rho}$ . If the message states are pure states  $|\phi_1\rangle, \dots, |\phi_f\rangle$ ,

we denote  $\rho_{A^{(1)}T^{(1)}}^{k,\rho}$  by  $\rho_{A^{(1)}T^{(1)}}^{k,|\phi_1,\dots,\phi_f\rangle}$ . Let  $d_\ell := |X_\ell|$  and  $d := \prod_{\ell=1}^f d_\ell$ .

**Lemma 1.** Suppose (10). For any  $k, \ell \in [f]$ , there exists a unitary  $U_{T^{(1)}}^{k \rightarrow \ell}$  on  $T^{(1)}$  such that

$$U_{T^{(1)}}^{k \rightarrow \ell} \rho_{A^{(1)}T^{(1)}}^{k,\rho} (U_{T^{(1)}}^{k \rightarrow \ell})^\dagger = \rho_{A^{(1)}T^{(1)}}^{\ell,\rho} \quad (12)$$

for any message states  $\rho$ .

*Proof.* Let  $\rho_{Q^{(1)} \otimes T^{(1)}}^k$  on  $Q^{(1)} \otimes T^{(1)}$  be the state on  $Q^{(1)} \otimes T^{(1)}$  for user's input  $k \in [f]$ . From the secrecy condition (10), the state on  $Q^{(1)}$  does not depend on the value of  $k$ . Since the state on  $Q^{(1)} \otimes T^{(1)}$  is a pure state, there exists a unitary  $U_{T^{(1)}}^{k \rightarrow \ell}$  on  $T^{(1)}$  that maps  $\rho_{Q^{(1)} \otimes T^{(1)}}^k$  to  $\rho_{Q^{(1)} \otimes T^{(1)}}^\ell$  by Proposition 2. This unitary  $U_{T^{(1)}}^{k \rightarrow \ell}$  does not depend on the message states  $\rho$ . Since the server's operation is not applied to  $T^{(1)}$ , the same unitary  $U_{T^{(1)}}^{k \rightarrow \ell}$  satisfies (12).  $\square$

*Proof of Theorem 1.* First, we prove that

$$\left\{ \rho_{A^{(1)}T^{(1)}}^{1,|s_1,\dots,s_f\rangle} \mid s_\ell \in [0 : d_\ell - 1], \ell \in [f] \right\} \quad (13)$$

is a set composed of orthogonal states. Let  $(s_1, \dots, s_f)$ ,  $(s'_1, \dots, s'_f)$  be any two different strings and  $k \in [f]$  be an index satisfying  $s_k \neq s'_k$ . We have

$$\text{Tr} \rho_{A^{(1)}T^{(1)}}^{k,|s_1,\dots,s_f\rangle} \rho_{A^{(1)}T^{(1)}}^{k,|s'_1,\dots,s'_f\rangle} = 0, \quad (14)$$

since the correctness condition (9) guarantees that the two states can be made orthogonal by the decoding unitary map  $\mathcal{D}^{(1)}$ . Furthermore, for the same  $(s_1, \dots, s_f)$  and  $(s'_1, \dots, s'_f)$ , Eq. (14) implies that

$$\text{Tr} \rho_{A^{(1)}T^{(1)}}^{1,|s_1,\dots,s_f\rangle} \rho_{A^{(1)}T^{(1)}}^{1,|s'_1,\dots,s'_f\rangle} = 0, \quad (15)$$

because there exists a unitary map  $U_{T^{(1)}}^{1 \rightarrow k}$  on  $T^{(1)}$  such that

$$U_{T^{(1)}}^{1 \rightarrow k} \rho_{A^{(1)}T^{(1)}}^{1,|s_1,\dots,s_f\rangle} (U_{T^{(1)}}^{1 \rightarrow k})^\dagger = \rho_{A^{(1)}T^{(1)}}^{k,|s_1,\dots,s_f\rangle}, \quad (16)$$

$$U_{T^{(1)}}^{1 \rightarrow k} \rho_{A^{(1)}T^{(1)}}^{1,|s'_1,\dots,s'_f\rangle} (U_{T^{(1)}}^{1 \rightarrow k})^\dagger = \rho_{A^{(1)}T^{(1)}}^{k,|s'_1,\dots,s'_f\rangle} \quad (17)$$

from Lemma 1. Since (15) holds for any different  $(s_1, \dots, s_f)$  and  $(s'_1, \dots, s'_f)$ , the set (13) is composed of orthogonal states.

Next, we consider the case where the user's input is  $k = 1$  and the server applies the CPTP map

$$\sum_{s_1,\dots,s_f} \frac{1}{d} \mathcal{E}^{(1)}[|s_1, \dots, s_f\rangle], \quad (18)$$

which is the uniform mixture of encoding maps. Then, the state on  $A^{(1)} \otimes R^{(1)}$  is

$$\rho_* := \sum_{s_1,\dots,s_f} \frac{1}{d} \mathcal{E}^{(1)}[|s_1, \dots, s_f\rangle] \circ \mathcal{D}^{(0)}(|1\rangle\langle 1| \otimes |0\rangle\langle 0|) \quad (19)$$

$$= \sum_{s_1,\dots,s_f} \frac{1}{d} \rho_{A^{(1)}T^{(1)}}^{1,|s_1,\dots,s_f\rangle}, \quad (20)$$

and the von Neumann entropy of  $\rho_*$  is

$$H(A^{(1)}T^{(1)})_{\rho_*} = H(\rho_*) \quad (21)$$

$$\stackrel{(e)}{=} \sum_{s_1,\dots,s_f} \frac{1}{d} H(\rho_{A^{(1)}T^{(1)}}^{1,|s_1,\dots,s_f\rangle}) + \log d \quad (22)$$

$$\geq \log d. \quad (23)$$

where (22) follows from the orthogonality of the states in (13). Furthermore, we have

$$H(A^{(1)}T^{(1)})_{\rho_*} \leq H(A^{(1)})_{\rho_*} + H(T^{(1)})_{\rho_*} \quad (24)$$

$$\stackrel{(a)}{=} H(A^{(1)})_{\rho_*} + H(Q^{(1)})_{\rho_{Q^{(1)}}^1} \quad (25)$$

$$\leq \log |A^{(1)}| + \log |Q^{(1)}| \quad (26)$$

$$= \text{CC}(\Phi). \quad (27)$$

Combining (23) and (27), we obtain the desired inequality (11).  $\square$

### B. Optimality of trivial protocol for one-server multi-round QPIR in blind setting

In this subsection, we extend the the optimality of the trivial solution to the case where the user and the server communicate multiple rounds in the blind setting. To be precise, we define the  $r$ -round QPIR protocol in the blind setting as follows (2-round protocol is depicted in Figure 3).

The message states are given as arbitrary  $f$  states  $\rho_1 \otimes \dots \otimes \rho_f$  on  $S^{(0)} = X_1 \otimes \dots \otimes X_f$ , where each of  $\rho_\ell$  is purified in  $X_\ell \otimes R_\ell$ . The server contains the system  $S^{(0)}$ . The user chooses the index of the targeted message  $K \in [f]$ , i.e.,  $\rho_k$  is the targeted quantum state when  $K = k$ . When  $K = k$ , the user prepares the initial state as  $|k\rangle \otimes |0\rangle \in A^{(0)} \otimes T^{(0)}$ . We assume that the user and the server contain local quantum registers, respectively, which enable that all local operations are written as unitary operations. A QPIR protocol  $\Phi$  is described by unitary maps  $\mathcal{D}^{(0)}, \dots, \mathcal{D}^{(r)}, \mathcal{E}^{(1)}, \dots, \mathcal{E}^{(r)}$  in the following steps.

- 1) **Query:** For all  $i \in [r]$ , the user applies a unitary map  $\mathcal{D}^{(i-1)}$  from  $A^{(i-1)} \otimes T^{(i-1)}$  to  $Q^{(i)} \otimes T^{(i)}$ , and sends  $Q^{(i)}$  to the sender.
- 2) **Answer:** For all  $i \in [r]$ , the server applies a unitary map  $\mathcal{E}^{(i)}$  from  $Q^{(i)} \otimes S^{(i-1)}$  to  $A^{(i)} \otimes S^{(i)}$  and sends  $A^{(i)}$  to the user.
- 3) **Reconstruction:** The user applies  $\mathcal{D}^{(r)}$  from  $A^{(r)} \otimes T^{(r)}$  to  $Y \otimes E$ , and outputs the state on  $Y$  as the protocol output.

The input-output relation  $\Lambda_\Phi$  of the protocol  $\Phi$  is written with a CPTP  $\Gamma_{\Phi,k}$  from  $X_{[f]}$  to  $Y$  as

$$\begin{aligned} \Lambda_\Phi(k, \rho_1, \dots, \rho_f) &= \Gamma_{\Phi,k}(\rho_{[f]}) \\ &= \text{Tr}_{S^{(r)}, E} \mathcal{D} * \mathcal{E}(\rho_{[f]} \otimes \mathcal{D}^{(0)}(|k\rangle\langle k| \otimes |0\rangle\langle 0|)), \end{aligned}$$

where  $\mathcal{D} * \mathcal{E} = (\mathcal{D}^{(r)} \circ \mathcal{E}^{(r)}) \circ \dots \circ (\mathcal{D}^{(1)} \circ \mathcal{E}^{(1)})$ . The QPIR protocol  $\Phi$  should satisfy the following conditions.

- **Correctness:** When  $|\psi_k\rangle\langle\psi_k|$  denotes a purification of  $\rho_k$  with the reference system  $R_k$ , the correctness is

$$\Gamma_{\Phi,k} \otimes \text{id}_{R_k}(\rho_{[f] \setminus \{k\}} \otimes |\psi_k\rangle\langle\psi_k|) = |\psi_k\rangle\langle\psi_k|$$

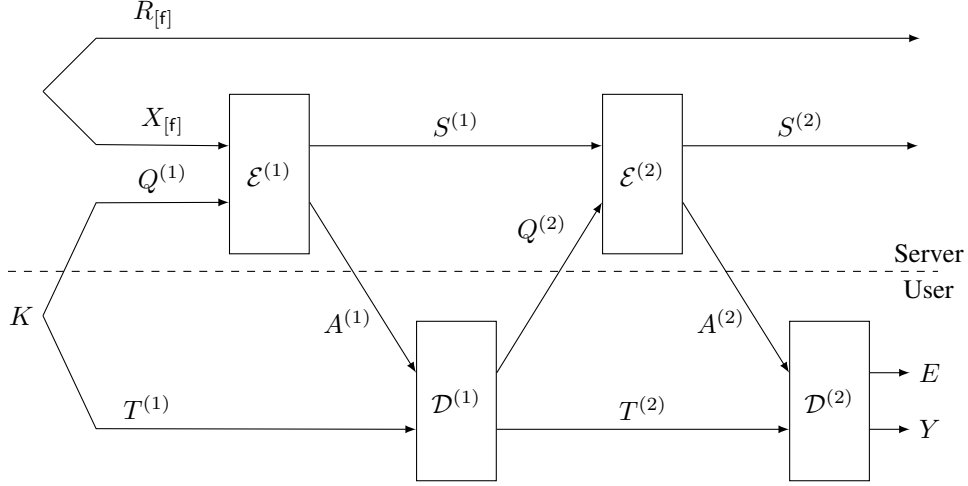


Fig. 3: 2-round QPIR protocol in the blind setting.

for any  $K = k$  and any state  $\rho_{[f]}$ .

- **User secrecy:** When the state on  $S^{(i-1)} \otimes Q^{(i)}$  with the target index  $K = k$  is denoted by  $\rho_{S^{(i-1)}Q^{(i)}}(k)$ , the user secrecy is

$$\rho_{S^{(i-1)}Q^{(i)}}(k) = \rho_{S^{(i-1)}Q^{(i)}}(k') \quad (28)$$

for any  $k, k', i$ .

The communication complexity of the one-server multi-round QPIR is written as  $\text{CC}(\Phi) = \sum_{i=1}^r \log |Q^{(i)}| + \log |A^{(i)}|$ .

**Theorem 2.** For any one-server multi-round QPIR protocol  $\Phi$  in the blind setting, the communication complexity  $\text{CC}(\Phi)$  is lower bounded by  $\sum_{\ell=1}^f \log |X_\ell|$ , where  $X_\ell$  is the system of the  $\ell$ -th message  $\rho_\ell$ .

For the proof of Theorem 2, we prepare the following lemmas.

**Lemma 2.**  $H(A^{(i)}) + H(Q^{(i+1)}) \geq H(T^{(i+1)}) - H(T^{(i)})$ .

*Proof.* Lemma 2 is shown by the relation

$$\begin{aligned} & H(A^{(i)}) + H(T^{(i)}) + H(Q^{(i+1)}) \\ & \stackrel{(b)}{\geq} H(A^{(i)}T^{(i)}) + H(Q^{(i+1)}) \\ & \stackrel{(c)}{=} H(Q^{(i+1)}T^{(i+1)}) + H(Q^{(i+1)}) \\ & \stackrel{(d)}{\geq} H(T^{(i+1)}). \end{aligned}$$

**Lemma 3.**  $H(R_{[f]}S^{(r)}) = H(R_{[f]}) + H(S^{(r)})$ .

*Proof.* Given the user's input  $k$ , the state on  $R_k \otimes Y$  is a pure state, and therefore,  $R_k$  is independent of any system except for  $Y$ . Thus, we have

$$H(R_{[f]}S^{(r)}) = H(R_{[f] \setminus \{k\}}S^{(r)}) + H(R_k) \quad (29)$$

for any  $k$ . Note that the state on  $R_{[f]} \otimes S^{(r)}$  does not depend on  $k$  due to the secrecy condition (28). Thus, applying (29) recursively for all  $k$ , we have

$$H(R_{[f]}S^{(r)}) = H(R_f) + H(R_{[f-1]}S^{(r)}) \quad (30)$$

$$= H(R_{f-1}R_f) + H(R_{[f-2]}S^{(r)}) = \dots \quad (31)$$

$$= H(R_{[f]}) + H(S^{(r)}). \quad (32)$$

□

*Proof of Theorem 2.* From Lemmas 2 and 3, we derive the following inequalities:

$$\text{CC}(\Phi) \geq \sum_{i=1}^r H(A^{(i)}) + H(Q^{(i)}) \quad (33)$$

$$= H(A^{(r)}) + H(Q^{(1)}) + \sum_{i=1}^{r-1} H(A^{(i)}) + H(Q^{(i+1)}) \quad (34)$$

$$\geq H(A^{(r)}) + H(Q^{(1)}) + H(T^{(r)}) - H(T^{(1)}) \quad (35)$$

$$\stackrel{(a)}{=} H(A^{(r)}) + H(T^{(r)}) \quad (36)$$

$$\stackrel{(b)}{\geq} H(A^{(r)}T^{(r)}) \stackrel{(a)}{=} H(R_{[f]}S^{(r)}) \quad (37)$$

$$= H(R_{[f]}) + H(S^{(r)}) \quad (38)$$

$$\geq H(R_{[f]}) = H(X_{[f]}), \quad (39)$$

where (35) is obtained by applying Lemma 2 for all  $i = 1, \dots, r-1$ , and (38) is from Lemma 3. Taking the maximum of  $H(X_{[f]})$  over all states  $\rho_1, \dots, \rho_f$ , we obtain  $\text{CC}(\Phi) \geq \sum_{\ell=1}^f \log |X_\ell|$ . □

#### IV. QPIR PROTOCOL WITH PRIOR ENTANGLEMENT IN BLIND SETTING

In the previous section, we proved that the trivial solution is optimal for one-server QPIR. In this section, we show that if we allow shared entanglement between the user and the servers, we can construct a QPIR protocol with lower communication complexity than the trivial solution.

Let  $m = \sum_{\ell=1}^f \log |X_\ell|$  be the size of all messages. To measure the amount of the prior entanglement, we count sharing one copy of  $|l_2\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$  as an *ebit*. Accordingly, we count sharing the state  $|l_d\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$  as  $\log d$  ebits.

**Theorem 3.** *Suppose there exists a C-QPIR protocol with communication complexity  $O(f(m))$  when  $O(g(m))$ -ebit prior entanglement is shared between the user and the server. Then, in the blind setting, there exists a QPIR protocol for quantum messages with communication complexity  $O(f(m))$  when  $O(m+g(m))$ -ebit prior entanglement is shared between the user and the server.*

The protocol satisfying Theorem 3 is a simple combination of quantum teleportation [43] and any C-QPIR protocol. For the description of the protocol, we use the generalized Pauli operators and maximally entangled state for  $d$ -dimensional systems defined in (6). We construct the QPIR protocol satisfying Theorem 3 as follows.

**Protocol 1.** Let  $\Phi_{cl}$  be a C-QPIR protocol and  $d_1, \dots, d_f$  be the size of the  $f$  classical messages. From this protocol, we construct a QPIR protocol for quantum messages as follows.

Let  $X_1, \dots, X_f$  be the quantum systems with dimensions  $d_1, \dots, d_f$ , respectively, and  $\rho_1, \dots, \rho_f$  be the quantum message states on systems  $X_1, \dots, X_f$ . The user and the server share the maximally entangled states  $|l_{d_\ell}\rangle$ , defined in (6), on  $Y_\ell \otimes Y'_\ell$  for all  $\ell \in [f]$ , where  $Y_{[f]}$  and  $Y'_{[f]}$  are possessed by the user and the server, respectively.

The user and the server perform the following steps.

- 1) For all  $\ell \in [f]$ , the server performs the generalized Bell measurement  $M_{XZ, d_\ell}$ , defined in (7), on  $X_\ell \otimes Y'_\ell$ , where the measurement outcome is written as  $m_\ell = (a_\ell, b_\ell) \in [0 : d_\ell - 1]^2$ .
- 2) The user and the server perform the C-QPIR protocol  $\Phi_{cl}$  to retrieve  $m_k = (a_k, b_k)$ .
- 3) The user recovers the  $k$ -th message  $\rho_k$  by applying  $X_{d_k}^{-a_k} Z_{d_k}^{b_k}$  on  $Y_k$ . ■

The correctness of the protocol is guaranteed by correctness of the teleportation protocol and the C-QPIR protocol  $\Phi_{cl}$ . When the  $\ell$ -th message state is prepared as  $\rho_\ell$  and its purification  $|\phi_\ell\rangle$  is denoted with the reference system  $R_\ell$ , after Step 1, the states on  $R_\ell \otimes Y_\ell$  is

$$(I \otimes X_{d_\ell}^{a_\ell} Z_{d_\ell}^{-b_\ell}) |\phi_\ell\rangle \quad (40)$$

for all  $\ell \in [f]$ . Thus after Step 3, the target state  $|\phi_k\rangle$  is recovered in  $R_k \otimes Y_k$ .

To analyze the secrecy of Protocol 1, note that only Step 2 has the communication between the user and the server. Thus the secrecy of Protocol 1 is guaranteed by the secrecy of the underlying protocol  $\Phi_{cl}$ . In the honest server model, Kerenidis et al. [14] proposed a C-QPIR protocol with communication complexity  $O(\log m)$  and prior entanglement  $O(m)$ . Therefore, we obtain the following corollary.

**Corollary 1.** *On the honest server model in the blind setting, there exists a QPIR protocol for quantum messages with*

*communication complexity  $O(\log m)$  and prior entanglement  $O(m)$ .*

One property of Protocol 1 is that all other states in the server are destroyed at Step 1. This is a disadvantage for the server but an advantage for the user since the user can retrieve other states  $\rho_\ell$  by retrieving classical information  $m_\ell \in [0 : d_\ell - 1]^2$ .

## V. TWO-SERVER SYMMETRIC QPIR PROTOCOLS IN VISIBLE SETTING

In this section, we propose two-server one-round QSPIR protocols with classical query in the visible setting. In the multi-server model, the servers cannot communicate with each other. In the visible setting, the server has the description of quantum states instead of the states. With a description of a state  $\rho$ , the server may generate multiple copies of  $\rho$ , without limitation of the no-cloning theorem, and apply quantum operations depending on the description of  $\rho$ . Our protocols in this section are symmetric QPIR (QSPIR) in which the user only obtains the information of the targeted message state. Thus, our protocols prove that the QSPIR is possible in the visible setting.

### A. Definition and main theorems

We propose three QSPIR protocols in the visible setting for pure states. The communication complexity of the protocols are summarized in Table III. Even if the QPIR's trivial solution of downloading all states is not a QSPIR protocol, we can evaluate the efficiency of our QSPIR protocols by comparison with the communication complexities of the QPIR's trivial solution. Compared to the communication complexity of the QPIR's trivial solution is  $f \log d$  qubits, the quantum communication complexities of our protocols do not scale with the number of messages  $f$  but scale with the dimension of the systems in which the message states are prepared. Thus, when the number of messages  $f$  is sufficiently greater than the dimension, the proposed protocols are more efficient than the QPIR's trivial solution of downloading all messages.

Our QSPIR protocols are included in the class of  $n$ -server QSPIR protocols in the visible setting with the classical queries described as follows. Let  $P(\mathbb{C}^d)$  be the set of pure states in  $\mathbb{C}^d$ . We formally define a QSPIR protocol  $\Phi$  for  $\mathcal{P} \subset P(\mathbb{C}^d)$ . The message states are given as arbitrary  $f$  states  $\psi = (|\psi_1\rangle, \dots, |\psi_f\rangle) \in \mathcal{P}^f$  and each server has the descriptions of all messages states. The user chooses the index of the targeted message  $K \in [f]$ , i.e.,  $|\psi_K\rangle$  is the targeted quantum state when  $K = k$ . A protocol  $\Phi$  constructed by the following steps.

- 1) **Query:** The user randomly encodes  $K$  as classical queries  $Q = (Q_1, \dots, Q_n) \in \mathcal{Q}_1 \times \dots \times \mathcal{Q}_n$  and sends  $Q_j$  to the  $j$ -th server. That is, the variable  $Q$  is subject to the conditional distribution  $p_{Q|K=k}$ , which is chosen by the user.
- 2) **Entanglement Sharing:** Independently of the queries, the servers share an entangled state  $\rho_{\text{init}}$  on  $S_1 \otimes \dots \otimes S_n$ , where  $S_j$  is contained in the  $j$ -th server.

TABLE III: Cost of Two-Server QSPIR Protocols in Visible Setting

	Message States	Classical Communication	Quantum Communication	Prior Entanglement
Protocol 3	Pure qubit states	2f bits	8 qubits	4 ebits
Protocol 4	Pure qudit states	2f bits	$4d^d \log d$ qubits	$2d^d \log d$ ebits
Protocol 2	Commutative unitary	2f bits	$4 \log d$ qubits	$2 \log d$ ebits

- 3) **Answer:** For all  $j \in [n]$ , the  $j$ -th server applies a CPTP map  $\mathcal{E}_j[\psi, q_j]$  from  $S_j$  to  $A_j$  and sends  $A_j$  to the user when  $Q_j = q_j$ .
- 4) **Reconstruction:** Let  $A := A_1 \otimes \cdots \otimes A_n$  and decompose  $A = Y \otimes Y'$ . The user performs a measurement by a POVM  $\{M, I - M\}$  on  $Y \subset A$ . If  $M$  is measured, the targeted state  $|\psi_k\rangle$  is recovered correctly in  $Y'$ . If the reconstruction fails, i.e.  $I - M$  is measured, repeat from Step 2.

The protocol  $\Phi$  should satisfy the following conditions.

- **Correctness:** At each execution of Step 4, the user recovers the targeted state  $|\psi_k\rangle$  with positive probability  $p$ .
- **User secrecy:** The user secrecy is

$$I(Q_j; K) = 0 \quad \forall j \quad (41)$$

for any distribution of  $K$ .

- **Server secrecy:** Let  $\rho_A(k, \psi)$  be the state on  $A$  with the target index  $k$  and the message states  $\psi = (|\psi_1\rangle, \dots, |\psi_f\rangle)$ . The server secrecy is

$$\rho_A(k, \psi) = \rho_A(k, \phi)$$

for any  $k \in [f]$  and any states  $\psi = (|\psi_1\rangle, \dots, |\psi_f\rangle)$ ,  $\phi = (|\phi_1\rangle, \dots, |\phi_f\rangle) \in \mathcal{P}^f$  such that  $|\psi_k\rangle = |\phi_k\rangle$ .

The average classical and quantum communication complexities are defined as

$$CC(\Phi)_c = \sum_{j=1}^n \log |Q_j|, \quad (42)$$

$$CC(\Phi)_q = \frac{1}{p} \sum_{j=1}^n \log |A_j|, \quad (43)$$

since the classical queries are uploaded once and the quantum answers are downloaded  $1/p$  times on average.

Our protocols will be defined for  $n = 2$  servers with the maximally entanglement states as the prior entanglement. The prior entanglement can be replaced by user's upload of the entangled states. However, we state our results with the prior entanglement because the entangled states can be prepared without any user's operation.

We prove the following two theorems.

**Theorem 4.** *In the visible setting, there exists a QSPIR protocol for  $\mathcal{P}(\mathbb{C}^2)$  with 2f-bit average classical communication, 8-qubit average quantum communication, and 4-ebit average prior entanglement.*

**Theorem 5.** *Let  $d \geq 2$ . In the visible setting, there exists a QSPIR protocol for  $\mathcal{P}(\mathbb{C}^d)$  with 2f-bit average classical communication,  $4d^d \log d$ -qubit average quantum communication, and  $2d^d \log d$ -ebit average prior entanglement.*

The protocols for pure states are constructed by the following idea. Any pure state is written as  $U|0\rangle$  with unitary matrices  $U$  which are decomposed by rotation operations and phase-shift operations. With this fact, the user requests the servers to apply certain rotation operations and phase-shift operations on bipartite entangled states so that the user can recover the targeted pure state after receiving the entangled state. To guarantee the user secrecy, we import to our protocols the same query structure of two-server classical PIR protocol by Chor et al. [1].

We denote by  $U(\mathbb{C}^d)$  the unitary group on  $\mathbb{C}^d$  and define the set of pure states associated with  $U(\mathbb{C}^d)$  as

$$\mathcal{S}(\mathbb{C}^d) = \{ |U\rangle \mid U \in U(\mathbb{C}^d) \}. \quad (44)$$

For a subset  $C$  of  $U(\mathbb{C}^d)$ , we denote

$$\mathcal{S}(C) := \{ |U\rangle \mid U \in C \} \subset \mathcal{P}(\mathbb{C}^d \otimes \mathbb{C}^d), \quad (45)$$

$$\mathcal{P}(C) := \{ U|0\rangle \mid U \in C \} \subset \mathcal{P}(\mathbb{C}^d). \quad (46)$$

We can find the following relation between QSPIR protocols for  $\mathcal{S}(C)$  and  $\mathcal{P}(C)$ .

**Proposition 3.** *Let  $C \subset U(\mathbb{C}^d)$ . If there exists a QSPIR protocol for  $\mathcal{S}(C)$  with communication complexity  $c$ , there exists a QSPIR protocol for  $\mathcal{P}(C)$  which succeeds with probability  $1/d$  and has the average communication complexity  $cd$ .*

*Proof.* We construct a QSPIR protocol for  $\mathcal{P}(C)$  as follows. After applying the QSPIR protocol for  $\mathcal{S}(C)$  whose output state is  $|U_k\rangle$  on  $A \otimes B$ , the user performs the basis measurement  $\{|0\rangle, \dots, |d-1\rangle\}$  on  $A$ . If the measurement outcome is 0, the resultant state on  $B$  is  $|\psi_k\rangle = U_k|0\rangle$ . Otherwise, repeat the process. Since the measurement outcome is 0 with probability  $1/d$ , the expected number of trials is  $d$ . Thus, the average communication complexity is  $cd$ .  $\square$

We also construct a QSPIR protocol for pure states represented by commutative unitary matrices.

**Theorem 6.** *Let  $C \subset U(\mathbb{C}^d)$  consist of commutative unitary matrices. In the visible setting, there exists a QSPIR protocol for  $\mathcal{S}(C)$  with 2f-bit classical communication,  $4 \log d$ -qubit quantum communication, and  $2 \log d$ -ebit prior entanglement.*

Combining Theorem 6 with Proposition 3, we have the following corollary.

**Corollary 2.** *Let  $C \subset U(\mathbb{C}^d)$  consist of commutative unitary matrices. In the visible setting, there exists a QSPIR protocol for  $\mathcal{P}(C)$  with 2f-bit classical communication,  $8d \log d$ -qubit average quantum communication, and  $4 \log d$ -ebit average prior entanglement.*



In the following subsections, we construct the QSPIR protocols to achieve the communication complexity of Theorems 4, 5, 6. Since the protocol for Theorem 6 is the most simplest and the similar idea is used in the other two protocols, we will first construct the protocol for Theorem 6 and then the other two protocols.

### B. QSPIR protocol for pure states described by commutative unitaries

In this subsection, we construct a two-server QSPIR protocol in the visible setting which achieves the communication complexity in Theorem 6.

**Protocol 2** (Two-server QSPIR protocol for pure states described by commutative unitaries). For commutative  $f$  unitaries  $U_1, \dots, U_f$  on  $\mathbb{C}^d$ , the message states are given as

$$|U_1\rangle, \dots, |U_f\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d. \quad (47)$$

When the user's target index  $K$  is  $k \in [f]$ , i.e., the targeted state is  $|U_k\rangle$ , our protocol is given as follows.

- 1) **Query:** The user chooses  $Q = (Q_1, \dots, Q_f) \in \{0, 1\}^f$  uniformly at random. The variable  $Q' = (Q'_1, \dots, Q'_f) \in \{0, 1\}^f$  is defined as

$$Q'_\ell = \begin{cases} Q_\ell & \text{for } \ell \neq k, \\ Q_\ell \oplus 1 & \text{for } \ell = k. \end{cases} \quad (48)$$

The user sends  $Q$  and  $Q'$  to Server 1 and Server 2, respectively.

- 2) **Entanglement Sharing:** Let  $A, A', B, B'$  be qudits. Server 1 and Server 2 share two maximally entangled state  $|I_d\rangle$  on  $A \otimes A'$  and  $B \otimes B'$ , where Server 1 (Server 2) contains  $A \otimes B$  ( $A' \otimes B'$ ).
- 3) **Answer:** When  $Q = q$  and  $Q' = q'$ , we define

$$(t_1, \dots, t_f) = q \oplus (1, \dots, 1), \quad (49)$$

$$(t'_1, \dots, t'_f) = q' \oplus (1, \dots, 1). \quad (50)$$

Server 1 applies

$$U_1^{q_1} \dots U_f^{q_f}, \quad (51)$$

$$U_1^{t_1} \dots U_f^{t_f} \quad (52)$$

on  $A$  and  $B$ , respectively, and sends  $A$  and  $B$  to the user. Similarly, Server 2 applies

$$\bar{U}_1^{q'_1} \dots \bar{U}_f^{q'_f}, \quad (53)$$

$$\bar{U}_1^{t'_1} \dots \bar{U}_f^{t'_f} \quad (54)$$

on  $A'$  and  $B'$ , respectively, and sends  $A'$  and  $B'$  to the user.

- 4) **Reconstruction:** The user outputs the state on  $A_1 \otimes A_2$  if  $Q_k = 1$ , otherwise outputs the state on  $B_1 \otimes B_2$ . ■

Protocol 2 satisfies the correctness, secrecy, and communication complexity, desired in Theorem 6, which is shown as follows.

- **Correctness:** Consider the case where  $Q_k = 1$ . When  $Q = q$ , the state on  $A \otimes A'$  after the measurement is

$$(U_1^{q_1} \dots U_f^{q_f} \otimes \bar{U}_1^{q'_1} \dots \bar{U}_f^{q'_f})|I_d\rangle \quad (55)$$

$$= (U_1^{q_1} \dots U_f^{q_f} \otimes \bar{U}_1^{q'_1} \dots \bar{U}_f^{q'_f})|I_d\rangle \quad (56)$$

$$= |U_1^{q_1} \dots U_f^{q_f} (U_f^\dagger)^{q'_f} \dots (U_1^\dagger)^{q'_1}\rangle \quad (57)$$

$$= |U_k\rangle, \quad (58)$$

where (58) follows from the commutativity of the unitaries  $U_1, \dots, U_f$ ,  $q_\ell \oplus q'_\ell = \delta_{\ell,k}$ , and  $(q_k, q'_k) = (1, 0)$ . By similar analysis, if  $Q_k = 0$ , the resultant state on  $B \otimes B'$  is  $|U_k\rangle$ .

- **Secrecy:** Throughout the protocol, the servers only obtain the queries, and each query is uniformly random  $f$  bits. Therefore, each server does not obtain any information of  $k$ . On the other hand, at the end of the protocol, the user obtains both of  $|U_k\rangle$  and  $|U_k^\dagger\rangle$ . Although  $|U_k^\dagger\rangle$  is transmitted additionally, no information of all other message states is leaked to the user.
- **Communication complexity:** The query is  $2f$  bits, the communication from the server to the user is 4 qudits, i.e.,  $4 \log d$  qubits, and prior entanglement is 2 copies of  $|I_d\rangle$ , i.e.,  $2 \log d$  ebits.

### C. QSPIR protocol for pure qubit states

In this subsection, we construct a two-server QSPIR protocol for pure qubit states in the visible setting which achieves the communication complexity in Theorem 4.

Define the rotation operation on  $\mathbb{C}^2$  and the phase-shift operation by

$$R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \quad S(\varphi) = \begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix}$$

for  $\theta, \varphi \in [0, 2\pi)$ . For any  $\varphi, \varphi', \theta, \theta'$ , we have

$$R(\theta)R(\theta') = R(\theta + \theta'), \quad S(\varphi)S(\varphi') = S(\varphi + \varphi'), \quad (59)$$

and therefore,  $S(\varphi)$  and  $S(\varphi')$  ( $R(\theta)$  and  $R(\theta')$ ) are commutative. We also have

$$R(\theta)^\top = R(-\theta), \quad S(\varphi)^\top = S(\varphi) \quad (60)$$

and

$$XR(\theta)X = R(-\theta), \quad XS(\varphi)X = S(-\varphi). \quad (61)$$

As special cases, we have  $Y := XZ = R(\pi/2)$  and  $Z = S(\pi)$ . Any pure qubit states  $|\psi\rangle$  are written with some  $\varphi \in [0, 2\pi)$  and  $\theta \in [0, \pi/2]$  as

$$|\psi\rangle = S(\varphi)R(\theta)|0\rangle. \quad (62)$$

Now, we construct a QSPIR protocol in the visible setting for qubit states, which achieves the communication complexity in Theorem 4.

**Protocol 3** (Two-server QSPIR protocol for qubit states). For any message qubit states  $|\psi_1\rangle, \dots, |\psi_f\rangle \in P(\mathbb{C}^2)$ , we choose the parameters  $\varphi_\ell$  and  $\theta_\ell$  as

$$|\psi_\ell\rangle = S(\varphi_\ell)R(\theta_\ell)|0\rangle. \quad (63)$$

When the user's target index  $K$  is  $k \in [f]$ , i.e., the targeted state is  $|\psi_k\rangle$ , our protocol is given as follows.

- 1) **Query:** The same as Protocol 2.
- 2) **Entanglement Sharing:** Let  $A, A', B, B'$  be qubits. Server 1 and Server 2 share two maximally entangled state  $|l_2\rangle$  on  $A \otimes A'$  and  $B \otimes B'$ , where Server 1 contains  $A \otimes B$  and Server 2 contains  $A' \otimes B'$ .
- 3) **Answer:** When  $Q = q$ , Server 1 calculates  $\tilde{\theta} := \sum_{\ell=1}^f q_\ell \theta_\ell$  and  $\tilde{\varphi} := \sum_{\ell=1}^f q_\ell \varphi_\ell$ , applies  $R(-\tilde{\theta})$  and  $S(\tilde{\varphi})$  on  $A$  and  $B$ , respectively, and sends  $A \otimes B$  to the user. Similarly, when  $Q' = q'$ , Server 2 calculates  $\tilde{\theta}' := \sum_{\ell=1}^f q'_\ell \theta_\ell$  and  $\tilde{\varphi}' := \sum_{\ell=1}^f q'_\ell \varphi_\ell$ , applies  $R(-\tilde{\theta}')$  and  $S(\tilde{\varphi}')$  on  $A'$  and  $B'$ , respectively, and sends  $A' \otimes B'$  to the user.
- 4) **Reconstruction:**
  - a) The user performs the Bell measurement  $M_{XZ}$  defined in (7) on  $A' \otimes B'$ . Depending on the measurement outcomes  $(a, b) \in \{0, 1\}^2$ , the user applies  $Y^{-a} \otimes Z^{a+b}$  on  $A \otimes B$  and performs the basis measurement  $\{|0\rangle, |1\rangle\}$  on  $A$ .
  - b) If  $Q_k = 1$  and the measurement outcome is 0, the state on  $B$  is  $|\psi_k\rangle$ . If  $Q_k = 0$  and the measurement outcome is 1, the user applies  $X$  operation on  $B$  and then the state on  $B$  is  $|\psi_k\rangle$ . This process succeeds with probability  $1/2$ . Otherwise, repeat from Step 2. ■

Protocol 3 satisfies the correctness, secrecy, and communication complexity, desired in Theorem 4, which is shown as follows.

- **Correctness:** When  $Q = q$ , after the operations of the servers, the states on  $A \otimes A'$  and  $B \otimes B'$  are

$$R(-\tilde{\theta}) \otimes R(-\tilde{\theta}') |l\rangle = |R(-\tilde{\theta})(R(-\tilde{\theta}'))^\top\rangle \quad (64)$$

$$= |R(-\tilde{\theta} + \tilde{\theta}')\rangle \quad (65)$$

$$= |R((-1)^{q_k} \theta_k)\rangle \in A \otimes A', \quad (66)$$

$$S(\tilde{\varphi}) \otimes S(\tilde{\varphi}') |l\rangle = |S(\tilde{\varphi})(S(\tilde{\varphi}'))^\dagger\rangle \quad (67)$$

$$= |S(\tilde{\varphi} - \tilde{\varphi}')\rangle \quad (68)$$

$$= |S((-1)^{q_k+1} \varphi_k)\rangle \in B \otimes B'. \quad (69)$$

After the Bell measurement of the user with the measurement outcome  $(a, b)$ , the state on  $A \otimes B$  is derived from (8) as

$$|R((-1)^{q_k} \theta_k) X^a Z^{-b} S((-1)^{q_k+1} \varphi_k)^\top\rangle \quad (70)$$

$$= |R((-1)^{q_k} \theta_k) Y^a Z^{-a-b} S((-1)^{q_k+1} \varphi_k)\rangle \quad (71)$$

$$= |Y^a R((-1)^{q_k} \theta_k) S((-1)^{q_k+1} \varphi_k) Z^{-a-b}\rangle. \quad (72)$$

After the user applies  $Y^{-a} \otimes Z^{a+b}$  on  $A \otimes B$  in Step 4-a), the state (72) is changed as

$$|R((-1)^{q_k+1} \theta_k) S((-1)^{q_k+1} \varphi_k)\rangle \in A \otimes B, \quad (73)$$

and if the basis measurement outcome in Step 4-b) is  $x \in \{0, 1\}$ , the last state on  $B$  is  $(R((-1)^{q_k} \theta_k) S((-1)^{q_k+1} \varphi_k))^\top |x\rangle = S((-1)^{q_k+1} \varphi_k) R((-1)^{q_k+1} \theta_k) |x\rangle$ . If the measurement

outcome  $x$  is 0 and  $q_k = 1$ , the resultant state is  $|\phi_k\rangle = S(\varphi_k) R(\theta_k) |0\rangle \in B$ . If the measurement outcome  $x$  is 1 and  $q_k = 0$ , the resultant state after the user's operation  $X$  is

$$XS(-\varphi_k) R(-\theta_k) |1\rangle = XS(-\varphi_k) XXR(-\theta_k) X |0\rangle \quad (74)$$

$$\stackrel{(e)}{=} S(\varphi_k) R(\theta_k) |0\rangle \quad (75)$$

$$= |\psi_k\rangle, \quad (76)$$

where (e) is from (61).

For each execution of Step 4, the user obtains  $|\psi_k\rangle$  with probability  $1/2$ . The probability to obtain  $|\psi_k\rangle$  within  $n$  repetition of Steps 3 and 4 is  $1 - 1/2^n$ , and the average number of repetitions is 2.

- **Secrecy:** Each server does not obtain any information of  $k$  since the query is the same as Protocol 2. At each repetition of Step 4, the user obtains the states of (66) and (69), which only depends on the state  $|\psi_k\rangle$ . Thus, the user obtains no information of the other states.
- **Communication complexity:** The query is  $2f$  bits. For each execution of Steps 2-4, necessary communication is 4 qubits and necessary prior entanglement is 2 ebits. Since the query is sent only once at Step 1, the classical communication complexity is  $2f$  bits. Thus, the average quantum communication complexity is 8 qubits, and the average size of entanglement is 4 ebits. If we replace the prior entanglement by the transmission of  $|l_2\rangle \otimes |l_2\rangle$  from the user to the servers, the average communication complexity is  $2f$  bits and 16 qubits.

Compared to the QPIR's trivial solution of downloading all quantum messages, which requires the communication of  $f$  qubits, the above protocol has less quantum communication on average when  $f > 16$  even if ebits are uploaded by the user. On the other hand, our protocol requires classical communication of  $2f$  bits.

#### D. QSPIR protocol for pure qudit states ( $d \geq 2$ )

In this subsection, we construct a two-server QSPIR protocol for pure qudit states in the visible setting which achieves the communication complexity in Theorem 5.

Similar to Protocol 3, we first consider the parameterization of pure states on  $d$ -dimensional systems. Define  $d \times d$  matrices  $R(\theta^1, \dots, \theta^{d-1})$  and  $S(\varphi^1, \dots, \varphi^{d-1})$  as

$$R(\theta^1, \dots, \theta^{d-1}) = R_1(\theta^1) \cdots R_{d-1}(\theta^{d-1}), \quad (77)$$

$$S(\varphi^1, \dots, \varphi^{d-1}) = |0\rangle\langle 0| + \sum_{s=1}^{d-1} e^{i\varphi^s} |s\rangle\langle s| \quad (78)$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\varphi^1} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & e^{i\varphi^{d-1}} \end{pmatrix}, \quad (79)$$

where  $R_s(\theta)$  is the rotation

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad (80)$$

with respect to the two basis elements  $|s-1\rangle$  and  $|s\rangle$ . Notice that  $S(\varphi^1, \dots, \varphi^{d-1})$  for all  $\varphi^1, \dots, \varphi^{d-1}$  ( $R_s(\theta^s)$  for all  $\theta^s$ ) are commutative but any two of  $R_1(\theta^1), \dots, R_{d-1}(\theta^{d-1})$  are not in general. We also have  $S(\varphi^1, \dots, \varphi^{d-1})^\top = S(\varphi^1, \dots, \varphi^{d-1})$ ,  $R_s(\theta^s)^\top = R_s(-\theta^s)$ , and

$$Z_d = S\left(\frac{2\pi\ell}{d}, \frac{4\pi\ell}{d}, \dots, \frac{2(d-1)\pi\ell}{d}\right).$$

It can be easily checked that any pure state  $|\psi\rangle \in P(\mathbb{C}^d)$  is written in the form

$$|\psi\rangle = S(\varphi^1, \dots, \varphi^{d-1})R(\theta^1, \dots, \theta^{d-1})|0\rangle \quad (81)$$

with  $\varphi^1, \dots, \varphi^{d-1} \in [0, 2\pi)$  and  $\theta^1, \dots, \theta^{d-1} \in [0, \pi/2]$ .

**Protocol 4** (Two-server QSPIR protocol for qudit states). For any message pure states  $|\psi_1\rangle, \dots, |\psi_f\rangle \in P(\mathbb{C}^d)$ , we choose the parameters  $\varphi_\ell^1, \dots, \varphi_\ell^{d-1}$  and  $\theta_\ell^1, \dots, \theta_\ell^{d-1}$  as

$$|\psi_\ell\rangle = S(\varphi_\ell^1, \dots, \varphi_\ell^{d-1})R(\theta_\ell^1, \dots, \theta_\ell^{d-1})|0\rangle. \quad (82)$$

When the user's target index  $K$  is  $k \in [f]$ , i.e., the targeted state is  $|\psi_k\rangle$ , our protocol is given as follows.

- 1) **Query:** The same as Protocol 2.
- 2) **Entanglement Sharing:** Server 1 and Server 2 share  $d$  copies of the maximally entangled state  $|I_d\rangle$ .
- 3) **Answer:** Similar to Step 3 of Protocol 3 and as analyzed in (66) and (69), Server 1 and Server 2 can jointly generate the following quantum states

$$|S(\varphi_k)\rangle, |R_1(\theta_k^1)\rangle, \dots, |R_{d-1}(\theta_k^{d-1})\rangle, \quad (83)$$

and

$$|S(-\varphi_k)\rangle, |R_1(-\theta_k^1)\rangle, \dots, |R_{d-1}(-\theta_k^{d-1})\rangle. \quad (84)$$

The servers generate and send these states to the user if it is requested in Step 4.

- 4) **Reconstruction:** For this step, remind (8): If the state is  $|A\rangle \otimes |B\rangle$  and Bell measurement  $M_{XZ}$  defined in (7) is performed with outcome  $(a, b)$ , the resultant state is  $|AX^a Z^{-b} B^\top\rangle$ .
  - a) The user requests the servers to send  $|S(\varphi_k)\rangle \in A \otimes A'$  and  $|R_1(-\theta_k^1)\rangle \in B \otimes B'$ . The user performs the Bell measurement  $M_{XZ}$  defined in (7) on  $A' \otimes B'$ . If the measurement outcome is  $(0, \alpha_1)$  for some  $\alpha_1$ , which happens with probability  $1/d$ , the user obtains the outcome of the following conversions

$$|S(\varphi_k)\rangle |R_1(-\theta_k^1)\rangle \mapsto |S(\varphi_k)Z^{\alpha_1} R_1(\theta_k^1)\rangle \quad (85)$$

$$= |Z^{\alpha_1} S(\varphi_k) R_1(\theta_k^1)\rangle, \quad (86)$$

where  $\mapsto$  represents the state reduction by the measurement. Otherwise, the user repeats Step 4-a.

- b) Next, the user requests  $|R_2(-\theta_k^2)\rangle$  to the servers and performs the same measurement  $M_{XZ}$ . If the measurement outcome is  $(0, \alpha_2)$  for some  $\alpha_2$ , the user obtains the outcome of the following conversion:

$$\begin{aligned} & |Z^{\alpha_1} S(\varphi_k) R_1(\theta_k^1)\rangle |R_2(-\theta_k^2)\rangle \\ & \mapsto |Z^{\alpha_1 + \alpha_2} S(\varphi_k) R_1(\theta_k^1) R_2(\theta_k^2)\rangle, \end{aligned}$$

If it fails to measure  $(0, \alpha_2)$ , restarts from Step 4-a. Repeating the similar conversions with  $|R_3(-\theta_k^3)\rangle, \dots, |R_{d-1}(-\theta_k^{d-1})\rangle$ , the user obtains

$$|Z^{\sum_{s=1}^{d-1} \alpha_s} S(\varphi_k) R_1(\theta_k^1) \dots R_{d-1}(\theta_k^{d-1})\rangle. \quad (87)$$

- c) The user performs Steps 4-a, 4-b with the states of (84) instead of (83). The user finally obtains  $\beta_1, \dots, \beta_{d-1} \in [0 : d-1]$  and

$$|Z^{\sum_{s=1}^{d-1} \beta_s} S(-\varphi_k) R_1(-\theta_k^1) \dots R_{d-1}(-\theta_k^{d-1})\rangle. \quad (88)$$

- d) Let  $X \otimes X'$  be the system of two qudits on which the state (87) is. The user performs the basis measurement  $\{|0\rangle, \dots, |d-1\rangle\}$  on  $X'$ . If the measurement outcome is 0, the user applies  $Z^{-\sum_{s=1}^{d-1} \alpha_s}$  on  $X$  and then the resultant state on  $X$  is the targeted state  $|\psi_k\rangle$ . This step is written as

$$|Z^{\sum_{s=1}^{d-1} \alpha_s} S(\varphi_k) R_1(\theta_k^1) \dots R_{d-1}(\theta_k^{d-1})\rangle \quad (89)$$

$$\mapsto |Z^{\sum_{s=1}^{d-1} \alpha_s} S(\varphi_k) R_1(\theta_k^1) \dots R_{d-1}(\theta_k^{d-1})|0\rangle \quad (90)$$

$$\mapsto |S(\varphi_k) R_1(\theta_k^1) \dots R_{d-1}(\theta_k^{d-1})|0\rangle \quad (91)$$

$$= |\psi_k\rangle. \quad (92)$$

Otherwise, repeat from Step 4-a. ■

Protocol 4 satisfies the correctness, secrecy, and communication complexity, desired in Theorem 5, which is shown as follows.

- **Correctness:** As described in Step 4, the user recovers  $|\psi_k\rangle$  with positive probability by repeating until success.
- **Secrecy:** This protocol satisfies the user secrecy, because the queries are the same as Protocol 3 and the number of requests in Step 4. Step 4-d is necessary since the states in (83) and (84) should be requested the same number of times. This protocol also satisfies the server secrecy, because the only information that the user obtains from the servers is states in (83) and (84) and these states only depend on the state  $|\psi_k\rangle$ .
- **Communication complexity:** At Step 1, the size of queries is  $2f$  bits. For downloading all states (83),  $2d \log d$ -qubit communication and  $d \log d$ -ebit are required. The probability to succeed to generate the state in (87) is  $1/d^{d-1}$  and therefore, the expected number of execution of Steps from 4-a to 4-c is  $d^{d-1}$ . Thus, for finishing Steps from 4-a to 4-c, the average quantum communication is less than  $2d^d \log d = d^{d-1} \cdot 2d \log d$  qubits and the average shared entanglement is less than  $d^d \log d = d^{d-1} \cdot d \log d$  ebits. Similarly, for Step 4-d, the same average quantum communication and the same average shared entanglement are required. Thus, Protocol 4 requires  $2f$ -bit classical communication,  $4d^d \log d$ -qubit average quantum communication, and  $2d^d \log d$ -ebit average prior entanglement.

The communication complexity of Protocol 4 does not scale with the number of message states  $f$ . Since the QPIR's trivial solution of downloading all messages requires  $f \log d$ -qubit quantum communication, Protocol 4 is more efficient on average if the number of messages  $f$  is greater than  $4d^d$ .

**Remark 1** (Comparison of Protocols 3 and 4 for qubit states). Both Protocols 3 and 4 can be applied for QPIR of qubit states. However, the average communication complexity of Protocol 3, which is 8 qubits and 4 ebits, is less than that of Protocol 4 for  $d = 2$ , which is 16 qubits and 8 ebits. The advantage of Protocol 3 comes from the commutation relation between the rotation operations  $R(\theta)$  and  $Y = XZ = R(\pi/2)$ . Since the reduced state after the Bell measurement is represented with  $Y, Z$  as (72) and  $Y$  is commutative with  $R(\theta)$  for any  $\theta$ , the user can reconstruct the targeted state efficiently as (73). On the other hand, the similar method cannot be applied for Protocol 4 because the rotation operations  $R(\theta)$  for  $d > 2$  are not commutative with any multiplication of  $X_d$  and  $Z_d$ . Thus, without using the commutative relation, Protocol 4 for  $d = 2$  results in greater communication complexity.

## VI. CONCLUSION

We have studied quantum private information retrieval for quantum messages in the blind and visible settings. We have proved that the trivial solution of downloading all messages is optimal for honest one-server QPIR, which is a similar result to the classical PIR but different from QPIR for classical messages. In the one-round case, the optimality is proved for both blind and visible settings, and in the multi-round case, it is proved for the blind setting. On the other hand, we have constructed efficient QPIR protocols with two cases. The first case is one-server QPIR with prior entanglement in the blind setting. We have constructed a reduction from any QPIR protocol for classical messages to a QPIR protocol for quantum messages and derived an efficient QPIR protocol from the protocol by Kerenidis et al. [14]. The second case is multi-server QSPIR in the visible setting. We have constructed three protocols for pure qubit states, pure qudit states, and pure states described by commutative unitaries. These protocols in the visible setting are symmetric QPIR protocols in which the user obtains no information other than the targeted message state. Thus, we proved that QSPIR is possible for quantum messages. Furthermore, these protocols are also more efficient than the QPIR's trivial solution when the number of messages are sufficiently greater than the dimension of quantum systems.

There are many open problems related to the study of QPIR for quantum messages. Our optimality proof of the trivial one-server QPIR protocol is for the one-round visible setting and the multi-round blind setting. It is unknown whether the optimality still applies for the multi-round one-server visible setting and the multi-server blind setting. Also, we have only considered QPIR with information-theoretic security. Our result does not preclude the possibility of the non-trivial one-server QPIR protocol with computational security. Furthermore, even if our QSPIR protocol for qudits is more efficient than the QPIR's trivial solution when the number of message states  $f$  is sufficiently large, the average communication complexity increases exponentially with the dimension  $d$  of the system. In addition, our QSPIR protocols are for pure states and it cannot be directly extended to protocols for the mixed state. Thus, more efficient QSPIR protocols for qudits and

QSPIR for mixed states are also open problems. Interesting applications of our QSPIR protocols can also be considered for other communication and computation problems. We leave these questions for interested readers.

## VII. ACKNOWLEDGEMENT

The authors are grateful to Prof. François Le Gall for helpful discussion and comments. SS is supported by JSPS Grant-in-Aid for JSPS Fellows No. JP20J11484. MH was supported in part by Guangdong Provincial Key Laboratory (Grant, No. 2019B121203002).

## REFERENCES

- [1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *Journal of the ACM*, 45(6):965–981, 1998.
- [2] C. Cachin, S. Micali, and M. Stadler, "Computationally Private Information Retrieval with Polylogarithmic Communication," *Advances in Cryptology - EUROCRYPT '99*, pp. 402–414, 1999.
- [3] H. Lipmaa, "First CPIR Protocol with Data-Dependent Computation," *Proceedings of the 12th International Conference on Information Security and Cryptology*, pp. 193–210, 2009.
- [4] 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.
- [5] S. Yekhanin, "Towards 3-query locally decodable codes of subexponential length," 39th STOC, 2007, pp. 266–274.
- [6] C. Devel, I. Goldberg, and N. Heninger, "Optimally Robust Private Information Retrieval," *21st USENIX Security Symposium*, August 2012.
- [7] H.-K. Lo, "Insecurity of quantum secure computations," *Phys. Rev. A*, 56(2): 1154–1162, 1997.
- [8] 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.
- [9] 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.
- [10] I. Kerenidis and R. de Wolf, "Quantum symmetrically-private information retrieval," *Information Processing Letters*, vol. 90, pp. 109–114, 2004.
- [11] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Physical Review A* 84, 022313, 2011.
- [12] Á. Baumeler and A. Broadbent, "Quantum Private Information Retrieval has linear communication complexity," *Journal of Cryptology*, vol. 28, pp. 161–175, 2015.
- [13] F. Le Gall, "Quantum Private Information Retrieval with Sublinear Communication Complexity," *Theory of Computing*, 8(16):369–374, 2012.
- [14] 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.
- [15] D. Aharonov, Z. Brakerski, K.-M. Chung, A. Green, C.-Y. Lai, O. Sattath, "On Quantum Advantage in Information Theoretic Single-Server PIR," In: Ishai Y., Rijmen V. (eds) *EUROCRYPT 2019*, Springer, Cham, vol. 11478, 2019.
- [16] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *Proceedings of 2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 1727–1731, 2019.
- [17] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2018 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019.
- [18] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, in press.
- [19] M. Allal, L. Holzbaur, T. Pillaha, and C. Hollanti, "Quantum Private Information Retrieval From Coded and Colluding Servers," *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 2, 2020.
- [20] W. Y. Kon and C. C. W. Lim, "Provably-secure symmetric private information retrieval with quantum cryptography," *arXiv:2004.13921 [quant-ph]*, 2020.

- [21] R. Jozsa and B. Schumacher, "A new proof of the quantum noiseless coding theorem," *J. Mod. Opt.*, 41(12), 2343–2349, 1994.
- [22] B. Schumacher, "Quantum coding," *Phys. Rev. A*, 51, 2738–2747, 1995.
- [23] R. Jozsa, M. Horodecki, P. Horodecki, and R. Horodecki, "Universal quantum information compression," *Phys. Rev. Lett.*, 81, 1714, 1998.
- [24] M. Horodecki, "Limits for compression of quantum information carried by ensembles of mixed states," *Phys. Rev. A*, 57, 3364–3369, 1998.
- [25] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "On quantum coding for ensembles of mixed states," *J. Phys. A Math. Gen.*, 34, 6767–6785, 2001.
- [26] M. Hayashi, "Exponents of quantum fixed-length pure state source coding," *Phys. Rev. A*, 66, 032321, 2002.
- [27] T. H. Chan, S.-W. Ho, and H. Yamamoto, "Private information retrieval for coded storage," in *Proceedings of 2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2842–2846, June 2015.
- [28] H. Sun and S. Jafar, "The capacity of private information retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4075–4088, 2017.
- [29] H. Sun and S. Jafar, "The Capacity of Symmetric Private Information Retrieval," 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1–5.
- [30] 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.
- [31] 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.
- [32] 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. 7, pp. 4243–4273, 2019.
- [33] 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.
- [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*, June 17–22, 2018.
- [35] K. Banawan and S. Ulukus, "The Capacity of Private Information Retrieval from Coded Databases," *IEEE Transactions on Information Theory*, vol. 64, no. 3, 2018.
- [36] C. Tian, H. Sun and J. Chen, "A Shannon-Theoretic Approach to the Storage-Retrieval Tradeoff in PIR Systems," *Proceedings of 2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 1904–1908, June 2018.
- [37] 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.
- [38] 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.
- [39] 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.
- [40] S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb, A. Sprintson, "Private information retrieval with side information," *IEEE Transactions on Information Theory* 66 (4), 2032–2043, 2019.
- [41] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti and C. Hollanti, "Private Information Retrieval From Coded Storage Systems With Colluding, Byzantine, and Unresponsive Servers," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3898–3906, 2019.
- [42] C. Bennett and S. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, 69 (20): 2881, 1992.
- [43] 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.