Song et al. *EPJ Quantum Technology* (2024) 11:55
https://doi.org/10.1140/epjqt/s40507-024-00266-6

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Prior entanglement exponentially improves one-server quantum private information retrieval for quantum messages

Seunghoan Song[1], François Le Gall[1] and Masahito Hayashi[2,3,1*]

*Correspondence:
hmasahito@cuhk.edu.cn;
hayashi@iqasz.cn
[2]School of Data Science, The Chinese University of Hong Kong, Shenzhen, Longgang District, Shenzhen, 518172, China
[3]International Quantum Academy (SIQA), Futian District, Shenzhen 518048, China
Full list of author information is available at the end of the article

Abstract

Quantum private information retrieval (QPIR) for quantum messages is a quantum communication task, in which a user retrieves one of the multiple quantum states from the server without revealing which state is retrieved. In the one-server setting, we find an exponential gap in the communication complexities between the presence and absence of prior entanglement in this problem with the one-server setting. To achieve this aim, as the first step, we prove that the trivial solution of downloading all messages is optimal under QPIR for quantum messages, which is a similar result to that of classical PIR but different from QPIR for classical messages. As the second step, we propose an efficient one-server one-round QPIR protocol with prior entanglement by constructing a reduction from a QPIR protocol for classical messages to a QPIR protocol for quantum messages in the presence of prior entanglement.

Keywords: Private information retrieval; Quantum private information retrieval; One-server model; Honest-server model; Quantum message

1 Introduction

1.1 Private information retrieval (PIR)

Entanglement is a valuable resource for quantum information processing, enabling various tasks including quantum teleportation [1] and dense coding, also known as entanglement-assisted communication [2]. Although entanglement-assisted communication enhances the speed not only for conventional communication but also for secret communication, their improvements are limited to constant times [3, 4]. In addition, it is often assumed in theoretical investigations of distributed quantum protocols that prior entanglement is available as a free resource because prior entanglement can be seen as a quantum counterpart of prior shared randomness [5, 6]. That is, one of great advantages of quantum system is to use prior entanglement instead of prior randomness. For further development of entanglement-assisted communication, we need to find significant improvement by entanglement-assisted communication.

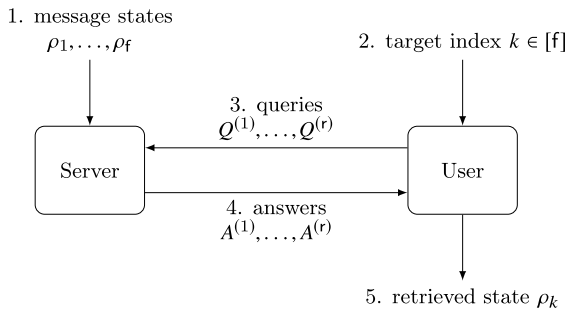

Figure 1 One-server QPIR protocol with quantum messages. At round i, the user uploads a query $Q^{(i)}$ and downloads an answer $A^{(i)}$

For this aim, we focus on private information retrieval (PIR) as Fig. 1, a task in which a user retrieves a message from a server without revealing which message has been retrieved, when the server possesses multiple messages. Hence, PIR is a key technology for keeping the privacy because it enables a person to hide his/her demand even with making his/her request. Therefore, it is a crucial issue for quantum information whether the use of entanglement enhances the performance of PIR.

Many papers [7–21] studied Quantum PIR (QPIR), i.e., PIR using quantum states, when the intended messages are given as the classical messages. This problem setting is simplified to C-QPIR. On the other hand, since various types of quantum information processings require the transmission of quantum states, i.e., the quantum messages [22–26], it is needed to develop QPIR for quantum messages, which is simplified to Q-QPIR, while no preceding paper studied this topic. In addition, in the multi-party quantum computing [27, 28], we often need to transmit quantum messages, i.e., quantum input states, instead of classical messages since it requires the protection of the coherence during the process of quantum computation. Therefore, for further development of quantum computer science, it is important to study various communication with quantum messages in addition to classical messages.

In this paper, to enhance quantum information technology, we study private information retrieval for quantum messages with one server, and present an exponential speedup through the use of prior entanglement as a significant improvement. Although there have been mainly two approaches: PIR with computational assumptions [29, 30] and PIR with multiple servers [31–33], recent attention has focused on information-theoretic aspects of PIR [34–48]. In this paper, we solely consider one-server QPIR without computational assumptions.

1.2 QPIR for classical messages

PIR has also been studied when quantum communication is allowed between the user and the server [7–21]. These papers consider the case when the total number of bits in the messages is m. For the secrecy in C-QPIR, we often focus on the potential information leakage in all rounds, which is called the *all-round criterion* in this paper and has been studied under several security models. One is the *honest-server model*, in which, we discuss the user's secrecy only when the server is honest, i.e., the server does not deviate from the protocol. The other is the *specious-server model*, in which, we discuss the user's secrecy even when the server deviates from the protocol as far as its dishonest operations are not revealed to

the user, which is called *specious adversary*. The secrecy under the specious-server model has a stronger requirement than the secrecy under the honest-server model. Interestingly, under the honest-server model, Le Gall [11] proposed a C-QPIR protocol with communication complexity $O(\sqrt{\mathsf{m}})$ in the all-round criterion, and Kerenidis et al. [12] improved this result to $O(\mathrm{poly}\log \mathsf{m})$ in another criterion, where the communication complexity in the quantum case is the total number of communicated qubits. Baumeler and Broadbent [10] considered the case when the specious-server model is adopted and the possible input states are extended to arbitrary superposition states. Then, they proved that the communication complexity is at least $\Theta(\mathsf{m})$, i.e., the trivial solution of downloading all messages is optimal also for this case. While indeed less realistic than the fully dishonest server model, investigating the honest model and the specious model is very often a fundamental (and necessary) step in cryptographic applications. Such investigations receive significant attention from the quantum cryptography community. For instance, the key paper [13] also focused on QPIR in the honest server model and the specious server model. These facts show that this problem setting has sufficient impact in the area of quantum computer science. In this paper, when arbitrary superposition states are allowed as input states, we consider the following; The user is required to recover the correct classical information only when the input state is a classical state. In other words, when the input state is a superposition state, any output is considered as a correct outcome.

Even when prior entanglement is allowed between the user and the server, the communication complexity is also lower bounded by $\Theta(\mathsf{m})$ under the specious-server model with the above extended possible input states [13]. Therefore, the advantage of prior entanglement is limited under the specious-server model with the above extended possible input states. In contrast, prior entanglement might potentially have polynomial improvement under the honest-server model, but it is still unclear how much prior entanglement improves communication complexity under the honest-server model.

When the server truly follows the protocol, the information obtained by the server is limited to the server's final state. Hence, the information leakage in the server's final state can be considered as another criterion, which is called the *final-state criterion*. While the final-state criterion under the honest-server model is a too weak setting, it is reasonable to consider the final-state criterion under the specious-server model, which is essentially equivalent to the cheat-sensitive setting studied in [49].

1.3 Our contributions

In this paper, for Q-QPIR protocols and the total number m of qubits, we show that the communication complexity is at least $\Theta(\mathsf{m})$, i.e., the trivial solution of downloading all messages is optimal for one-server Q-QPIR even in the final-state criterion and even with the honest-server model if prior entanglement is not allowed between the server and the user. This fact shows that prior entanglement between the server and the user is necessary for further improvement under the one-server model even for Q-QPIR under the honest-server model, the weakest secrecy requirement. To overcome this problem, we propose a one-server Q-QPIR protocol with prior entanglement between the server and the user, which achieves the communication complexity $O(\log \mathsf{m})$. That is, prior entanglement has exponential improvement for Q-QPIR under the honest-server model.

1.4 Organization of this paper

The remainder of the paper is organized as follows. Section 2 gives the definitions of several concepts and the outline of our results including the comparison with existing results. Section 3 is the technical preliminaries of the paper. Section 4 presents our results for C-QPIR protocol with communication complexity $O(\log \mathsf{m})$. Section 5 derives the lower bound of the communication complexity for Q-QPIR in the final-state criterion under the honest-server model when prior entanglement is not shared. Section 6 proposes an efficient Q-QPIR protocol with prior entanglement under various settings. Section 7 is the conclusion of the paper.

2 Definitions and outline of our results

2.1 Definitions of various concepts

To briefly explain our results, we prepare the definitions of various concepts to cover C-QPIR protocols and Q-QPIR protocols in a common framework.

2.1.1 Correctness, complexity, and unitary-type

To discuss the properties of our QPIR protocols, we prepare several concepts. First, we define the set $\mathcal{S}$ of possible quantum states as a subset of the set $\mathcal{S}(\mathcal{H}_d)$ of states on $\mathbb{C}^d$. A QPIR protocol is called a QPIR protocol with $\mathbb{C}^d$ over the set $\mathcal{S}$ when it works when the set $\mathcal{S}$ is the set of possible quantum states. For example, when $\mathcal{S}$ is the set $\mathcal{C}$ of orthogonal pure states $\{|j\rangle\}_{j=0}^{d-1}$, a QPIR protocol is a C-QPIR protocol discussed in [10]. In contrast, when $\mathcal{S}$ is the set $\mathcal{Q}$ of all pure states on the system $\mathbb{C}^d$, a QPIR protocol is a Q-QPIR protocol. When we do not identify the set $\mathcal{S}$, we consider that it is given as the above case. We denote the number of messages by f. A QPIR protocol Φ has two types of inputs. The first input is composed of f messages, whose systems are written as $\mathcal{H}_1, \ldots, \mathcal{H}_{\mathsf{f}}$. Their state is written as f states $(\rho_1, \ldots, \rho_{\mathsf{f}}) \in \mathcal{S}^{\mathsf{f}}$. The second input is the choice of the label of the message intended by the user, which is written as the random variable K. The quantum system to describe the variable K is denoted by $\mathcal{K}$. We denote the remaining initial user's and server's systems by $\mathcal{R}_u$ and $\mathcal{R}_s$, respectively. The output of the protocol is a state ρ_{out} on $\mathcal{H}_d$.

A QPIR protocol Φ has bilateral communication. The communication from the user to the servers is the upload communication, and the communication from the servers to the users is the download communication. The communication complexity is composed of the upload complexity and the download complexity. The upload complexity is the sum of the communication sizes of all upload communications, and the download complexity is the sum of the communication sizes of all download communications. The sum of the upload and download complexity is called the communication complexity. We adopt the communication complexity as the optimality criterion under various security conditions.

A QPIR protocol Φ is called a deterministic protocol when the following two conditions hold. The upload complexity and the download complexity are determined only by the protocol Φ. When the user and the servers are honest, the output is determined only by $(\rho_1, \ldots, \rho_{\mathsf{f}})$ and K. When Φ is a deterministic protocol, we denote the output state by $\Phi_{out}(\rho_1, \ldots, \rho_{\mathsf{f}}, K) = \rho_{out}$. The upload complexity, the download complexity, and the communication complexity are denoted by $UC(\Phi)$, $DC(\Phi)$, and $CC(\Phi)$, respectively. Hence, the communication complexity $CC(\Phi)$ is calculated as $UC(\Phi) + DC(\Phi)$. A protocol Φ is called correct when the protocol is a deterministic protocol and the relation $\Phi_{out}(\rho_1, \ldots, \rho_{\mathsf{f}}, k) = \rho_k$ holds for any elements $k \in [\mathsf{f}]$ and $(\rho_1, \ldots, \rho_{\mathsf{f}}) \in \mathcal{S}^{\mathsf{f}}$.

Another important class of QPIR protocols is unitary-type protocols. When a QPIR protocol Φ satisfies the following conditions, it is called *unitary-type*.

- The initial states $\rho_{\mathcal{R}_s}$ on $\mathcal{R}_s$ and $\rho_{\mathcal{R}_u}$ on $\mathcal{R}_u$ are pure.
- At each round, both the user and the server apply only unitary operations to the systems under their control.
- A measurement is done only when the user reads out the message as the outcome of the protocol.

The reference [13] refers to the above property as measurement-free due to the third condition while it assumes the first and second conditions implicitly. Since the first and second conditions are more essential, we call it unitary-type.

2.1.2 Secrecy

In this paper, we address only the secrecy of the user's choice. There are two security criteria. One is the final-state criterion, in which, it is required that the server's final state does not depend on the user's choice K. The other is the all-round criterion, in which, it is required that the server's state in any round does not depend on the user's choice K. When we consider the secrecy, we may extend the set of possible inputs to $\tilde{\mathcal{S}}$ that includes the set $\mathcal{S}$. For example, in the case of C-QPIR, the set $\mathcal{S}$ is given as the set $\mathcal{C}$. Then, we can choose $\tilde{\mathcal{S}}$ as the set $\mathcal{C}$ or $\mathcal{Q}$. The case with $\tilde{\mathcal{S}} = \mathcal{C}$ is called the classical input case, and the case with $\tilde{\mathcal{S}} = \mathcal{Q}$ is called the superposition input case. Instead, in the case of Q-QPIR, the set $\mathcal{S}$ is given as the set $\mathcal{Q}$. Hence, the set $\tilde{\mathcal{S}}$ is chosen as the same set $\mathcal{Q}$.

Even when we fix the security criterion and the sets $\mathcal{S}$ and $\tilde{\mathcal{S}}$, there still exist three models for the secrecy for a QPIR protocol Φ. The first one is the honest-server model, which assumes that the servers are honest. We say that a QPIR protocol Φ satisfies the secrecy in the final-state criterion under the honest-server model with input states $\tilde{\mathcal{S}}$ when the following condition holds. When the user and the servers are honest, the server has no information for K in the final state, i.e., the relation

$$\rho_{S,F}(\rho_1, \ldots, \rho_{\mathsf{f}}, k) = \rho_{S,F}(\rho_1, \ldots, \rho_{\mathsf{f}}, k') \tag{1}$$

holds for any $k, k' \in [\mathsf{f}]$ and $(\rho_1, \ldots, \rho_{\mathsf{f}}) \in \tilde{\mathcal{S}}^{\mathsf{f}}$, where $\rho_{S,F}(\rho_1, \ldots, \rho_{\mathsf{f}}, K)$ is the final state on the server dependent of the variable K. In the condition (1), the states ρ_k is chosen from $\tilde{\mathcal{S}}$, not from $\mathcal{S}$. We say that a QPIR protocol Φ satisfies the secrecy in the all-round criterion under the honest-server model with input states $\tilde{\mathcal{S}}$ when the following condition holds, the server has no information for K in all rounds, i.e., the relation

$$\rho_{S,j}(\rho_1, \ldots, \rho_{\mathsf{f}}, k) = \rho_{S,j}(\rho_1, \ldots, \rho_{\mathsf{f}}, k') \tag{2}$$

holds for any $k, k' \in [\mathsf{f}]$ and $(\rho_1, \ldots, \rho_{\mathsf{f}}) \in \tilde{\mathcal{S}}^{\mathsf{f}}$, where $\rho_{S,j}(\rho_1, \ldots, \rho_{\mathsf{f}}, K)$ is the state on the server dependent of the variable K when the server receives the query in the j-th round. The following is the meaning of the secrecy in the all-round criterion under the honest-server model. Assume that the user and the server are honest. Even when the server stops the protocol at the j-th round for any j, the server cannot obtain any information for K.

The second model is called the specious-server model introduced in [50]. When the server applies other operations that deviate from the original protocol, such an operation is called an attack. An attack of the server is called a specious attack when the attack satisfies

the following conditions. The server sends the answer at the time specified by the protocol, but the contents of the answer do not follow the protocol. Also, the server does not access the information under the control of the user. In addition, the attack is not revealed to the user under the condition that the user is honest, i.e., there exists the server's operation $\mathcal{F}_{S,j}$ such that the relation

$$(\mathcal{F}_{S,j} \otimes \iota)\tilde{\rho}_j(\rho_1, \ldots, \rho_{\mathsf{f}}, k) = \rho_j(\rho_1, \ldots, \rho_{\mathsf{f}}, k) \tag{3}$$

holds for any $k \in [\mathsf{f}]$ and $(\rho_1, \ldots, \rho_{\mathsf{f}}) \in \tilde{\mathcal{S}}^{\mathsf{f}}$, where $\rho_j(\rho_1, \ldots, \rho_{\mathsf{f}}, K)$ ($\tilde{\rho}_j(\rho_1, \ldots, \rho_{\mathsf{f}}, K)$) is the state on the whole system dependently of the variable K when the user receives the answer in the j-th round under the assumption that the user is honest and the server is honest (the server makes the attack). Notice that the definition of a specious attack depends on the choice of the set $\tilde{\mathcal{S}}$. The meaning of (3) is the following. When the user decides to stop the protocol to check whether the server follows the protocol after the user receives the answer in the j-th round, the user asks the server to submit the evidence that the server follows the protocol. Then, the server sends his system after applying the operation $\mathcal{F}_{S,j}$. When $\tilde{\mathcal{S}}$ is chosen to be the set $\mathcal{Q}$ of pure states, a specious attack coincides with a so-called 0-specious adversary, which is introduced in [13, Definition 2.4] because it is sufficient to check the case with even t in [13, Definition 2.4]. Also, when $\tilde{\mathcal{S}}$ is chosen to be the set $\mathcal{C}$, the secrecy in the all-round criterion under the specious server model coincides with the anchored 0-privacy under 0-specious servers [13].

We say that a QPIR protocol Φ satisfies the secrecy in the final-state criterion (the all-round criterion) under the specious-server model with input states $\tilde{\mathcal{S}}$ when the following condition holds. When a server performs a specious attack and the user is honest, the server obtains no information about the user's request K in all rounds, i.e., the condition (1) (the condition (2)) holds. In fact, the secrecy condition in the final-state criterion is weaker than the secrecy condition in the all-round criterion even under the specious-server model. The secrecy condition in the final-state criterion under the specious-server model is essentially equivalent to the cheat-sensitive secrecy condition considered in [49].

The third model is called the dishonest-server model. We say that a QPIR protocol Φ satisfies the secrecy under the dishonest-server model when the following condition holds. When the server applies an attack and the user is honest, the server obtains no information of the user's request K, i.e., the condition (1) holds. In the dishonest-server model, the server is allowed to make any attack under the following conditions. The server sends the answer at the time specified by the protocol, but the contents of the answer do not follow the protocol. Also, the server does not access the information under the control of the user. Thus, the server can send any information on each round under this condition. Hence, the ability of the attack does not depend on the set $\tilde{\mathcal{S}}$. Also, the server can store the state received in any round. Hence, the server can obtain the same information in the final state as the information in the j-th round.

Further, when the protocol has only one round and we adopt the all-round criterion, there is no difference among the honest-server model, the specious-server model, and the dishonest-server model because all information obtained by the server is reduced to the state on the server when the server received the query in the first round. As a result, the information obtained by the server does not depend on the server's operation, i.e., the server's attack model.

Remark 1 In the papers [10, 13], the security against specious adversaries means the secrecy in the all-round criterion under the specious-server model with input states $\mathcal{Q}$ for C-QPIR in our definition. Instead, in the paper [13], the anchored specious security means the secrecy in the all-round criterion under the specious-server model with input states $\mathcal{C}$ for C-QPIR in our definition. The papers [10, 13] did not consider the final-state criterion.

2.2 Outline of results and comparison

2.2.1 Optimality of trivial solution for one-server Q-QPIR

First, we discuss our result for one-server Q-QPIR for the honest-server model without prior entanglement, and its relation to existing results. The result by the reference [10] is summarized as follows. The C-QPIR protocol discussed in [10] is considered as a QPIR protocol over the set $\mathcal{C}$. The reference [10] showed that the trivial protocol over the set $\mathcal{C}$ is optimal in the all-round criterion under the specious-server model with input states $\mathcal{Q}$, i.e., when the secrecy in the all-round criterion is imposed under the specious-server model with input states $\mathcal{Q}$. Since the set $\mathcal{C} = \{|j\rangle\}_{j=0}^{d-1}$ is included in the set $\mathcal{Q}$, a Q-QPIR protocol over the set $\mathcal{Q}$ works a QPIR protocol over the set $\mathcal{C}$. Hence, the result by [10] implies the optimality of the trivial protocol over the set $\mathcal{Q}$ in the all-round criterion under the specious-server model. In addition, such an impossibility result was extended to the case with prior entanglement by the paper [13].

However, the secrecy in the all-round criterion under the specious-server model is a stronger condition than the secrecy in the final-state criterion under the honest-server model because the secrecy in the all-round criterion is a stronger condition the secrecy in the final-state criterion and the specious-server model allows the server to have a larger choice than the honest-server model.

To seek further possibility for C-QPIR protocols, in Sects. 4.1 and 4.2, inspired by the idea presented in [49], we propose more efficient one-round C-QPIR protocols in the final-state criterion under the honest-server and specious-server models with input states $\mathcal{C}$ or $\mathcal{Q}$ whose communication complexities are at most $4\log \mathsf{m}$. In addition, the reference [11] proposed a C-QPIR protocol in the all-round criterion under the honest one-server model that has communication complexity $O(\sqrt{\mathsf{m}})$. The reference [12] also proposed a C-QPIR protocol with communication complexity $O(\mathrm{poly}\log \mathsf{m})$ without prior entanglement and a C-QPIR protocol with communication complexity $O(\log \mathsf{m})$ with prior entanglement. In Sect. 4.3, we show that these two protocols satisfy the secrecy in the all-round criterion under the honest-server model with input states $\mathcal{C}$. In addition, using a conversion result [13], we show that these two protocols satisfy the secrecy in the all-round criterion under the specious-server model with input states $\mathcal{C}$.

Hence, we cannot exclude the possibility of more efficient one-server Q-QPIR protocols than the trivial solution in the final-state criterion or under the honest one-server model. Furthermore, while the trivial solution is optimal under the honest-server model of classical PIR [51], its optimality proof uses the communication transcript between the server and the user, which is based on classical communication. Unfortunately, we cannot apply the same technique under the honest one-server model of Q-QPIR because quantum states cannot be copied because of the no-cloning theorem. Therefore, we have a question of whether there exists a Q-QPIR protocol over pure states that satisfies the secrecy in the final-state criterion under the honest-server model, and improves the communication complexity over the trivial protocol.

Table 1 Optimal communication complexity of one-server C-QPIR

security criterion	input	server	Optimal communication complexity			
			without PE		with PE	
			one-round	multi-round	one-round	multi-round
final-state	classical	honest	$O(\log \mathsf{m})^*$ [Section IV A]	$O(\log \mathsf{m})^*$ [Section IV A]	$O(\log \mathsf{m})^*$ [Section IV A]	$O(\log \mathsf{m})^*$ [12]+[Lemma 8]
		specious	$O(\log \mathsf{m})^*$ [Section IV B]	$O(\log \mathsf{m})^*$ [Section IV B]	$O(\log \mathsf{m})^*$ [Section IV B]	$O(\log \mathsf{m})^*$ [12]+[Corollary 1]
	superposition	honest	$O(\log \mathsf{m})^*$ [Section IV A]	$O(\log \mathsf{m})^*$ [Section IV A]	$O(\log \mathsf{m})^*$ [Section IV A]	$O(\log \mathsf{m})^*$ [Section IV A]
		specious	?	?	?	?
all-round	classical	honest	$\Theta(\mathsf{m})$ [10]	$O(\text{poly} \log \mathsf{m})^*$ [12]+[Lemma 7]	$\Theta(\mathsf{m})$ [13]	$O(\log \mathsf{m})^*$ [12]+[Lemma 8]
		specious		$O(\text{poly} \log \mathsf{m})^*$ [12]+[Corollary 1]		$O(\log \mathsf{m})^*$ [12]+[Corollary 1]
	superposition	honest		?		?
		specious		$\Theta(\mathsf{m})$ [10]		$\Theta(\mathsf{m})$ [13]
dishonest				$\Theta(\mathsf{m})$ [10]		$\Theta(\mathsf{m})$ [13]

m is the total size of messages. * expresses the case when each message size is fixed. The symbol [12] + [Lemma 8] shows that the protocol was proposed in [12], but its secrecy is shown in Lemma 8 of this paper. These notations are applied to Table 2 as well.

Table 2 Optimal communication complexity of one-server Q-QPIR

security criterion	server	Optimal communication complexity			
		without PE		with PE	
		one-round	multi-round	one-round	multi-round
final-state	honest	$\Theta(\mathsf{m})$ [Theorem 1]	$\Theta(\mathsf{m})$ [Theorem 1]	$O(\log \mathsf{m})^*$ [Corollary 2]	$O(\log \mathsf{m})^*$ [Corollary 2]
	specious	$\Theta(\mathsf{m})$ [Theorem 1]	$\Theta(\mathsf{m})$ [Theorem 1]	$O(\log \mathsf{m})^*$ [Corollary 2]	$O(\log \mathsf{m})^*$ [Corollary 2]
all-round	honest	$\Theta(\mathsf{m})$ implied by [10]	$\Theta(\mathsf{m})$ [Theorem 1]	$\Theta(\mathsf{m})$ implied by [13]	$O(\log \mathsf{m})^*$ [Corollary 3]
	specious		$\Theta(\mathsf{m})$ implied by [10]		$\Theta(\mathsf{m})$ implied by [13]
dishonest			$\Theta(\mathsf{m})$ implied by [10]		$\Theta(\mathsf{m})$ implied by [13]

This table employs the same notations as Table 1.

As its solution, we show that the trivial solution is optimal for one-server Q-QPIR in the final-state criterion for the honest-server model. In Tables 1 and 2, we summarize the comparison of our results with previous results for the one-server case. In our proof, the entropic inequalities are the key instruments for the proof. Since the pair of the final-state criterion and the honest-server model is the weakest attack model, this result implies that the trivial solution is also optimal for any attack model.

2.2.2 One-server Q-QPIR protocol with prior entanglement

However, the above discussion assumes that there is no prior entanglement shared between the sender and the user. Hence, secondly, with prior entanglement between the user and the server, we prove that there exists an efficient Q-QPIR protocol on the honest-server model or on the final-state criterion. To be precise, we propose a method to construct a Q-QPIR protocol of communication complexity $O(f(\mathsf{m}))$ with prior entanglement from a C-QPIR protocol of communication complexity $O(f(\mathsf{m}))$ with prior entanglement. This method is based on the combination of C-QPIR and quantum teleportation [1]. The proposed Q-QPIR protocol inherits the security of the C-QPIR protocol. With this property, we show three types of Q-QPIR protocols of communication complexity $O(\log \mathsf{m})$ with prior entanglement. One is the secrecy in the final-state criterion under the honest-server model. The second is the secrecy in the final-state criterion under the specious-server model. The third is the secrecy in the all-round criterion under the honest-server

model. Combining this result with the above result, we find that prior entanglement realizes an exponential speedup for one-server Q-QPIR in the final-state criterion or under the honest-server model. Therefore, the obtained results are summarized as Table 1 in terms of the communication complexity m.

3 Preliminaries

We define $[a:b] = \{a, a+1, \ldots, b\}$ and $[a] = \{1, \ldots, a\}$. The dimension of a quantum system X is denoted by $|X|$. The von Neumann entropy is defined as $H(X) = H(\rho_X) = \mathrm{Tr}\, \rho_X \log \rho_X$, where ρ_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*) *The inequality* $H(XY) \le H(X) + H(Y)$ *holds, and the equality holds for product states on* $X \otimes Y$.

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

(*d*) $H(XY) + H(X) \ge H(Y)$.

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

The property (*d*) is proved as follows. Since other properties can be easily shown, we omit their proofs. For example, see the book [52, Sects. 3.1 and 8.1]. Let Z be the reference system in which the state on XYZ is pure. Then, $H(XY) + H(X) = H(Z) + H(X) \ge H(XZ) = H(Y)$. Throughout the paper, we use the symbols (*a*), (*b*), (*c*), (*d*), (*e*) to denote which property is used, e.g., $\overset{(a)}{=}$ means that the equality holds from the property (*a*).

Next, for a TP-CP map from the system $\mathcal{H}_X$ to the system $\mathcal{H}_Y$ and a state ρ on $\mathcal{H}_X$, we define the transmission information $I(\rho, \Gamma)$. We choose a purification $|\psi\rangle$ of ρ with the environment $\mathcal{H}_Z$. Then, the transmission information $I(\rho, \Gamma)$ is defined as

$$I(\rho, \Gamma) := H(\rho) + H(\Gamma(\rho)) - H((\iota_Z \otimes \Gamma)(|\psi\rangle\langle\psi|)), \tag{4}$$

where ι_Z is the identity operation on $\mathcal{H}_Z$. When Γ is the identity operator,

$$I(\rho, \Gamma) = 2H(\rho). \tag{5}$$

Throughout this paper, $\mathbb{C}^d$ expresses the d-dimensional Hilbert space spanned by the orthogonal basis $\{|s\rangle\}_{s=0}^{d-1}$. For a $d_1 \times d_2$ matrix

$$\mathsf{M} = \sum_{s=0}^{d_1-1} \sum_{t=0}^{d_2-1} m_{st} |s\rangle\langle t| \in \mathbb{C}^{d_1 \times d_2}, \tag{6}$$

we define

$$|\mathsf{M}\rangle\!\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d_1-1} \sum_{t=0}^{d_2-1} m_{st} |s\rangle|t\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}. \tag{7}$$

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

$$(\mathsf{B} \otimes \mathsf{C}^\top)|\mathsf{A}\rangle\!\rangle = |\mathsf{BAC}\rangle\!\rangle. \tag{8}$$

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

$$\mathsf{X}_d = \sum_{s=0}^{d-1} |s+1\rangle\langle s|, \tag{9}$$

$$\mathsf{Z}_d = \sum_{s=0}^{d-1} \omega^s |s\rangle\langle s|, \tag{10}$$

$$|\mathsf{I}_d\rangle\!\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} |s,s\rangle, \tag{11}$$

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

$$\mathbf{M}_{\mathsf{XZ},d} = \{|\mathsf{X}^a\mathsf{Z}^b\rangle\!\rangle \mid a,b \in [0:d-1]\}. \tag{12}$$

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

$$|\mathsf{A}\mathsf{X}^a\mathsf{Z}^{-b}\mathsf{B}^\top\rangle\!\rangle \in A \otimes B. \tag{13}$$

We also define the dual basis

$$|u_j\rangle := \sum_{k=0}^{d-1} \frac{1}{\sqrt{d}} e^{\frac{2\pi kji}{d}} |k\rangle. \tag{14}$$

4 Protocols for C-QPIR

4.1 One-round C-QPIR of the final-state criterion under honest-server model

This section presents a protocol that satisfies the secrecy in the final-state criterion under the honest-server model with the input states $\mathcal{C}$. We assume that the ℓ-th message X_ℓ is an element of $\mathbb{Z}_{d_\ell}$ for $\ell \in [\mathsf{f}]$. We define d as the maximum $\max_{\ell\in[\mathsf{f}]} d_\ell$.

Protocol 1 The following protocol is denoted by $\Phi_{\mathsf{f},d}$.

0) **Preparation**: The server prepares $\mathsf{f}+1$ quantum systems $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_\mathsf{f}$, where $\mathcal{H}_0$ is spanned by $\{|j\rangle\}_{j=0}^{d-1}$, and $\mathcal{H}_\ell$ is spanned by $\{|j\rangle\}_{j=0}^{d_\ell-1}$. When the ℓ-th message is X_ℓ, the state on the quantum system $\mathcal{H}_\ell$ is set to be $|X_\ell\rangle$. Also, the state on the quantum system $\mathcal{H}_0$ is set to be $|0\rangle$. The user prepares the system $\mathcal{K}$ spanned by $\{|\ell\rangle\}_{\ell=1}^{\mathsf{f}}$.
1) **Query (upload)**: The user sets the state on the system $\mathcal{K}$ to be $|K\rangle$. The user sends the system $\mathcal{K}$ to the server.
2) **Answer (download)**: The server applies the measurement based on the computation basis $\{|j\rangle\}$ on the systems $\mathcal{H}_1, \ldots, \mathcal{H}_\mathsf{f}$ with the projective state reduction. The server applies the controlled unitary $U := \sum_{\ell=1}^{\mathsf{f}} |\ell\rangle\langle\ell| \otimes U_\ell$ on $\mathcal{K} \otimes \mathcal{H}_0 \otimes \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_\mathsf{f}$, where U_ℓ acts only on $\mathcal{H}_0 \otimes \mathcal{H}_\ell$ and is defined as

$$U_\ell := \sum_{j'=0}^{d-1} \sum_{j=0}^{d_\ell-1} |j+j'\rangle\langle j'| \otimes |j\rangle\langle j|. \tag{15}$$

The server sends the system $\mathcal{K} \otimes \mathcal{H}_0$ to the user.

3) **Reconstruction**: The user measures $\mathcal{H}_0$, and obtains the message X_K.

Lemma 1 *Protocol 1 is correct and satisfies the secrecy in the final-state criterion under the honest-server model with the input states $\mathcal{C}$.*

Its upload and download complexities are $UC(\Phi_{\mathsf{f},d}) = \log \mathsf{f}$ and $DC(\Phi_{\mathsf{f},d}) = \log \mathsf{f} + \log d$. The communication complexity is $CC(\Phi_{\mathsf{f},d}) = 2\log \mathsf{f} + \log d$. When d is fixed, $CC(\Phi_{\mathsf{f},d}) = 2\log \mathsf{m} + o(\mathsf{m})$.

Proof The correctness of Protocol 1 can be checked as follows. Since $U_\ell |0\rangle \otimes |X_\ell\rangle = |X_\ell\rangle \otimes |X_\ell\rangle$, we have

$$U|K\rangle|0\rangle|X_1\rangle \cdots |X_{\mathsf{f}}\rangle = |K\rangle|X_K\rangle|X_1\rangle \cdots |X_{\mathsf{f}}\rangle. \tag{16}$$

Hence, the user gets the state $|K\rangle|X_K\rangle$, which contains the correct information X_K.

As shown in the following; Protocol 1 satisfies the secrecy in the final-state criterion under the honest-server model with the input states $\mathcal{C}$. We assume that the server and the user are honest. Since the server follows the protocol, the server has only the f systems $\mathcal{H}_1, \ldots, \mathcal{H}_{\mathsf{f}}$. The final state on the composite system $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{\mathsf{f}}$ is $|X_1\rangle \cdots |X_{\mathsf{f}}\rangle$, which does not depend on the user's choice K. Hence, the above secrecy holds. □

Lemma 1 can be strengthened as follows.

Lemma 2 *When we add the measurement with the computational basis on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{\mathsf{f}}$ in Step 2) in Protocol 1 before the unitary U is applied, the protocol is correct and satisfies the secrecy in the final-state criterion under the honest-server model even with the input states $\mathcal{Q}$.*

Proof Even when the initial states in $\mathcal{H}_1, \ldots, \mathcal{H}_{\mathsf{f}}$ prepared as quantum states, due to the measurement, the initial states in $\mathcal{H}_1, \ldots, \mathcal{H}_{\mathsf{f}}$ are convex mixtures of states $\{|j\rangle\langle j|\}$. Hence, the final state on the composite system $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{\mathsf{f}}$ is the same as the state after the measurement, which does not depend on user's choice K. Hence, the above secrecy holds. □

The following lemma shows the importance of measurement in Lemma 2.

Lemma 3 *Protocol 1 does not satisfy the secrecy in the final-state criterion under the honest-server model even with the input states $\mathcal{Q}$.*

Proof Assume that the server set initial state in $\mathcal{H}_\ell$ to be $\sum_{j=1}^{d_\ell} \frac{1}{\sqrt{d_\ell}}|j\rangle$. Also, we assume that the server and the user follow Steps 1), 2), 3). Then, the final state on $\mathcal{H}_K \otimes \mathcal{H}_0$ is $\sum_{j=1}^{d_\ell} \frac{1}{\sqrt{d_\ell}}|j\rangle|j\rangle$. That is, the final state on $\mathcal{H}_K$ is the completely mixed state. In contrast, the final state on $\mathcal{H}_\ell$ is the same as the initial state for $\ell \neq K$. Hence, the secrecy condition (1) does not hold. □

Also, we have the following lemma. That is, we need to modify Protocol 1 for the specious-server model.

Lemma 4 *Protocol 1 does not satisfy the secrecy in the final-state criterion under the specious-server model even with the input states $\mathcal{Q}$.*

Proof A specious server is allowed to make a measurement if the measurement does not destroy the quantum state. Since the state on the composite system $\mathcal{K}\otimes\mathcal{H}_0\otimes\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ is one of the computation basis, it is not destroyed by the measurement of the computation basis. Hence, the server can obtain the user's choice K without state demolition. This fact shows that the specious-server model is needed in order to forbid such an insecure protocol. However, as shown in Sect. 5, even under the honest-server model, a protocol similar to Protocol 1 does not work when the messages are given as quantum states. □

4.2 One-round C-QPIR of the final-state criterion under specious-server model

Protocol 1 presented in the previous subsection does not work under the specious-server model. To resolve this problem, this section presents a protocol that satisfies the secrecy in the final-state criterion under the specious-server model with the input states $\mathcal{C}$. We assume that each message X_ℓ is an element of $\mathbb{Z}_{d_\ell}$. We define d as the maximum $\max_\ell d_\ell$.

Protocol 2 The following protocol is denoted by $\Phi_{\mathsf{f},d}$.

0) **Preparation**: The server prepares $\mathsf{f}+2$ quantum systems $\mathcal{H}'_0,\mathcal{H}'_1,\mathcal{H}_1,\ldots,\mathcal{H}_{\mathsf{f}}$, where $\mathcal{H}'_0$, $\mathcal{H}'_1$ is spanned by $\{|j\rangle\}_{j=0}^{d-1}$, and $\mathcal{H}_\ell$ is spanned by $\{|j\rangle\}_{j=0}^{d_\ell-1}$. When the ℓ-th message is X_ℓ, the state on the quantum system $\mathcal{H}_\ell$ is set to be $|X_\ell\rangle$. Also, the state on the quantum system $\mathcal{H}'_0$, $\mathcal{H}'_1$ is set to be $|0\rangle$. The user prepares the systems $\mathcal{K}_0$,$\mathcal{K}_1$ spanned by $\{|\ell\rangle\}_{\ell=1}^{\mathsf{f}}$.
1) **Query (upload)**: The user generates the binary random variable A and the variable $B\in[\mathsf{f}]$ subject to the uniform distribution. The user sets the state on the system $\mathcal{K}_A$ to be $|K\rangle$, and the state on the system $\mathcal{K}_{A\oplus1}$ to be $\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle$. The user sends the systems $\mathcal{K}_0$, $\mathcal{K}_1$ to the server.
2) **Answer (download)**: The server applies the controlled unitary $U:=\sum_{\ell=1}^{\mathsf{f}}|\ell\rangle\langle\ell|\otimes U_\ell$ on $\mathcal{K}_0\otimes\mathcal{H}'_0\otimes\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$, where U_ℓ acts only on $\mathcal{H}'_0\otimes\mathcal{H}_\ell(=\mathcal{H}'_1\otimes\mathcal{H}_\ell)$ and is defined as

$$U_\ell:=\sum_{j'=0}^{d-1}\sum_{j=0}^{d_\ell-1}|j+j'\rangle\langle j'|\otimes|j\rangle\langle j|. \tag{17}$$

Then, the server applies the controlled unitary U on $\mathcal{K}_1\otimes\mathcal{H}'_1\otimes\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$. The server sends the systems $\mathcal{K}_0\otimes\mathcal{H}'_0$, $\mathcal{K}_1\otimes\mathcal{H}'_1$ to the user.
3) **Reconstruction**: The user measures $\mathcal{H}'_A$, and obtains the message X_K.

Lemma 5 *Protocol 2 is correct and satisfies the secrecy in the final-state criterion under the specious-server model with the input states $\mathcal{C}$.*

Its upload and download complexities are $UC(\Phi_{\mathsf{f},d})=2\log\mathsf{f}$ and $DC(\Phi_{\mathsf{f},d})=2\log\mathsf{f}+2\log d$. The communication complexity is $CC(\Phi_{\mathsf{f},d})=4\log\mathsf{f}+2\log d$. When d is fixed, $CC(\Phi_{\mathsf{f},d})=4\log\mathsf{m}+o(\mathsf{m})$.

Proof The correctness of Protocol 2 can be checked as follows. Due to the relation (16), when $A=0$, the state on the whole system $\mathcal{K}_0\otimes\mathcal{H}'_0\otimes\mathcal{K}_1\otimes\mathcal{H}'_1\otimes\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ before

the server sends back the system is $|K\rangle|X_K\rangle\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle|X_1\rangle\cdots|X_{\mathsf{f}}\rangle$. Hence, the user receives the state $|K\rangle|X_K\rangle\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle$, which contains the correct information X_K. Similarly, when $A=1$, the user receives a state containing the correct information X_K.

Next, we show that Protocol 2 satisfies the secrecy in the final-state criterion under the specious-server model with the input states $\mathcal{C}$. Assume that the server and the user follow the protocol. Then, the resultant state in the server's system $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ is the product state $|X_1\rangle\ldots|X_{\mathsf{f}}\rangle$. The resultant state in $\mathcal{K}_A\otimes\mathcal{H}'_A$ is $|K\rangle|X_K\rangle$. The resultant state in $\mathcal{K}_{A\oplus1}\otimes\mathcal{H}'_{A\oplus1}$ is $\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle$.

Hence, when $A=0$, the specious server needs to generate the state $|K\rangle|X_K\rangle\frac{1}{\sqrt{\mathsf{f}}}\times\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle$ from the state $|K\rangle\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle$. Also, when $A=1$, the specious server needs to generate the state $\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle|K\rangle|X_K\rangle$ from the state $\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|K\rangle$.

Since the resultant states $|K\rangle|X_K\rangle\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle$ and $\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|X_\ell\rangle|K\rangle|X_K\rangle$ are unitarily equivalent to the states $|K\rangle\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle$ and $\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{B}|\ell\rangle|K\rangle$, it is sufficient to discuss whether the server can get certain information from the state family $\mathcal{F}:=\{|k\rangle\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{b}|\ell\rangle,\frac{1}{\sqrt{\mathsf{f}}}\sum_{\ell=1}^{\mathsf{f}}\mathsf{Z}_{\mathsf{f}}^{b}|\ell\rangle|k\rangle\}_{k,b=1}^{\mathsf{f}}$ without disturbance.

However, due to Koashi-Imoto [53, 54] theory (Proposition 3 in the Appendix), any measurement obtains no information for K. When the states need to be recovered because the state family $\mathcal{F}$ satisfies the condition (A) in the Appendix. Therefore, when the server keeps the condition for the specious server, the server cannot obtain any information for K. □

Unfortunately, adding the measurement in Step 2) cannot guarantee that the protocol satisfies the secrecy in the final-state criterion under the specious-server model with the input states $\mathcal{Q}$. That is, we have the following lemma.

Lemma 6 *Even when we add the measurement with the computational basis on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ in Step* 2) *before the unitary U is applied, the protocol does not satisfy the secrecy in the final-state criterion under the specious-server model with the input states $\mathcal{Q}$.*

Proof Assume that the server sets a general initial pure state on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$, which is potentially a superposition state. When the server applies the measurement with the computational basis on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ in Step 2) after the unitary U is applied, the state on $\mathcal{K}_0\otimes\mathcal{H}'_0\otimes\mathcal{K}_1\otimes\mathcal{H}'_1$ is not changed. Further, even when the order of the above measurement and the unitary U is exchanged, the state on $\mathcal{K}_0\otimes\mathcal{H}'_0\otimes\mathcal{K}_1\otimes\mathcal{H}'_1$ is not changed. Therefore, even when the server does not make the measurement with the computational basis on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ in Step 2) before the unitary U is applied, the state sent to the user is not changed.

Now, we assume that the server sets the initial state in $\mathcal{H}_\ell$ to be $|\Psi_\ell\rangle:=\sum_{j=1}^{d_\ell}\frac{1}{\sqrt{d_\ell}}|j\rangle$. When U_ℓ is applied, the resultant state on $\mathcal{H}_\ell$ is the completely mixed state $\rho_{mix,\ell}$. Otherwise, it is $|\Psi_\ell\rangle$. The resultant state on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_{\mathsf{f}}$ does not depend on whether the measurement on the computational basis on $\mathcal{K}_0\otimes\mathcal{K}_1$ is done before the unitary U. Hence, we can consider the following. When $K=\ell$, U_ℓ is applied with probability 1. Otherwise, U_ℓ is applied with probability $\frac{1}{\mathsf{f}}$. Therefore, when $K=\ell$, the resultant state on $\mathcal{H}_\ell$ is the completely mixed state $\rho_{mix,\ell}$. Otherwise, the resultant state on $\mathcal{H}_\ell$ is $\frac{1}{\mathsf{f}}\rho_{mix,\ell}+(1-\frac{1}{\mathsf{f}})|\Psi_\ell\rangle\langle\Psi_\ell|$. Hence, the server obtains a certain information for the value K in the final state. □

4.3 C-QPIR in all-round criterion

In this section, we discuss the secrecy in the all-round criterion of the C-QPIR protocol with communication complexity $O(\mathrm{poly}\log \mathsf{m})$ under the fixed message size $d = 2$ from [12, Sect. 5], which does not use any prior entanglement, and the C-QPIR protocol with communication $O(\log \mathsf{m})$ under the fixed message size $d = 2$ from [12, Sect. 6], which uses $\Theta(\mathsf{m})$ ebits of prior entanglement. Although these protocols fix the message size d to be 2, they can be generalized to protocols whose message sizes are fixed to an arbitrary d by treating $\lceil \log_2 d \rceil$ messages as one message.

4.3.1 Secrecy of the protocol from [12, *Sect.* 5] *under the honest server model*

The protocol from [12, Sect. 5] works for the case $d = 2$. The server's input is thus $(a_1, \ldots, a_{\mathsf{f}})$ for $a_1, \ldots, a_{\mathsf{f}} \in \{0,1\}$. The user's input is an index $K \in \{1, \ldots, \mathsf{f}\}$.

The main idea is to simulate a classical multi-server PIR protocol with $s = O(\log \mathsf{m})$ servers that has total communication complexity $O(\mathrm{poly}\log \mathsf{m})$. Such protocols are known to exist (see, e.g., [51]) and can be described generically as follows. The user picks a uniform random variable G from $\{1, \ldots, \mathsf{g}\}$, computes an s-tuple of queries $\{q_1(G,K), \ldots, q_s(G,K)\}$ from (G,K) by using a function q_t, and asks query $q_t(G,K)$ to the t-th server. Here, for each $t \in \{1, \ldots, s\}$, the function q_t satisfies the condition that the distribution of query $q_t(G,K)$ is independent of K. Each server t then sends its answer $\mathsf{ans}_t(q_t(G,K))$ to the user, who recovers a_K from $\{\mathsf{ans}_1(q_1(G,K)), \ldots, \mathsf{ans}_s(q_s(G,K))\}$.

The protocol from [12, Sect. 5] simulates this protocol using only one server. The protocol uses $2s + 1$ quantum registers denoted $Q, Q_1, \ldots, Q_s, Ans_1, \ldots, Ans_s$. For each $t \in \{1, \ldots, s\}$, let us define the following quantum state:

$$
\begin{aligned}
&|\Phi_t\rangle \\
=&\frac{1}{\sqrt{\mathsf{g}}} \sum_g |q_1(g,K), \ldots, q_s(g,K)\rangle_Q \, |q_1(g,K)\rangle_{Q_1} \cdots |q_s(g,K)\rangle_{Q_s} \\
&\otimes |\mathsf{ans}_1(q_1(g,K))\rangle_{Ans_1} \cdots |\mathsf{ans}_{t-1}(q_{t-1}(g,K))\rangle_{Ans_{t-1}} \\
&\otimes |0\rangle_{Ans_t} \cdots |0\rangle_{Ans_s} .
\end{aligned}
$$

Note that we have in particular

$$
\begin{aligned}
&|\Phi_1\rangle \\
=&\frac{1}{\sqrt{\mathsf{g}}} \sum_g |q_1(g,K), \ldots, q_s(g,K)\rangle_Q \, |q_1(g,K)\rangle_{Q_1} \cdots |q_s(g,K)\rangle_{Q_s} \\
&\otimes |0\rangle_{Ans_1} \cdots |0\rangle_{Ans_s} .
\end{aligned}
$$

The protocol from [12, Sect. 5] consists of the following interaction between the user and the server (some details of the manipulations of the states are omitted since they are irrelevant to the secrecy proof):

1. The user prepares the state $|\Phi_1\rangle$.
2. The user and the server iterate the following for $t = 1$ to s:
   2.1 The user sends Registers Q_t, Ans_t to the server;

2.2 The server applies a controlled unitary, where the controlling system is Q_t and the controlled system is Ans_t. Then, the server sends back Registers Q_t, Ans_t to the user.

3. The user measures the joint system composed of Registers $Q, Q_1, \ldots, Q_s, Ans_1, \ldots, Ans_s$ to obtain the outcome a_K after certain unitary operations.

We now show the secrecy of this protocol under the honest server model.

Lemma 7 *The protocol from* [12, *Sect.* 5] *is unitary-type and satisfies the secrecy in the all-round criterion under the honest server model when the set $\tilde{\mathcal{S}}$ of possible inputs is $\mathcal{C}$.*

Proof The protocol is clearly unitary-type. The remaining task is then to show the secrecy of this protocol in the all-round criterion under the honest server model when the set $\tilde{\mathcal{S}}$ of possible inputs is $\mathcal{C}$. Observe that at each iteration there is only a message sent to the server, at Step 2.1. We thus only need to show that for each t, this message does not reveal any information about K. The state of the whole system at the end of Step 2.1 of the t-th iteration is $|\Phi_t\rangle$. The state of the server, obtained by tracing out all registers except Q_t, Ans_t of $|\Phi_t\rangle\langle\Phi_t|$ is

$$\frac{1}{\mathsf{g}} \sum_{g} |q_t(g,K)\rangle_{Q_t} |0\rangle_{Ans_t} \langle q_t(g,K)|_{Q_t} \langle 0|_{Ans_t} . \tag{18}$$

Since the distribution of query $q_t(G,K)$ is independent of K, we conclude that the whole state of the server at the end of Step 2.1 is independent of K, for each t. □

4.3.2 Secrecy of the protocol from [12, *Sect.* 6] *under the honest server model*

The protocol from [12, Sect. 6] works for the case $d = 2$ and $\mathsf{f} = 2^{\mathsf{h}}$, for $\mathsf{h} \geq 1$. The server's input is thus $(a_1, \ldots, a_{\mathsf{f}})$ for $a_1, \ldots, a_{\mathsf{f}} \in \{0,1\}$. The user's input is an index $K \in \{1, \ldots, \mathsf{f}\}$.

The protocol uses $2\mathsf{h} + 2$ quantum registers denoted $R_1, \ldots, R_{\mathsf{h}}, \mathsf{R}'_1, \ldots, \mathsf{R}'_{\mathsf{h}}, Q_0, Q_1$. For each $p \in \{1, \ldots, \mathsf{h}\}$, let us define the following quantum state over the two registers R_t, R'_p:

$$|\Phi_p\rangle = \frac{1}{\sqrt{2^{2^{\mathsf{h}-p}}}} \sum_{z \in \{0,1\}^{2^{\mathsf{h}-p}}} |z\rangle_{R_p} |z\rangle_{\mathsf{R}'_p} .$$

For any binary string $z \in \{0,1\}^s$ with s even, we denote $z[0]$ the first half of z, and $z[1]$ the second half of z. For any binary strings $z, z' \in \{0,1\}^s$, we write $z \oplus z' \in \{0,1\}^s$ the string obtained by taking the bitwise parity of z and z'.

The protocol from [12, Sect. 6] assumes that the server and the user initially share the state

$$|\Phi_1\rangle \otimes \cdots \otimes |\Phi_{\mathsf{h}}\rangle \cdots \otimes |0\rangle_{Q_0} |0\rangle_{Q'_0} ,$$

where $R_1, \ldots, R_{\mathsf{h}}, Q_0, Q_1$ are owned by the server and $R'_1, \ldots, R'_{\mathsf{h}}$ are owned by the user. The protocol consists of the following interaction between the user and the server (some details of the manipulations of the states are omitted since they are irrelevant to the secrecy proof):

1. For p from 1 to h the server and the user do the following:

1.1 The server applies a unitary V_p (defined in [12, Eq. (27)]) on Registers R_{p-1}, R_p, Q_0, Q_1 and then sends Registers Q_0, Q_1 to the user;
1.2 If the p-th bit of its input K is 0, the user applies the Pauli gate Z on Register Q_0. If the p-th bit of K is 1, the user applies Z on Register Q_1. The user then sends back Registers Q_0, Q_1 to the server.
1.3 The server applies again the unitary V_p on Registers R_{p-1}, R_p, Q_0, Q_1, and then applies a Hadamard transform on each qubit in Register R_p.
1.4 The user applies a Hadamard transform on each qubit in Register R'_p.

2. The server sends Register R_{h} to the user. The user measures the joint system composed of Registers $R'_1, \ldots, \mathsf{R}'_{\mathsf{h}}$ and Register R_{h}, and performs some classical post-processing on the outcome to obtain a_K

The following lemma from [12] will be useful for our secrecy proof: Lemma 2 in [12] shows that the state of the whole system at the end of Step 1.3 is

$$|\Psi_p\rangle \otimes \bigotimes_{j=p+1}^{\mathsf{h}} |\Phi_j\rangle_{(R_j,R'_j)} \otimes |0\rangle_{Q_0} |0\rangle_{Q'_0}$$

with

$$|\Psi_p\rangle = \frac{1}{\sqrt{2^{2^{\mathsf{h}-1}} \cdots 2^{2^{\mathsf{h}-p}}}} \sum_{y^1,\ldots,y^p} \bigotimes_{j=1}^{p} |y^j\rangle_{R_j} |y^{j-1}[i_j] \oplus y^j\rangle_{R'_j},$$

where the sum is over all strings $y^1 \in \{0,1\}^{2^{\mathsf{h}-1}}, \ldots, y^p \in \{0,1\}^{2^{\mathsf{h}-p}}$ and we use the convention that y^0 is the server's input $(a_1, \ldots, a_{\mathsf{f}})$.[1] Here the server owns Registers $R_1, \ldots, R_{\mathsf{h}}, Q_0, Q_1$ while the user owns Registers $R'_1, \ldots, R'_{\mathsf{h}}$.

We now show the secrecy of this protocol under the honest server model (see also Appendix B in [13]).

Lemma 8 *The protocol from* [12, *Sect.* 6] *is unitary-type and satisfies the secrecy in the all-round criterion under the honest server model when the set $\tilde{\mathcal{S}}$ of possible inputs is $\mathcal{C}$.*

Proof The protocol is clearly unitary-type. The remaining task is then to show the secrecy of this protocol in the all-round criterion under the honest server model when the set $\tilde{\mathcal{S}}$ of possible inputs is $\mathcal{C}$. Since the initial state does not depend on K, it is sufficient to show that the whole state on Register $R_1, \ldots, R_{\mathsf{h}}, Q_0, Q_1$ at the end of Step 1.2 of the p-th round is independent of K.

Observing that tracing out Registers $R'_1, \ldots, R'_j$ from $|\Psi_p\rangle \langle\Psi_p|$ gives the state

$$\frac{1}{2^{2^{\mathsf{h}-1}} \cdots 2^{2^{\mathsf{h}-p}}} \sum_{y^1,\ldots,y^p} |y^1\rangle_{R_1} \cdots |y^p\rangle_{R_p} \langle y^1|_{R_1} \cdots \langle y^p|_{R_p},$$

which is independent of K, we find that the whole state on Register $R_1, \ldots, R_{\mathsf{h}}, Q_0, Q_1$ at the end of Step 1.3 of the p-th round is independent of K, for each p. Since the unitaries

[1] Observe that y^{j-1} is a binary string of length $2^{\mathsf{h}-(j-1)}$, and then $y^{j-1}[i_j]$ is a binary string of length $2^{\mathsf{h}-(j-1)-1} = 2^{\mathsf{h}-j}$. The term $y^{j-1}[i_j] \oplus y^j$ in the definition of $|\Psi_p\rangle$ is thus well defined.

applied in Step 1.3 by the server are independent of K, we conclude that the whole state on Register $R_1, \dots, R_{\mathsf{h}}, Q_0, Q_1$ at the end of Step 1.2 of the p-th round is independent of K. □

4.3.3 Secrecy under the specious server model

Finally, we discuss the secrecy under the specious server model. We will rely on the following theorem from [13] for unitary-type QPIR protocols.

Proposition 2 (Theorem 3.2 in [13]) *When a unitary-type QPIR protocol satisfies the secrecy in the all-round criterion under the honest server model with the set $\tilde{\mathcal{S}} = \mathcal{C}$, it satisfies the secrecy in the all-round criterion under the specious server model with the same set $\tilde{\mathcal{S}} = \mathcal{C}$.*

We thus obtain the following corollary of Lemmas 7 and 8.

Corollary 1 *The protocols from* [12, *Sect.* 5] *and* [12, *Sect.* 6] *satisfy the secrecy in the all-round criterion under the specious server model when the set $\tilde{\mathcal{S}}$ of possible inputs is $\mathcal{C}$.*

Therefore, when the message size d is fixed to a constant, there exists a C-QPIR protocol with communication complexity $O(\mathrm{poly}\log \mathsf{m})$ ($O(\log \mathsf{m})$) and without any prior entanglement (with prior entanglement) that satisfies the secrecy in the all-round criterion under the specious server model when the set $\tilde{\mathcal{S}}$ of possible inputs is $\mathcal{C}$.

5 Optimality of trivial protocol in final-state criterion for Q-QPIR under honest server model

In this section, we prove that the trivial solution of downloading all messages is optimal for Q-QPIR. In particular, this section, unlike the references [10, 13], we show the optimality in the final-state criterion under the honest-server model. Since our setting is discussed under the honest-server model, the secrecy in the final-state criterion is required only when the server follows the determined state preparation process and determined quantum operations. In the formal description of our protocols, we consider that the user and the server apply CPTP maps but we describe the CPTP maps by the equivalent representation with the unitary maps and the local quantum memories.

To be precise, we define the r-round Q-QPIR protocol as follows. A 2-round protocol is depicted in Fig. 2, and the symbols are summarized as Table 3. The message states are given as arbitrary f states $\rho_{[\mathsf{f}]} := \rho_1 \otimes \cdots \otimes \rho_{\mathsf{f}}$ on $S^{(0)} = X_1 \otimes \cdots \otimes X_{\mathsf{f}}$, where each of ρ_ℓ is purified in $X_\ell \otimes R_\ell$. We use the notation $R_{[\mathsf{f}]} := R_1 \otimes \cdots \otimes R_{\mathsf{f}}$. The server contains the system $S^{(0)}$. The user chooses the index of the targeted message $K \in [\mathsf{f}]$, i.e., ρ_k is the targeted quantum state when $K = k$. When $K = k$, the user prepares the initial state as $|k\rangle \otimes |0\rangle \in A^{(0)} \otimes T^{(0)}$. Although we consider the model in which the user and the server apply CPTP maps, we describe it by the equivalent representation with the unitary maps and the local quantum memories. A Q-QPIR protocol Φ is described by unitary maps $\mathcal{D}^{(0)}, \dots, \mathcal{D}^{(\mathsf{r})}, \mathcal{E}^{(1)}, \dots, \mathcal{E}^{(\mathsf{r})}$ in the following steps.

1. **Query (upload)**: For all $i \in [\mathsf{r}]$, 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. Here, $T^{(i)}$ are the user's local quantum systems for describing the CPTP maps applied by the user.

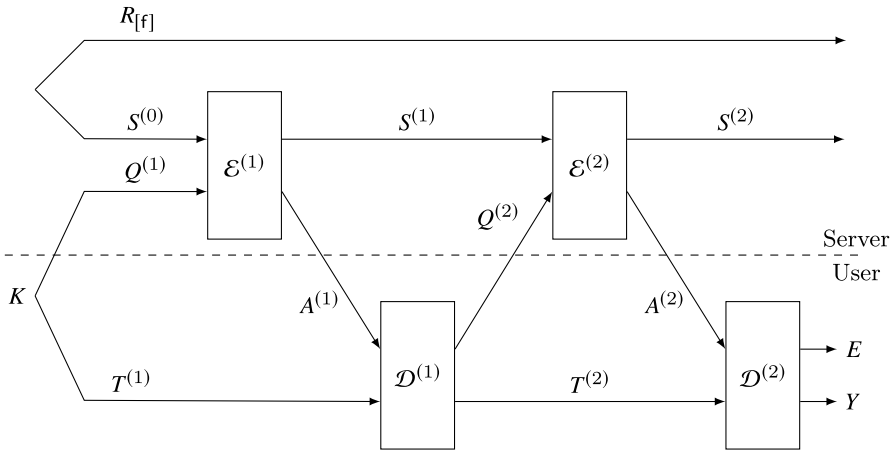

Figure 2 2-round QPIR protocol. The user sends the systems $Q^{(1)}$ and $Q^{(2)}$ to the server. The server sends the systems $A^{(1)}$ and $A^{(2)}$ to the user. The initial state $\rho_{[f]}$ on $S^{(0)}$ is arbitrary chosen. $R_{[f]}$ is the reference of the system $S^{(0)}$

Table 3 Definition of symbols

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

2. **Answer (download)**: 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. Here, $S^{(i)}$ are the server's local quantum systems for describing the CPTP maps applied by the server.
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 Λ_Φ of the protocol Φ is written with a CPTP $\Gamma_{\Phi,k}$ from $S^{(0)}$ to Y as

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

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

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

$$\Gamma_{\Phi,k} \otimes \mathrm{id}_{R_k}(\rho_{[f]\setminus\{k\}} \otimes |\psi_k\rangle\langle\psi_k|) = |\psi_k\rangle\langle\psi_k| \tag{19}$$

  for any $K = k$ and any state $\rho_{[f]}$.
- **Secrecy**: When the final state on $S^{(r)} \otimes R_{[f]}$ with the target index $K = k$ is denoted by $\rho^k_{S^{(r)}R_{[f]}}$, the secrecy is

$$\rho^k_{S^{(r)}R_{[f]}} = \rho^{k'}_{S^{(r)}R_{[f]}} \tag{20}$$

  for any k, k'.

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

Theorem 1 *For any multi-round Q-QPIR protocol* Φ, *the communication complexity* $\mathrm{CC}(\Phi)$ *is lower bounded by* $\sum_{\ell=1}^{\mathsf{f}} \log |X_\ell|$, *where* X_ℓ *is the system of the* ℓ*-th message* ρ_ℓ.

For the proof of Theorem 1, we prepare the following lemmas.

Lemma 9 $H(A^{(i)}) + H(Q^{(i+1)}) \geq H(T^{(i+1)}) - H(T^{(i)})$.

Proof Lemma 9 is shown by the relation

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

Here, (b), (c), and (d) express the respective properties presented in Proposition 1. □

Lemma 10 *The relation* $H(R_{[\mathsf{f}]}S^{(\mathsf{r})}) \geq \sum_{\ell=1}^{\mathsf{f}} H(R_\ell)$ *holds.*

Proof Given the user's input k, Correctness (19) guarantees that the final state on $R_k \otimes Y$ is a pure state, and therefore, R_k is independent of any system except for Y. Thus, R_k is independent of $R_{[\mathsf{f}]\setminus\{k\}}S^{(\mathsf{r})}$. The secrecy condition (20) guarantees that the final state on $R_{[\mathsf{f}]} \otimes S^{(\mathsf{r})}$ does not depend on k. Hence, $R_1, \ldots, R_{\mathsf{f}}$, and $S^{(\mathsf{r})}$ are independent of each other. Therefore, we have

$$H(R_{[\mathsf{f}]}S^{(\mathsf{r})}) = H(S^{(\mathsf{r})}) + \sum_{\ell=1}^{\mathsf{f}} H(R_\ell) \geq \sum_{\ell=1}^{\mathsf{f}} H(R_\ell). \tag{21}$$

Proof of Theorem 1 We choose the initial state on $R_\ell \otimes X_\ell$ to be the maximally entangled state for $\ell = 1, \ldots, \mathsf{f}$. From Lemmas 9 and 10, we derive the following inequalities:

$$\begin{aligned}
&\mathrm{CC}(\Phi) \geq \sum_{i=1}^{\mathsf{r}} \left(H(A^{(i)}) + H(Q^{(i)})\right) \\
&= H(A^{(\mathsf{r})}) + H(Q^{(1)}) + \sum_{i=1}^{\mathsf{r}-1} \left(H(A^{(i)}) + H(Q^{(i+1)})\right) \\
&\geq H(A^{(\mathsf{r})}) + H(Q^{(1)}) + H(T^{(\mathsf{r})}) - H(T^{(1)}) \qquad (22) \\
&= H(A^{(\mathsf{r})}) + H(T^{(\mathsf{r})}) \qquad (23) \\
&\overset{(b)}{\geq} H(A^{(\mathsf{r})}T^{(\mathsf{r})}) \overset{(a)}{=} H(R_{[\mathsf{f}]}S^{(\mathsf{r})}) \\
&\geq \sum_{\ell=1}^{\mathsf{f}} H(R_\ell) = \sum_{\ell=1}^{\mathsf{f}} \log |X_\ell|, \qquad (24)
\end{aligned}$$

where (a) and (b) express the respective properties presented in Proposition 1. In addition, (22) is obtained by applying Lemma 9 for all $i = 1, \dots, \mathsf{r}-1$. The step (23) follows from $H(Q^{(1)}) = H(T^{(1)})$ which holds due to the property (a) in Proposition 1, because the state on $Q^{(1)}T^{(1)}$ is the pure state as the state on $Q^{(0)}T^{(0)}$ is the pure state. The step (24) follows from Lemma 10. □

6 Q-QPIR protocol with prior entanglement under honest-server model

In the previous section, we proved that the trivial solution is optimal even in the final-state criterion under the honest one-server model of Q-QPIR. In this section, we construct a Q-QPIR protocol with lower communication complexity under various secrecy models than the trivial solution when we allow shared entanglement between the user and the server.

Let $\mathsf{m} = \sum_{\ell=1}^{\mathsf{f}} \log |X_\ell|$ be the size of all messages. To measure the amount of the prior entanglement, we count sharing one copy of $|\mathsf{I}_2\rangle\!\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ as an *ebit*. Accordingly, we count sharing the state $|\mathsf{I}_d\rangle\!\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ as $\log d$ ebits.

Theorem 2 *Suppose there exists a C-QPIR protocol under a certain secrecy model with communication complexity $f(d_1, \dots, d_{\mathsf{f}})$ when $g(d_1, \dots, d_{\mathsf{f}})$-ebit prior entanglement is shared between the user and the server. Then, there exists a Q-QPIR protocol under the same secrecy model with communication complexity $f(d_1^2, \dots, d_{\mathsf{f}}^2)$ when $\mathsf{m} + g(d_1, \dots, d_{\mathsf{f}})$-ebit prior entanglement is shared between the user and the server.*

The protocol satisfying Theorem 2 is a simple combination of quantum teleportation [1] 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 (11). Hence, the type of guaranteed secrecy in the original C-QPIR protocol is inherited to the converted QPIR protocol. We construct the Q-QPIR protocol satisfying Theorem 2 as follows.

Protocol 3 Let Φ_{cl} be a C-QPIR protocol and $d_1, \dots, d_{\mathsf{f}}$ be the size of the f classical messages. From this protocol, we construct a Q-QPIR protocol as follows.

Let $X_1, \dots, X_{\mathsf{f}}$ be the quantum systems with dimensions $d_1, \dots, d_{\mathsf{f}}$, respectively, and $\rho_1, \dots, \rho_{\mathsf{f}}$ be the quantum message states on systems $X_1, \dots, X_{\mathsf{f}}$. The user and the server share the maximally entangled states $|\mathsf{I}_{d_\ell}\rangle\!\rangle$, defined in (11), on $Y_\ell \otimes Y'_\ell$ for all $\ell \in [\mathsf{f}]$, where $Y_{[\mathsf{f}]}$ and $Y'_{[\mathsf{f}]}$ are possessed by the user and the server, respectively.

The user and the server perform the following steps.

1) **Preparation**: For all $\ell \in [\mathsf{f}]$, the server performs the generalized Bell measurement $\mathbf{M}_{\mathsf{XZ},d_\ell}$, defined in (12), 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) **Use of C-QPIR protocol**: The user and the server perform the C-QPIR protocol Φ_{cl} to retrieve $m_k = (a_k, b_k)$.
3) **Reconstruction**: The user recovers the k-th message ρ_k by applying $\mathsf{X}_{d_k}^{-a_k}\mathsf{Z}_{d_k}^{b_k}$ on Y_k.

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

$R_\ell \otimes Y_\ell$ is

$$(\mathsf{I} \otimes \mathsf{X}_{d_\ell}^{a_\ell} \mathsf{Z}_{d_\ell}^{-b_\ell}) |\phi_\ell\rangle \tag{25}$$

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

To analyze the secrecy of Protocol 3, note that only Step 2 has the communication between the user and the server. Thus the secrecy of Protocol 3 is guaranteed by the secrecy of the underlying protocol Φ_{cl}.

Protocol 1 (Protocol 2) is a one-round C-QPIR protocol in the final-state criterion under the honest-server model (the specious-server model) with input states $\mathcal{C}$ with communication complexity $2\log \mathsf{f} + \log d$ ($4\log \mathsf{f} + 2\log d$). Therefore, the combination of Protocols 1 and 3 and the combination of Protocols 2 and 3 yield the following corollary.

Corollary 2 *There exists a Q-QPIR protocol with communication complexity* $2\log \mathsf{f} + \log d^2 = 2\log \mathsf{f}d$ ($4\log \mathsf{f} + 2\log d^2 = 4\log \mathsf{f}d$) *and prior entanglement* m *that satisfies the secrecy in the final-state criterion under the honest-server model* (*the specious-server model*). *When d is a constant, the communication complexity is* $2\log \mathsf{m} + o(\mathsf{m})$ ($4\log \mathsf{m} + o(\mathsf{m})$).

Proof The case under the honest-server model is trivial. Hence, we show the desired statement under the specious-server model.

Assume that the server makes a specious attack. The user's state at the end of Step 2) of Protocol 3 is the pair of entanglement halves σ_1 and the state transmitted at Step 2) of Protocol 2 σ_2. Due to the specious condition, the state σ_1 needs to be one of the states $\{\mathsf{X}^a\mathsf{Z}^b \rho_K (\mathsf{X}^a\mathsf{Z}^b)^\dagger\}_{(a,b)\in[0:d-1]^2}$ with equal probability. That is, using the random variable $(a,b) \in [0:d-1]^2$ under the uniform distribution, the state σ_1 is written as $\mathsf{X}^a\mathsf{Z}^b \rho_K (\mathsf{X}^a\mathsf{Z}^b)^\dagger$. Hence, the state σ_2 needs to be decided according to the random variable (a,b) in the same way as the honest case. That is, the state σ_2 satisfies the condition for the state transmitted by a specious server of Protocol 2 at Step 2). Since Protocol 2 satisfies the secrecy under the final-state criterion under the specious-server model with input states $\mathcal{C}$, the specious server obtains no information in the final state. That is, the combined Q-QPIR protocol with prior entanglement satisfies the secrecy under the final-state criterion under the specious-server model. □

Combining Theorem 2 and Corollary 1, we obtain the following corollary.

Corollary 3 *There exists a Q-QPIR protocol with communication complexity* $O(\log \mathsf{m})$ *and prior entanglement of* $\Theta(\mathsf{m})$ *ebits that satisfies the secrecy in the all-round criterion under the honest-server model when the message size d is fixed to a constant.*

One property of Protocol 3 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 ρ_ℓ if the user could retrieve classical information $m_\ell \in [0:d_\ell - 1]^2$ corresponding to the state ρ_ℓ.

7 Conclusion

We have shown an exponential gap for the communication complexity of one-server Q-QPIR in the final-state criterion or under the honest-server model between the existence

and the non-existence of prior entanglement. For this aim, as the first step, we have proposed an efficient one-server one-round C-QPIR protocol in the final-state criterion. Also, we have shown that the protocols proposed in [12] satisfies the secrecy in the all-round criterion under the honest server model. Then, as the second step, we have proved that the trivial solution of downloading all messages is optimal even in the final-state criterion for honest one-server Q-QPIR, which is a similar result to that of classical PIR but different from C-QPIR. As the third step, we have developed a conversion from any C-QPIR protocol to a Q-QPIR protocol, which yields an efficient Q-QPIR protocol with prior entanglement from a C-QPIR protocol. The proposed protocols exhibit an exponential improvement over the Q-QPIR's trivial solution.

In fact, Protocols 1 and 2 work as one-server one-round C-QPIR protocol in the final-state criterion under the honest-server model or the specious-server model. However, Theorem 1 shows that no analogy of Protocol 1 nor 2 works for Q-QPIR protocol under similar settings without prior entanglement. This impossibility is caused by the no-cloning property of the quantum system, i.e., the property that the noiseless channel has no information leakage to the third party, because the proof of Theorem 1 relies on the fact that noiseless quantum communication ensures that the entropy of the final state on the third party is equal to the entropy of the final state on the composite system comprising the output system and the reference system. This impossibility is one of the reasons for our obtained exponential gap.

The above exponential gap has been established under three problem settings. The first and the second are the final-state criterion under the honest-server model and under the specious-server model. The third is the all-round criterion under the honest-server model. In other words, other problem settings do not have such an exponential improvement by using prior entanglement. This exponential improvement is much larger than the improvement achieved through the use of dense coding [2]. This exponential improvement can be considered as a useful application of prior entanglement. It is an interesting open problem to find similar exponential improvement by using prior entanglement.

Appendix: Koashi-Imoto theory

Here, we discuss Koashi-Imoto theory [53] under the following assumption. We assume a state family $\mathcal{S} = \{\rho_x\}_{x\in\mathcal{X}}$ on $\mathcal{H}$ satisfies the following condition.

(A) When a subspace $\mathcal{K} \subset \mathcal{H}$ satisfies the condition $P_{\mathcal{K}}\rho_x = \rho_x P_{\mathcal{K}}$ for any element $x \in \mathcal{X}$, the $\mathcal{K}$ is $\{0\}$ or $\mathcal{H}$, where $P_{\mathcal{K}}$ is the projection to $\mathcal{K}$,

Under the above assumption, we have the following proposition.

Proposition 3 *Assume the assumption* (*A*). *We consider a POVM* $\{M_y\}_{y\in\mathcal{Y}}$ *on* $\mathcal{H}$. *When there exists a TP-CP map* Γ_y *for any element* $y \in \mathcal{Y}$ *such that the relation* $\sum_y \Gamma_y(\sqrt{M_y}\rho_x \times \sqrt{M_y}) = \rho_x$ *holds for any element* $x \in \mathcal{X}$, *then* M_y *is a constant times of the identity operator.*

To prove Proposition 3, we rewrite Theorem 9 of [54] under the assumption (A).

Proposition 4 ([54, Theorem 9], [53]) *Assume the assumption* (*A*). *When a TP-CP map* Γ *satisfies the relation* $\Gamma(\rho_x) = \rho_x$ *holds for any element* $x \in \mathcal{X}$, *then* Γ *is the identity operator.*

Proof We choose the TP-CP map $\Gamma(\rho) := \sum_y \Gamma_y(\sqrt{M_y}\rho\sqrt{M_y})$. The TP-CP map Γ satisfies the condition for Proposition 4. We choose Steinspring representation of Γ_y as an ancilla

system $\mathcal{R}$, an initial pure state ρ_0 on $\mathcal{R}$, and a unitary U_y on $\mathcal{H} \otimes \mathcal{R}$ such that $\Gamma_y(\rho) = \mathrm{Tr}_R U_y(\rho \otimes \rho_0)U_y^\dagger$, where we can choose $\mathcal{R}$ and ρ_0 commonly for Γ_y. Here, we assume that $\mathcal{R}$ is spanned by $\{|1\rangle_R, \ldots, |d_R\rangle_R\}$ and ρ_0 is $|1\rangle_{RR}\langle 1|$.

Therefore, we have $\sum_y \mathrm{Tr}_R U_y(\sqrt{M}_y \rho \sqrt{M}_y \otimes \rho_0)U_y^\dagger = \rho$. Since the above relation holds for any pure state ρ, $\mathrm{Tr}_R U_y(\sqrt{M}_y \rho \sqrt{M}_y \otimes \rho_0)U_y^\dagger$ is a constant times of ρ for any x. Further, since $\mathrm{Tr}_R U_y(\sqrt{M}_y \rho \sqrt{M}_y \otimes \rho_0)U_y^\dagger$ is a pure state for any pure state ρ, ${}_R\langle j|U_y|1\rangle_R$ is a constant times of ${}_R\langle 1|U_y|1\rangle_R$ for $j = 2, \ldots, d_R$. Since U_y is a unitary, ${}_R\langle j|U_y|1\rangle_R$ is also a unitary. Thus, ${}_R\langle j|U_y|1\rangle_R \sqrt{M}_y \rho \sqrt{M}_y ({}_R\langle j|U_y|1\rangle_R)^\dagger$ is a constant times of ρ. Thus, $\sqrt{M}_y$ is a constant times of a unitary. That is, $\sqrt{M}_y$ is a constant times of the identity operator. □

Abbreviations
PIR, private information retrieval; QPIR, quantum private information retrieval; C-QPIR, quantum private information retrieval for the classical messages; Q-QPIR, quantum private information retrieval for the quantum messages.

Author contributions
S. S. initiated this project, and prepared figures 1 and 2. M. H. prepared Tables I, II, and III. F. L. contributed Section IV-C. M. H. and S. S. wrote the main manuscript text except for Section IV-C. All authors reviewed the manuscript.

Funding
SS was supported by Research Fellow of the Japan Society for the Promotion of Science No. JP20J11484. FLG was partially supported by Japan Society of the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (S) under Grant 24H00071, for Scientific Research (A) under Grants 20H00579 and 21H04879, and for Scientific Research (B) under Grant 20H04139. MH was supported in part by the National Natural Science Foundation of China No. 62171212.

Data Availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author details
[1]Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya, 464-8602, Japan. [2]School of Data Science, The Chinese University of Hong Kong, Shenzhen, Longgang District, Shenzhen, 518172, China. [3]International Quantum Academy (SIQA), Futian District, Shenzhen 518048, China.

Received: 21 April 2024 Accepted: 26 August 2024 Published online: 06 September 2024

References

1. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett. 1993;70(13):1895–9.
2. Bennett CH, Wiesner SJ. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett. 1992;69:2881.
3. Wang C, Deng F-G, Li Y-S, Liu X-S, Long G-L. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A. 2005;71:044305.
4. Wu J, Long G-L, Hayashi M. Quantum secure direct communication with private dense coding using a general preshared quantum state. Phys Rev Appl. 2022;17:064011.
5. Gavoille C, Kosowski A, Markiewicz M. What can be observed locally? Round-based models for quantum distributed computing. In: Proc. DISC'09: proceedings of the 23rd international conference on distributed computing. 2009. p. 243–57.
6. Elkin M, Klauck H, Nanongkai D, Pandurangan G. Can quantum communication speed up distributed computation? In: PODC'14: proceedings of the 2014 ACM symposium on principles of distributed computing. 2014. p. 166–75.
7. Kerenidis I, de Wolf R. Exponential lower bound for 2-query locally decodable codes via a quantum argument. In: Proc. 35th ACM symposium on theory of computing (STOC' 03). 2003. p. 106–15.
8. Kerenidis I, de Wolf R. Quantum symmetrically-private information retrieval. Inf Process Lett. 2004;90:109–14.
9. Olejnik L. Secure quantum private information retrieval using phase-encoded queries. Phys Rev A. 2011;84:022313.
10. Baumeler Ä, Broadbent A. Quantum private information retrieval has linear communication complexity. J Cryptol. 2015;28:161–75.

11. Le Gall F. Quantum private information retrieval with sublinear communication complexity. Theory Comput. 2012;8(16):369–74.
12. Kerenidis I, Laurière M, Le Gall F, Rennela M. Information cost of quantum communication protocols. Quantum Inf Comput. 2016;16(3–4):181–96.
13. Aharonov D, Brakerski Z, Chung K-M, Green A, Lai C-Y, Sattath O. On quantum advantage in information theoretic single-server PIR. In: Ishai Y, Rijmen V, editors. EUROCRYPT 2019. vol. 11478. Cham: Springer; 2019.
14. Song S, Hayashi M. Capacity of quantum private information retrieval with multiple servers. IEEE Trans Inf Theory. 2021;67(1):452–63.
15. Song S, Hayashi M. Capacity of quantum private information retrieval with collusion of all but one of servers. IEEE J Sel Areas Inf Theory. 2021;2(1):380–90.
16. Song S, Hayashi M. Capacity of quantum private information retrieval with colluding servers. IEEE Trans Inf Theory. 2021;67(8):5491–508.
17. Allaix M, Holzbaur L, Pllaha T, Hollanti C. Quantum private information retrieval from coded and colluding servers. IEEE J Sel Areas Inf Theory. 2020;1(2):599–610.
18. Allaix M, Song S, Holzbaur L, Pllaha T, Hayashi M, Hollanti C. On the capacity of quantum private information retrieval from MDS-coded and colluding servers. IEEE J Sel Areas Commun. 2022;40(3):885–98.
19. Kon WY, Lim CCW. Provably secure symmetric private information retrieval with quantum cryptography. Entropy. 2021;23(1):54.
20. Wang C, Kon WY, Ng HJ, Lim CC. Experimental symmetric private information retrieval with measurement-device-independent quantum network. Light: Sci Appl. 2022;11:268.
21. Wang C, Kon WY, Ng HJ, Lim CC. Experimental symmetric private information retrieval with quantum key distribution. In: Sciarrino F, Treps N, Giustina M, Silberhorn C, editors. Quantum information and measurement VI 2021. Technical digest series. Optica Publishing Group; 2021.
22. Wiesner S. Conjugate coding. SIGACT News. 1983;15(1):78–88.
23. Gottesman D, Chuang I. Quantum Digital Signatures. 2001. arXiv:quant-ph/0105032.
24. Mochon C. Quantum weak coin flipping with arbitrarily small bias. 2007. arXiv:0711.4114.
25. Chailloux A, Kerenidis I. Optimal quantum strong coin flipping. In: Proc. 50th annual IEEE symposium on foundations of computer science, FOCS 2009. Atlanta, Georgia, USA. October 25-27, 2009. 2009. p. 527–33.
26. Aharonov D, Chailloux A, Ganz M, Kerenidis I, Magnin L. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. SIAM J Comput. 2016;45(3):633–79.
27. Crépeau C, Gottesman D, Smith A. Secure multi-party quantum computing. In: STOC'02: proceedings of the thiry-fourth annual ACM symposium on theory of computing. 2002. p. 643–52.
28. Goyal V, Liang X, Malavolta G. On concurrent multi-party quantum computation. In: Handschuh H, Lysyanskaya A, editors. Advances in cryptology – CRYPTO 2023. CRYPTO 2023. Lecture notes in computer science. vol. 14085. Cham: Springer; 2023.
29. Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication. In: Advances in cryptology - EUROCRYPT'99. 1999. p. 402–14.
30. Lipmaa H. First CPIR protocol with data-dependent computation. In: Proceedings of the 12th international conference on information security and cryptology. 2009. p. 193–210.
31. Beimel A, Stahl Y. Robust information-theoretic private information retrieval. In: Proceedings of the 3rd international conference on security in communication networks (SCN'02). 2003. p. 326–41.
32. Yekhanin S. Towards 3-query locally decodable codes of subexponential length. J ACM. 2008;55(1):1–6.
33. Devet C, Goldberg I, Heninger N. Optimally robust private information retrieval. In: 21st USENIX security symposium. 2012.
34. Chan TH, Ho S-W, Yamamoto H. Private information retrieval for coded storage. In: Proc. IEEE international symposium on information theory (ISIT2015). Hong Kong, China. June, 14–19, 2015. 2015. p. 2842–6.
35. Sun H, Jafar S. The capacity of private information retrieval. IEEE Trans Inf Theory. 2017;63(7):4075–88.
36. Sun H, Jafar S. The capacity of symmetric private information retrieval. In: 2016 IEEE globecom workshops (GC Wkshps). Washington. 2016. p. 1–5.
37. Sun H, Jafar S. The capacity of robust private information retrieval with colluding databases. IEEE Trans Inf Theory. 2018;64(4):2361–70.
38. Banawan K, Ulukus S. The capacity of private information retrieval from coded databases. IEEE Trans Inf Theory. 2018;64(3):1945–56.
39. Freij-Hollanti R, Gnilke OW, Hollanti C, Karpuk DA. Private information retrieval from coded databases with colluding servers. SIAM J Appl Algebra Geom. 2017;1(1):647–64.
40. Kumar S, Lin H-Y, Rosnes E, Graell i Amat A. Achieving maximum distance separable private information retrieval capacity with linear codes. IEEE Trans Inf Theory. 2019;65(7):4243–73.
41. Lin H-Y, Kumar S, Rosnes E, Graell i Amat A. An MDS-PIR capacity-achieving protocol for distributed storage using non-MDS linear codes. In: Proc. IEEE international symposium on information theory (ISIT2018), Talisa Hotel in Vail. Colorado, USA. June, 17–22, 2018. 2018. p. 966–70.
42. Tian C, Sun H, Chen J. A Shannon-theoretic approach to the storage-retrieval tradeoff in PIR systems. In: Proc. IEEE international symposium on information theory (ISIT2018), Talisa Hotel in Vail. Colorado, USA. June, 17–22, 2018. 2018. p. 1904–8.
43. Wang Q, Skoglund M. Symmetric private information retrieval for MDS coded distributed storage. In: Proceedings of 2017 IEEE international conference on communications (ICC). 2017. p. 1–6.
44. Tandon R. The capacity of cache aided private information retrieval. In: Proc. 2017 55th annual Allerton conference on communication, control, and computing (Allerton). 2017. p. 1078–82.
45. Banawan K, Ulukus S. The capacity of private information retrieval from byzantine and colluding databases. IEEE Trans Inf Theory. 2019;65(2):1206–19.
46. Holzbaur L, Freij-Hollanti R, Li J, Hollanti C. Towards the capacity of private information retrieval from coded and colluding servers. IEEE Trans Inf Theory. 2022;68(1):517–37.
47. Kadhe S, Garcia B, Heidarzadeh A, El Rouayheb S, Sprintson A. Private information retrieval with side information. IEEE Trans Inf Theory. 2019;66(4):2032–43.

48. Tajeddine R, Gnilke OW, Karpuk D, Freij-Hollanti R, Hollanti C. Private information retrieval from coded storage systems with colluding, byzantine, and unresponsive servers. IEEE Trans Inf Theory. 2019;65(6):3898–906.
49. Giovannetti V, Lloyd S, Maccone L. Quantum private queries. Phys Rev Lett. 2008;100:230502.
50. Dupuis F, Nielsen JB, Salvail L. Secure two-party quantum evaluation of unitaries against specious adversaries. In: Proc. 30th annual conference on advances in cryptology (CRYPTO'10). Berlin: Springer; 2010. p. 685–706.
51. Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. J ACM. 1998;45(6):965–81.
52. Hayashi M. Quantum information theory: mathematical foundation, graduate texts in physics. Berlin: Springer; 2017.
53. Koashi M, Imoto N. Phys Rev A. 2002;66:022318.
54. Hayden P, Jozsa R, Petz D, Winter A. Commun Math Phys. 2004;246:359.

Publisher's Note