Two-Server Oblivious Transfer for Quantum Messages

Masahito Hayashi* and Seunghoan Song

Oblivious transfer is considered as a cryptographic primitive task for quantum information processing over a quantum network. It is an essential building block for secure multiparty computation. It is known that one-server oblivious transfer is impossible. When the task is the transmission of classical messages, protocols for two-server oblivious transfer exist, i.e., existing protocols work under the assumption that two servers do not communicate with each other. However, when the task is the transmission of a quantum state, no existing method works even under the above two-server assumption. Two-server oblivious transfer protocols for quantum messages are proposed for the first time.

1. Introduction

The construction of quantum internet is the ultimate goal of quantum technology.[1,2] Quantum state communication and entanglement sharing over long distances are basic functions of the quantum internet, but to fully extract its potential, it is essential to find out its applications. Although major efforts are devoted to the developments of quantum algorithm with single user, obtained quantum algorithms are still limited. To extract the merit of quantum information processing, it is better to focus on secure quantum computation because a quantum system is very sensitive for an intended operation. Therefore, one promising direction is distributed quantum protocols and algorithms with security. For example, quantum network coding has been studied from theory to experiment[1–18] and blind quantum computation has also been extensively studied.[19–28]

As another distributed secure quantum protocol, this paper studies two-server quantum oblivious transfer (Q-TQOT) for the transmission of quantum states. Oblivious transfer is the task that the user downloads the intended message among several messages from the servers under two requirements. As the first condition, the user’s choice of the intended message is not leaked to the servers, which is called the user secrecy, when the user is honest and the servers make arbitrary operations. As the second condition, the information of other messages is not leaked to the user, which is called the server secrecy, when the servers are honest and the user makes arbitrary operations. Although several studies[29,30] proposed protocols for one-server oblivious transfer, they are not secure. It is known that one-server oblivious transfer is impossible even with the quantum system without a certain assumption.[31] Although recently, Wang et al.[32] proposed a protocol for one-server oblivious transfer, its security is the computational security, which is based on the computational assumption.

However, if there are two servers that do not communicate with each other, oblivious transfer is possible without the computational assumption when the messages are given as classical information. That is, two-server oblivious transfer for classical messages (C-TOT) is available, and is often called two-server symmetric private information retrieval (SPIR) for classical messages. It is known that oblivious transfer is an essential building block for secure multiparty computation.[33,34] In secure multiparty computation, it is natural to restrict the number of colluding players. Hence, two-server oblivious transfer is helpful for secure multiparty computation. For this reason, it is natural to study two-server oblivious transfer with the quantum setting without the computational assumption.

Although two-server oblivious transfer for classical messages is possible by using classical communication, the use of quantum communication improves its communication speed. In the following, this problem setting with quantum communication is simplified to classical two-server quantum oblivious transfer (C-TQOT). Several studies were done on this problem when the message is classical information and a noiseless quantum channel is available. For example, Kerenidis and de Wolf[35,36] studied this problem by relaxing the secrecy criterion. When the number of messages is fixed, the preceding study[37] derived the optimal transmission rate for this problem, which is defined similarly to its classical counterpart[38,39] as the optimal communication efficiency for arbitrary-long classical messages. It proved that a protocol can be constructed without any communication loss when the message is classical information, a noiseless quantum channel is available, and prior entanglement among servers is allowed. The papers[40,41] and Allaix et al.[42,43] also considered this problem with colluding servers in which secrecy of the protocol is preserved even if some servers may communicate and...
collude. Kon and Lim[44] constructed a two-server oblivious transfer protocol with quantum-key distribution and Wang et al.[45,46] implemented two-server oblivious transfer protocols experimentally. Their implementation attracts much attention as a new and novel quantum technology.

Besides the above studies, in the quantum network, it is often required to transmit quantum messages, i.e., quantum states as a subprotocol in various quantum computation tasks.[47–51] However, no preceding paper studied two-server oblivious transfer for quantum messages, which is simplified to Q-TQOT. In fact, it is not trivial to establish an efficient protocol to achieve this task of Q-TQOT as follows.

For example, the trivial method to download all states from the servers satisfies the user secrecy condition, but does not satisfy the server secrecy condition. When both servers share the classical information to describe the target quantum state and they send this classical information by using C-TQOT, in order that the user recovers the desired quantum state precisely, both servers need to send infinitely-large size of information to the user. Hence, when the zero-error condition is imposed, such simple use of C-TQOT does not work. When the servers and the user share prior entanglement, a simple combination of the quantum teleportation and C-TQOT does not work as follows. In order that a server uses quantum teleportation to send a quantum state, the server has to make a Bell measurement. However, the outcome of this measurement cannot be shared. Since C-TQOT requires the sharing of the message between two servers, C-TQOT cannot be applied to the outcome of the Bell measurement in the quantum teleportation. Therefore, it is much demanded to develop protocols achieving the task of Q-TQOT.

Our requirement is to realize both secrecy conditions simultaneously. This paper proposes various protocols to satisfy both conditions. In our proposed protocols, two servers have classical descriptions of f quantum messages \(\rho_1, \ldots, \rho_f\). To implement the desired protocol, we assume that the two servers share several entangled states. The protocol is outlined as follows while several variants exist. The user intends to get only one quantum state \(\rho_{\phi}\) and sends query \(Q\) and \(Q'\) to Servers 1 and 2, respectively while its label \(K\) is not leaked to both servers. That is, while the combination of \(Q\) and \(Q'\) identifies the label \(K\), one query \(Q\) nor \(Q'\) does not determine \(K\). Later, both servers send the user their entanglement half after a certain quantum operation determined by queries \(Q\) and \(Q'\). Finally, the user makes a decoding operation to recover the state \(\rho_{\phi}\).

The remainder of the paper is organized as follows. Section 2 gives the definitions of several concepts. Section 3 presents the outline of our protocol constructions. Section 4 is the technical preliminaries of the paper. Sections 5–12 are devoted to the construction of our protocols. Section 13 is the conclusion of the paper.

2. Definitions of Various Concepts

To briefly explain our results, we prepare the definitions of various concepts.

2.1. Correctness and Complexity

To discuss the properties of our Q-TQOT protocols, we prepare several concepts. First, we define the set \(S\) of possible quantum states as a subset of the set \(S(H_f)\) of states on \(H_f := \mathbb{C}^d\). A Q-TQOT protocol is called a Q-TQOT protocol over the set \(S\) when it works when the set \(S\) is the set of possible quantum states. We denote the number of messages by \(f\). A Q-TQOT protocol \(\Phi\) has two types of inputs. The first input is \(f\) states \((\rho_1, \ldots, \rho_f) \in S^f\). 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 output of the protocol is a state \(\rho_{\phi} = \Phi_{S} (\rho_1, \ldots, \rho_f, K)\) on \(H_f\).

A Q-TQOT protocol \(\Phi\) 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 communication complexity. We adopt communication complexity as the optimality criterion under various security conditions.

A Q-TQOT protocol \(\Phi\) is called a deterministic protocol when the following two conditions hold. The upload complexity and the download complexity are determined only by the protocol \(\Phi\). When the user and the servers are honest, the output is determined only by \((\rho_1, \ldots, \rho_f)\) and \(K\). Otherwise, it is called a probabilistic protocol. When \(\Phi\) is a deterministic protocol, we denote the output state by \(\Phi_{\text{out}}(\rho_1, \ldots, \rho_f, K) = \rho_{\phi}\). 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 \(UC(\Phi) + DC(\Phi)\).

Next, we consider the case when \(\Phi\) is a probabilistic protocol. Even when the user and the servers are honest, the user has a random variable \(X\) that determines the upload complexity, the download complexity, and the output state \(\rho_{\phi}\). We denote the distribution of \(X\) by \(P_{\phi}\), and denote the upload complexity, the download complexity, the communication complexity, and the output state by \(UC_X(\Phi)\), \(DC_X(\Phi)\), \(CC_X(\Phi)\), and \(\rho_{\phi,X}(\rho_1, \ldots, \rho_f, K) = \rho_{\phi}\), respectively.

A deterministic protocol \(\Phi\) is called correct when the relation \(\Phi_{\text{out}}(\rho_1, \ldots, \rho_f, \ell) = \rho_\ell\) holds for any elements \(\ell \in [f]\) and \((\rho_1, \ldots, \rho_f) \in S^f\). A probabilistic protocol \(\Phi\) is called \(\alpha\)-correct when the relation \(\Phi_{\text{out}}(\rho_1, \ldots, \rho_f, \ell) = \rho_\ell\) holds at least probability \(\alpha\) for any elements \(\ell \in [f]\) and \((\rho_1, \ldots, \rho_f) \in S^f\).

2.2. User and Server Secrecy

A Q-TQOT protocol \(\Phi\) has two types of secrecy. One is the user secrecy and the other is server secrecy. We say that a Q-TQOT protocol \(\Phi\) satisfies the user secrecy when the following condition holds. Consider the case when the user is honest and the servers apply the following attacks. The servers send the answer at the time specified by the protocol, but the contents of the answer do not follow the protocol. Also, the servers do not access
the information under the control of the user. Such servers are called dishonest. In this case, no server obtains the information of the user’s request $K$, i.e., the condition

$$\rho_{\text{out}}(J|K) = \rho_{\text{out}}(J|\ell)$$

holds for any $\ell \in [f]$, where $\rho_{\text{out}}(J|K)$ is the final state on Server $J$ dependent of the variable $K$ (Figure 1).

In contrast, we say that a Q-TQOT protocol $\Phi$ satisfies the server secrecy when the following condition holds. Consider the case when the servers are honest, the user makes the following attack, and the user’s output state $\rho_{\text{out}}$ equals $\rho_K$. The user sends the query at the time specified by the protocol, but the contents of the query do not follow the protocol. Also, the user does not access the information under the control of the servers. Such users are called dishonest. In this case, the user obtains no information for other messages $\rho_\ell$ with $\ell \neq K$.

2.3. Blind and Visible Settings

Q-TQOT can be studied in two distinct settings, called the blind and visible settings, in which quantum state compression has also been extensively studied$^{[52-57]}$. In the blind setting$^{[52-54,57]}$, the servers contain quantum systems $X_1, \ldots, X_t$ with the message states $\rho_1, \ldots, \rho_t$, respectively, but does not know the states of the systems. Due to the no-cloning theorem, the servers cannot generate more copies of the message states and the server’s operations are independent of the message states. Each server accesses these systems in the encoding process. A Q-TQOT protocol of the blind setting is suitable for the case where the servers generate the message states by some quantum algorithm and perform the Q-TQOT task.

On the other hand, in the visible setting$^{[55-57]}$, the servers contain the descriptions of the message states $\rho_1, \ldots, \rho_t$, which can be considered as continuous variables. 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. 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 Q-TQOT task.

3. Outline of Obtained Protocols

In this section, we propose various Q-TQOT protocols in the visible setting, which are summarized in Table 1. Our protocols prove that the Q-TQOT is possible in the visible setting. In the two-server model, we assume that the servers do not communicate with each other.

The goal is to construct Protocol 7, i.e., a protocol that works with general mixed states in a qudit system. This protocol is constructed by a combination of various subprotocols that work with the respective submodel. Figure 2 describes the protocols to be used as subprotocols in each protocol construction. In fact, when we restrict our state model into a submodel, we can realize much smaller download complexity. First, we propose Protocol 1 that works only with real pure qubit states. Then, using Protocol 1, we propose Protocol 2 that works only with real pure qudit states. Next, we propose Protocol 3, i.e., a protocol that works when the states to be transmitted are limited to a state given by a commutative group. These three protocols realize much smaller download complexity, and realize the user secrecy and the server secrecy.

Combining Protocol 2 with a simple modification of Protocol 3, as a simple protocol, we propose Protocol 4 that works with general pure states in a qudit system. This protocol does not have the user secrecy nor the server secrecy under a dishonest setting. To realize the user secrecy, combining Protocols 2 and 3, we propose Protocol 5 that works with general pure states in a qudit system. This protocol realizes the server secrecy. However, it does not have the user secrecy. To realize the user secrecy, combining Protocols 2 and 3 in a way different from Protocol 5, we propose Protocol 6 that works with general pure states in a qudit system. This protocol realizes the user secrecy and the server secrecy. To adopt mixed states, modifying Protocol 6, we propose Protocol 7 that works with general mixed states in a qudit system.

4. 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 $|X|$.

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

$$M = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} m_{ij} |s\rangle \langle t| \in C^{d \times d}$$

we define

$$|M\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} m_{ij} |s\rangle |t\rangle \in C^d \otimes C^d$$

For $A, B, C \in C^{d \times d}$, we have the relation

$$\langle B \otimes C \rangle |A\rangle = |BAC\rangle$$

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

$$X_d = \sum_{s=0}^{d-1} |s+1\rangle \langle s|$$

...
Table 1. Q-TQOT Protocols in Visible Setting.

| Protocol | Message States | Upload Complexity | Download Complexity | Prior Entanglement | User Secrecy | Server Secrecy | deterministic or probabilistic (correctness) |
|----------|----------------|--------------------|---------------------|---------------------|--------------|----------------|---------------------------------------------|
| Protocol 1 | real qubit pure states | 2f bits | 2 qubits | 1 ebit | Yes | Yes | deterministic (correct) |
| Protocol 2 | real qubit pure states | 2f bits | 2(d - 1) qubits | d - 1 ebits | Yes | Yes | deterministic (correct) |
| Protocol 3 | qudit commutative unitary pure states | 2f bits | 2 log d qubits | log d ebit | Yes | Yes | deterministic (correct) |
| Protocol 4 | qudit pure states | 2f bits + 4 log d qubits | 2(d - 1) + 4 log d qubits | d - 1 ebits | No | No | deterministic (correct) |
| Protocol 5 | qudit pure states | 2f bits + 2d bits in average | 2d(d - 1) + 4d log d qubits in average | d(d - 1) + 2d log d ebits in average | No | Yes | probabilistic (correct) |
| Protocol 6 | qudit pure states | 2f bits | 2n(d - 1) + 4n log d qubits | n(d - 1) + 2n log d ebits | Yes | Yes | probabilistic \((1 - (\frac{1}{2^d})^n)\)-correct |
| Protocol 7 | qudit mixed states | 2f bits | 2n(d - 1) + 4n log d qubits | n(d - 1) + (2n + 1) log d ebits | Yes | Yes | probabilistic \((1 - (\frac{1}{2^d})^n)\)-correct |

Protocols 4 and 5 can be converted for mixed message states by increasing the prior entanglement by log d ebit.

\[
Z_d = \sum_{j=0}^{d-1} \alpha^j |s\rangle\langle s| \tag{6}
\]

\[
|I_d\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |s, j\rangle
\tag{7}
\]

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

\[
M_{x,z,d} = \{|x\rangle\langle z|\} \quad (12)
\]

If there is no confusion, we denote \(X_d, Z_d, I_d, M_{x,z,d}\) 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 \(|A\rangle\langle A| \otimes |B\rangle\langle B|\) and the measurement \(M_{x,z}\) is performed on \(A' \otimes B'\) with outcome \((a, b) \in [0 : d - 1]^2\), the resultant state is

\[
|AX^aZ^bB^r\rangle \in A \otimes B \tag{9}
\]

Also, we define the unitary \(V\) on \(C^d \otimes C^d\) as

\[
V |j\rangle |j'\rangle = |j\rangle |j' + j\rangle \tag{10}
\]

which implies the relation \(V |j\rangle |0\rangle = |j\rangle |j\rangle\). We define the following state

\[
|+\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \in C^d \tag{11}
\]

5. Symmetric QPIR Protocol for Pure Real Qubit States

In this subsection, we construct a two-server Q-TQOT protocol for pure qubit states in the visible setting. Define the rotation operation on \(C^2\) and the phase-shift operation by

\[
R(\theta) := \begin{pmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{pmatrix}, \quad S(\varphi) := \begin{pmatrix}
e^{-\imath \varphi /2} & 0 \\
0 & e^{\imath \varphi /2}
\end{pmatrix} \tag{12}
\]

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

\[
R(\theta)R(\theta') = R(\theta + \theta'), \quad S(\varphi)S(\varphi') = S(\varphi + \varphi') \tag{13}
\]

and therefore, \(S(\varphi)\) and \(S(\varphi')\) \((R(\theta)\) and \(R(\theta')\)) are commutative. Then, we have

\[
R(\theta)^T = R(-\theta), \quad S(\varphi)^T = S(\varphi) \tag{14}
\]
and
\[ X R(\theta) X = R(-\theta), \quad X S(\varphi) X = S(-\varphi) \] (15)

As special cases, we have \( Y = X Z = R(\pi/2) \) and \( Z = S(\pi) \). Also, we have
\[ |R(\theta)| = \frac{\cos \theta}{\sqrt{2}} |00\rangle + \frac{\sin \theta}{\sqrt{2}} |10\rangle \] (16)

We define the unitary \( T \) on \( C^2 \otimes C^2 \) as
\[ T(\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)) = |00\rangle, \quad T(\frac{1}{\sqrt{2}} (|10\rangle - |01\rangle)) = |10\rangle \] (17)
\[ T(\frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)) = |01\rangle, \quad T(\frac{1}{\sqrt{2}} (|10\rangle + |01\rangle)) = |11\rangle \] (18)

Then, using Equation (16), we have
\[ T|R(\theta)| = \cos \theta |00\rangle + \sin \theta |10\rangle = (R(\theta)|00\rangle) |0\rangle \] (19)

Any normalized real vector can be written as
\[ \left( \begin{array}{c} \cos \theta \\ \sin \theta \end{array} \right) = R(\theta)|0\rangle \] (20)

Using the above description, we construct a Q-TQOT protocol in the visible setting for real qubit states.

Protocol 1 (Q-TQOT protocol for real qubit pure states). For any message real qubit states \( |\psi_1\rangle, \ldots, |\psi_s\rangle \in P(\mathbb{R}^2) \), we choose the parameters \( \theta_1, \ldots, \theta_s \) as
\[ |\psi_{s_k}\rangle = R(\theta_{s_k})|0\rangle \] (21)

When the user’s target index \( K \) is \( k \in [s] \), i.e., the targeted state is \( |\psi_k\rangle \), our protocol is given as follows (Figure 1).

1) **Entanglement Sharing**: Let \( A, A' \) be qubits. Before starting the protocol, Server 1 and Server 2 share a maximally entangled state \( |I_{2}\rangle \) on \( A \otimes A' \), where Server 1 (Server 2) contains \( A (A') \).

2) **Query**: The user chooses \( Q = (Q_1, \ldots, Q_s) \in Z^s \) uniformly random. The variable \( Q' = (Q'_1, \ldots, Q'_t) \in \{0, 1\}^t \) is defined as
\[ Q' = \begin{cases} Q_k & \text{for } \ell \neq k \\ Q_k \oplus 1 & \text{for } \ell = k \end{cases} \] (22)

The user sends \( Q \) and \( Q' \) to Server 1 and Server 2, respectively.

3) **Answer**: When \( Q = q \) and \( Q' = q' \), Server 1 applies \( R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k}) \) on \( A \), and sends \( A \) to the user. Similarly, Server 2 applies \( R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k}) \) on \( A' \), and sends \( A' \) to the user.

4) **Reconstruction**: When both servers are honest, the user receives the following state on \( A \otimes A' \):
\[ R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k}) \otimes R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k})^\top |I_{2}\rangle = |R((-1)^{s+1} \theta_{s_k})\rangle |0\rangle \] (23)

1. The user applies the unitary \( T \) on \( A \otimes A' \). Then, the resultant state is \( (R((-1)^{s+1} \theta_{s_k})|0\rangle) |0\rangle = (Z^{s+1} R(\theta_{s_k})|0\rangle) |0\rangle \) due to Equation (19).

2. The user traces out \( A' \) and applies \( Z^{s+1} \) on \( A \). Then, the resultant state on \( A \) is \( R(\theta_{s_k})|0\rangle \).

Here, the relation Equation (23) is derived as follows.
\[ R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k}) \otimes R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k})^\top |I_{2}\rangle = |R((-1)^{s+1} \theta_{s_k})\rangle |0\rangle \] (24)

The first equation follows from Equations (7) and (14). The second equation follows from Equation (22). The third equation follows from the following fact. When \( q_k = 1 \), \( q'_k = q_k - 1 \). When \( q_k = 0 \), \( q'_k = q_k + 1 \). Hence, \( q_k - q'_k = (-1)^{s+1} \).

Protocol 1 satisfies the correctness, secrecy, and communication complexity, which is shown as follows.

**Lemma 1.** Protocol 1 is a correct Q-TQOT protocol that satisfies the user secrecy and the server secrecy. Its upload complexity and its download complexity are \( 2t \) bits and two qubits, respectively. The required prior entanglement is one copy of \( |I_{2}\rangle \), i.e., one ebit.

**Proof.** The correctness and the complexity are shown during the protocol description. The secrecy can be shown as follows. Throughout the protocol, the servers only obtain the queries, and each query is uniformly random \( t \) bits. Therefore, each server does not obtain any information of \( k \). Hence, the user secrecy holds. On the other hand, at the end of the step of answer, the user obtains the state \( |R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k})\rangle |0\rangle \) = \( T \otimes T |R(\sum_{\ell=1}^{t} q'_\ell \theta_{s_k})\rangle |0\rangle \). That is, for any dishonest queries \( q, q' \), the state depends only on \( \sum_{\ell=1}^{t} q'_\ell \theta_{s_k} \). In order to recover the \( R(\theta_{s_k})|0\rangle \), \( \sum_{\ell=1}^{t} q'_\ell \theta_{s_k} \) needs to have a one-to-one relation to \( \theta_{s_k} \). Hence, when the user recovers the quantum message \( R(\theta_{s_k})|0\rangle \), he can obtain no information for other \( \theta_{s_k} \). Hence, the server secrecy holds.

\[ \Box \]

6. **Symmetric QPIR Protocol for Pure Real Qudit States**

To construct a Q-TQOT protocol for real qudit states, we first consider the parameterization of pure real states on \( d \)-dimensional systems. Define \( d \times d \) matrix \( R(\theta^1, \ldots, \theta^{d-1}) \) as
\[ R(\theta^1, \ldots, \theta^{d-1}) = R_{d-1}(-\theta^1) \cdots R_1(-\theta^{d-1}) \] (25)

where \( R_i(\theta) \) is the rotation \( \left( \begin{array}{cc} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{array} \right) \) (26)

with respect to the two basis elements \( |s\rangle \) and \( |s\rangle \). We also have \( R(\theta^1)^\top = R_1(-\theta^1) \). Any real vector can be written as
\[ R(\theta^1, \ldots, \theta^{d-1})|0\rangle \] (27)
Now, we construct a Q-TQOT protocol in the visible setting for real qudit states.

Protocol 2 (Q-TQOT protocol for real qubit pure states). For any message pure states \( |\psi_1\rangle, \ldots, |\psi_q\rangle \in \mathbb{P}(\mathbb{R}^d) \), we choose the parameters \( \theta_1, \ldots, \theta_{d-1} \) as

\[
|\psi_r\rangle = R(\theta_1^r, \ldots, \theta_{d-1}^r)|0\rangle 
\]

(28)

When the user’s target index \( K \) is \( k \in [q] \), i.e., the targeted state is \( |\psi_k\rangle \), our protocol is given as follows.

1) **Entanglement Sharing**: Let \( A_1, \ldots, A_{d-1}, A'_1, \ldots, A'_{d-1} \) be qubits. Before starting the protocol, Server 1 and Server 2 share \( d-1 \) maximally entangled states \( |I_j\rangle \) on \( A_j \otimes A'_j, j = 1, \ldots, d-1 \), where Server 1 (Server 2) contains \( A_1, \ldots, A_{d-1}, (A'_1, \ldots, A'_{d-1}) \).

2) **Query**: The same as Protocol 1.

3) **Answer**: When \( Q = q \) and \( Q' = q' \), Server 1 applies \( R(\sum_{j} \rho_j) |0\rangle \otimes \cdots \otimes R(\sum_{j} \rho_j^{-1}) |0\rangle \) on \( A_1 \otimes \cdots \otimes A_{d-1} \) and sends \( A_1, \ldots, A_{d-1} \) to the user. Similarly, Server 2 applies \( R(\sum_{j} \rho_j^{'-1}) |0\rangle \) on \( A'_1 \) for \( j = 1, \ldots, d-1 \), and sends \( A'_1, \ldots, A'_{d-1} \) to the user.

4) **Reconstruction**: When both servers are honest, the user receives \( |\mathcal{R}(\sum_{j} \rho_j^{'-1}) |0\rangle \otimes \cdots \otimes |\mathcal{R}(\sum_{j} \rho_j^{-1}) |0\rangle \). For commutative unitaries, the states \( |\mathcal{R}(\sum_{j} \rho_j^{'-1}) |0\rangle \), i.e., the targeted state is \( |\psi_k\rangle \).

When the user recovers the message, the user applies Kraus operators \( \{ F_{j,1}, F_{j,2} \} \) to the input system \( A_j \otimes A'_j \) and the output system \( H_{j+2} \), where

\[
F_{j,1} := \frac{1+i}{\sqrt{2}} |0\rangle \langle u_j^+ | + \frac{1}{\sqrt{2}} |1\rangle \langle 1 | 0 \rangle + |2 \rangle \langle 1 | 1 \rangle
\]

(29)

\[
F_{j,2} := \frac{1+i}{\sqrt{2}} |0\rangle \langle u_j^{-} | + \frac{1}{\sqrt{2}} |1\rangle \langle 1 | 0 \rangle + |2 \rangle \langle 1 | 1 \rangle
\]

(30)

and \( |u_j^\pm \rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm i |1\rangle) \). When both servers are honest, the result state is \( R(\theta_1^r, \ldots, \theta_{d-1}^r)|0\rangle \).

The user makes the following procedure inductively for \( j = 1, \ldots, q-1 \).

4) **Protocol Description**: The secrecy can be shown as follows. Throughout the protocol, the user obtains the queries, and each query is uniformly random \( f \) bits. Therefore, the user does not obtain any information of \( k \). Hence, the user secrecy holds.

Proof. The correctness and the complexity shown during the protocol description. The secrecy can be shown as follows. In order that the user recovers the state \( R(\theta_1^r, \ldots, \theta_{d-1}^r) |0\rangle \), the states \( |\mathcal{R}(\sum_{j} \rho_j^{'-1}) |0\rangle \) has one-to-one relation to \( |\psi_k\rangle \) for \( j = 1, \ldots, d-1 \). Hence, \( |\mathcal{R}(\sum_{j} \rho_j^{'-1}) \rangle \) has no information for other \( \theta_j \), and \( |\psi_k\rangle \).

Hence, the protocol secrecy holds.

7. Q-TQOT Protocol for Pure States Described by Commutative Unitaries

In this subsection, we construct a two-server Q-TQOT protocol for pure states described by commutative unitaries in the visible setting.

Protocol 3 (Q-TQOT protocol for pure states described by commutative unitaries). For commutative \( f \) unitaries \( U_1, \ldots, U_f \) on \( \mathbb{C}^d \), the message states are given as

\[
|U_1\rangle, \ldots, |U_f\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d
\]

(33)

When the user’s target index \( K \) is \( k \in [q] \), i.e., the targeted state is \( |U_k\rangle \), our protocol is given as follows.

1. **Entanglement Sharing**: Let \( A, A', B, B' \) be qudits. Server 1 and Server 2 share two maximally entangled states \( |I_j\rangle \) on \( A \otimes A' \) and \( B \otimes B' \), where Server 1 (Server 2) contains \( A \otimes B (A' \otimes B') \).

2. **Query**: The same as Protocol 1.

3. **Answer**: When \( Q = q \) and \( Q' = q' \), Server 1 applies

\[
U_1^q \cdots U_f^q
\]

(34)

\[
U_1^{-q} \cdots U_f^{-q}
\]

(35)

on \( A \) and \( B \), respectively, and sends \( A \) and \( B \) to the user. Similarly, Server 2 applies

\[
\bar{U}_1^q \cdots \bar{U}_f^q
\]

(36)

\[
\bar{U}_1^{-q} \cdots \bar{U}_f^{-q}
\]

(37)
4. **Reconstruction:** The user outputs the state on $A \otimes A'$ if $q_k = 1$, otherwise outputs the state on $B \otimes B'$.

Protocol 3 satisfies the correctness, secrecy, and communication complexity, which is as follows.

**Lemma 3.** Protocol 3 is a correct Q-TQOT protocol that satisfies the user secrecy and the server secrecy. Its upload complexity and its download complexity are $2d$ bits and $2 \log d$ qubits, respectively. The required prior entanglement is one copy of $|I_d\rangle$, i.e., $\log d$ ebits.

**Proof.** To consider correctness, we consider the case where $Q_k = 1$. When $Q = q$, the state on $A \otimes A'$ after the measurement is

$$
(U_0^{(1)} \cdots U_0^{(d)} \otimes U_0^{(d)} \cdots U_0^{(d)})|I_d\rangle = (U_0^{(1)} \cdots U_0^{(d)} \otimes U_0^{(d)} \cdots U_0^{(d)})|I_d\rangle = (U_0^{(1)} \cdots U_0^{(d)} \otimes U_0^{(d)} \cdots U_0^{(d)}) = |U_0\rangle
$$

where Equation (38) follows from the commutativity of the unitaries $U_1, \ldots, U_d$, $q \otimes q' = \delta_{q,q'}$, and $(q, q') = (1, 0)$. By similar analysis, if $Q_k = 0$, the resultant state on $B \otimes B'$ is $|U_0\rangle$.

The secrecy can be shown as follows. Since the queries are the same as Protocol 1, the user secrecy holds.

When both servers are honest and the user is dishonest, at the end of the protocol, the user obtains both of $|\bigotimes_{r=1}^{d} U_r^{(d)}|I_d\rangle$ and $|\bigotimes_{r=1}^{d} U_r^{(d)}\rangle = |\bigotimes_{r=1}^{d} U_r^{(d)}\rangle$. To order that the user recovers $|U_0\rangle$, the state $|\bigotimes_{r=1}^{d} U_r^{(d)}\rangle = |\bigotimes_{r=1}^{d} U_r^{(d)}\rangle$ needs to have one-to-one relation to $|U_0\rangle$. To realize this relation, $q_r$, equals $q_r'$ for $\ell \neq k$. In this case, both states have no information for all other message states. Hence, no information for all other message states is leaked to the user.

**8. Deterministic Q-TQOT Protocol for Pure Qudit States**

We first consider the parameterization of pure states on d-dimensional systems.

Define $d \times d$ matrix $S(\varphi^1, \ldots, \varphi^{d-1})$ as

$$
S(\varphi^1, \ldots, \varphi^{d-1}) = [000] + \sum_{\ell=1}^{d-1} e^{i\varphi^\ell} [s]$$

where

$$
= \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & e^{i\varphi^1} & 0 & 0 \\
0 & 0 & \ddots & 0 \\
0 & 0 & 0 & e^{i\varphi^{d-1}}
\end{pmatrix}
(39)
$$

Notice that $S(\varphi^1, \ldots, \varphi^{d-1})$ for all $\varphi^1, \ldots, \varphi^{d-1}$ are commutative. We also have $S(\varphi^1, \ldots, \varphi^{d-1}) = S(\varphi^1, \ldots, \varphi^{d-1})$. It can be easily checked that any pure state $|\psi\rangle \in \mathbb{P}(C^d)$ is written in the form

$$
|\psi\rangle = S(\varphi^1, \ldots, \varphi^{d-1})R(\theta^1, \ldots, \theta^{d-1})|0\rangle
(40)
$$

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

Protocol 4 (Q-TQOT protocol for qudit pure states). For any message pure states $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathbb{P}(C^d)$, we choose the parameters $\varphi^1, \ldots, \varphi^{d-1}$ and $\theta^1, \ldots, \theta^{d-1}$ as

$$
|\psi_{\ell}\rangle = S(\varphi^1, \ldots, \varphi^{d-1})R(\theta^1, \ldots, \theta^{d-1})|0\rangle
$$

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) **Entanglement Sharing:** The same as Entanglement Sharing of Protocol 2.
2) **Query 1:** The same as Query of Protocol 1.
3) **Answer 1:** The same as Answer of Protocol 2.
4) **Reconstruction 1:**
   1. The same as Reconstruction of Protocol 2. We denote the output system $H_d$.
   2. When $q_k = 1$, the user sends qudits $B, B'$ to be the completely mixed state. Then, he applies the isometry $V$ from $H_d$ to $A \otimes A'$. When $q_k = 0$, the user sends qudits $A, A'$ to be the completely mixed state. Then, he applies the isometry $V$ from $H_d$ to $B, B'$.
5) **Query 2:** The user sends the system $A \otimes B (A' \otimes B')$ to Server 1 (Server 2).
6) **Answer 2:** When $Q = q$ and $Q' = q'$, Server 1 applies $S(\sum_{r=1}^{d-1} q_r \varphi^r, \ldots, \sum_{r=1}^{d-1} q_r \varphi^r) \otimes S(-\sum_{r=1}^{d-1} q_r \varphi^r, \ldots, -\sum_{r=1}^{d-1} q_r \varphi^r)\rangle$ on $A \otimes B$, and sends $A \otimes B$ to the user. Similarly, Server 2 applies $S(\sum_{r=1}^{d-1} q'_r \varphi^r, \ldots, \sum_{r=1}^{d-1} q'_r \varphi^r) \otimes S(-\sum_{r=1}^{d-1} q'_r \varphi^r, \ldots, -\sum_{r=1}^{d-1} q'_r \varphi^r)$ on $A' \otimes B'$, and sends $A' \otimes B'$ to the user.
7) **Reconstruction 2:** When $q_k = 1$, the user discards $B, B'$. Then, he applies the partial isometry $V'$ from $A \otimes A'$ to $A$. When $q_k = 0$, the user discards $A, A'$. Then, he applies the partial isometry $V'$ from $B \otimes B'$ to $A$.

Protocol 4 satisfies the correctness, secrecy, and communication complexity, which is as follows.

**Lemma 4.** Protocol 4 is a correct Q-TQOT protocol. Its upload complexity and its download complexity are $2f$ bits plus $4 \log d$ qubits and $2(d-1) + 4 \log d$ qubits, respectively. The required prior entanglement is $d-1$ copies of $|I_d\rangle$ and two copies of $|I_d\rangle$, i.e., $(d-1) + 2 \log d$ ebits.

**Proof.** To show correctness, we assume that the servers and the user are honest. When $q_k = 1$, at the end of Step 3), the state on qudits $A \otimes A'$ is $V(R(\theta^1, \ldots, \theta^{d-1})|0\rangle|0\rangle$. At the end of the protocol, the state on $A$ is

$$
V' S \left( \sum_{r=1}^{d-1} (q_r - q_r') \varphi^r, \ldots, \sum_{r=1}^{d-1} (q_r - q_r') \varphi^{r-1} \right)
$$

$$
\cdot V(R(\theta^1, \ldots, \theta^{d-1})|0\rangle|0\rangle)
$$

$$
= V' S(\varphi^1, \ldots, \varphi^{d-1}) V(R(\theta^1, \ldots, \theta^{d-1})|0\rangle|0\rangle)
$$

$$
= S(\varphi^1, \ldots, \varphi^{d-1}) R(\theta^1, \ldots, \theta^{d-1})|0\rangle|0\rangle
$$

(41)

When $q_k = 0$, at the end of Step 3), the state on $B \otimes B'$ is $V(R(\theta^1, \ldots, \theta^{d-1})|0\rangle|0\rangle)$. At the end of the protocol, the state on
A is
\[
V^{\dagger}S\left(\sum_{r=1}^{f}(-q_r + q'_r)\varphi^{r_1}_{r}, \ldots, \sum_{r=1}^{f}(-q_r + q'_r)\varphi^{-1}_{r}\right)
\]
\[
\cdot -V(R(\theta^1_{1}, \ldots, \theta^{d-1}_{1})|0\rangle)\langle 0|
\]
\[
=V^{\dagger}S(\varphi^{1}_{1}, \ldots, \varphi^{d-1}_{1})V(R(\theta^1_{1}, \ldots, \theta^{d-1}_{1})|0\rangle)\langle 0|
\]
\[
=(S(\varphi^{1}_{1}, \ldots, \varphi^{d-1}_{1})R(\theta^1_{1}, \ldots, \theta^{d-1}_{1})|0\rangle)\langle 0| (43)
\]

In fact, when the user and the servers are honest, the user has only the system A at the end of the protocol so that the user has no information for another \(\varphi_{r}\). Also, since both servers do not make any measurements in Answer 2, both servers obtain information only from Query 1. Since the queries are the same as Protocol 1, both servers have no information for the user's choice \(K\). However, when one of them is not honest, the secrecy does not hold.

9. Secrecy Problems in Protocol 4

This subsection presents several attacks by a dishonest user or a dishonest server in Protocol 4. First, we show an attack by a dishonest server in Protocol 4. Under Protocol 4, we assume that the user and Server 2 are honest, but Server 1 is dishonest. Consider that Server 1 intends to identify whether \(K = 1\) or not. Hence, we consider the following behavior of Server 1. In Answer 1, Server 1 applies \(R(q_{1} \oplus 1)\theta^{1}_{1} + \sum_{r=2}^{f} q_{r} \theta^{r}_{1}\) on \(A'\) for \(j = 1, \ldots, d - 1\). In Answer 2, Server 1 measures the received systems A and B with the basis \(|0\rangle, \ldots, |d - 1\rangle\), and sends back the resultant state. When the outcome on A does not correspond to the basis \(|0\rangle\) and \(Q_{1} = 1\), Server 1 finds that the variable \(K\) is not 1. This is because the outcome on A is 0 when the variable \(K\) is 1 and \(Q_{1} = 1\). When the outcome on B does not correspond to the basis \(|0\rangle\) and \(Q_{2} = 0\), Server 1 finds that the variable \(K\) is not 1. This is because the outcome on B is 0 when the variable \(K\) is 1 and \(Q_{2} = 0\). Hence, Protocol 4 does not have the user secrecy.

Next, we present an attack by a dishonest user in Protocol 4. Under Protocol 4, we assume that both servers are honest, but the user is dishonest. Consider that the user intends to get the receiving state by modifying the state sent to the server. To avoid this problem, we consider a protocol, in which, the user sends only the classical information to the servers. That is, by modifying Protocol 4 slightly, we construct a Q-TQOT protocol for pure qudit states in the visible setting which achieves the user secrecy and the server secrecy.

Protocol 5 (Q-TQOT protocol for qudit pure states). For any message pure states \(|\psi_{1}\rangle, \ldots, |\psi_{n}\rangle\in\mathbb{C}^3\), we choose the variables \(\varphi^{1}_{1}, \ldots, \varphi^{d-1}_{1}\) and \(\theta^{1}_{1}, \ldots, \theta^{d-1}_{1}\) as \((41)\). When the user’s target index \(K\) is \(k\in\{1, \ldots, n\}\), i.e., the targeted state is \(|\psi_{k}\rangle\), our protocol is given as follows.

1) Entanglement Sharing: Let \(A_{1,1}, \ldots, A_{j,d-1}, A'_{1,1}, \ldots, A'_{j,d-1}\) and \(A_{j}, A'_{j}, B_{j}, B'_{j}\) be qubits and qudits, respectively, for \(j = 1, \ldots, n\) with sufficiently large \(n\). Before starting the protocol, Server 1 and Server 2 share \(n(d - 1)\) maximally entangled state \(|\ell_{j}\rangle\) on \(A_{j} \otimes A'_{j}, \ldots, A_{j,d-1} \otimes A'_{j,d-1}\) with \(j = 1, 2, \ldots, n\), where Server 1 (Server 2) contains \(A_{j,1}, \ldots, A_{j,d-1}, (A'_{j,1}, \ldots, A'_{j,d-1})\). Server 1 and Server 2 share \(2n\) copies of the maximally entangled state \(|\ell_{j}\rangle\) on \(A_{j} \otimes A'_{j}, B_{j} \otimes B'_{j}\) for \(j = 1, 2, \ldots, n\).

2) Query 1: The same as Protocol 1.

The following steps are given inductively for \(j = 1, 2, \ldots, \) up to stopping the protocol.

3j-1) Answer j:
1. The servers perform the same operations on \(A_{j,1}, \ldots, A_{j,d-1}, A'_{j,1}, \ldots, A'_{j,d-1}\) as Answer of Protocol 2.
2. The servers perform the same operations on \(A_{j}, A'_{j}, B_{j}, B'_{j}\) as Answer 2 of Protocol 4.

3j) Reconstruction j:
1. The user applies the same operation to \(A_{j,1}, \ldots, A_{j,d-1}, A'_{j,1}, \ldots, A'_{j,d-1}\) as Reconstruction of Protocol 2. Then, the user obtains the system \(H_{1,d}, \ldots, H_{n,d}\) as its outputs.
2. When \(q_{j} = 1\), the user measures the system \(H_{j,\ldots, j,d} \otimes A'_{j}\) with the basis \(M_{\ell,j,d} = \{|z'\rangle | a, b \in \{0, \ldots, d - 1\}\},\) obtains the outcome \((a_{j}, b_{j})\), and applies \(Z^{-b}\). When \(q_{j} = 0\), the user keeps the system \(A_{j}\) as the final output system.

When \(q_{j} = 0\), the user measures the system \(H_{j,\ldots, j,d} \otimes B'_{j}\) with the basis \(M_{\ell,j,d}\), obtains the outcome \((a_{j}, b_{j})\), and applies \(Z^{-b}\). When \(a_{j} = 0\), the user keeps the system \(B_{j}\) as the final output system.

3j+1) Query j+1: The user informs the servers whether \(a_{j} = 0\) or not. If \(a_{j} = 0\), the protocol is terminated. Otherwise, the protocol proceeds to Step 3(j+2).

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

Lemma 5. Protocol 5 is a correct Q-TQOT protocol that satisfies the server secrecy. Its upload complexity and its download complexity are \(2f + 2d\) bits and \((2d - 1) + 4\log d)\) qubits, respectively, in average. The consumed prior entanglement is \(d(d - 1)\) copies of \(|\ell_{j}\rangle\) and \(2d\) copies of \(|\ell_{j}\rangle\), i.e., \((d - 1 + 2\log d)\) ebits in average.

Proof. The correctness is shown as follows. We assume that the servers and the user are honest. At
When $q_k$, recovers $\mathcal{H}_j$, load complexity is $(2(\log n - 1))$. Hence, the user secrecy holds. In the following, as a protocol to satisfy the above condition, we construct a probabilistic Q-TQOT protocol for pure qudit states in the visible setting that achieves the user secrecy and the server secrecy. The following protocol achieves the required properties.

Protocol 6 (Q-TQOT protocol for qudit pure states). For any message pure states $|\psi_1\rangle, \ldots, |\psi_r\rangle \in \mathcal{P}(C^d)$, we choose the parameters $\omega_1, \ldots, \omega_r$ and $\theta_{1j}, \ldots, \theta_{rj}$ as Equation (41). 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) Entanglement Sharing: Let $A_1, \ldots, A_d, A_{d+1}, \ldots, A_{d+k}$ and $A_j, A_j', B_j, B_j'$ be qubits and qudits, respectively, for $j = 1, \ldots, n$. Before starting the protocol, Server 1 and Server 2 share $n(d-1)$ maximally entangled state $|I_j\rangle$ on $A_1 \otimes A_{d+1} \otimes \ldots \otimes A_{d+k}$.

2) Query: The same as Protocol 1.

3) Answer: The servers make the same operation as Answer j of Protocol 5 for $j = 1, \ldots, n$.

4) Reconstruction:

1. The user applies the same operation to $A_1, \ldots, A_d, A_{d+1}, \ldots, A_{d+k}$ as Reconstruction of Protocol 2 for $j = 1, \ldots, n$. Then, the user obtains the system $H_{1}, \ldots, H_{n}$ as its outputs.

2. When $a_j = 0$, the user measures the system $H_{1} \otimes B_j'$ with the basis $M_{kz,j} = \{ |x\rangle \} \otimes a, b \in \{ 0 : d - 1 \}$, obtains the outcome $(a_j, b_j)$, and applies $Z^{-b_j}$ for $j = 1, 2, \ldots, n$. When $a_j = 0$, the user keeps the system $A_j$ as the final output system.

When $a_j = 0$, the user measures the system $H_{1} \otimes B_j'$ with the basis $M_{kz,j}$, obtains the outcome $(a_j, b_j)$, and applies $Z^{-b_j}$ for $j = 1, 2, \ldots, n$. When $b_j = 0$, the user keeps the system $B_j'$ as the final output system.

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

**Lemma 6.** Protocol 6 is a $1 - \left(\frac{1}{2}\right)^r$-correct Q-TQOT protocol that satisfies the user secrecy and the server secrecy. Its upload complexity and its download complexity are $2f$ bits and $2n(d-1) + 4n \log d$ qudits, respectively. The required prior entanglement is $n(d-1)$ copies of $|I_j\rangle$ and $2n$ copies of $|I_j\rangle$, i.e., $n(d-1) + 2n \log d$ qudits.

**Proof.** The correctness can be shown in the same way as the correctness of Protocol 5 in Lemma 5. That is, when the user obtains the outcome $b_j = 0$ at least with one element $j$ among $1, \ldots, n$, the user recovers $S(|\psi_1\rangle, \ldots, |\psi_r\rangle) = 0$. Otherwise, the user cannot recover it. This protocol works correctly with probability $1 - \left(\frac{1}{2}\right)^r$.

The complexity is calculated as follows. The upload complexity is $2f$ bits. The download complexity is $2n(d-1) + 4n \log d$ qudits. The secrecy is shown as follows. Since each server receives uniformly random $f$ bits as Query, the server does not obtain any information of $k$. Hence, the user secrecy holds.

11. Probabilistic Q-TQOT Protocol for Pure Qudit States

Protocols 4 and 5 do not achieve the user secrecy. If the query is composed only of the same query as Query 1 of Protocol 1, the user secrecy holds. In the following, as a protocol to satisfy the above condition, we construct a probabilistic Q-TQOT protocol for pure qudit states in the visible setting that achieves the user secrecy and the server secrecy. The following protocol achieves the required properties.
Assume that the servers are honest. At the end of Answer, the user has the states \(|R(\sum_{i=1}^{d-1} (q_i, q_i') \theta_i)|\) for \(j = 1, \ldots, d - 1\), \(|S(\sum_{i=1}^{d-1} (q_i, q_i') \phi_i, \sum_{i=1}^{d-1} (q_i, q_i') \psi_i)|\), and \(|S(\sum_{i=1}^{d-1} (q_i, q_i') \phi_i, \sum_{i=1}^{d-1} (q_i, q_i') \psi_i)|\). In order to recover the state \(S(\phi_1, \ldots, \phi_{d-1}|\theta_1, \ldots, \theta_{d-1})|0\), these states need to contain the information for \(\phi_1, \ldots, \phi_{d-1}\) and \(\theta_1, \ldots, \theta_{d-1}\).

This condition holds only when \(\sum_{i=1}^{d-1} (q_i, q_i') \phi_i, \sum_{i=1}^{d-1} (q_i, q_i') \psi_i\) are constant times of \(\phi_{i-1}, \phi_i, \theta_{i-1}, \theta_i\) for \(\ell \neq k\). Hence, the server secrecy holds.

### 12. Two-Server Symmetric QPIR Protocols with Mixed States in Visible Setting

The Q-TQOT protocols in the previous sections are for the retrieval of pure states. The aim of this section is showing the following theorem, which works with mixed states and has scalability.

**Theorem 1.** For a positive number \(0 < \alpha < 1\), a large dimension \(d\), and a large positive integer \(f\), there exists a probabilistic \(\alpha\)-correct Q-TQOT protocol for mixed states with the following properties on \(C^d\). The upload and download complexity are \(2f\) and \(O(d^2f)\). It satisfies the user secrecy and the server secrecy. It needs \(O(d^f)\)-bit prior entanglement.

To show this theorem, we convert these protocols to Q-TQOT protocols for mixed states. For this conversion, we first give a decomposition of mixed states, and then construct the protocol for mixed states.

#### 12.1. Decomposition of Mixed States

If a protocol is based on the blind setting, it works with mixed states. However, since our protocols in previous sections are based on the visible setting, they do not work with mixed states because they need the description of a pure state as the input. To resolve this problem, we can consider the following method: The servers randomly choose the pure state to be sent. To accomplish this method, we decompose a mixed state \(\rho\) on a \(d\)-dimensional Hilbert space as \(\rho = \sum_{i=0}^{d-1} p_i |\psi_i\rangle \langle \psi_i|\). One canonical decomposition is given by using the diagonalization of \(\rho\). To implement the above-mentioned method based on this decomposition, the servers have to share a random variable that is subject to the distribution \(|p_i\rangle\). However, in this method, the probabilities \(p_i\) depend on the state \(\rho\), and take continuous values. This idea does not work with the diagonalization of \(\rho\). However, if the probability distribution \(|p_i\rangle\) is limited to the uniform distribution, the above idea works well.

We choose the decomposition \(|\psi_i\rangle \langle \psi_i|\) for \(i = 0, \ldots, d-1\) for \(\rho\) to satisfy \(\rho = \sum_{i=0}^{d-1} p_i |\psi_i\rangle \langle \psi_i|\). Generally, a state \(\rho\) has various decompositions. Based on the computation basis \(|j\rangle\) of \(\rho\), we uniquely choose the decomposition according to the method given in Appendix A.

Then, we define the vector

\[|\phi\rangle := \sum_{j=0}^{d-1} \omega^{\ell} |j\rangle \langle \psi_i| \quad (\forall j \in [0 : d - 1]) \]  

(44)

where \(\omega = \exp(2\pi i / d)\) and \(\ell = \sqrt{-1}\). Then, the state \(\rho\) is decomposed by the vectors in Equation (44) as

\[\rho = \sum_{j=0}^{d-1} 1 / d |\phi\rangle \langle \phi|\]  

(45)

Notice that this decomposition is unique because the vectors \(|\psi_0\rangle, \ldots, |\psi_{d-1}\rangle\) are uniquely chosen from the state \(\rho\).

#### 12.2. Q-TQOT Protocol for Mixed States

Next, we construct two-server Q-TQOT protocols for mixed states \(\rho_1, \ldots, \rho_n\) on \(d\)-dimensional Hilbert spaces by converting Protocol 6. The same conversion can be applied to Protocols 4 and 5.

Without losing generality, we assume that the servers share the decomposition Equation (45) of the mixed states, e.g., by the process in Appendix A. For the states \(\rho_j\) with \(j \in [f]\), we denote the vectors in Equation (44) as \(|\phi_{i_0,j}\rangle, \ldots, |\phi_{i_{d-1},j}\rangle\).

We define a Q-TQOT protocol for mixed states from Protocol 6 as follows.

Protocol 7 (Q-TQOT protocol for qudit mixed states). For any mixed states \(\rho_1, \ldots, \rho_n\), we choose pure states \(|\phi_{i_0,j}\rangle, \ldots, |\phi_{i_{d-1},j}\rangle\in P(C^d)\) for \(j = 0, \ldots, d - 1\) according to the method given in Appendix A. Then, for pure states \(|\phi_{i_0,j}\rangle, \ldots, |\phi_{i_{d-1},j}\rangle\in P(C^d)\), we choose the parameters \(\phi_{i_0,1}, \ldots, \phi_{i_{d-1},1}\) and \(\theta_{i_0,j}, \ldots, \theta_{i_{d-1},j}\) as Equation (41) for \(j = 0, \ldots, d - 1\). When the user’s target index \(K\) is \(k \in [f]\), i.e., the targeted state is \(\rho_k\), our protocol is given as follows.

1. **Entanglement Sharing:** Let \(A, A', A''\) and \(B, B'\) be qubits and qudits, respectively, for \(j = 1, \ldots, n\). Before starting the protocol, Server 1 and Server 2 share \(n(d - 1)\) maximally entangled state \(|I_j\rangle\) on \(A_1 \otimes A'_1, \ldots, A_{d-1} \otimes A'_{d-1}\) with \(j = 1, 2, \ldots, n\), where Server 1 (Server 2) contains \(A_1, \ldots, A_{d-1}\) (\(A'_1, \ldots, A'_{d-1}\)). Server 1 and Server 2 share \(2n + 1\) copies of the maximally entangled state \(|I_y\rangle\) on \(A \otimes A' \otimes A'' \otimes B \otimes B'\) for \(j = 1, 2, \ldots, n\).
2. **Query:** The same as Protocol 1.
3. **Answer:** Servers 1 and 2 measure the system \(A\) and \(A'\) with the computation basis \(|j\rangle\) of \(\rho_j\), respectively and obtain the common outcome \(j\). Then, Servers 1 and 2 make the same as the answer of Protocol 6 with \(|\psi_j\rangle = |\phi_{i_0,j}\rangle, \ldots, |\psi_{i_{d-1},j}\rangle = |\phi_{i_{d-1},j}\rangle\).
4. **Reconstruction:** The user makes the same operation as Reconstruction of Protocol 6.

Entanglement Sharing step of Protocol 7 requires one more copy of the maximally entangled state \(|I_j\rangle\) in comparison with Entanglement Sharing step of Protocol 6. Since the outcome \(j\) in Answer step obeys the uniform distribution, the relation Equation (45) and the correctness of Protocol 6 guarantee the correctness of Protocol 7. Since the user’s behavior of Protocol 7 is the
same as that of Protocol 6, the user secrecy of Protocol 6 implies the user secrecy of Protocol 7. The server secrecy of Protocol 6 implies that the user cannot obtain any information for $|\varphi_{j,\gamma}\rangle$ for $j \neq k$. Hence, the server secrecy of Protocol 7 holds. Also, Protocol 7 has the same upload and download complexity as those of Protocol 6. In summary, we have the following lemma.

**Lemma 7.** Protocol 7 is a $1 - (\frac{d-1}{d})^n$-correct Q-TQOT protocol that satisfies the user secrecy and the server secrecy. Its upload complexity and its download complexity are $2n$ bits and $2n(d-1) + 4n \log d$ qubits, respectively. The required pre-entanglement is $n(d-1)$ copies of $|\Omega_i\rangle$ and $2n$ copies of $|\Omega_j\rangle$, i.e., $n(d-1) + 2n \log d$ ebits.

Theorem 1 can be shown by applying Lemma 7 to the case with $n = -d \log(1 - \alpha)$ because $1 - (\frac{d-1}{d})^n$ converges to $\alpha$ under this choice.

### 13. Conclusion

We have constructed a Q-TQOT protocol that enables the user to download the intended mixed state among $f$ mixed states. Existing protocols work with only classical messages. The proposed protocol satisfies the user secrecy and the server secrecy. To construct this protocol, we have constructed several protocols that work only in submodels.

There are many open problems related to the study of QPIR for quantum messages. The communication complexity of our protocols increases exponentially the number of qubits to be transmitted. Thus, constructing more efficient Q-TQOT protocols for qubits is also an open problem. Since our protocol has only two servers, there is a possibility that the communication complexity can be decreased by the extension to more than two servers. Studying this direction is an interesting future problem. Interesting applications of our Q-TQOT protocols can also be considered for other communication and computation problems. We leave these questions as another future problem.

Indeed, the papers [40–43,58,59] discussed the case with colluding servers. Another interesting future problem is to extend our results to the case with colluding servers.

### Appendix A: Diagonalization Process of Mixed States

In Equation (45), we introduced a decomposition of mixed states $\rho$ but it depends on the choice and order of the orthogonal unit eigenvectors of $\rho$. In this appendix, we give one method to uniquely determine the eigenvectors $|\psi_0\rangle, \ldots, |\psi_{\dim E_i}\rangle$ and their order.

We fix an orthonormal basis $B = \{|0\rangle, \ldots, |d-1\rangle\}$ and represent vectors $|\gamma\rangle$ with coordinates $|\gamma\rangle = (c_0, \ldots, c_{d-1})$ with respect to $B$. Consider the spectral decomposition $\rho = \sum_{i=0}^{\dim E_i} q_i P_i$, with $q_1 < q_2 < \cdots < q_\dim E_i$, where $P_i$ are orthogonal projections to eigenspaces $E_i$.

If $\dim E_i = 1$ for all $i$, we choose the unit eigenvector $|\psi_i\rangle = (\cos \theta_i, \sin \theta_i, \ldots, \sin \theta_{d-1}) \in E_i$ such that the first nonzero coordinate $c_{ij}$ is a positive real number. Then, the vectors $|\psi_i\rangle$ are uniquely determined and ordered.

If there exist $\dim E_i \geq 2$, for all $i$ with $\dim E_i \geq 2$, we choose the orthonormal eigenvectors $|\psi_{ij}\rangle = (\cos \theta_{ij}, \sin \theta_{ij}, \ldots, \sin \theta_{d-1}) \in E_i$ ($\forall j \in E_i$) so that the first nonzero coordinate $c_{i,j} \in E_i$ is positive real number and $j_1 < j_2$. Next, we concatenate the vectors as

$$|\gamma_{\dim E_i}\rangle = (|\psi_{i,1}\rangle, \ldots, |\psi_{i,\dim E_i}\rangle)$$

Then, the vectors $|\psi_{ij}\rangle$ are uniquely determined and ordered.

### Acknowledgements

M.H. was supported in part by the National Natural Science Foundation of China (Grants no. 62171212). S.S. was supported by the Japan Society for the Promotion of Science Grant-in-Aid for JSPS Fellows No. JP20J11484.

### Conflict of Interest

The authors declare no conflict of interest.

### Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

### Keywords

oblivious transfer, quantum state message, symmetric information retrieval, two servers, visible setting

Received: June 21, 2023
Published online: February 8, 2024

[1] H. J. Kimble, *Nature* 2008, 453, 1023.
[2] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, S. Yamashita, in STACS 2007 SE - 52 (Eds.: W. Thomas, P. Weil), vol. 4393, Springer, Berlin Heidelberg, 2007, pp. 610–621.
[3] M. Hayashi, *Phys. Rev. A* 2007, 76, 40301.
[4] H. Kobayashi, F. Le Gall, H. Nishimura, M. Rötteler, in Automata, Languages and Programming SE - 52 (Eds.: S. Albers, A. Marchetti-Spaccamela, Y. Matias, S. Nikoletseas, W. Thomas), vol. 5555, Springer, Berlin Heidelberg, 2009, pp. 622–633.
[5] D. Leung, J. Oppenheim, A. Winter, *IEEE Trans. Inform. Theory* 2010, 56, 3478.
[6] A. Jain, M. Franceschetti, D. A. Meyer, *J. Math. Phys.* 2011, 52, 032201.
[7] S. Song, M. Hayashi, *IEEE Trans. Inform. Theory* 2020, 66, 1178.
[8] G. Chiribella, G. M. D’Ariano, P. Perinotti, *Phys. Rev. Lett.* 2008, 101, 060401.
[9] G. Chiribella, G. M. D’Ariano, P. Perinotti, *Phys. Rev. A* 2009, 80, 022339.
[10] M. Hayashi, S. Song, *Phys. Rev. Res.* 2020, 2, 033079.
[11] A. Beaudrap, S. Herbert, *Quantum, Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften* 2020, 4, 356.
[12] H. Lu, Z.-D. Li, X.-F. Yin, R. Zhang, X.-F. Fang, L. Li, N.-L. Liu, F. Xu, Y.-A. Chen, J.-W. Pan, *npj Quantum Inf.* 2019, 5, 89.
[13] X. Pan, X. Chen, G. Xu, Z. Li, Y. Yang, *Quantum Science and Technology*, vol. 7, IOP Publishing, Bristol, England 2021, p. 015006.
[14] H. V. Nguyen, Z. Babar, D. Alanis, P. Bosinís, D. Chandra, M. A. M. Izhar, S. X. Ng, L. Hanzo, *IEEE Access* 2017, 5, 17288.
[15] P. Pathumsoot, T. Matsuio, T. Saitoh, M. Hajdušek, S. Suwanna, R. V. Meter, *Phys. Rev. A* 2020, 101, 052301.
[16] X.-B. Pan, G. Xu, Z.-P. Li, X.-B. Chen, Y.-X. Yang, *Quantum Inf. Process.* 2021, 20, 65.
[17] X. Pan, X. Chen, G. Xu, H. Ahmard, T. Shang, Z.-P. Li, Y.-X. Yang, *CMC-Comput. Mater. Contin.* 2021, 69, 3967.
[18] N. Walk, J. Eisert, *PRX Quantum* 2021, 2, 040339.
[19] A. M. Childs, *Quantum Inf. Comput.* 2005, 5, 456.
[20] A. Broadbent, J. Fitzsimons, E. Kashefi, *Proc. 50th Annual Symp. on Found. of Comput. Sci.*, IEEE, Piscataway, NJ 2009, pp. 517–526.
[21] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, P. Walther, *Science* 2012, 335, 303.
[22] T. Morimae, K. Fujii, Nat. Commun. 2012, 3, 1036.
[23] T. Morimae, Phys. Rev. A 2014, 89, 060302(R).
[24] A. Mantri, C. A. P. Delgado, J. F. Fitzsimons, Phys. Rev. Lett. 2013, 111, 230502.
[25] T. Morimae, K. Fujii, Phys. Rev. Lett. 2013, 111, 020502.
[26] Q. Li, W. H. Chan, C. Wu, Z. Wen, Phys. Rev. A 2014, 89, 040302(R).
[27] Y. B. Sheng, L. Zhou, Sci. Rep. 2015, 5, 7815.
[28] M. Hayashi, T. Morimae, Phys. Rev. Lett. 2015, 115, 220502.
[29] C. Crepeau, J. Kilian, in Proceedings of 29th Annual Symposium on Foundations of Computer Science, IEEE, Piscataway, NJ 1988, p. 42.
[30] C. H. Bennett, G. Brassard, C. Crepeau, M.-H. Skubiszewska, in Proceedings of Advances in Cryptology—CRYPTO’91, 11th Annual International Cryptology Conference, Springer, Berlin 1991.
[31] H.-K. Lo, Phys. Rev. A 1997, 56, 1154.
[32] P. Wang, R. Zhang, G. Jiang, Z. Sun, Adv. Quantum Technol. 2021, 5, 2100125.
[33] Y. Ishai, M. Prabhakaran, A. Sahai, in Advances in Cryptology—CRYPTO 2008, (Ed.: D. Wagner), vol. 5157, Springer, Berlin 2008.
[34] D. Feng, K. Yang, Secur. Saf. 2022, 1, 2021001.
[35] I. Kerenidis, R. de Wolf, Proceedings of 35th ACM STOC, 2003, pp. 106–115.
[36] I. Kerenidis, R. de Wolf, Inf. Process. Lett. 2004, 90, 109.
[37] S. Song, M. Hayashi, IEEE Trans. Inf. Theory 2021, 67, 452.
[38] H. Sun, S. Jafar, IEEE Trans. Inf. Theory 2017, 63, 4075.
[39] H. Sun, S. Jafar, 2016 IEEE Globecom Workshops (GC WKSHPS), IEEE, Washington, DC, 2016, pp. 1–5.
[40] S. Song, M. Hayashi, IEEE J. Sel. Areas Inf. Theory 2021, 2, 380.
[41] S. Song, M. Hayashi, IEEE Trans. Inf. Theory 2021, 67, 5491.
[42] M. Allaix, L. Holzbaur, T. Pliaha, C. Hollanti, IEEE J. Sel. Areas Inf. Theory 2020, 1, 599.
[43] M. Allaix, S. Song, L. Holzbaur, T. Pliaha, M. Hayashi, C. Hollanti, IEEE J. Sel. Areas Commun. 2022, 40, 885.
[44] W. Y. Kon, C. C. W. Lim, Entropy 2021, 23, 54.
[45] C. Wang, W. Y. Kon, H. J. Ng, C. C. Lim, Light Sci. Appl. 2022, 11, 268.
[46] C. Wang, W. Y. Kon, H. J. Ng, C. C. Lim, Quantum Information and Measurement VI 2021, Technical Digest Series, (Eds.: F. Sciarrino, N. Treps, M. Giustina, C. Silberhorn), Optica Publishing Group, Washington, D.C. 2021.
[47] S. Wiesner, SIGACT News 1983, 15, 78.
[48] D. Gottesman, I. Chuang, Quantum Digital Signatures, 2001, arXiv: quant-ph/0105032.
[49] C. Mochon, Quantum weak coin flipping with arbitrarily small bias, 2007, arXiv: 0711.4114.
[50] A. Chailloux, I. Kerenidis, in 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, IEEE Computer Society, Atlanta, Georgia, USA 2009, pp. 527–533.
[51] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, L. Magnin, SIAM J. Comput. 2016, 45, 633.
[52] R. Jozsa, B. Schumacher, J. Mod. Opt. 1994, 41, 2343.
[53] B. Schumacher, Phys. Rev. A 1995, 51, 2738.
[54] R. Jozsa, M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. 1998, 81, 1714.
[55] M. Horodecki, Phys. Rev. A 1998, 57, 3364.
[56] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, B. Schumacher, J. Phys. A Math. Gen. 2001, 34, 6767.
[57] M. Hayashi, Phys. Rev. A 2002, 66, 032321.
[58] H. Sun, S. Jafar, IEEE Trans. Inf. Theory 2018, 64, 2361.
[59] R. Freij-Hollanti, O. W. Gnilke, C. Hollanti, D. A. Karpuk, SIAM J. Appl. Algebra Geometry 2017, 1, 647.