Quantum Private Information Retrieval for Quantum Messages

Seunghoan Song[1], Masahito Hayashi[2,1]

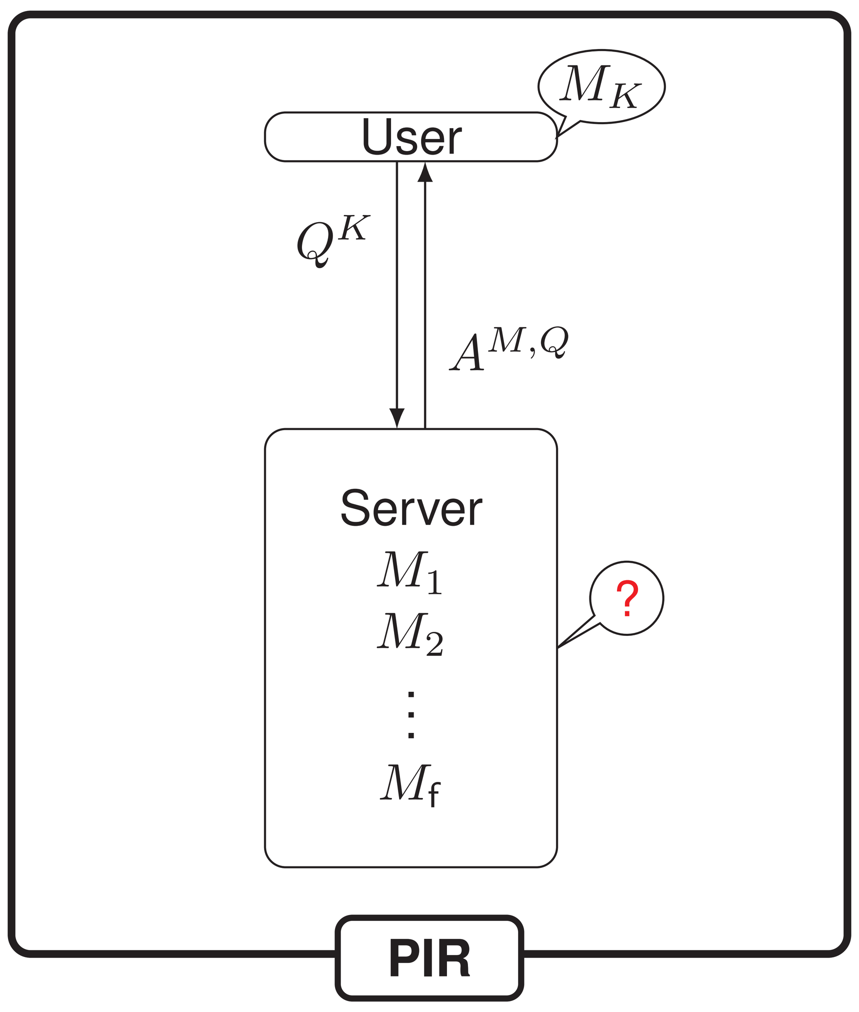
(arXiv:2101.09041)

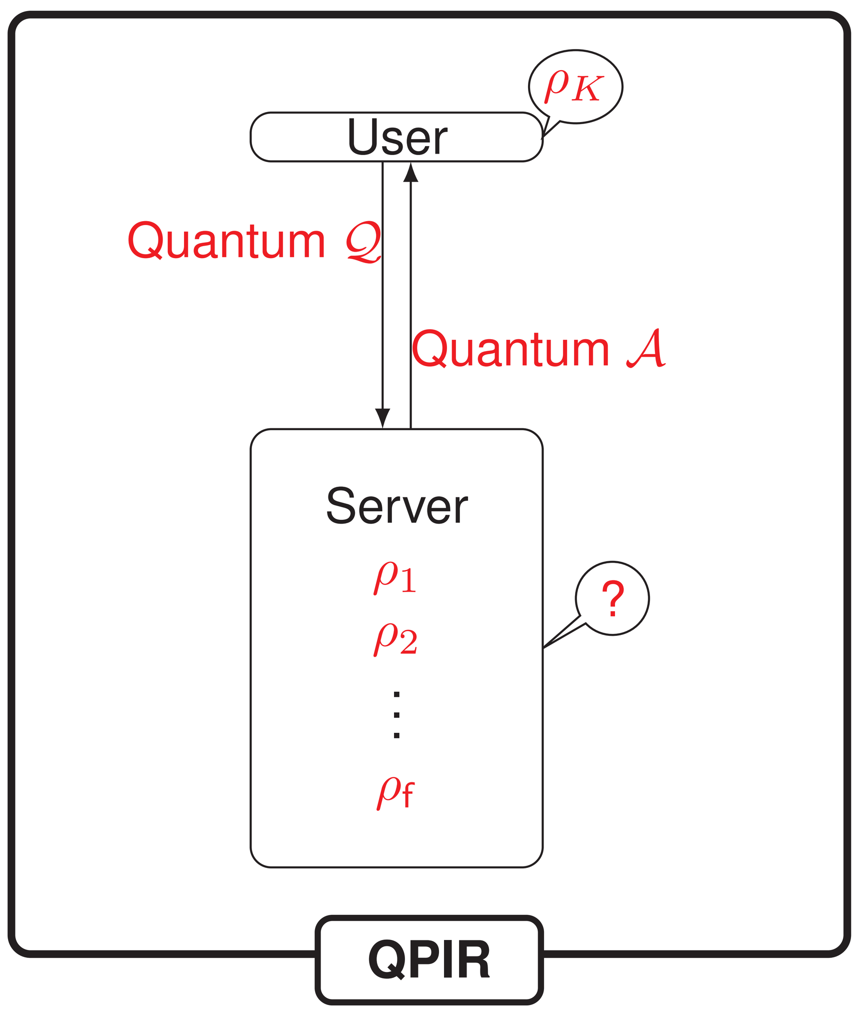
[1]Nagoya University, [2]Southern University of Science and Technology

I. Private Information Retrieval (PIR)

Private Information Retrieval

Private Information Retrieval (PIR) is the problem to retrieve one of f messages from server(s) without revealing the identity of the retrieved message.





- "Downloading all" messages in the server is optimal for the classical case [Chor et al.95].
- Existing Quantum PIR (QPIR) studies mainly focused on QPIR for classical message retrieval with quantum communication. [Le Gall12], [Baumeler and Broadbent 15], [Aharonov et al.19], $\cdots$

Blind and Visible Settings for State Preparation

1. **Blind Setting**: The server(s) contains quantum systems $\mathcal{A}_1, \ldots, \mathcal{A}_{\mathsf{f}}$ with states $\rho_1, \ldots, \rho_{\mathsf{f}}$.

- The server(s) does not know the states $\rho_1, \ldots, \rho_{\mathsf{f}}$.
- Copying the states are impossible by no cloning theorem.

2. **Visible Setting**: The server(s) contains the description of $\rho_1, \ldots, \rho_{\mathsf{f}}$.

- The server(s) knows the states.
- The server(s) may generate multiple copies of $\rho_1, \ldots, \rho_{\mathsf{f}}$.
- The server(s) may apply operations depending on the description of $\rho_1, \ldots, \rho_{\mathsf{f}}$.

II. Main Results

- "Downloading all" has communication complexity $O(\mathsf{m})$.

– m: the total size of messages/states in a server.
– Communication complexity (CC) = Query cost + Download cost.

[Result 1]: "Downloading all" is optimal for one-server QPIR.

Messages	Server Model	Optimal CC	Ref.
Classical	Honest	$O(\text{poly} \log \mathsf{m})$	[Kerenidis et al. 16]
Classical	Specious*	$\Theta(\mathsf{m})$	[Baumeler-Broadbent 15]
Quantum (blind)	Honest	$\Theta(\mathsf{m})$	[This paper]
Quantum (visible)	Honest	$\Theta(\mathsf{m})$ (for one-round)	[This paper]

∗ Specious server does malicious actions without noticed by the user.

[Result 2]: There exists an efficient one-server QPIR protocol with shared entanglement.

Messages	Server Model	Optimal CC	Ref.
Classical	Honest	$O(\log \mathsf{m})$	[Kerenidis et al. 16]
Classical	Specious	$\Theta(\mathsf{m})$	[Aharonov et al. 19]
Quantum (blind/visible)	Honest	$O(\log \mathsf{m})$	[This paper]

[Result 3]: There exist efficient two-server quantum symmetric PIR (QSPIR) protocols on the visible setting.
(QSPIR is the QPIR in which the user obtains no information except for ρ_K.)

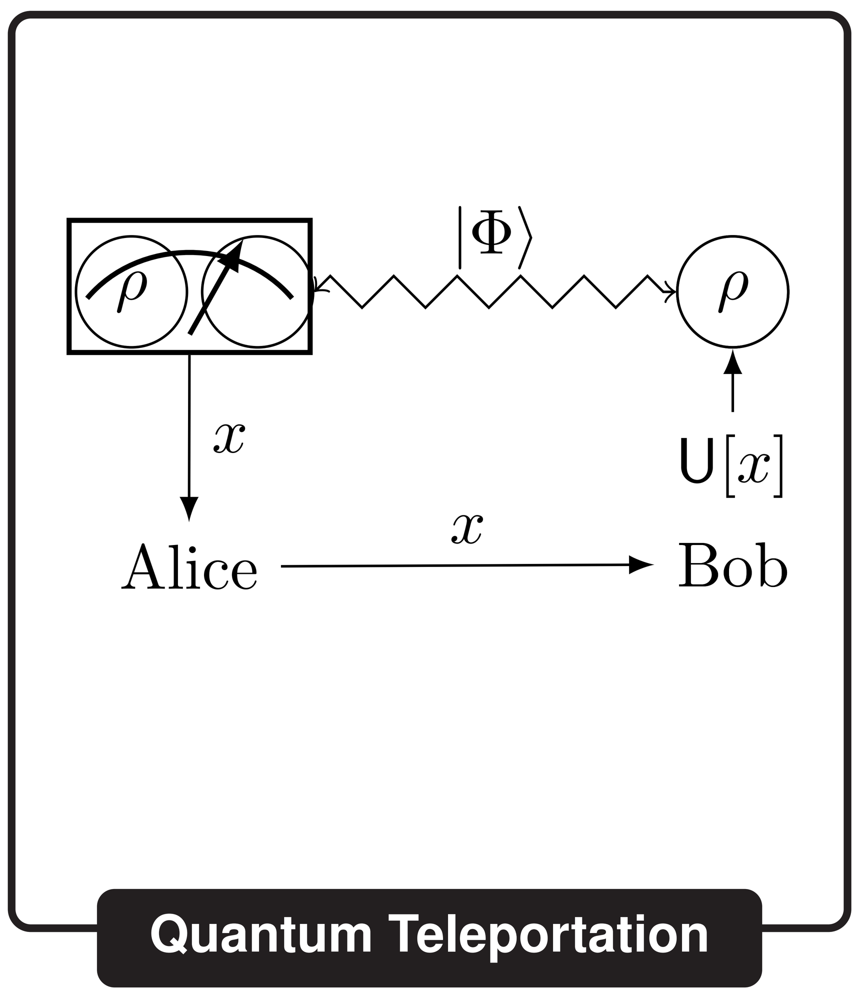
	Protocol 1	Protocol 2
Dimension of pure states	$d = 2$	$d \geq 2$
Classical Communication	2f bits	2f bits
Quantum Communication	8 qubits	$4d^d \log d$ qubits
Prior Entanglement	4 ebits	$2d^d \log d$ ebits

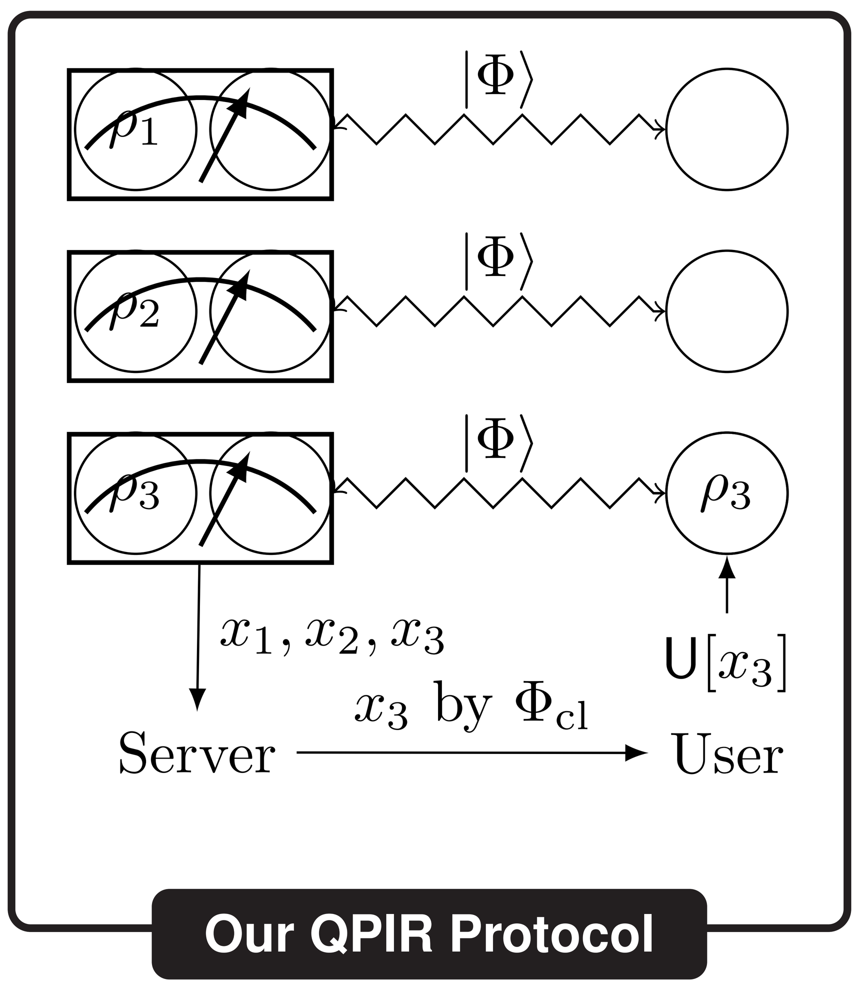
$(\mathsf{m} = \mathsf{f} \log d)$

III. [Result 2] One-Server QPIR with Entanglement

Theorem 1 *Let Φ_{cl} be a QPIR protocol for classical messages with communication complexity $O(f(\mathsf{m}))$ and $O(g(\mathsf{m}))$ ebits. In the blind setting, there exists a QPIR protocol for quantum messages with communication complexity $O(f(\mathsf{m}))$ and $O(\mathsf{m} + g(\mathsf{m}))$ ebits.*

[Proof idea] Quantum teleportation + QPIR for classical messages Φ_{cl}.





IV. [Result 3] Two-Server QSPIR for Pure Qubit States

Idea 1. Decomposition of pure qubit states + 2. Classical two-server PIR

1. Decomposition of pure qubit states

- Decomposition of pure states Any pure qubit states $|\psi\rangle$ are written as

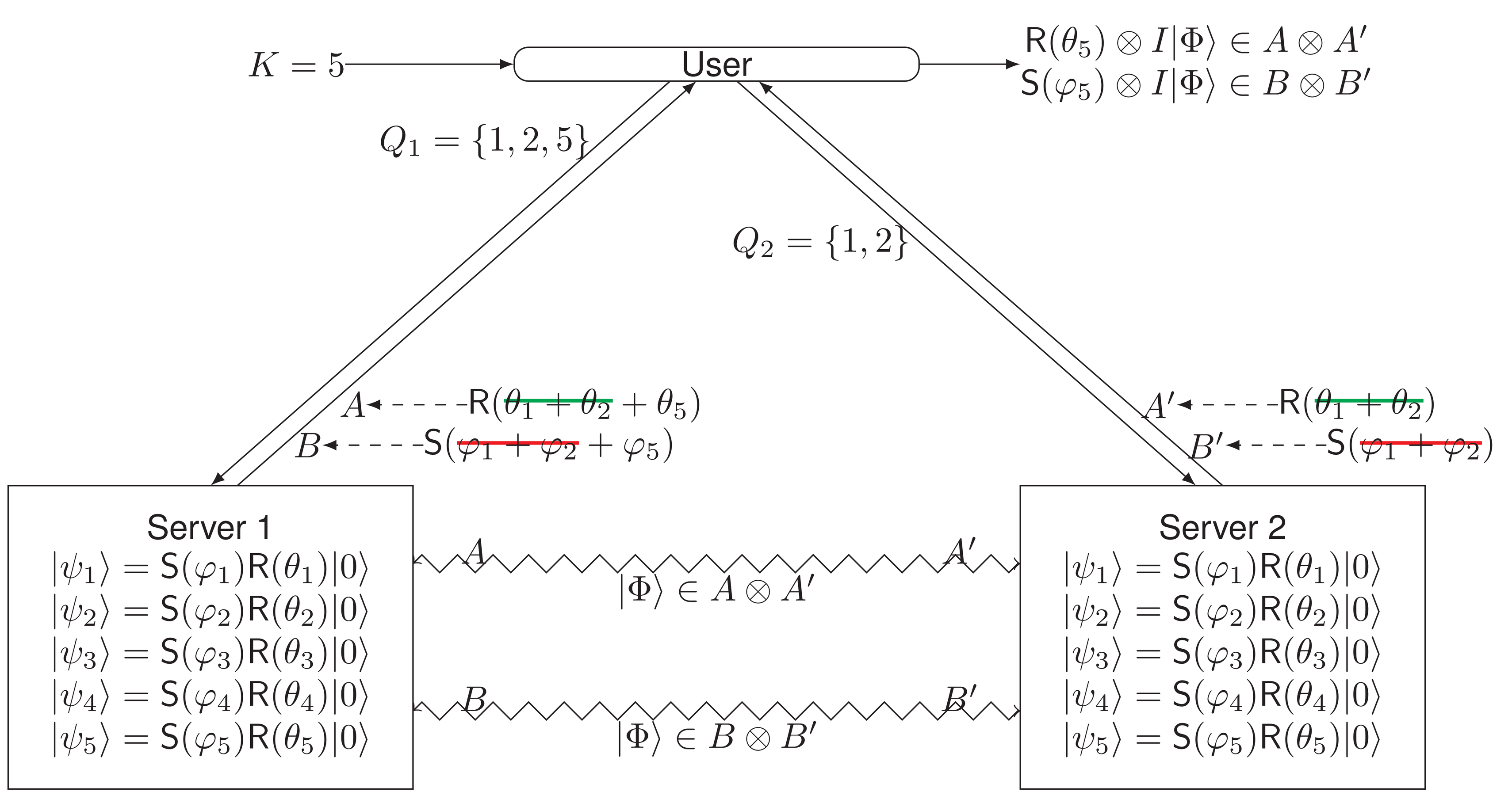
$$|\psi\rangle = \mathsf{S}(\varphi)\mathsf{R}(\theta)|0\rangle$$

with some $\varphi \in [0, 2\pi)$ and $\theta \in [0, \pi/2]$, where

[Rotation] $\mathsf{R}(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, [Phase-shift] $\mathsf{S}(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\sqrt{-1}\varphi} \end{pmatrix}$.

- $\mathsf{R}(\theta)\mathsf{R}(\theta') = \mathsf{R}(\theta + \theta')$, $\mathsf{S}(\varphi)\mathsf{S}(\varphi') = \mathsf{S}(\varphi + \varphi')$.
- $\mathsf{R}(\theta) \otimes \mathsf{R}(\theta')|\Phi\rangle = \mathsf{R}(\theta - \theta') \otimes I|\Phi\rangle$,
  $\mathsf{S}(\varphi) \otimes \mathsf{S}(\varphi')|\Phi\rangle = \mathsf{S}(\varphi - \varphi') \otimes I|\Phi\rangle$.

2. QSPIR protocol induced from classical two-server PIR



- **User secrecy**: Each of Q_1 and Q_2 is random subset of $\{1, \ldots, 5\}$.
- **Server secrecy**: The received states $\mathsf{R}(\theta_5) \otimes I|\Phi\rangle$ and $\mathsf{S}(\varphi_5) \otimes I|\Phi\rangle$ are independent of other states.
- **Correctness**: The targeted state $|\psi_5\rangle$ is recovered by the following steps.

1. Received state: $\mathsf{R}(\theta_5) \otimes I|\Phi\rangle \in A \otimes A'$ and $\mathsf{S}(\varphi_5) \otimes I|\Phi\rangle \in B \otimes B'$
2. Apply bell measurement on $A' \otimes B'$: $\mathsf{R}(\theta_5) \otimes \mathsf{S}(\varphi_5)|\Phi\rangle \in A \otimes B$.
3. Apply basis measurement $\{|0\rangle, |1\rangle\}$ on B: $|\psi_5\rangle = \mathsf{S}(\theta_5)\mathsf{R}(\theta_5)|0\rangle \in A$.