Capacity of Quantum Private Information Retrieval with Multiple Servers

(arXiv:1903.10209, 1903.12556.)

Masahito Hayashi

Graduate School of Mathematics, Nagoya University

Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology (SUSTech)

Peng Cheng Laboratory, Shenzhen

Centre for Quantum Technologies, National University of Singapore

Joint work with Seunghoan Song

Summary

QPIR with multiple servers: A user retrieves a classical file by downloading quantum systems from multiple servers each of which containing the whole classical file set without revealing the identity of the retrieved file to any individual server.

QPIR capacity: Maximum rate of the file size over the whole dimension of the downloaded quantum systems.

QPIR capacity with multiple servers is *1* when the preexisting entanglement among servers are assumed.

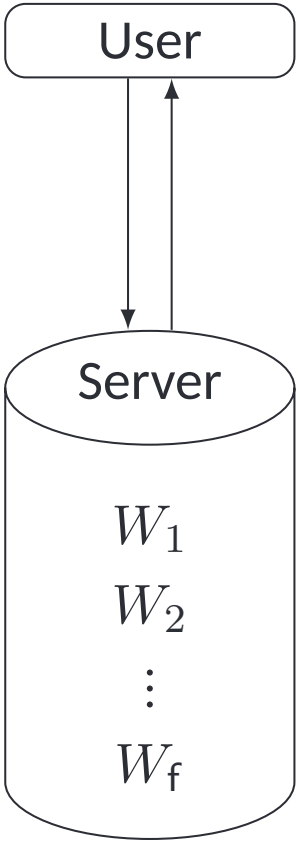
Our rate-one protocol requires *only two servers*.

Our capacity-achieving protocol *outperforms* its classical counterpart in the sense of the capacity, server secrecy, and upload cost.

Strong converse property hold even when any secrecy condition is imposed.

Private Information Retrieval (PIR)

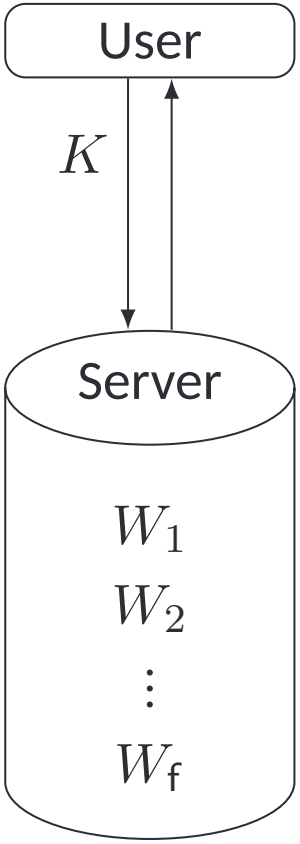
What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



<Download>

Private Information Retrieval (PIR)

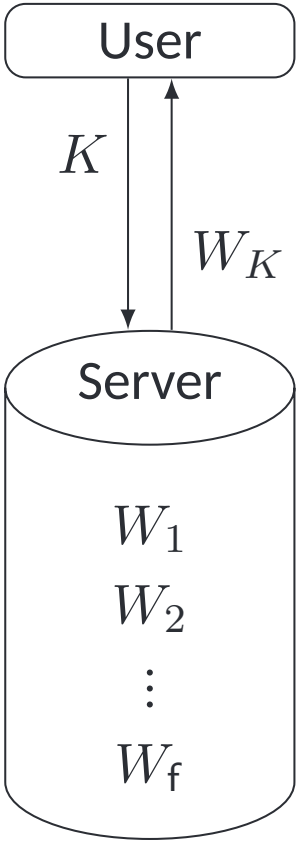
What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



<Download>

Private Information Retrieval (PIR)

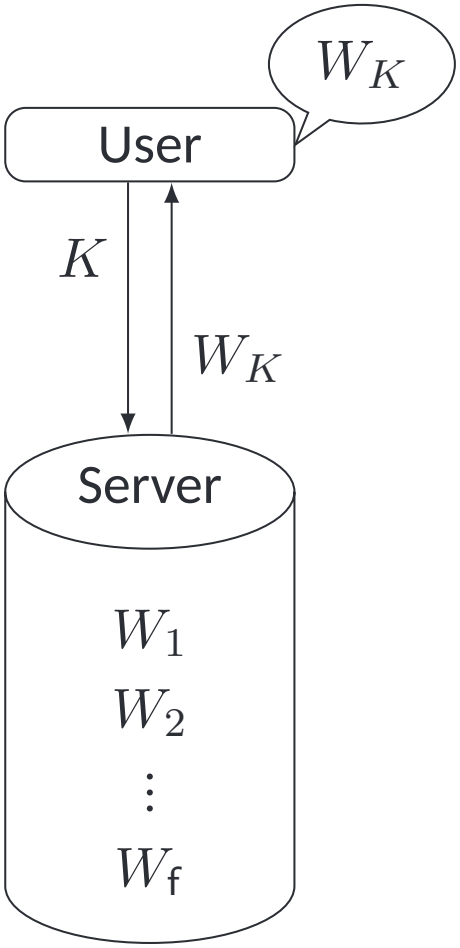
What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



<Download>

Private Information Retrieval (PIR)

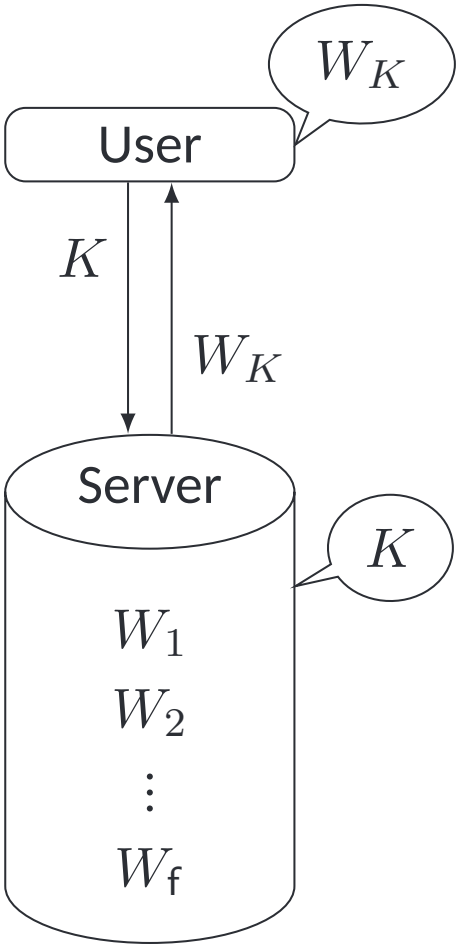
What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



<Download>

Private Information Retrieval (PIR)

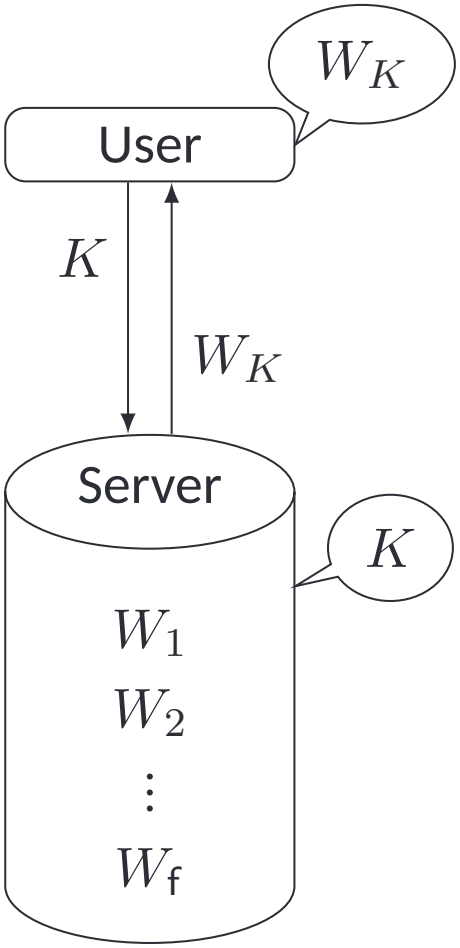
What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



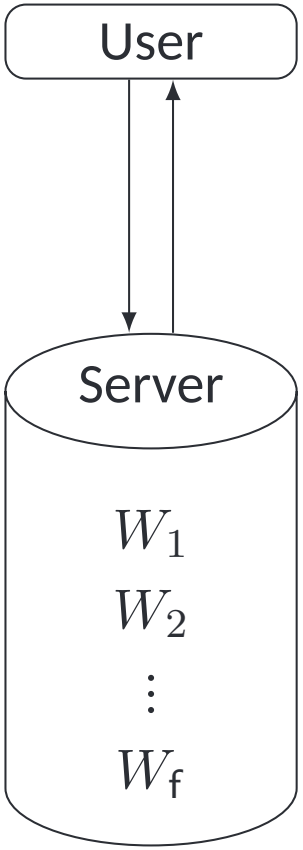
<Download>

Private Information Retrieval (PIR)

What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



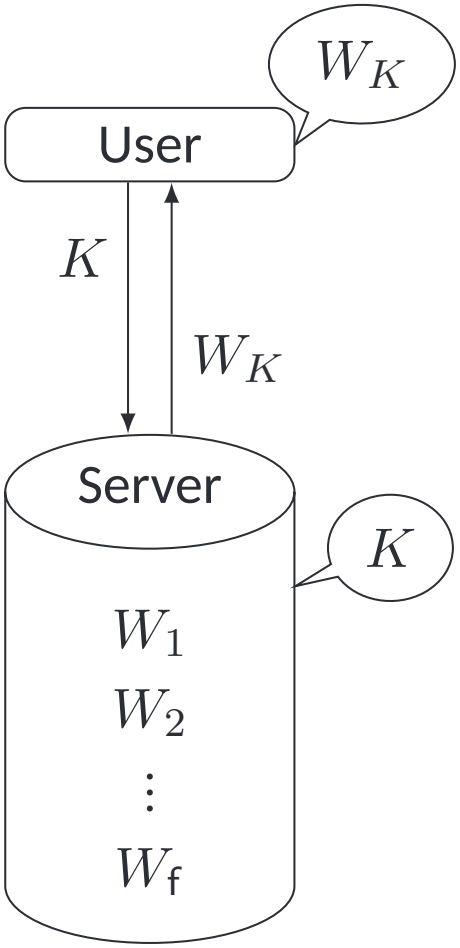
<Download>



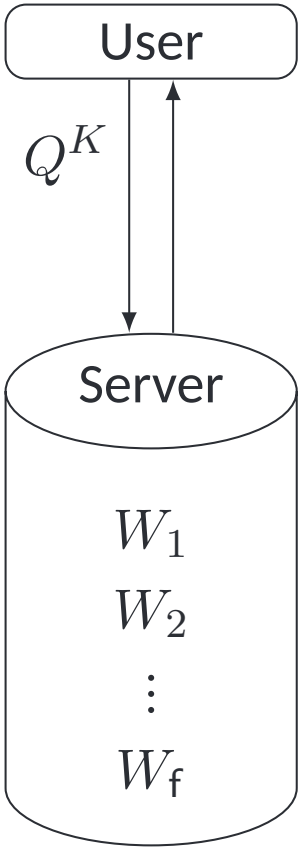
<PIR>

Private Information Retrieval (PIR)

What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



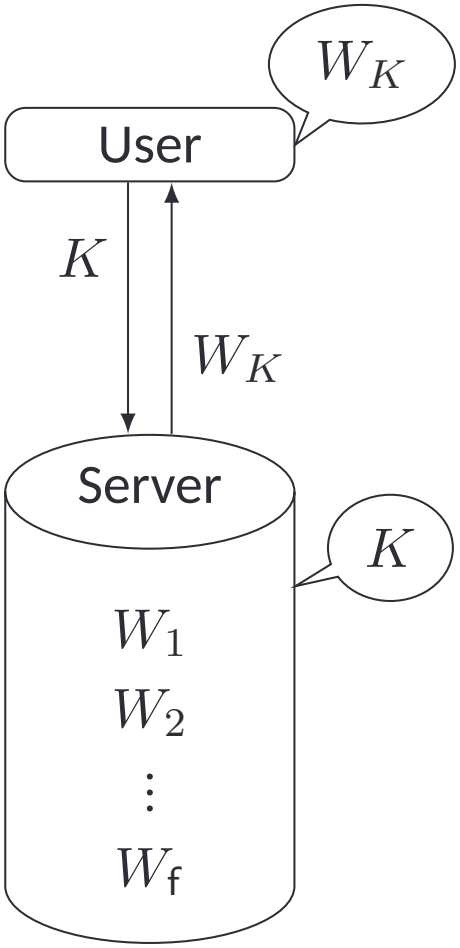
<Download>



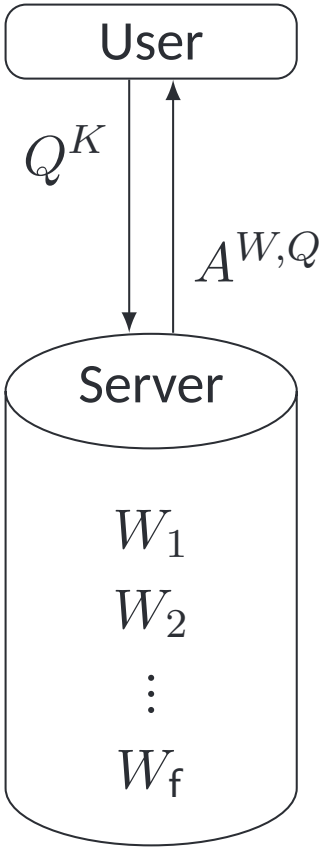
<PIR>

Private Information Retrieval (PIR)

What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



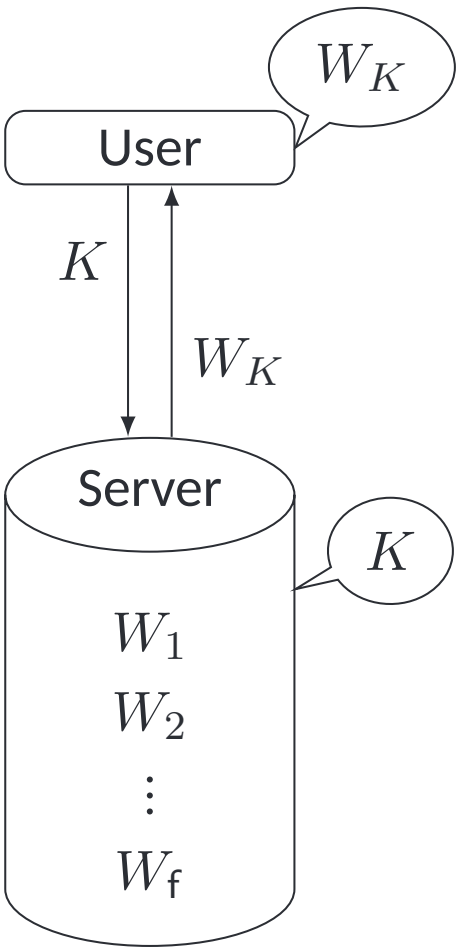
<Download>



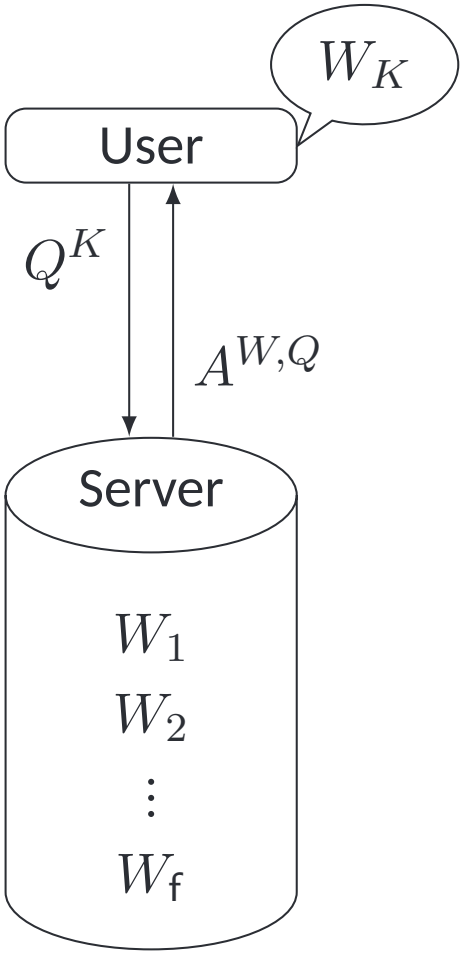
<PIR>

Private Information Retrieval (PIR)

What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



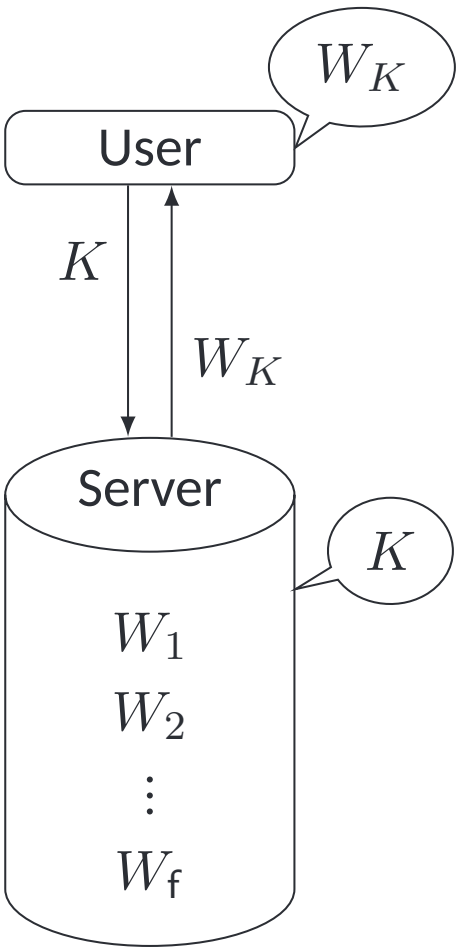
<Download>



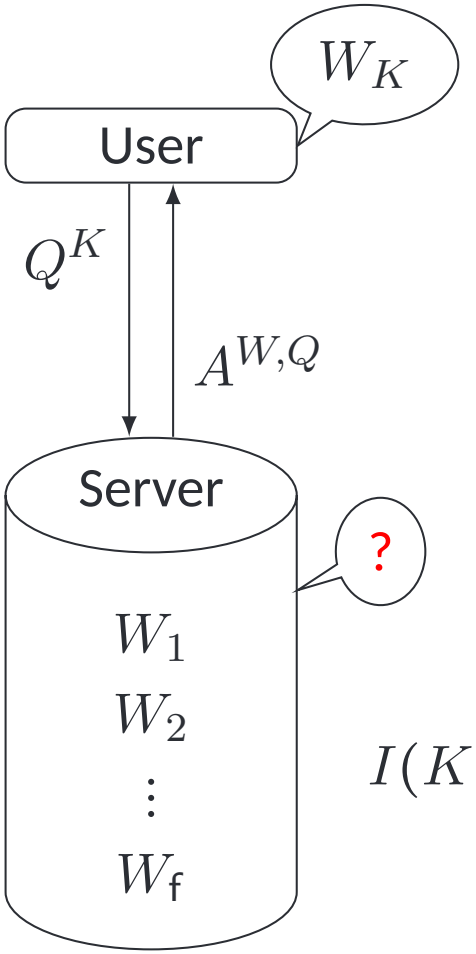
<PIR>

Private Information Retrieval (PIR)

What is PIR? The method to download a file from servers without revealing which file is downloaded [Chor et al.95].



<Download>

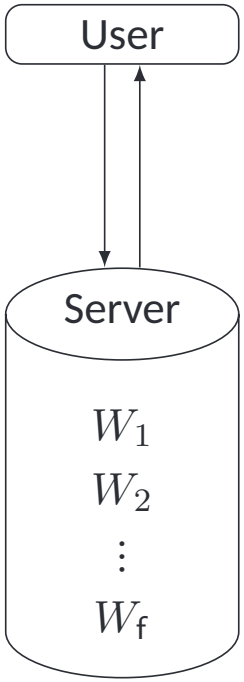


$I(K;Q^K) = 0$

<PIR>

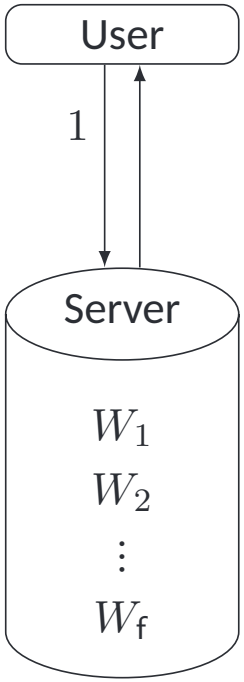
Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].



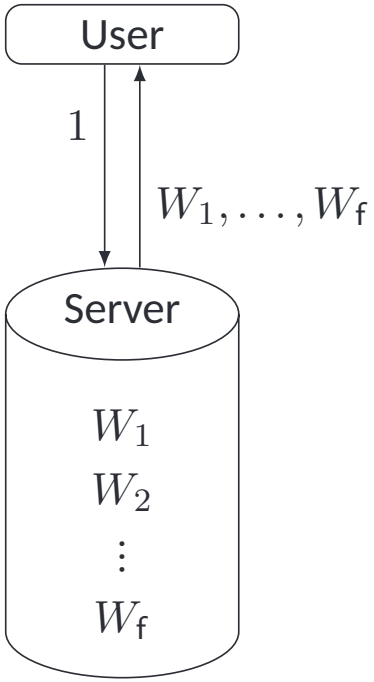
Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].



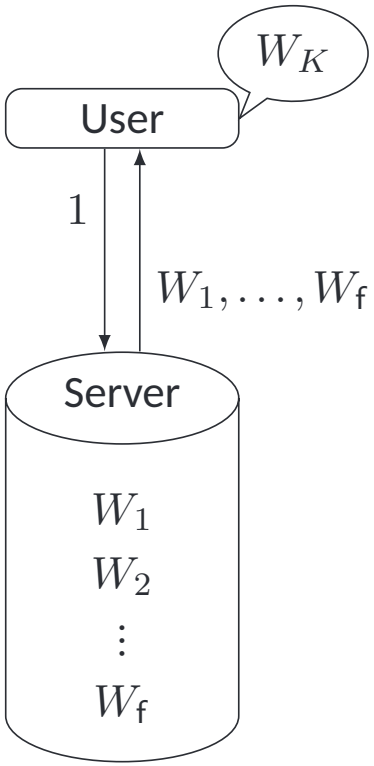
Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].



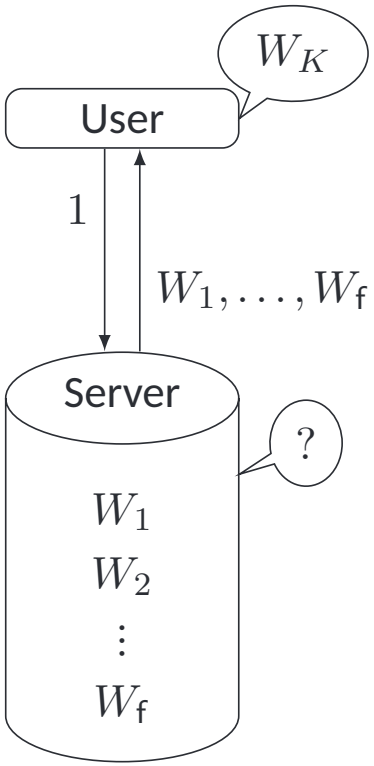
Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].



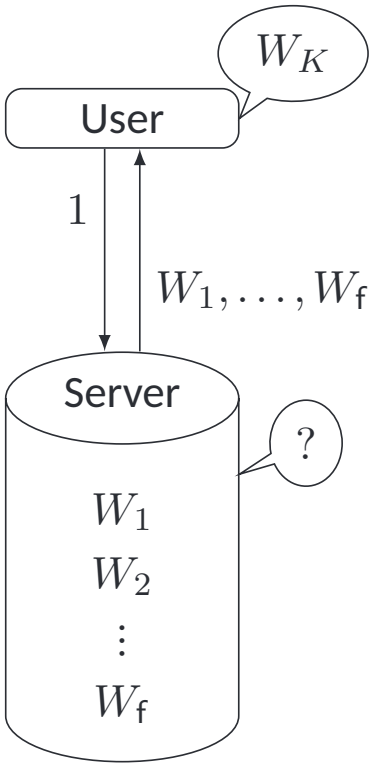
Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].



Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].

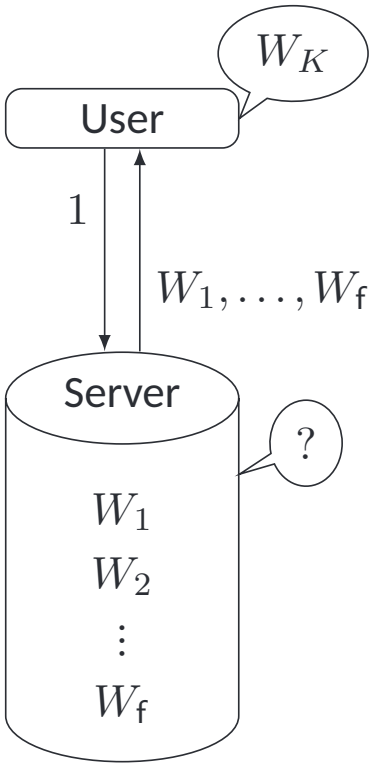


Problems

1. No server secrecy: User obtains files other than W_K.
2. Cost is too large.

Simple Solution for Classical PIR

- **Simple Solution for Classical PIR:** Downloading all files.
- Downloading all files is optimal on communication complexity [Chor et al.95].

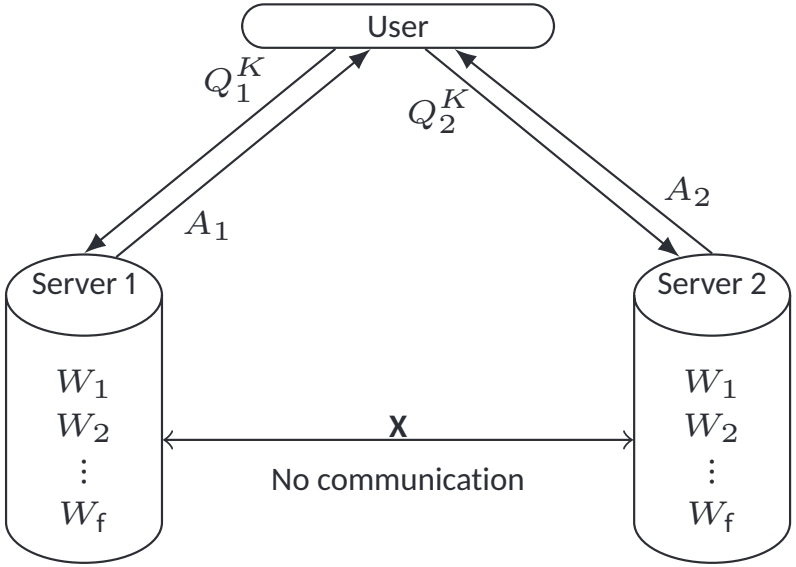


Problems

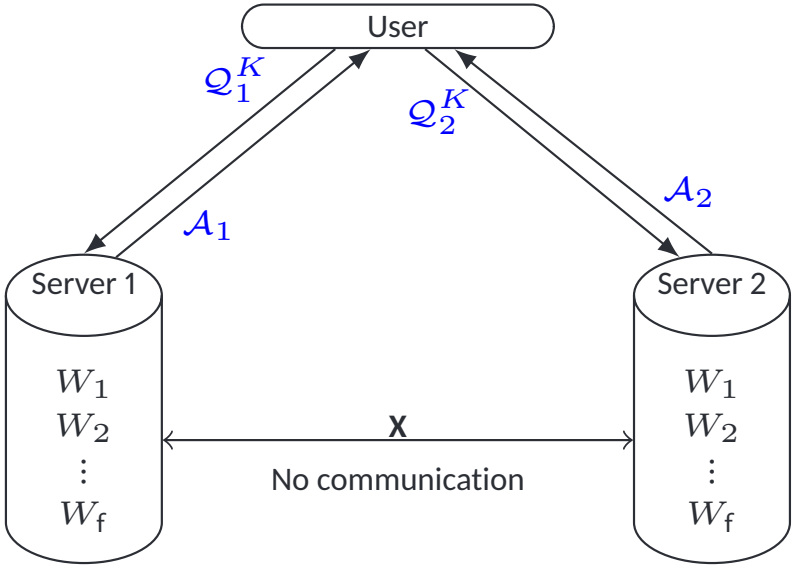
1. No server secrecy: User obtains files other than W_K.
2. Cost is too large.

Our QPIR protocol solves these two problems.

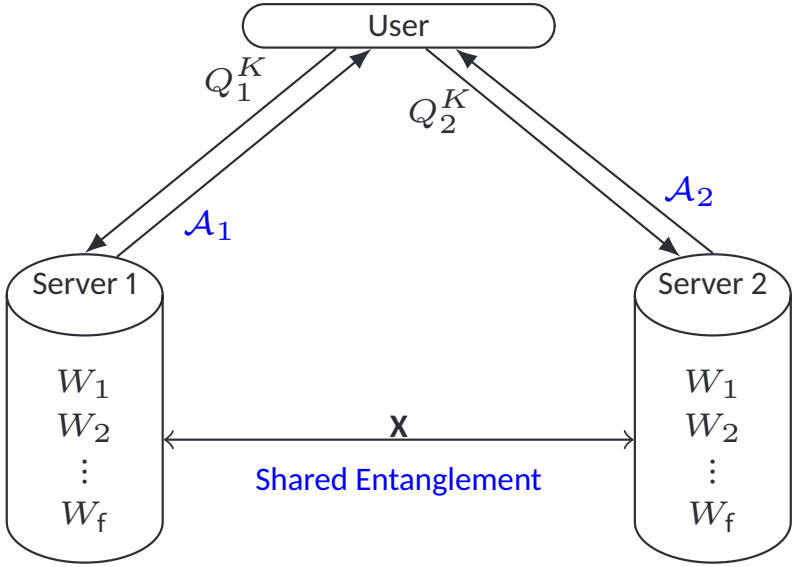
Multiple Server PIR Models



<Multi-Server PIR>



<Multi-Server Quantum PIR (two-way)>



<Multi-Server Quantum PIR **(Our Model)**>

Server Secrecy of PIR

[Server Secrecy]: $$I(\underbrace{Q, A}_{\text{user's info.}}; \underbrace{W_1, \ldots, W_{K-1}, W_{K+1}, \ldots, W_{\mathsf{f}}}_{\text{files other than } W_K} | K) = 0.$$

Question: Does there exist a PIR protocol with server secrecy?

- Single-server PIR with server secrecy (Oblivious Transfer)
  - Classical PIR: No.
  - Quantum PIR (two-way): No [Mayers97, Lo-Chau98].
- Multi-server PIR with server secrecy
  - Classical PIR: No [Gertner et al.00]. (Yes with shared randomness among servers)
  - Quantum PIR (two-way): Yes [Kerenidis-deWolf04].

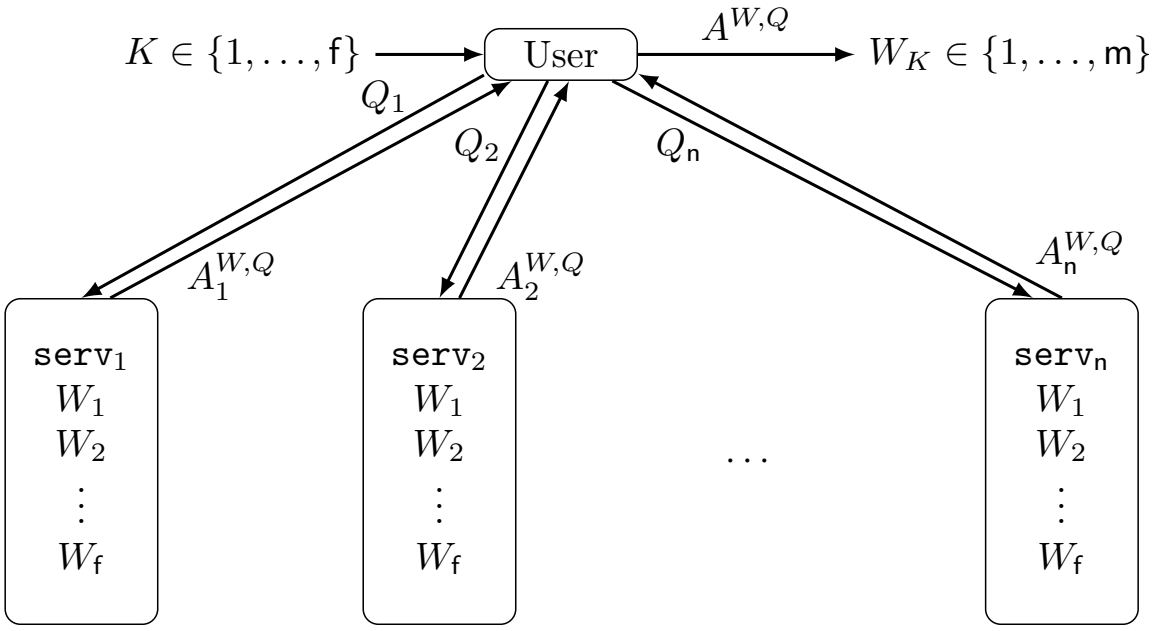
Server Secrecy of PIR

[Server Secrecy]: $$I(\underbrace{Q, A}_{\text{user's info.}}; \underbrace{W_1, \ldots, W_{K-1}, W_{K+1}, \ldots, W_{\mathsf{f}}}_{\text{files other than } W_K} | K) = 0.$$

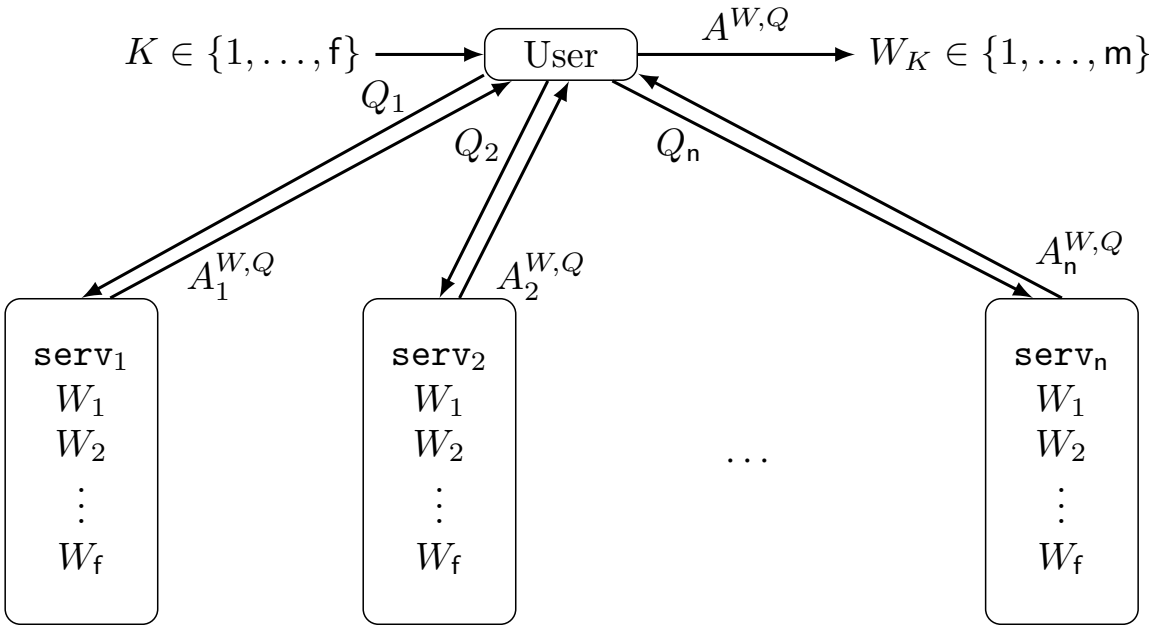
Question: Does there exist a PIR protocol with server secrecy?

- Single-server PIR with server secrecy (Oblivious Transfer)
  - Classical PIR: No.
  - Quantum PIR (two-way): No [Mayers97, Lo-Chau98].
- Multi-server PIR with server secrecy
  - Classical PIR: No [Gertner et al.00]. (Yes with shared randomness among servers)
  - Quantum PIR (q. download and shared entanglement): **Yes (Our Result).**
  - Quantum PIR (two-way): Yes [Kerenidis-deWolf04].

Classical PIR Capacity

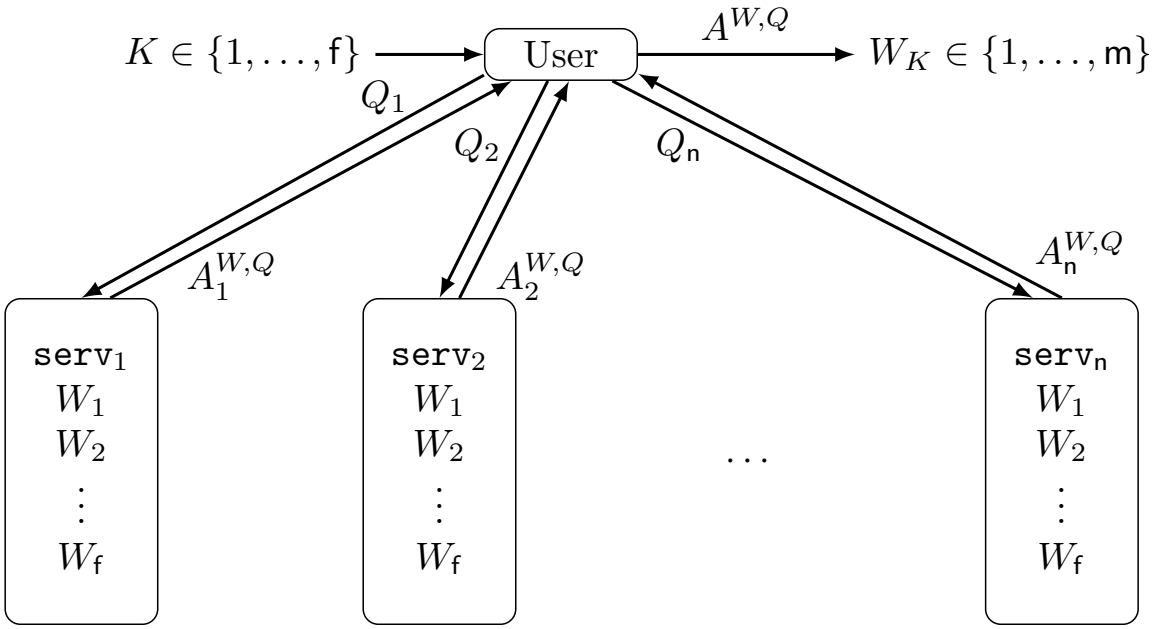


Classical PIR Capacity



Information-Theoretic Approach [Sun-Jafar16], [Banawan-Ulukus17], ...

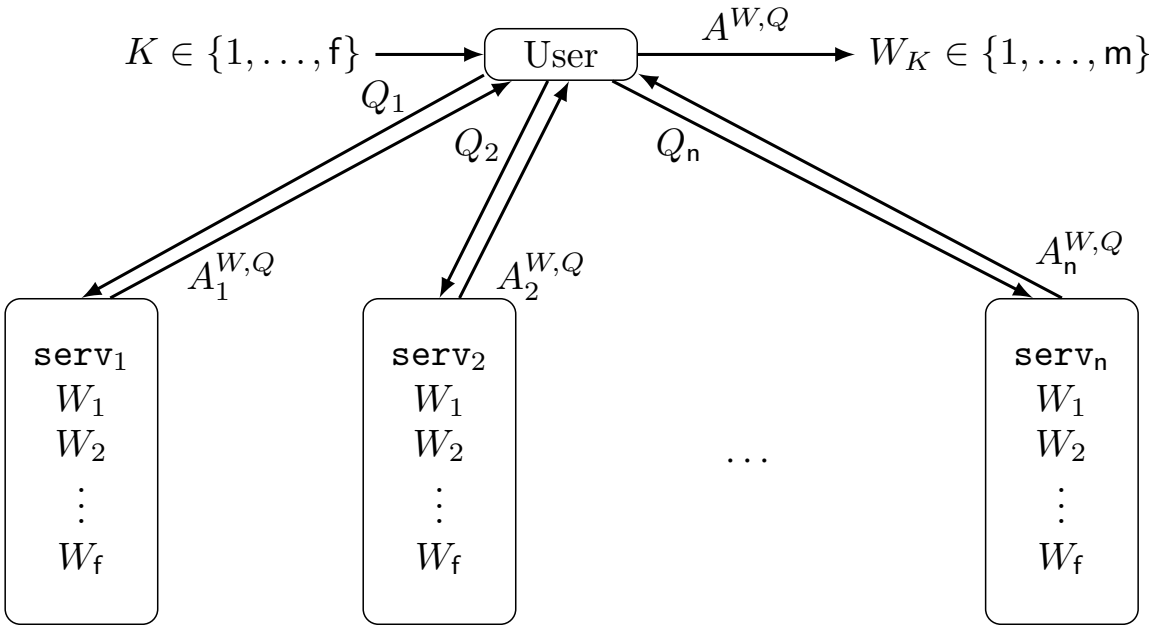
Classical PIR Capacity



Information-Theoretic Approach [Sun-Jafar16], [Banawan-Ulukus17], ...

- (n, f): Numbers of servers and files. $\leftarrow$ **Fixed**

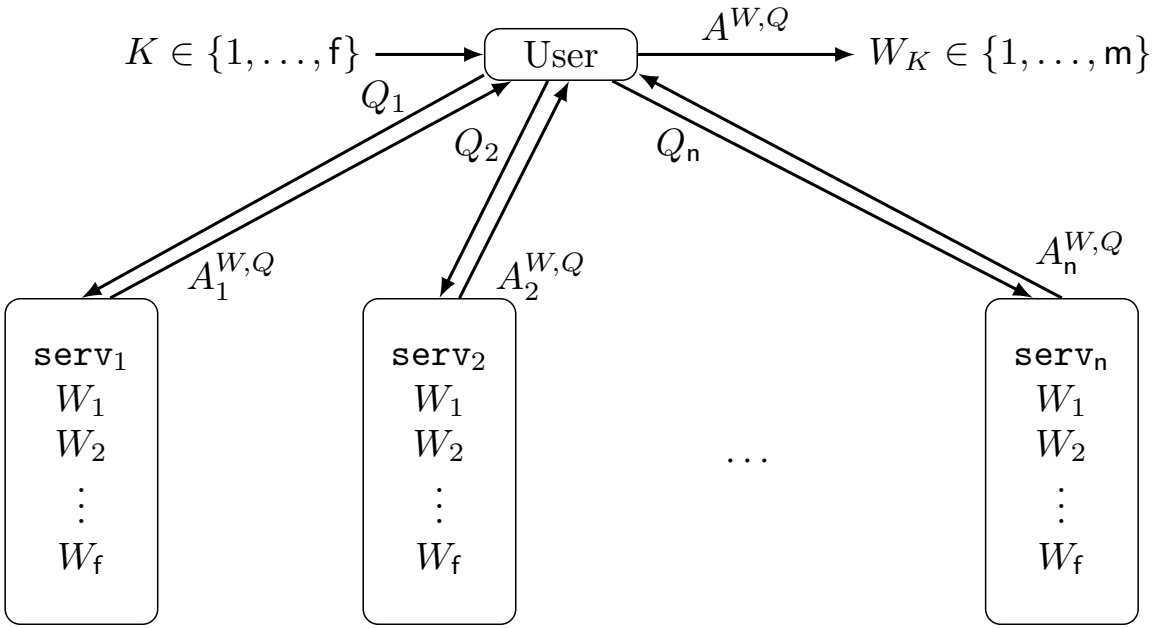
Classical PIR Capacity



Information-Theoretic Approach [Sun-Jafar16], [Banawan-Ulukus17], ...

- (n, f): Numbers of servers and files. ← **Fixed**
- m: File size. ← **Arbitrary** $(W_1, \ldots, W_\mathsf{f} \in \{1, \ldots, \mathsf{m}\})$

Classical PIR Capacity



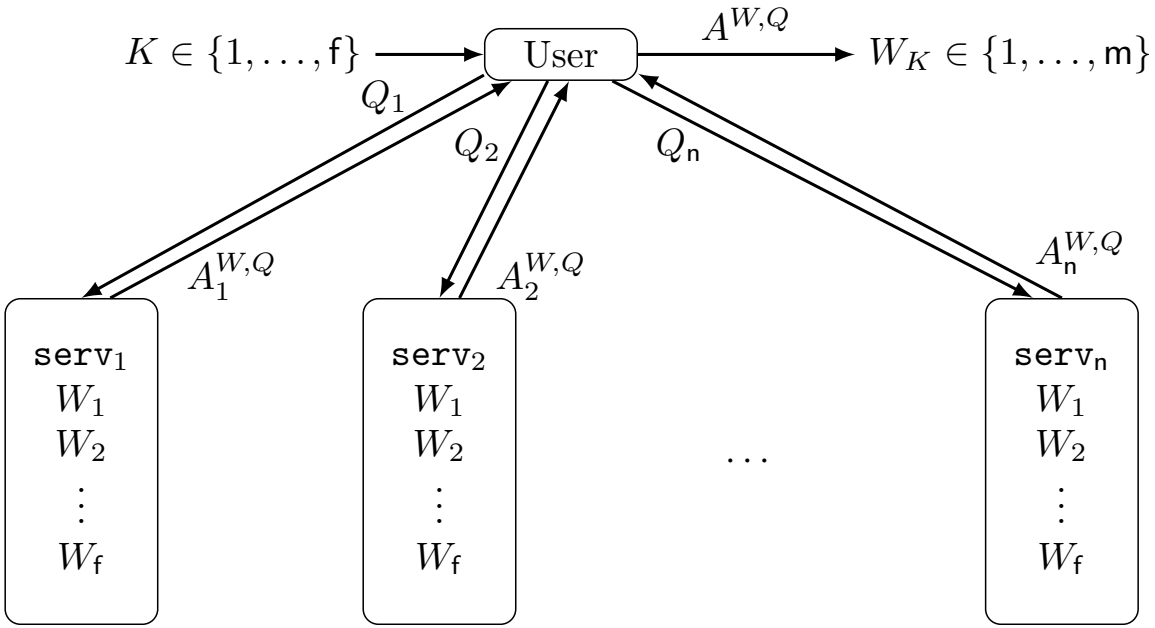
Information-Theoretic Approach [Sun-Jafar16], [Banawan-Ulukus17], ...

- (n, f): Numbers of servers and files. ← **Fixed**
- m: File size. ← **Arbitrary** $(W_1, \ldots, W_{\mathsf{f}} \in \{1, \ldots, \mathsf{m}\})$
- PIR Rate and Capacity (c.f. upload cost is negligible)

$$R = \frac{\text{(File size)}}{\text{(Download size)}}, \quad C_{\text{classical}} = \sup R$$

($\star$ The rate of "downloading all files" is $1/\mathsf{f}$.)

Classical PIR Capacity



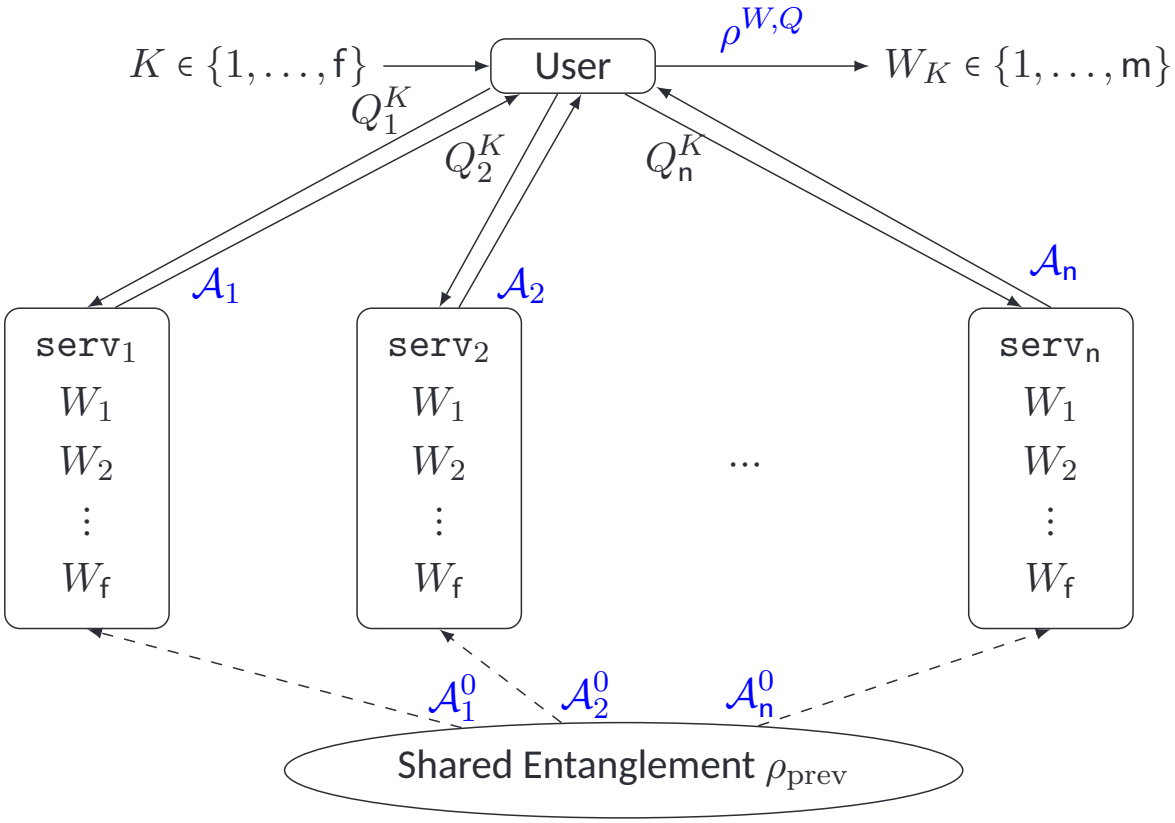
Information-Theoretic Approach [Sun-Jafar16], [Banawan-Ulukus17], ...

- (n, f): Numbers of servers and files. ← **Fixed**
- m: File size. ← **Arbitrary** $(W_1, \ldots, W_{\mathsf{f}} \in \{1, \ldots, \mathsf{m}\})$
- PIR Rate and Capacity (c.f. upload cost is negligible)

$$R = \frac{\text{(File size)}}{\text{(Download size)}}, \quad C_{\text{classical}} = \sup R = \frac{1 - 1/\mathsf{n}}{1 - (1/\mathsf{n})^{\mathsf{f}}} < 1.$$

($\star$ The rate of "downloading all files" is $1/\mathsf{f}$.)

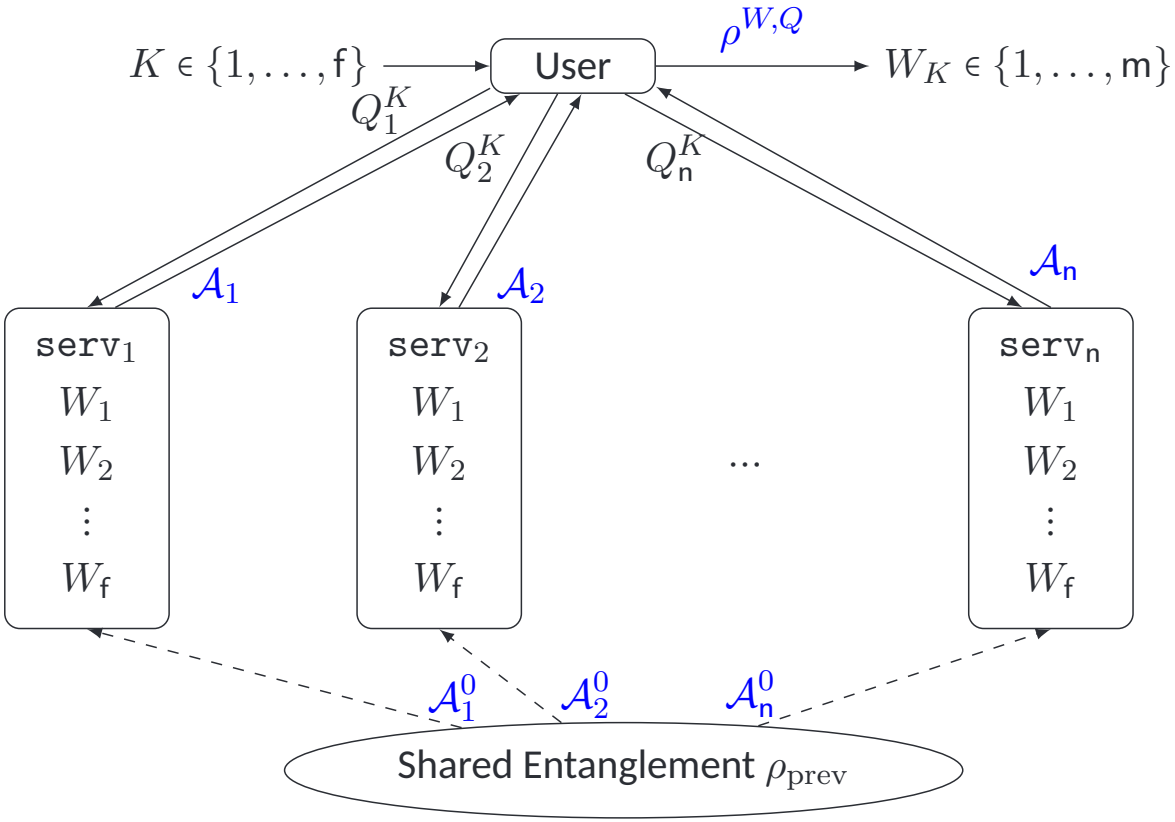
Quantum PIR Capacity



Our QPIR Model

- Classical files.
- Shared entangled state.
- Classical upload.
- Quantum download.
- Quantum measurement.

Quantum PIR Capacity



Our QPIR Model

- Classical files.
- Shared entangled state.
- Classical upload.
- Quantum download.
- Quantum measurement.

Information-Theoretic Approach

- (n, f): Numbers of servers and files. ← **Fixed**
- m: File size. ← **Arbitrary**
- QPIR Rate and Capacity

$$R = \frac{\text{(File size)}}{\text{(Download size)}} \text{ (bit/qubit)}, \qquad C_{\mathrm{quantum}} = \sup R = 1.$$

Main Theorem

Theorem: Capacity of QPIR

The capacity of the quantum private information retrieval with f files and n ≥ 2 servers sharing preexisting entanglement is

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

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

$$C_{\text{exact}}^{\alpha,\beta,\gamma,\theta} := \sup_{\substack{\{\mathsf{m}_\ell\}_{\ell=1}^{\infty}, \\ \{\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}}} \left\{ \limsup_{\ell\to\infty} R \;\middle|\; \underbrace{P_{\text{err}}^{(\mathsf{m}_\ell)}}_{\text{Error Probab.}} \leq \alpha, \; \underbrace{\max_t I(K;\mathfrak{serv}_t)}_{\text{User Secrecy}} \leq \gamma, \right.$$

$$\left. \underbrace{I(W_{K^c};\mathfrak{user}|K)}_{\text{Server Secrecy}} \leq \beta, \; \limsup_{\ell\to\infty} \underbrace{\frac{\log U}{\log D}}_{\text{Upload Cost}} \leq \theta \right\}.$$

$$C_{\text{asymp}}^{\alpha,\beta,\gamma,\theta} := \sup_{\substack{\{\mathsf{m}_\ell\}_{\ell=1}^{\infty}, \\ \{\Psi_{\text{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^{\infty}}} \left\{ \liminf_{\ell\to\infty} R \;\middle|\; \limsup_{\ell\to\infty} P_{\text{err}} \leq \alpha, \; \limsup_{\ell\to\infty} I(W_{K^c};\mathfrak{user}|K) \leq \beta, \right.$$

$$\left. \limsup_{\ell\to\infty} \max_t I(K;\mathfrak{serv}_t) \leq \gamma \;, \; \limsup_{\ell\to\infty} \frac{\log U}{\log D} \leq \theta \right\},$$

Main Theorem

Theorem: Capacity of QPIR

The capacity of the quantum private information retrieval with f files and n ≥ 2 servers sharing preexisting entanglement is

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

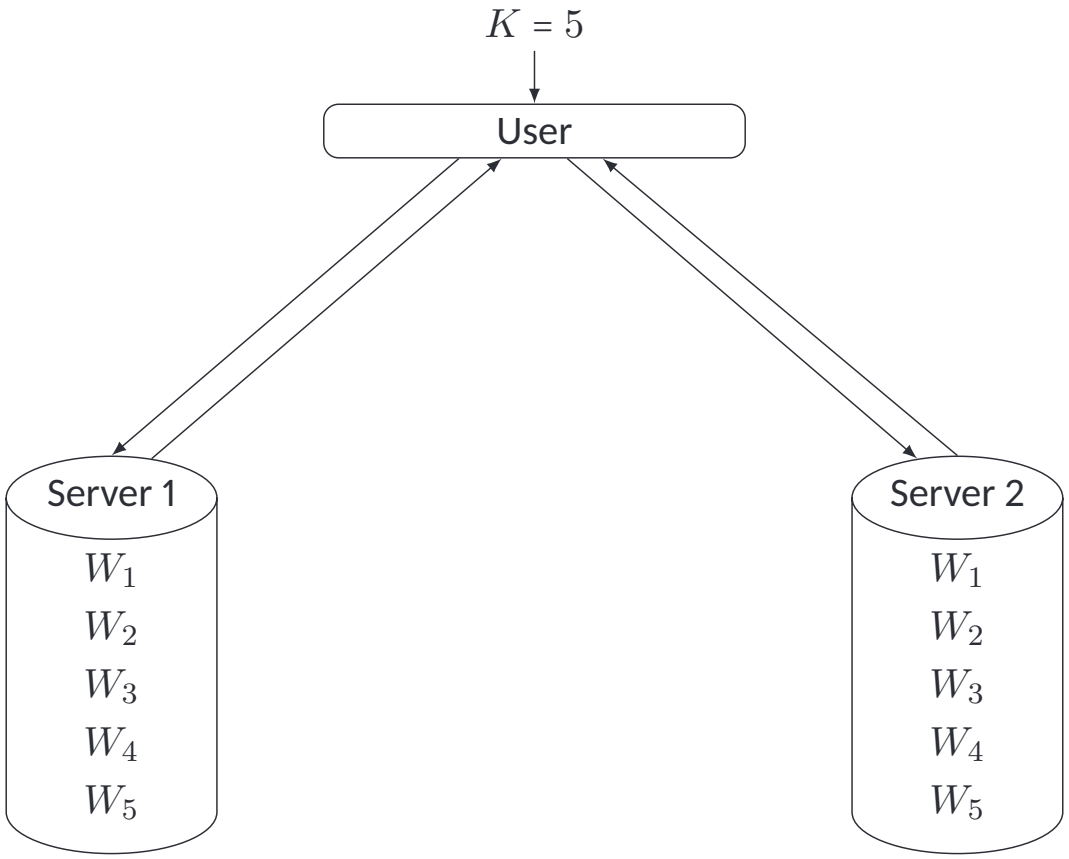
$$\forall \alpha \in [0,1) \text{ and } \forall \beta, \gamma, \theta \in [0,\infty].$$

(Proof) For any $\alpha \in [0,1)$,

$$\underbrace{1 \leq C_{\text{exact}}^{0,0,0,0}}_{\text{Rate-one protocol}} \leq C_{\text{exact}}^{\alpha,\beta,\gamma,\theta} \leq C_{\text{asymp}}^{\alpha,\beta,\gamma,\theta} \leq \underbrace{C_{\text{asymp}}^{\alpha,\infty,\infty,\infty} \leq 1}_{\text{Strong Converse}}$$

(α: Error Probab. β: User Secrecy γ: Server Secrecy θ: Upload Cost)

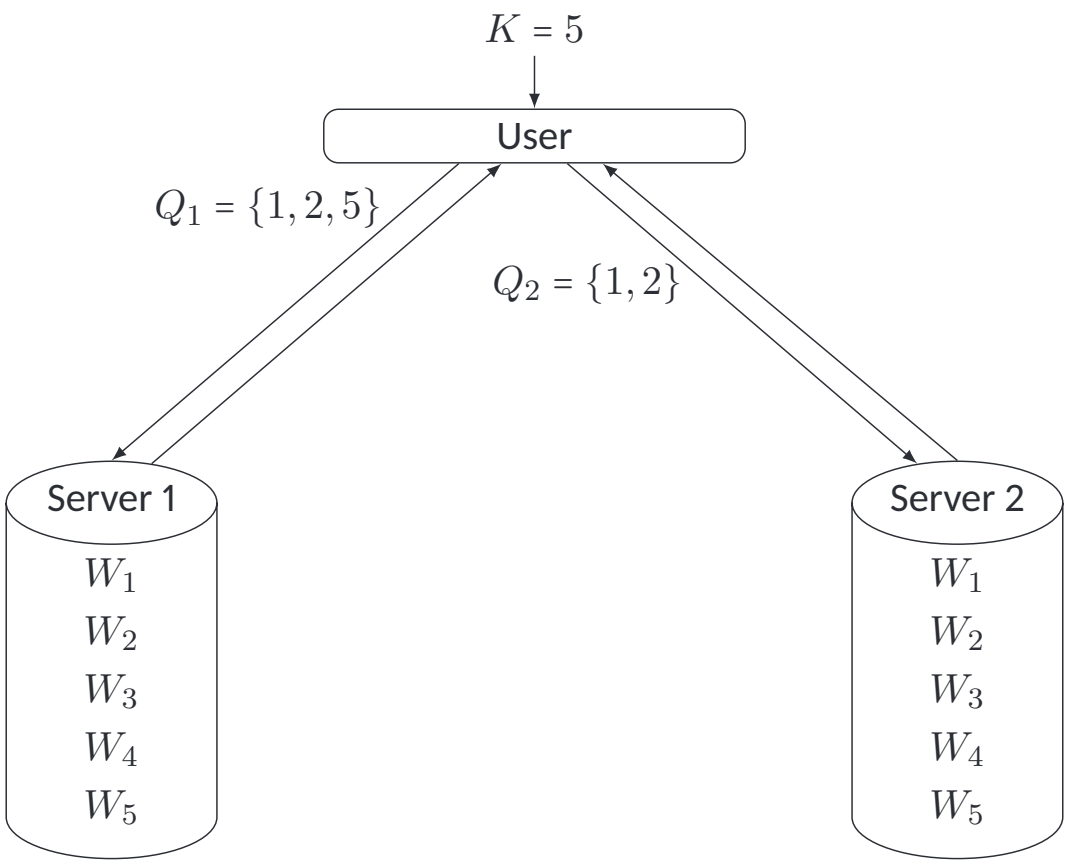
Classical Two-Server PIR Protocol [Chor et al.95]



Classical PIR Protocol

1. Q_1: a random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
2. Servers return $A_1 = \sum_{i \in Q_1} W_i,\ A_2 = \sum_{i \in Q_2} W_i$.
3. User recovers $W_K = \pm(A_1 - A_2)$.

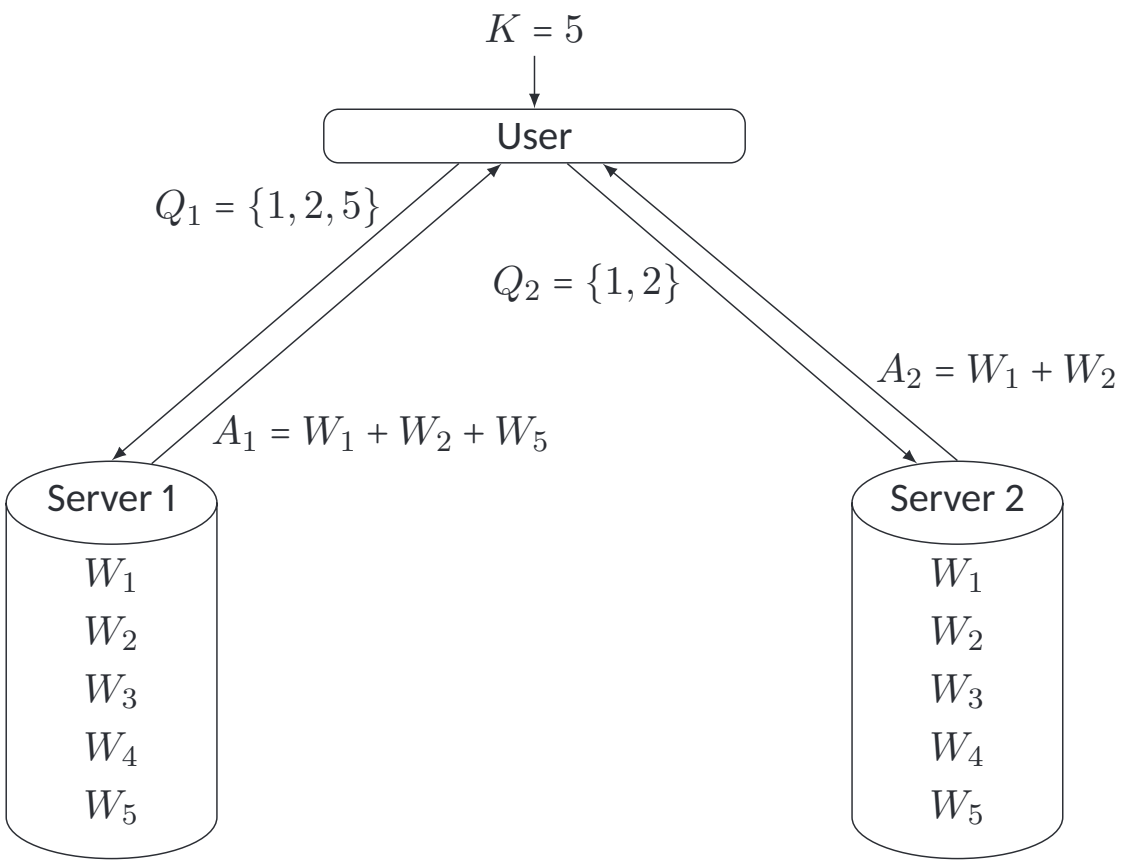
Classical Two-Server PIR Protocol [Chor et al.95]



Classical PIR Protocol

1. Q_1: a random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
2. Servers return $A_1 = \sum_{i \in Q_1} W_i,\ A_2 = \sum_{i \in Q_2} W_i$.
3. User recovers $W_K = \pm(A_1 - A_2)$.

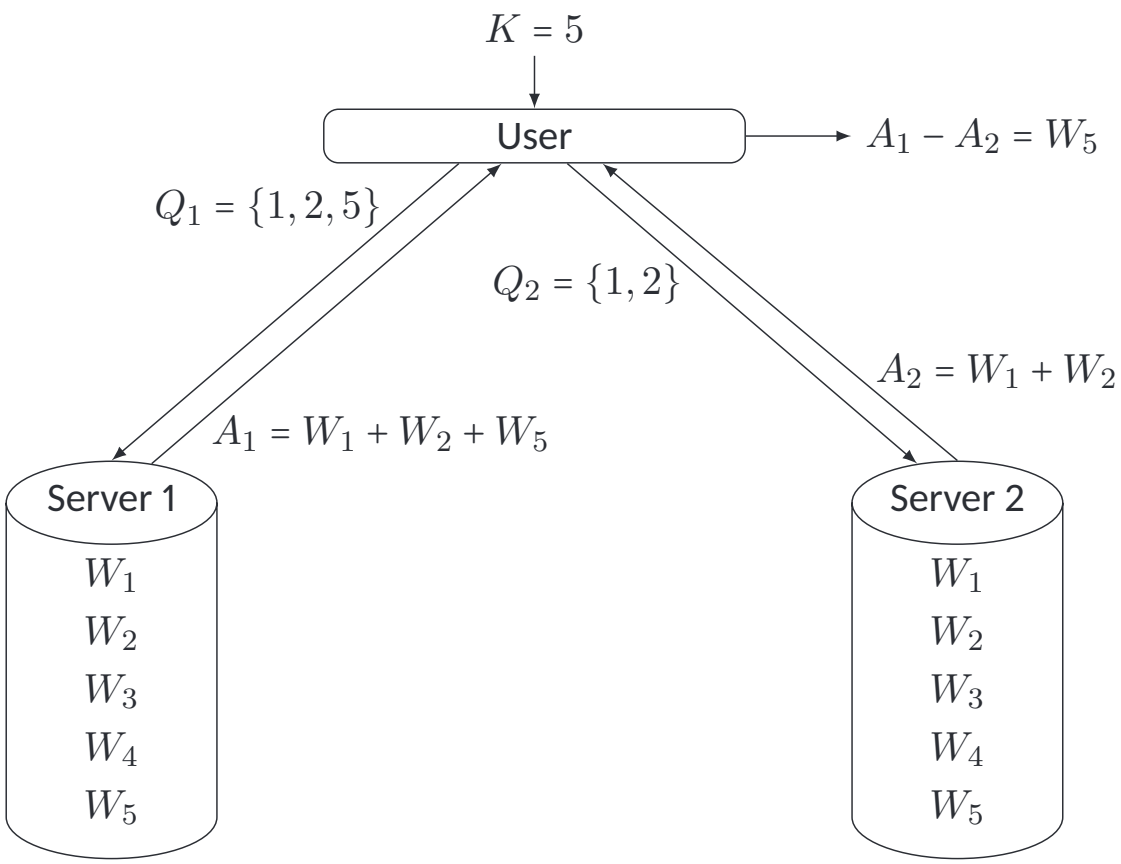
Classical Two-Server PIR Protocol [Chor et al.95]



Classical PIR Protocol

1. Q_1: a random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
2. Servers return $A_1 = \sum_{i \in Q_1} W_i,\ A_2 = \sum_{i \in Q_2} W_i$.
3. User recovers $W_K = \pm(A_1 - A_2)$.

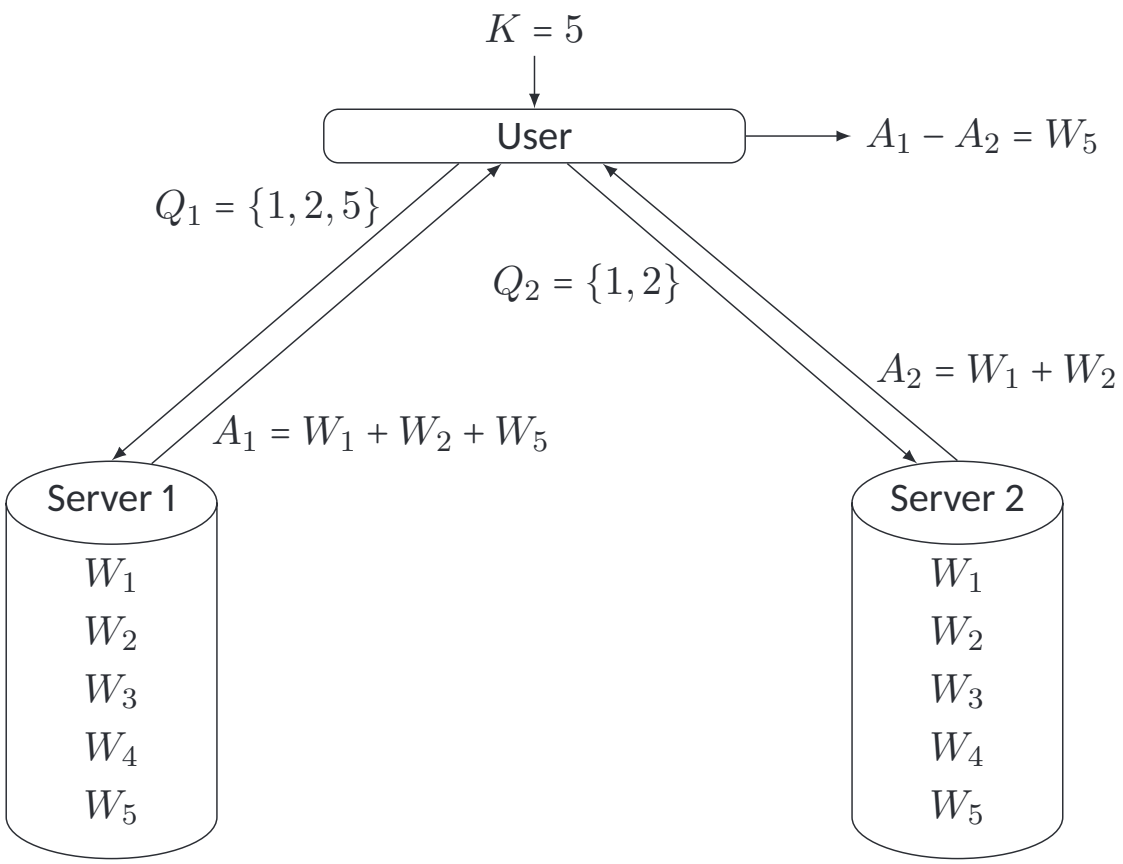
Classical Two-Server PIR Protocol [Chor et al.95]



Classical PIR Protocol

1. Q_1: a random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
2. Servers return $A_1 = \sum_{i \in Q_1} W_i,\ A_2 = \sum_{i \in Q_2} W_i$.
3. User recovers $W_K = \pm(A_1 - A_2)$.

Classical Two-Server PIR Protocol [Chor et al.95]

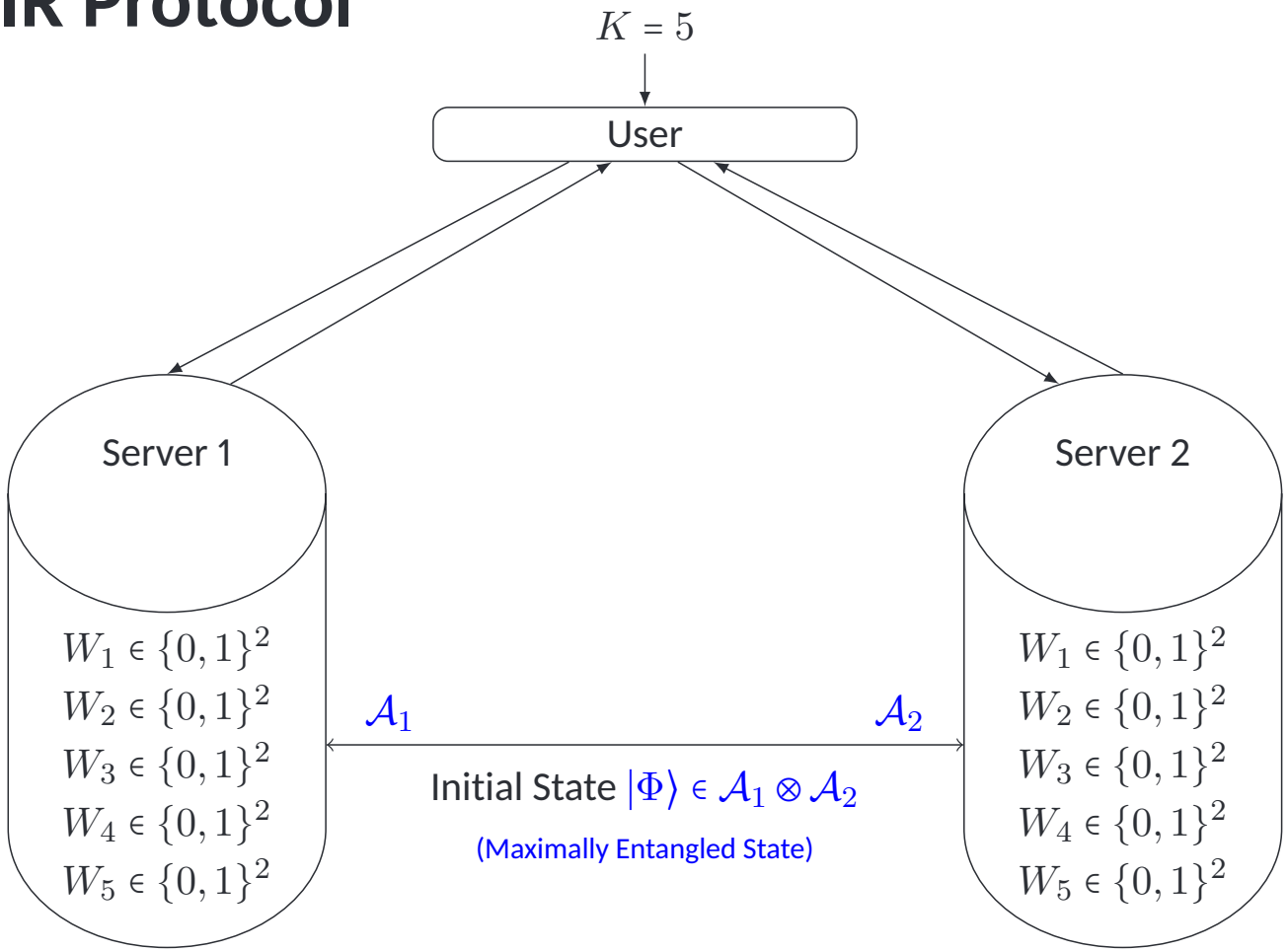


Classical PIR Protocol

1. Q_1: a random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
2. Servers return $A_1 = \sum_{i \in Q_1} W_i,\ A_2 = \sum_{i \in Q_2} W_i$.
3. User recovers $W_K = \pm(A_1 - A_2)$.

$$\begin{cases} I(Q_1, K) = I(Q_2, K) = 0. \\ \text{No Server Secrecy.} \end{cases}$$

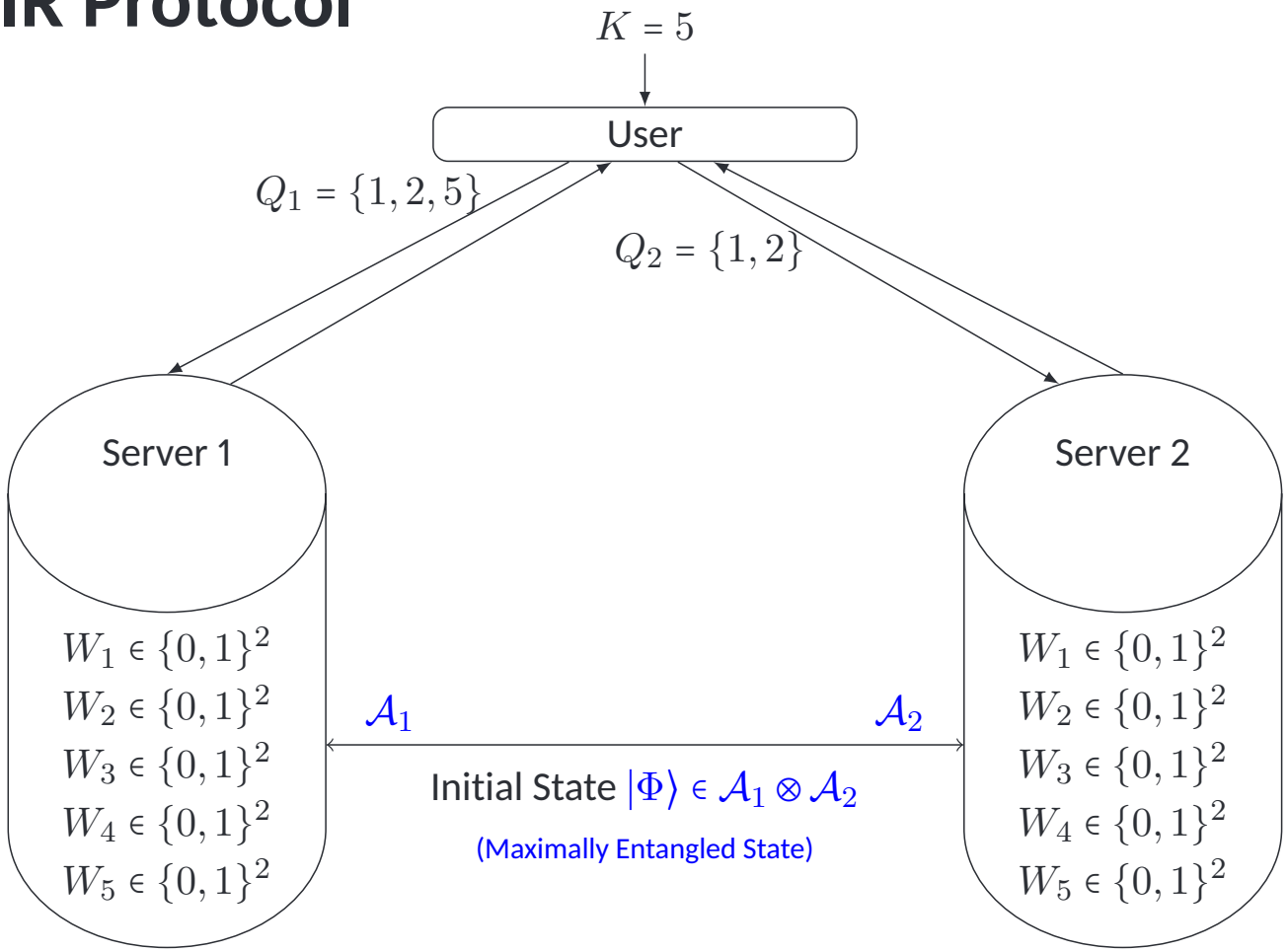
QPIR Protocol



QPIR Protocol (Files $W_1, \ldots, W_\mathsf{f} \in \mathbb{Z}_\ell^2 := \{0, \ldots, \ell - 1\}^2$)

1. Servers share maximally entangled state $|\Phi\rangle := (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
2. Q_1: A random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
3. Server 1 applies $\mathsf{W}(\sum_{i \in Q_1} W_i)$ on $\mathcal{A}_1$ $\qquad$ $(\mathsf{W}(a,b) := \mathsf{X}^a \mathsf{Z}^b)$,
   Server 2 applies $\overline{\mathsf{W}(\sum_{i \in Q_2} W_i)}$ on $\mathcal{A}_2$.
4. User performs PVM $\mathbf{M}_{\mathbb{Z}_\ell^2} := \{(\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle \mid a, b \in \mathbb{Z}_\ell\}$.

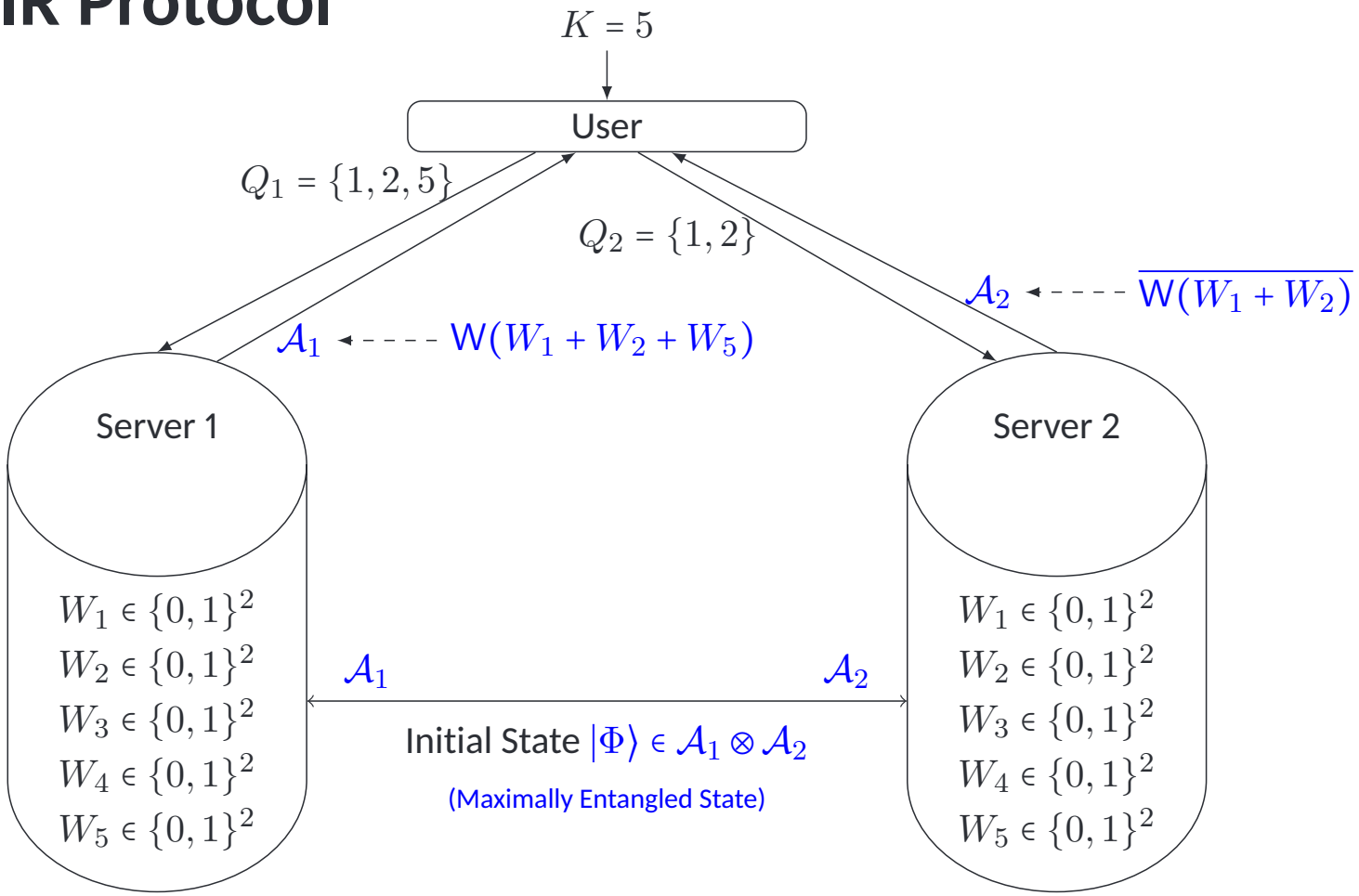
QPIR Protocol



QPIR Protocol (Files $W_1, \ldots, W_\mathsf{f} \in \mathbb{Z}_\ell^2 := \{0, \ldots, \ell - 1\}^2$)

1. Servers share maximally entangled state $|\Phi\rangle := (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
2. Q_1: A random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
3. Server 1 applies $\mathsf{W}(\sum_{i \in Q_1} W_i)$ on $\mathcal{A}_1$ $\qquad$ $(\mathsf{W}(a, b) := \mathsf{X}^a \mathsf{Z}^b)$,
   Server 2 applies $\overline{\mathsf{W}(\sum_{i \in Q_2} W_i)}$ on $\mathcal{A}_2$.
4. User performs PVM $\mathbf{M}_{\mathbb{Z}_\ell^2} := \{(\mathsf{W}(a, b) \otimes \mathsf{I})|\Phi\rangle \mid a, b \in \mathbb{Z}_\ell\}$.

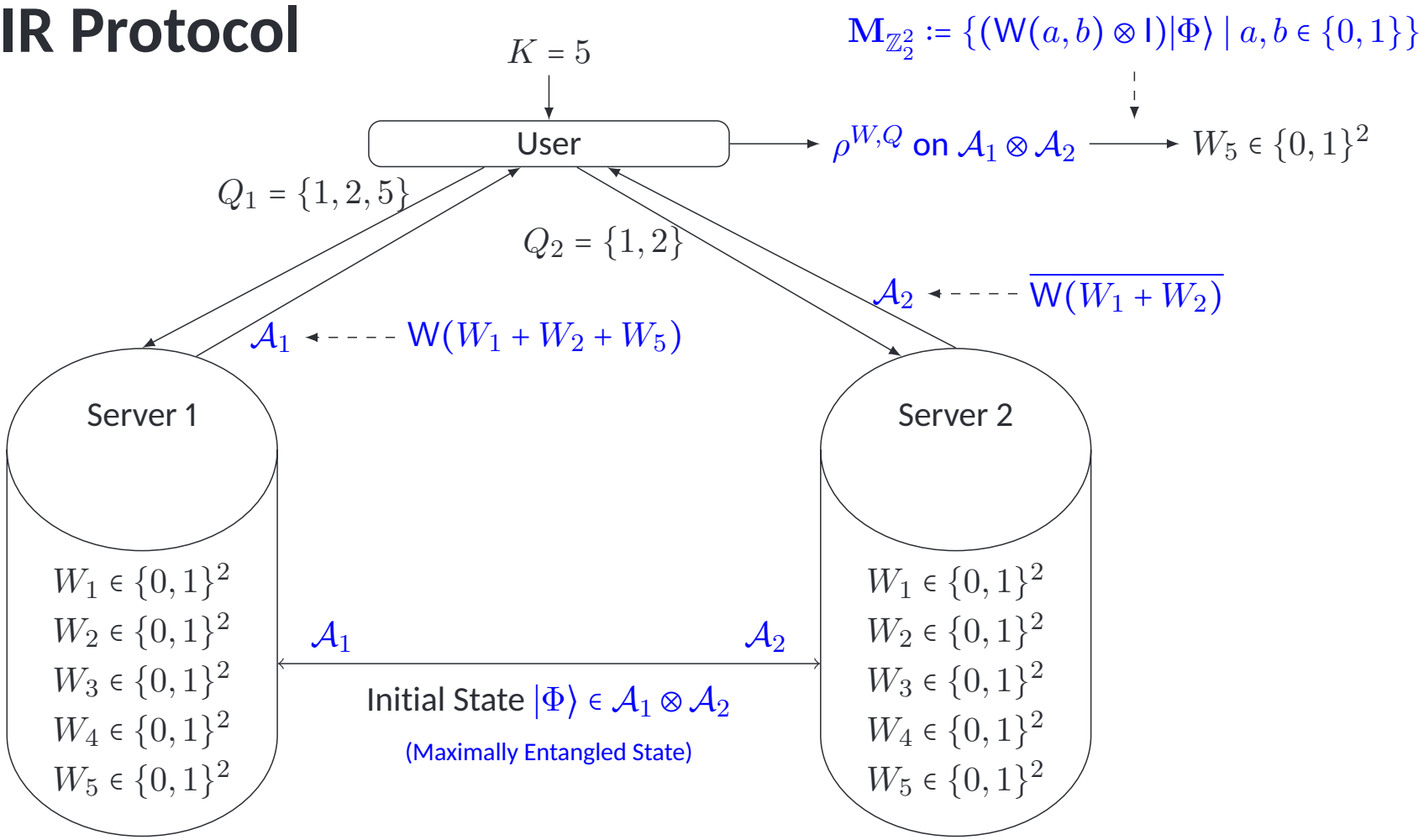
QPIR Protocol



QPIR Protocol (Files $W_1, \ldots, W_\mathsf{f} \in \mathbb{Z}_\ell^2 := \{0, \ldots, \ell - 1\}^2$)

1. Servers share maximally entangled state $|\Phi\rangle := (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
2. Q_1: A random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
3. Server 1 applies $\mathsf{W}(\sum_{i \in Q_1} W_i)$ on $\mathcal{A}_1$ $\qquad$ $(\mathsf{W}(a, b) := \mathsf{X}^a \mathsf{Z}^b)$,
   Server 2 applies $\overline{\mathsf{W}(\sum_{i \in Q_2} W_i)}$ on $\mathcal{A}_2$.
4. User performs PVM $\mathbf{M}_{\mathbb{Z}_\ell^2} := \{(\mathsf{W}(a, b) \otimes \mathsf{I})|\Phi\rangle \mid a, b \in \mathbb{Z}_\ell\}$.

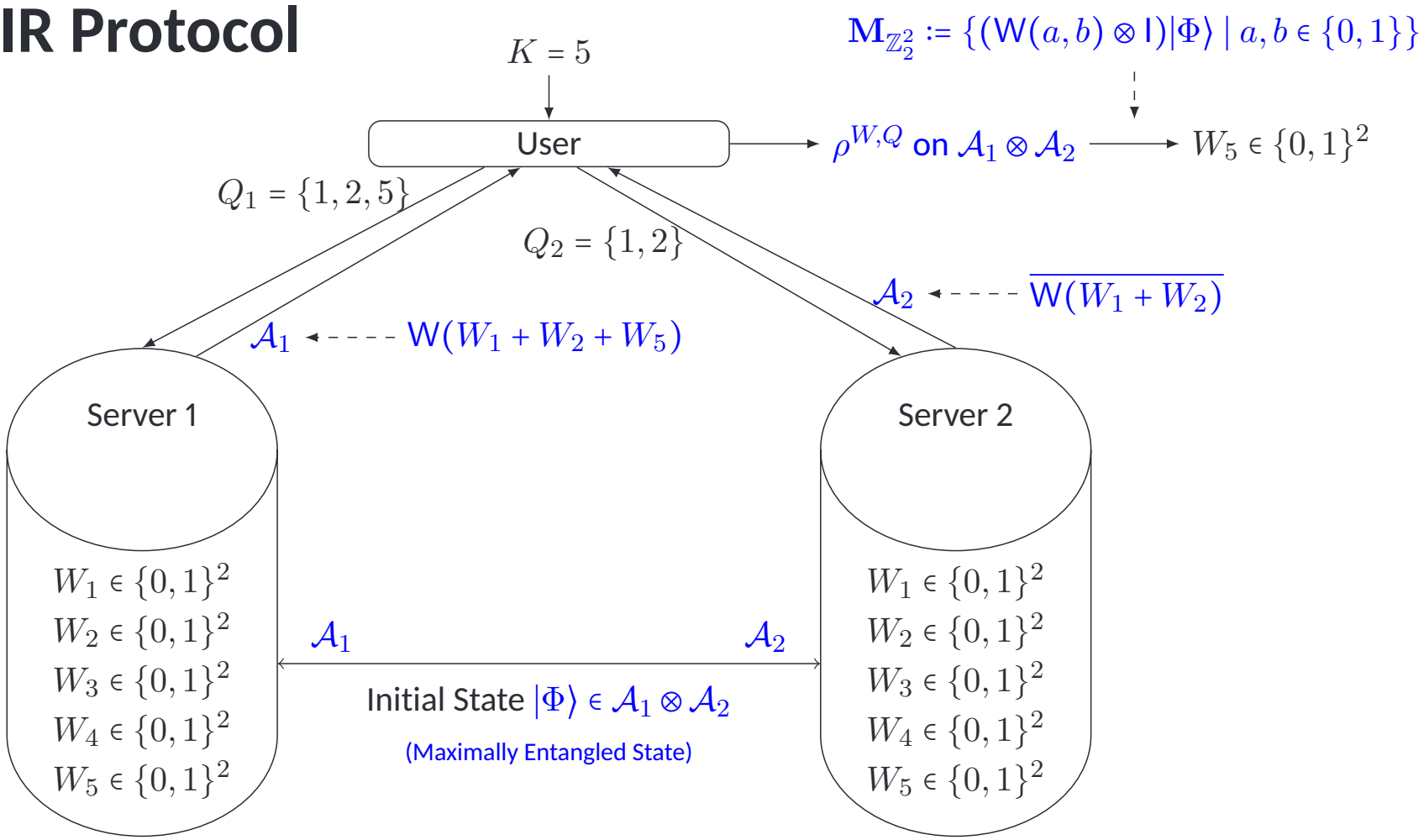
QPIR Protocol



QPIR Protocol (Files $W_1, \ldots, W_\mathsf{f} \in \mathbb{Z}_\ell^2 := \{0, \ldots, \ell - 1\}^2$)

1. Servers share maximally entangled state $|\Phi\rangle := (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
2. Q_1: A random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
3. Server 1 applies $\mathsf{W}(\sum_{i \in Q_1} W_i)$ on $\mathcal{A}_1$ $\qquad$ $(\mathsf{W}(a,b) := \mathsf{X}^a \mathsf{Z}^b)$,
   Server 2 applies $\overline{\mathsf{W}(\sum_{i \in Q_2} W_i)}$ on $\mathcal{A}_2$.
4. User performs PVM $\mathbf{M}_{\mathbb{Z}_\ell^2} := \{(\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle \mid a,b \in \mathbb{Z}_\ell\}$.

QPIR Protocol

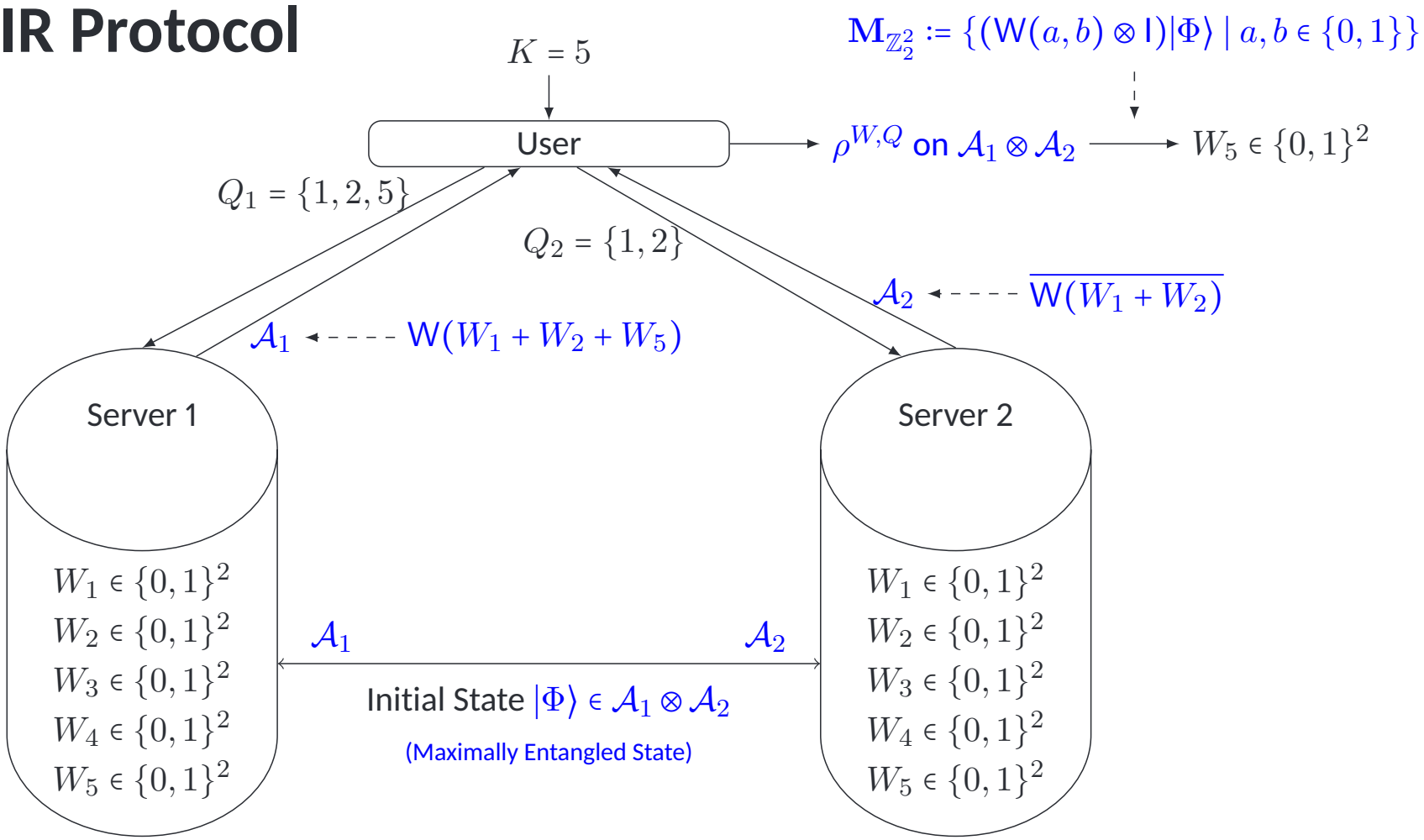


Error Probability is 0 because

$$|\Phi\rangle \mapsto \left(\mathsf{W}\left(\sum_{i\in Q_1} W_i\right) \otimes \overline{\mathsf{W}\left(\sum_{i\in Q_2} W_i\right)}\right)|\Phi\rangle = \left(\mathsf{W}\left(\sum_{i\in Q_1} W_i - \sum_{i\in Q_2} W_i\right) \otimes \mathsf{I}\right)|\Phi\rangle = (\mathsf{W}(\pm W_K) \otimes \mathsf{I})|\Phi\rangle$$

and PVM is $\mathbf{M}_{\mathbb{Z}_\ell^2} := \{(\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle \mid a,b \in \mathbb{Z}_\ell\}$.

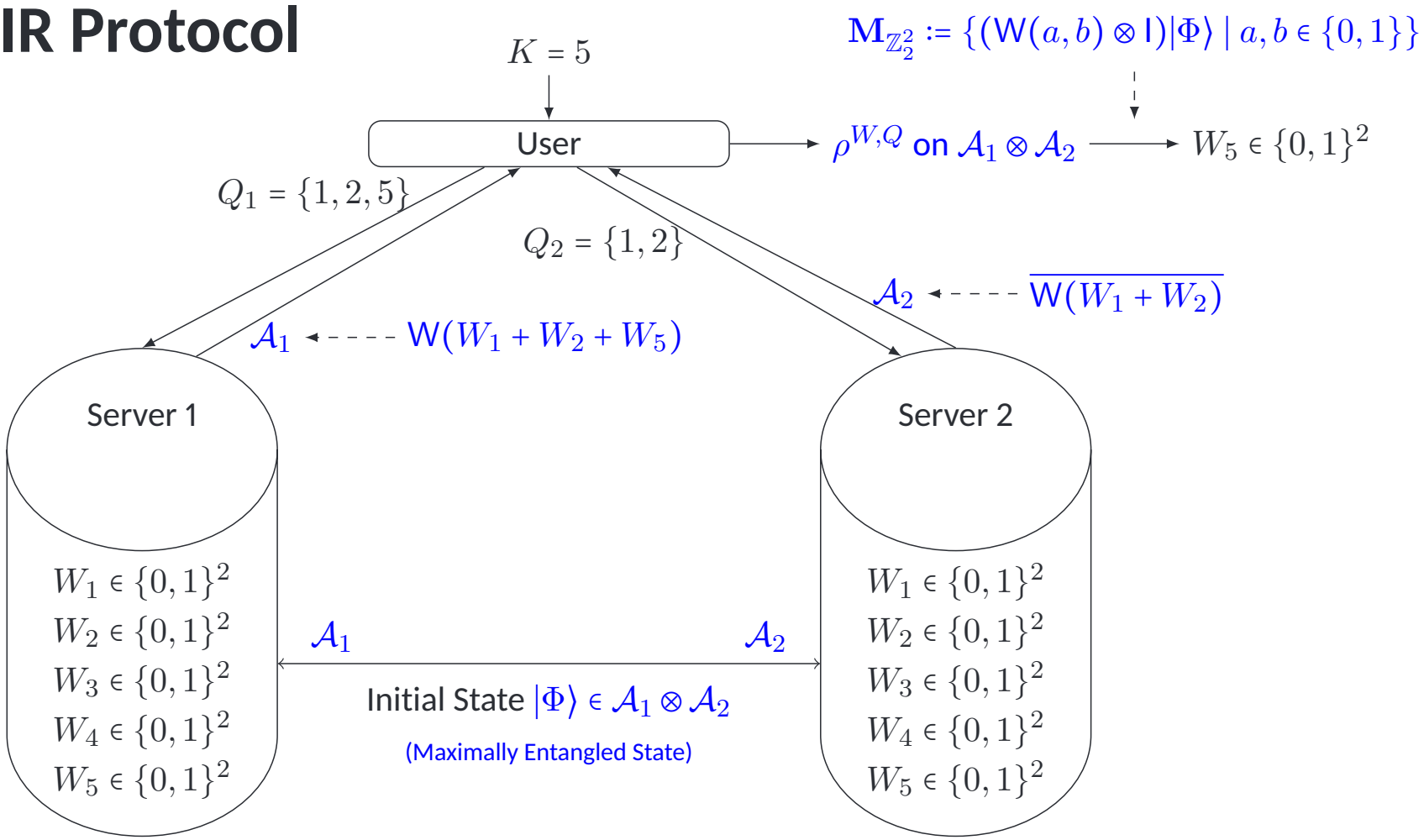
QPIR Protocol



Server Secrecy: The state $(\mathsf{W}(\pm W_K) \otimes \mathsf{I})|\Phi\rangle$ is independent of $\{W_1, \ldots, W_\mathsf{f}\} - \{W_K\}$.

User Secrecy: each of Q_1 and Q_2 is independent of K.

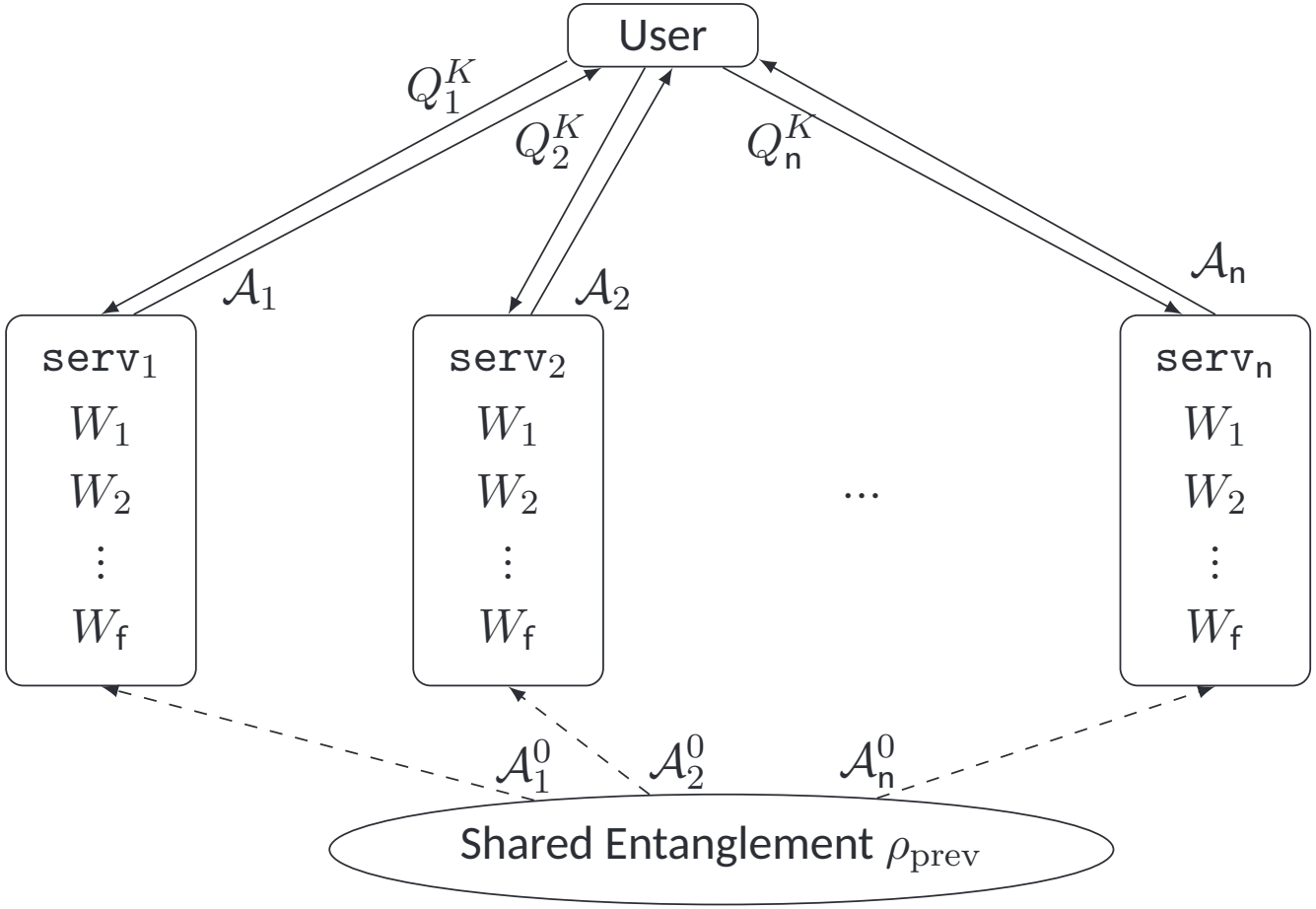
QPIR Protocol



Costs

- Download cost: $\log \dim \mathcal{A}_1 + \log \dim \mathcal{A}_2 = 2 \log \ell$.
- File size: $\log |\mathbb{Z}_\ell^2| = 2 \log \ell$.
- Rate $R = \frac{\text{(File size)}}{\text{(Download size)}} = 1$.

Strong Converse

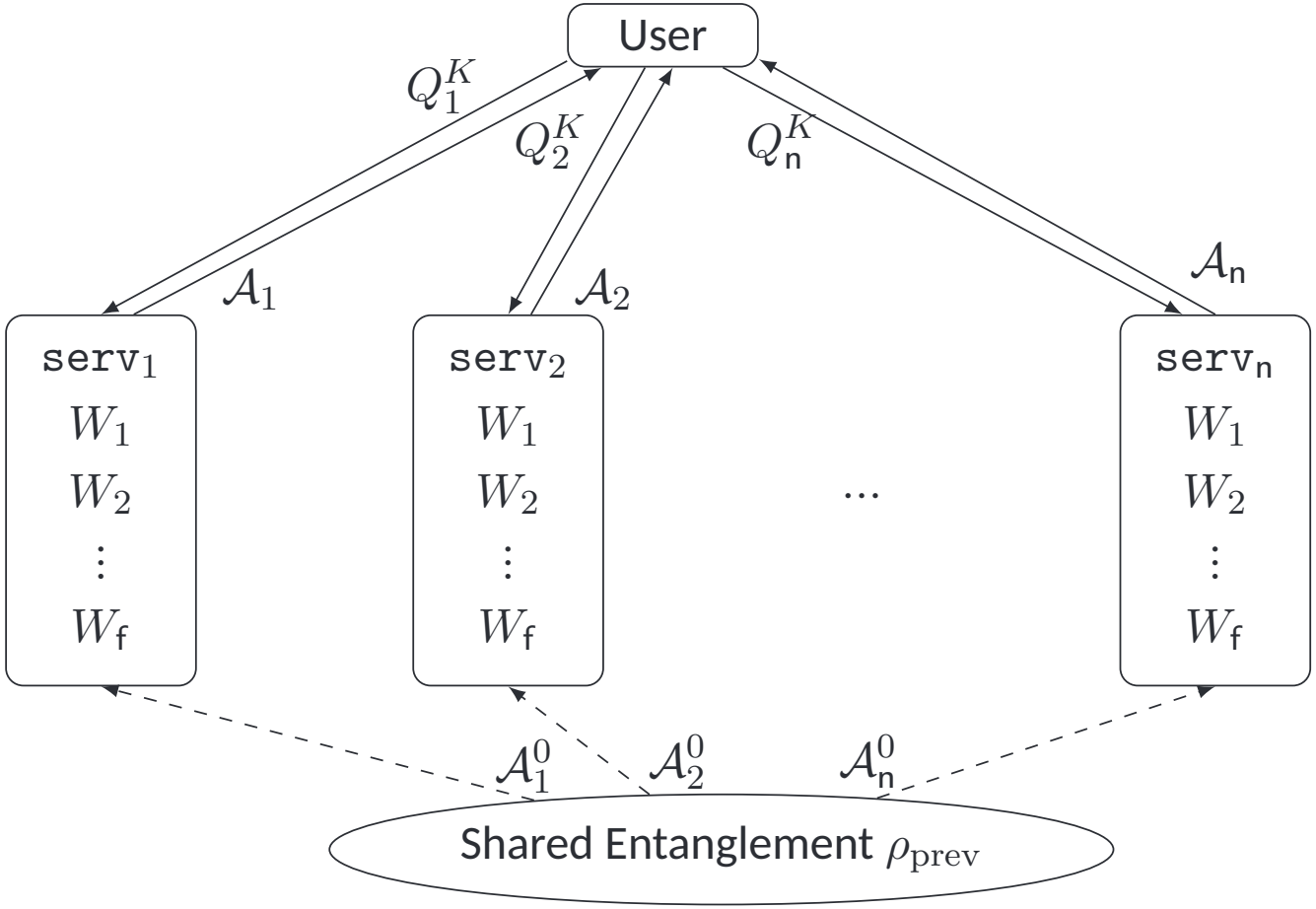


- Quantum upload is not allowed.

  $\Longrightarrow$ No shared entanglement between the user and all servers.

  $\Longrightarrow$ If n qubits are downloaded, at most n bits are transmitted.

Strong Converse

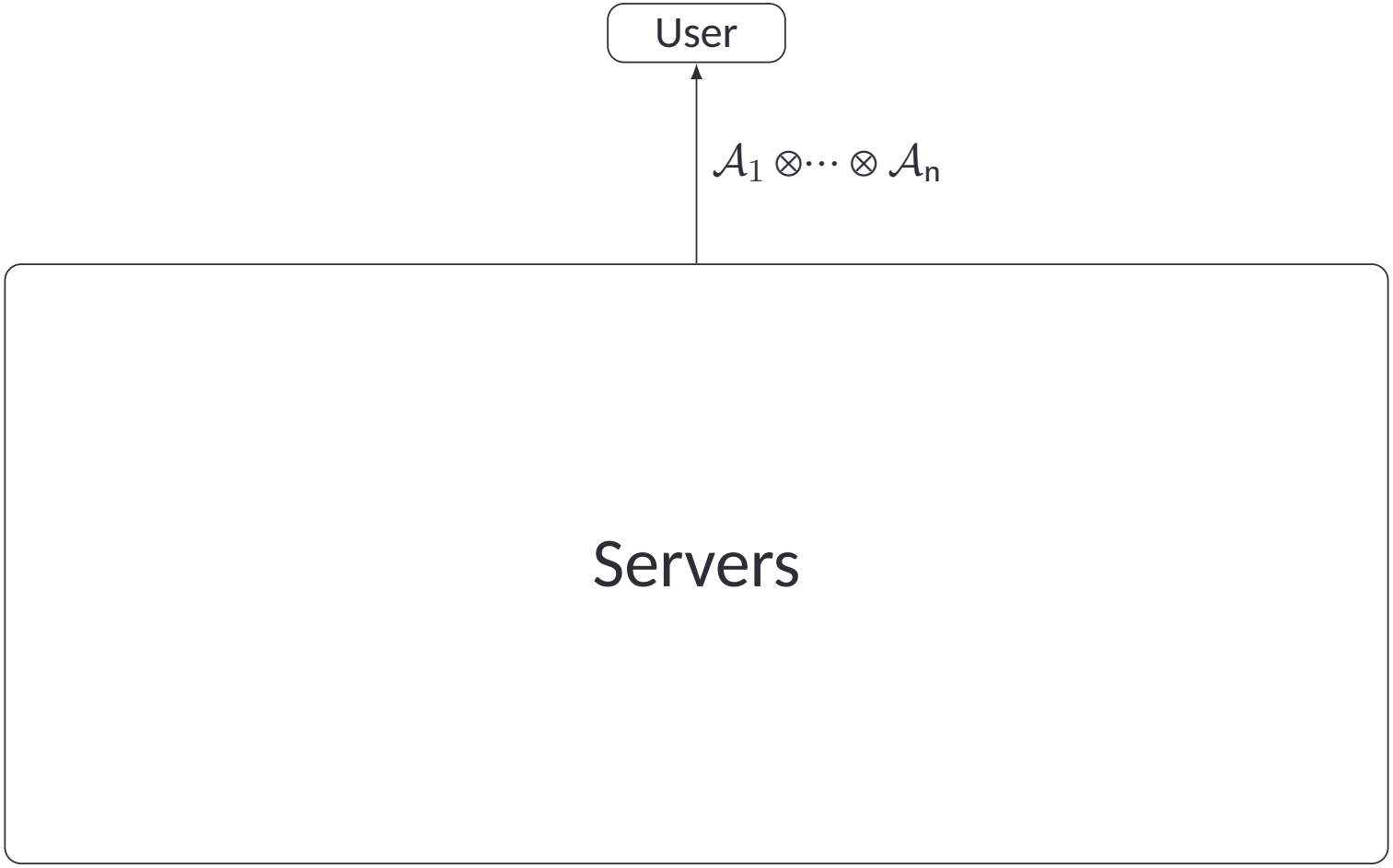


- Quantum upload is not allowed.

  $\Longrightarrow$ No shared entanglement between the user and all servers.

  $\Longrightarrow$ If n qubits are downloaded, at most n bits are transmitted.

Strong Converse



- Quantum upload is not allowed.

  $\Longrightarrow$ No shared entanglement between the user and all servers.

  $\Longrightarrow$ If n qubits are downloaded, at most n bits are transmitted.

Classical PIR vs. Quantum PIR Capacities (Multi-Server)

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\dfrac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 §
PIR with server secrecy	$1-n^{-1}$ [Sun-Jafar16-2] †	1 §
Multi-round PIR	$\dfrac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1 ¶
PIR with collusion of $n-1$ servers	$\dfrac{1/n}{1-(1-1/n)^{f}}$ [Sun-Jafar18-2]	$\dfrac{2}{n}$ (ITW2019, arXiv:1903.12556) ‖

$*$ n: num. of servers, f: num. of files.

† Shared randomness among servers is necessary.

‡ Files are coded by (n, k) MDS code.

§ With strong converse.

‖ When n is even.

¶ To show the converse, we employ result by [Ding et al. 2019]

Conclusion

- The QPIR capacity is 1 regardless of the security level.
- The QPIR capacity is greater than the classical PIR capacity.

$$C_{\text{quantum}} = 1 > C_{\text{classical}} = \frac{1 - 1/\mathsf{n}}{1 - (1/\mathsf{n})^{\mathsf{f}}}.$$

- The optimal QPIR protocol is constructed only with two-server.
- Our QPIR protocol achieves server secrecy.

Open Question

Server Secrecy on Multi-server PIR

- Classical PIR without shared randomness: No [Gertner et al.00].
- Quantum PIR (q. download and without shared entanglement): ?
- Quantum PIR (q. download and shared entanglement): Yes (Our Result).
- Quantum PIR (two-way): Yes [Kerenidis-Wolf04].