Information-Theoretic Aspects of Quantum Private Information Retrieval

Seunghoan Song

Graduate School of Mathematics,

Nagoya University

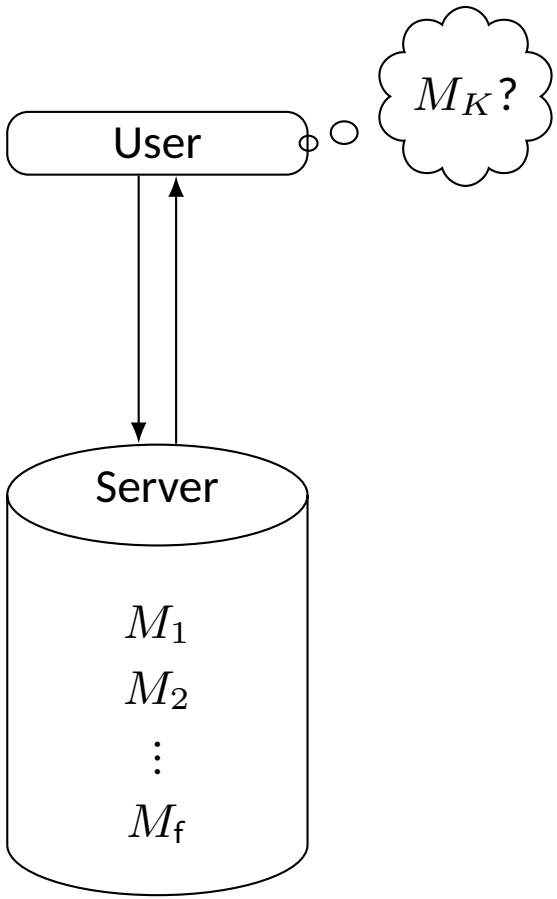
December 4, 2020

Contents

Contents

Private Information Retrieval (PIR)

What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].

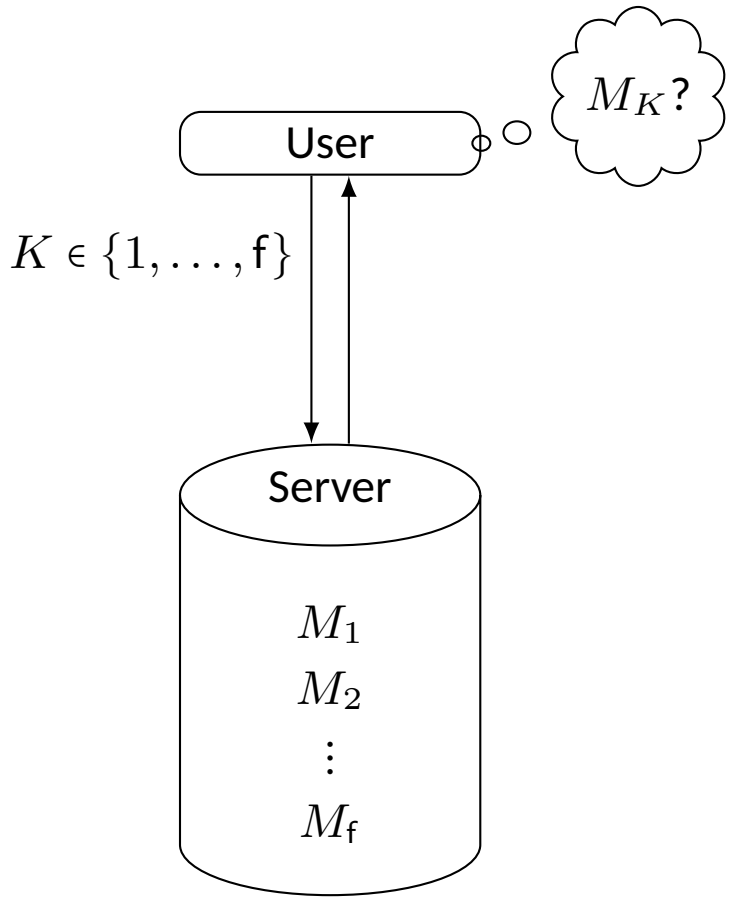


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].

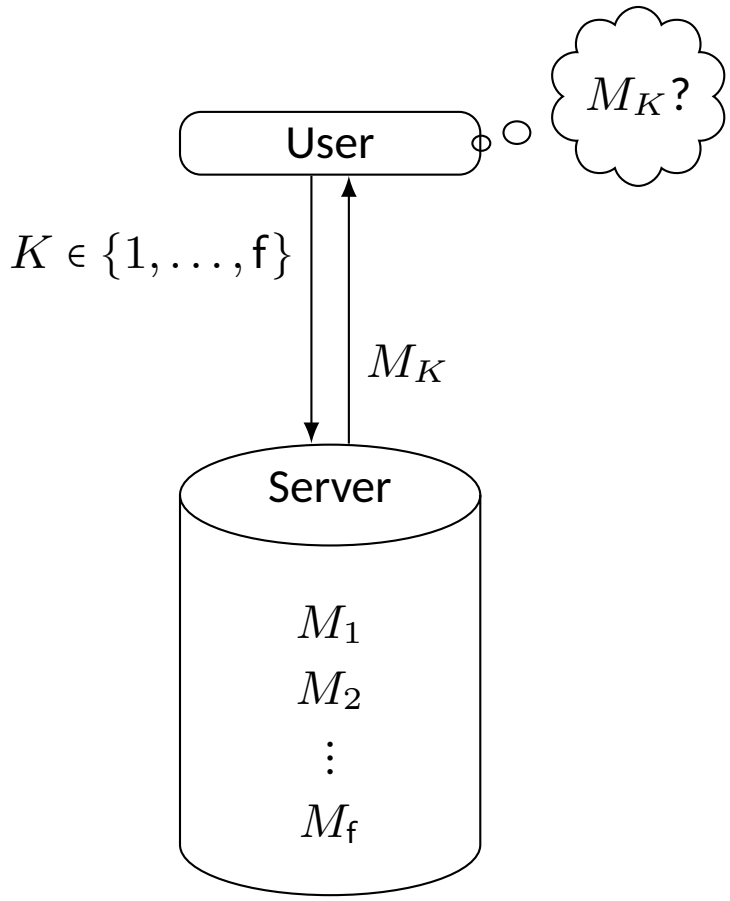


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].

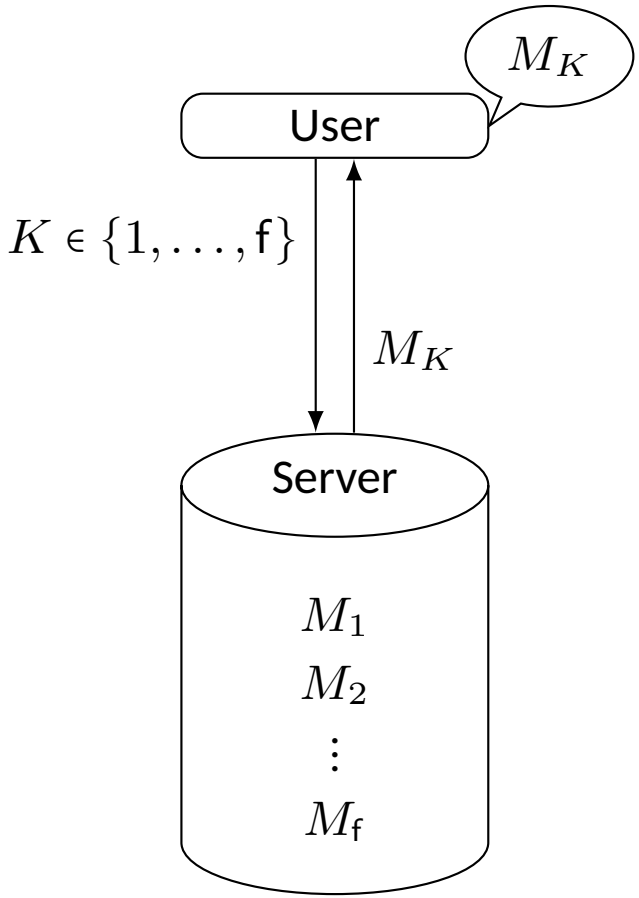


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].

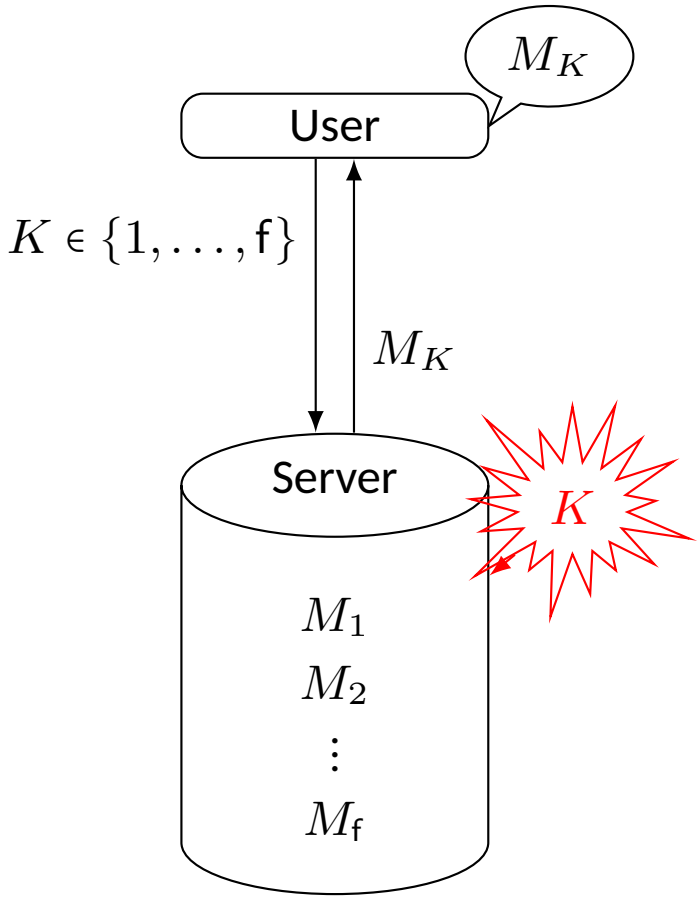


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].

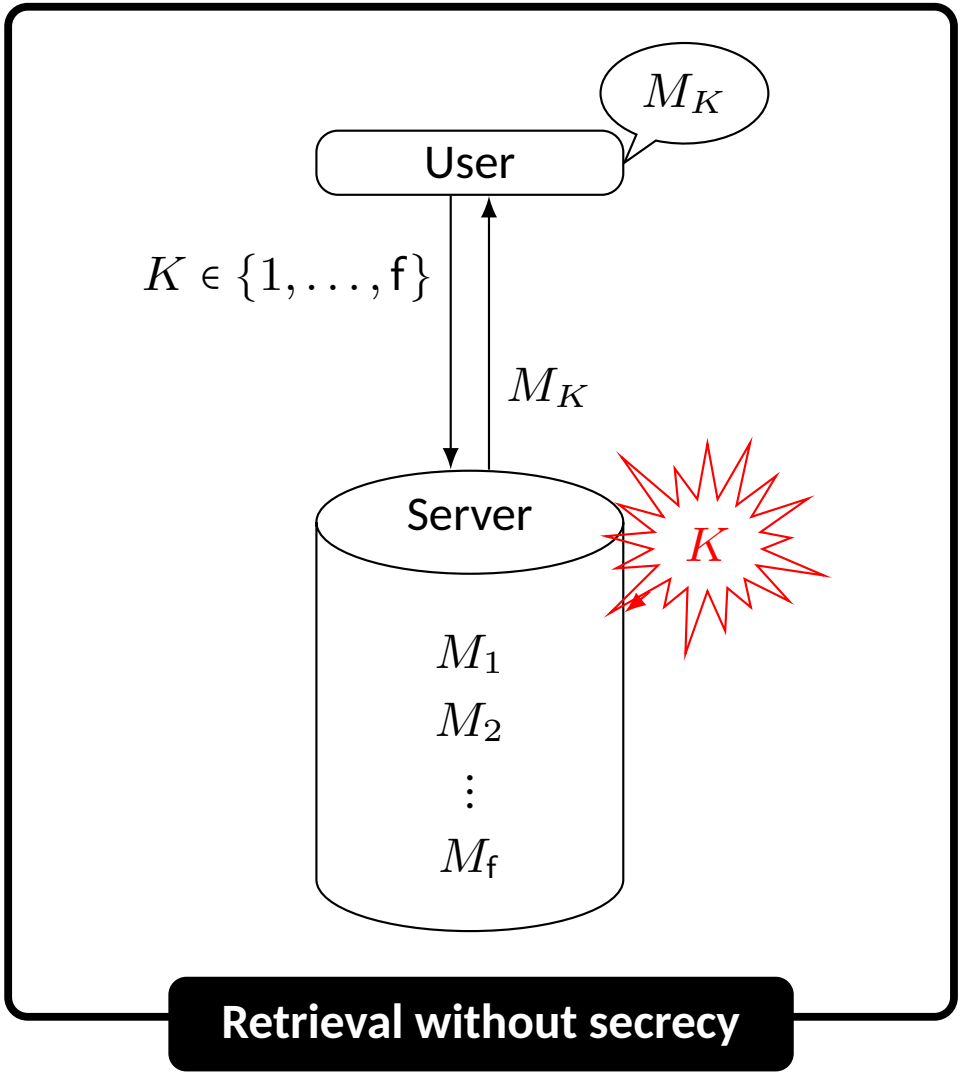


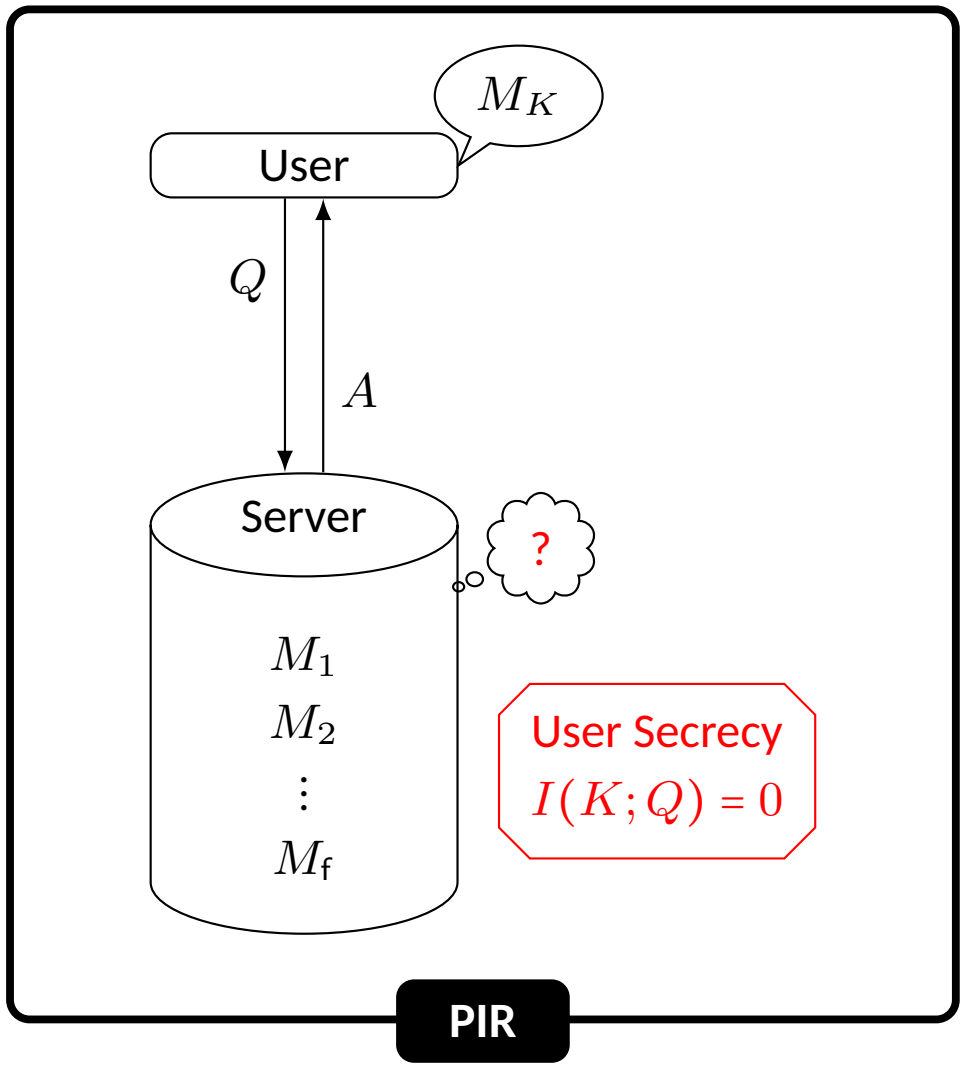
Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

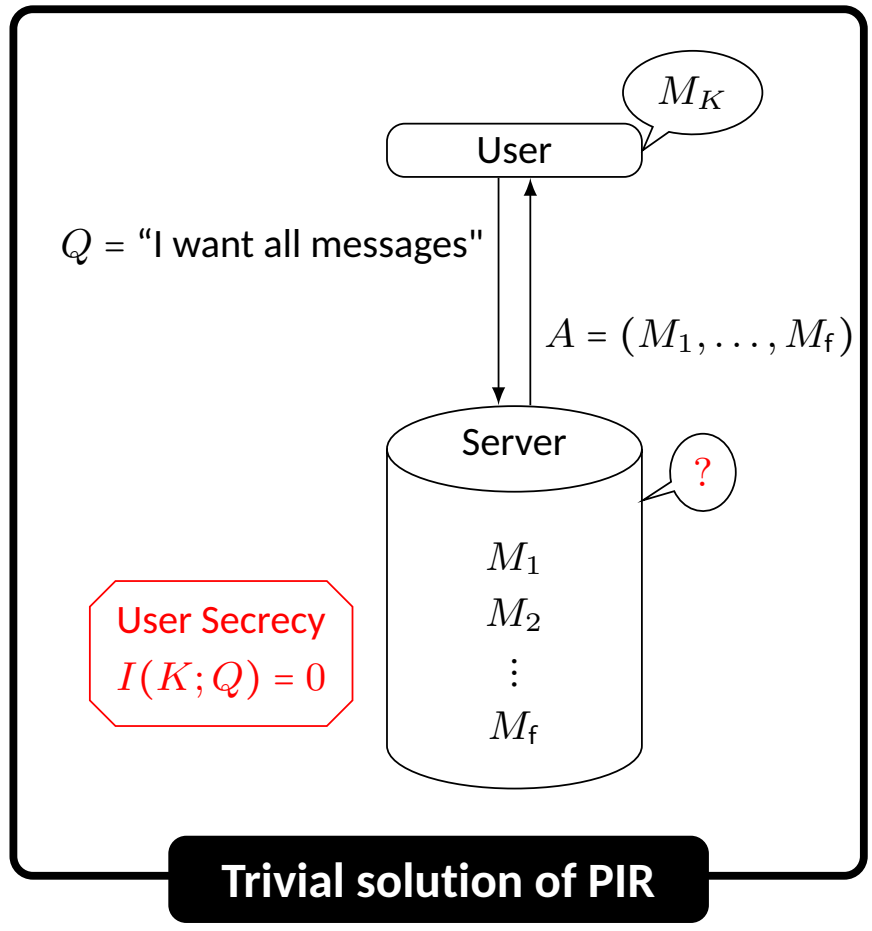
What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].





Solutions for PIR

- Downloading all messages is the trivial solution.
- *Trivial solution* is optimal [Chor et al.95].

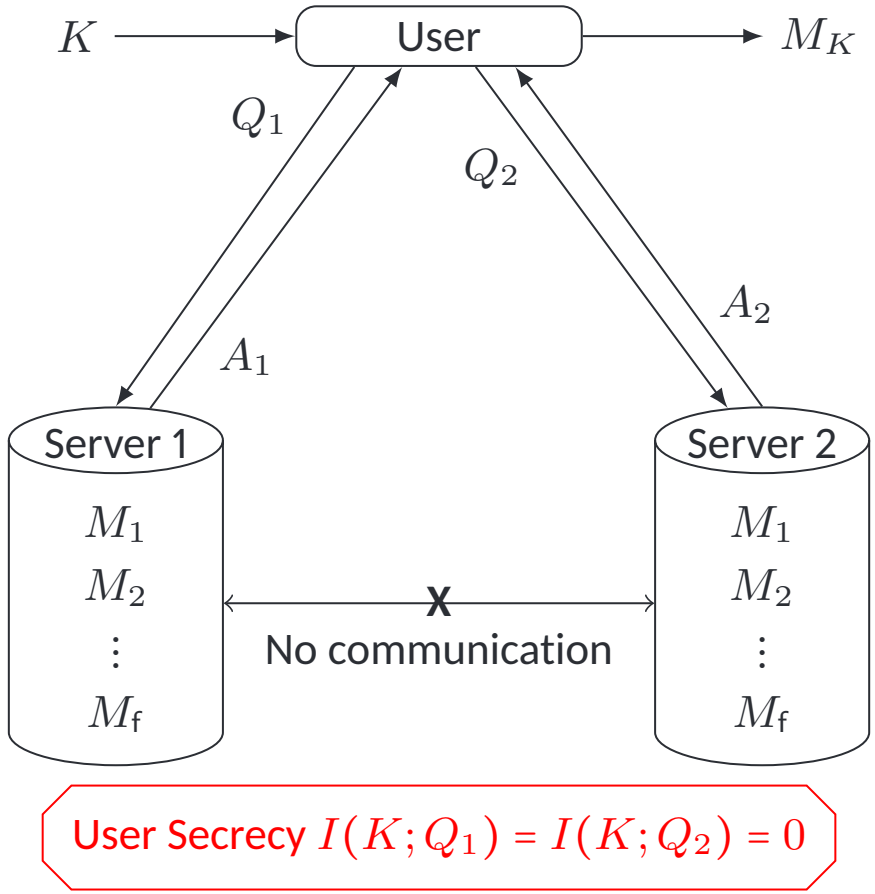


There have been two approaches to find efficient PIR protocols.

1. PIR with computational assumption. [Kushilevitz and Ostrovsky 97], [Cachin et al. 99], [Lipmaa 10], ...
2. PIR with multiple non-communicating servers.

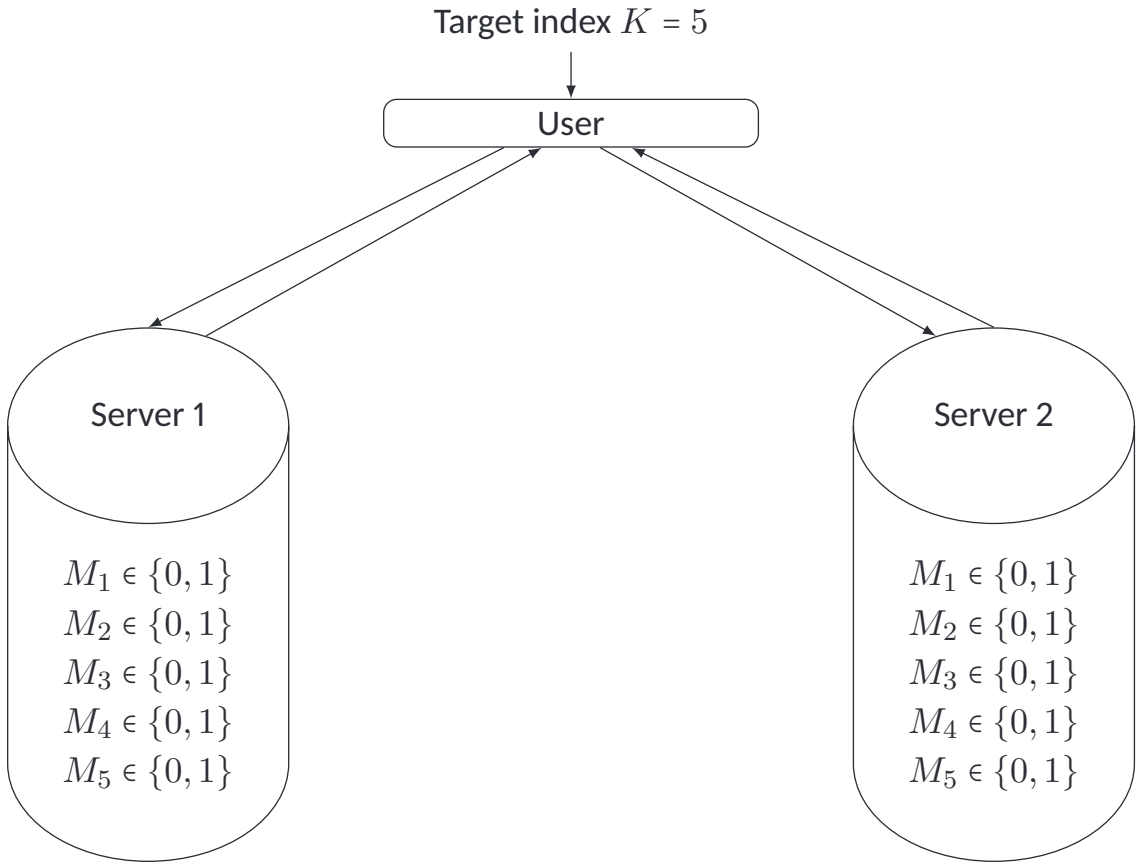
This talk only treats 2.

Multi-Server PIR



- Servers do not communicate with each other.
- User secrecy is $I(K;Q_j) = 0$ for all j.
- Most protocols are one-round protocols.

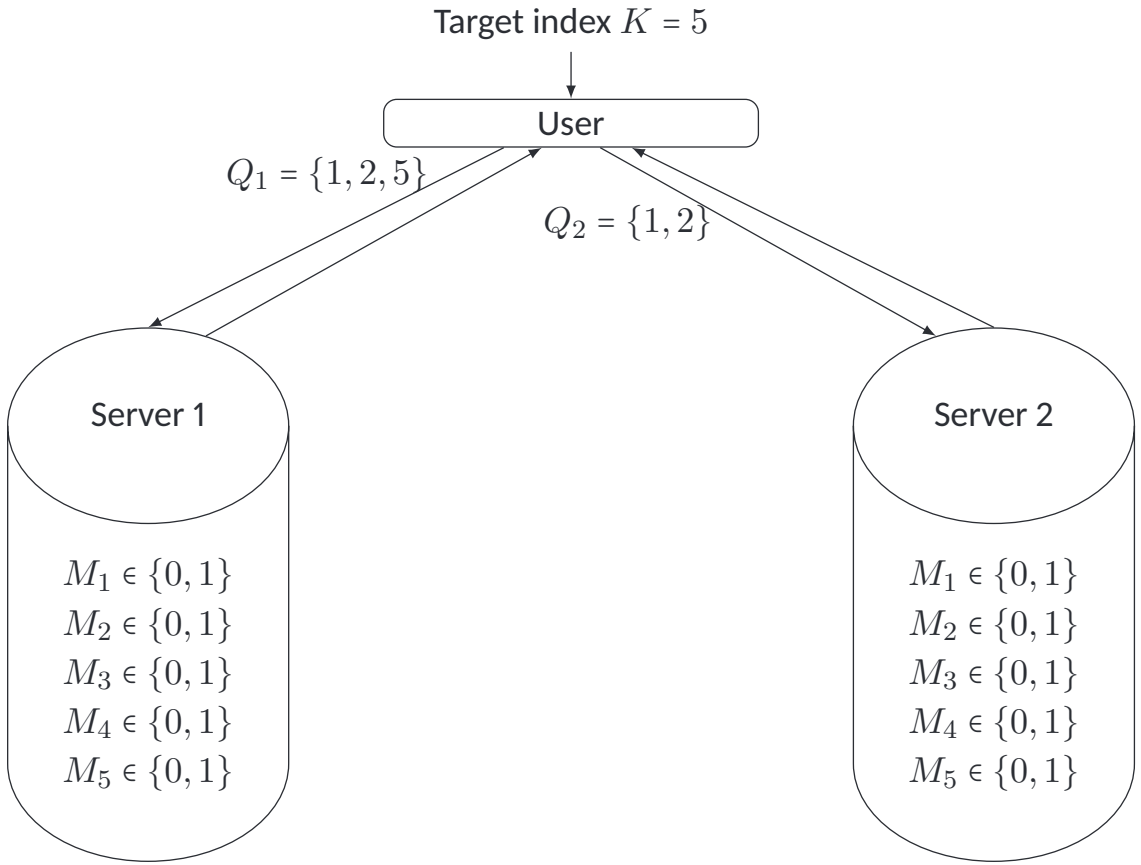
Example: Two-Server PIR Protocol [Chor et al.95]



Two-server 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 $A_1 = \sum_{i \in Q_1} M_i,\ A_2 = \sum_{i \in Q_2} M_i$.
3. User recovers $M_K = \pm(A_1 - A_2)$.

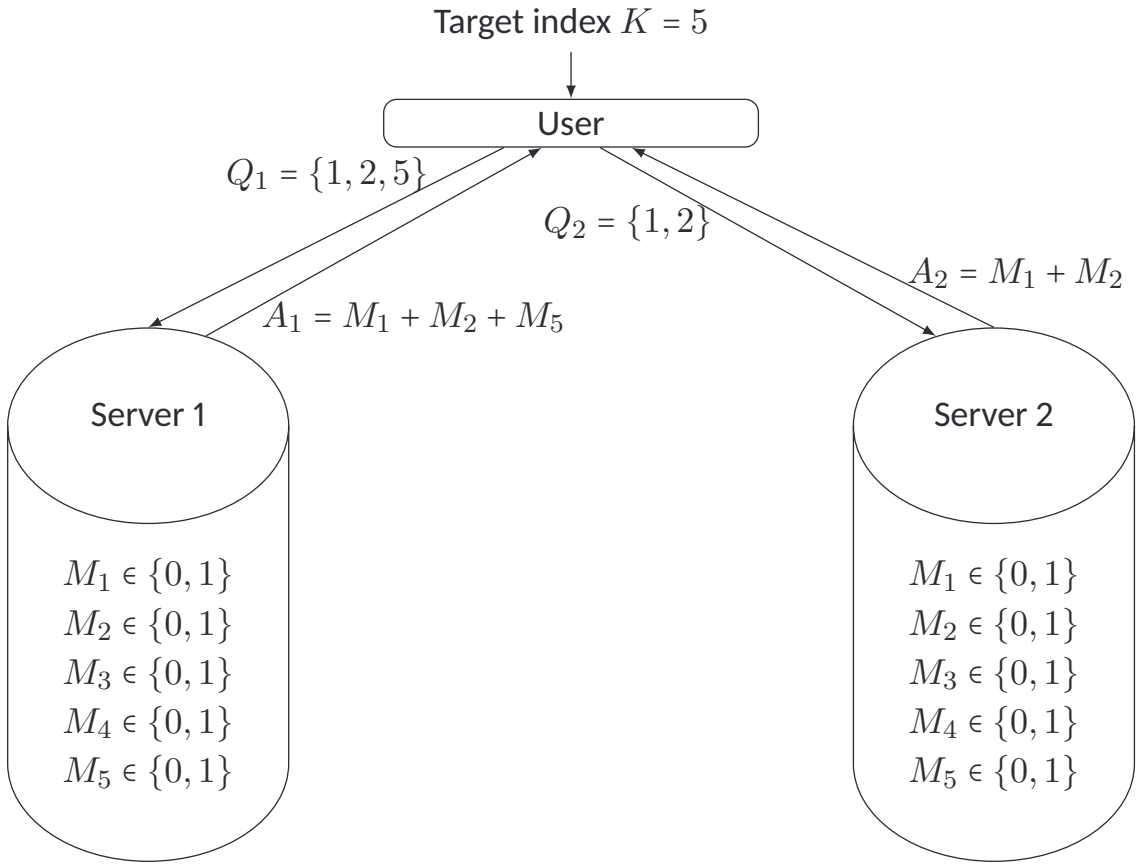
Example: Two-Server PIR Protocol [Chor et al.95]



Two-server 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 $A_1 = \sum_{i \in Q_1} M_i,\ A_2 = \sum_{i \in Q_2} M_i$.
3. User recovers $M_K = \pm(A_1 - A_2)$.

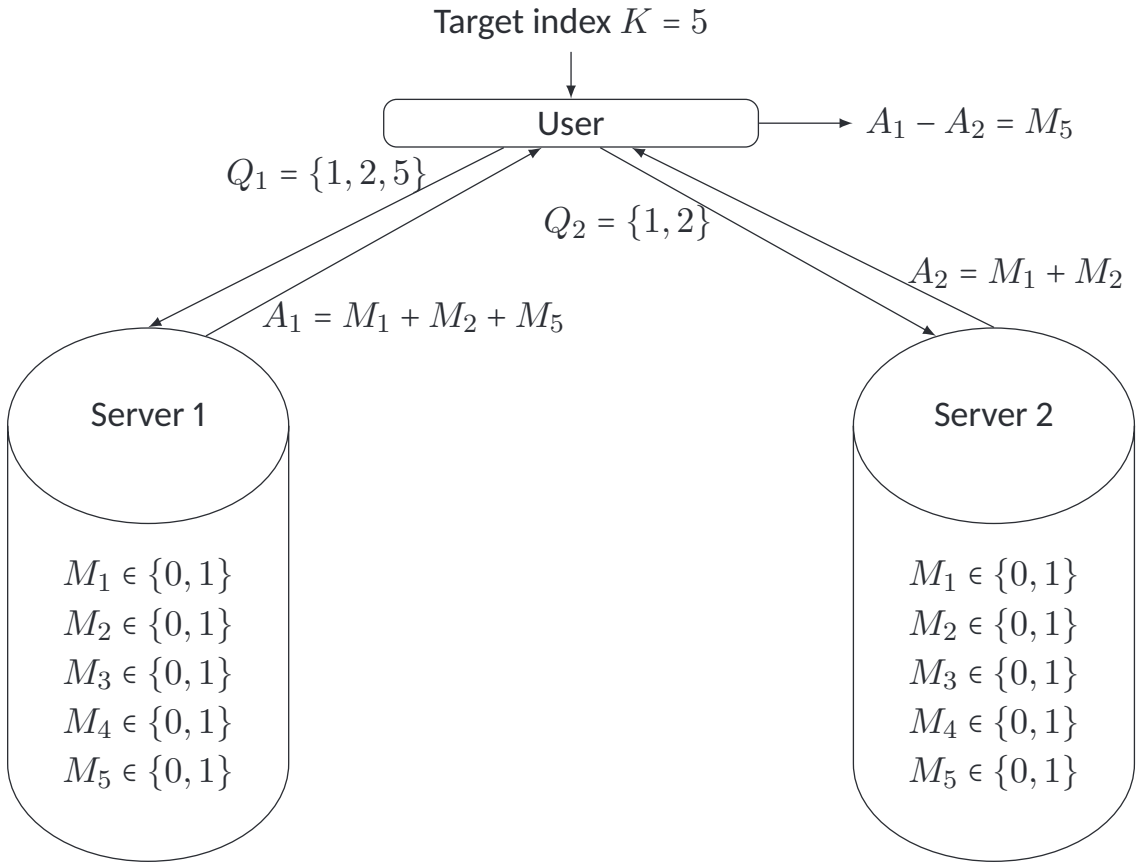
Example: Two-Server PIR Protocol [Chor et al.95]



Two-server 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 $A_1 = \sum_{i \in Q_1} M_i,\ A_2 = \sum_{i \in Q_2} M_i$.
3. User recovers $M_K = \pm(A_1 - A_2)$.

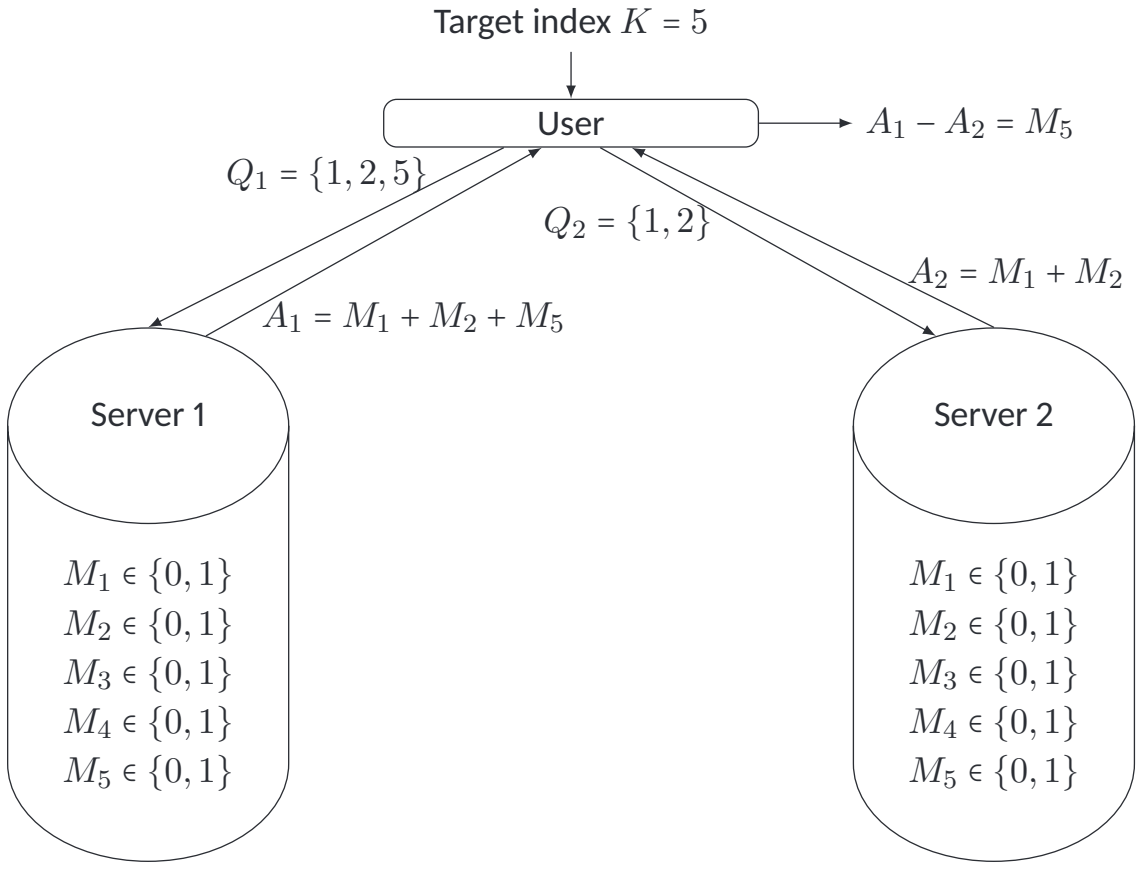
Example: Two-Server PIR Protocol [Chor et al.95]



Two-server 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 $A_1 = \sum_{i \in Q_1} M_i,\ A_2 = \sum_{i \in Q_2} M_i$.
3. User recovers $M_K = \pm(A_1 - A_2)$.

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



Two-server 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 $A_1 = \sum_{i \in Q_1} M_i,\ A_2 = \sum_{i \in Q_2} M_i$.
3. User recovers $M_K = \pm(A_1 - A_2)$.

$$\begin{cases} I(Q_1; K) = I(Q_2; K) = 0. \\ \text{2 bits are downloaded.} \end{cases}$$

Information-Theoretic Approach to PIR

Information Theory

On various communication tasks, the **information theory** often discusses

- optimal efficiency
- optimal protocols

with arbitrary many usages of resources.

(ex) Data compression.

Let $X_1, \ldots, X_{\mathsf{f}} \overset{\text{i.i.d.}}{\sim} p(x)$.

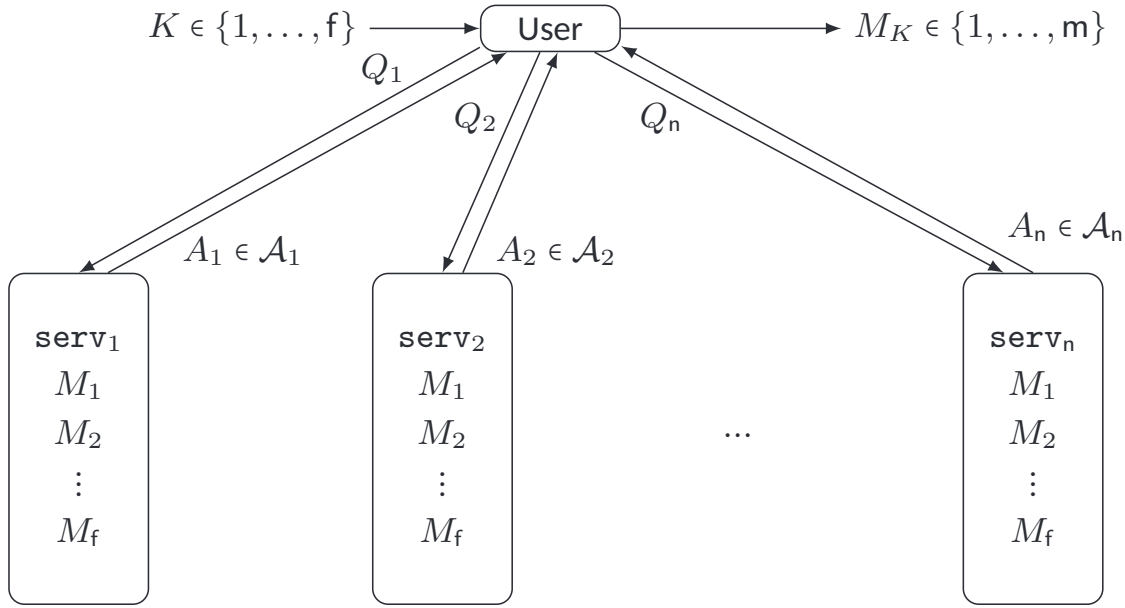
$$\underbrace{(X_1, \ldots, X_{\mathsf{f}})}_{\text{length } \mathsf{f}} \xrightarrow{\text{Encoding}} \underbrace{(Y_1, \ldots, Y_k)}_{\text{length } k \le \mathsf{f}} \xrightarrow{\text{Decoding}} (X_1, \ldots, X_{\mathsf{f}})$$

Rate $R_{\mathsf{f}} = \frac{k}{\mathsf{f}}$, Optimal Rate $R^* = \inf\{\limsup_{\mathsf{f}\to\infty} R_{\mathsf{f}} \mid P_{\mathrm{err}}^{(\mathsf{f})} \to 0\} = H(p)$.

Information-theoretic approach to multi-server PIR

- Optimal efficiency when the message size is arbitrary.
- Optimal protocol.

Information-Theoretic Approach to PIR [Sun-Jafar16] (cont.)



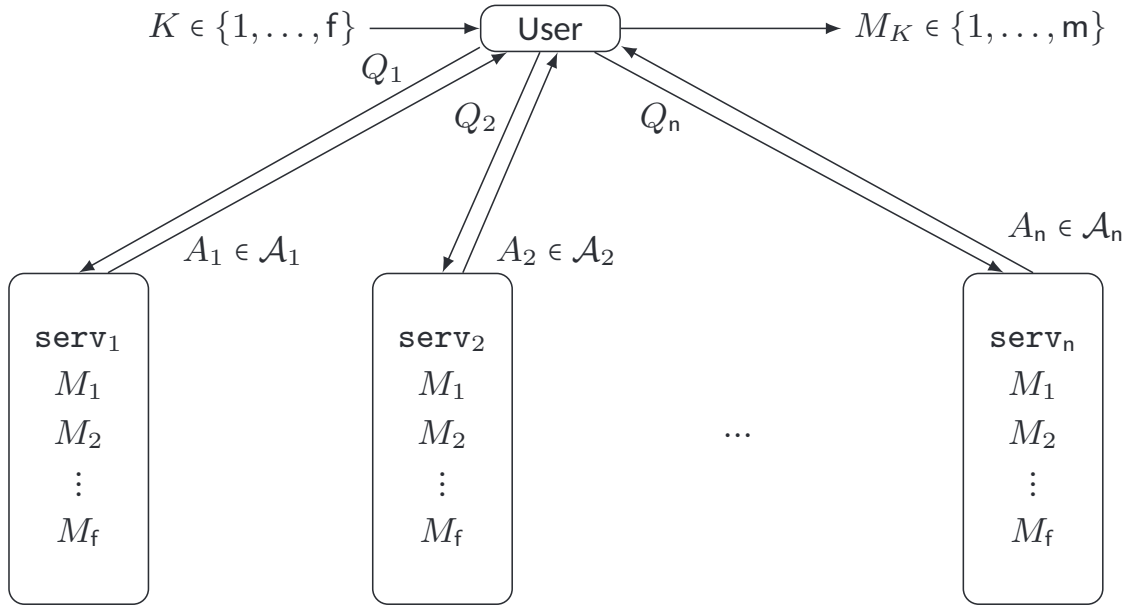
- n = # servers, f = # messages, m = size of M_K (i.e., $M_i \in \{1, \ldots, \mathsf{m}\}$).
- PIR Rate: # of retrieved bits per 1-bit download.

$$R = \frac{(\text{Size of } M_K)}{(\text{Total download size})} = \frac{\log \mathsf{m}}{\sum_{j=1}^{\mathsf{n}} \log |\mathcal{A}_i|}$$

  - $R \leq 1$ from definition.
  - The rate of "downloading all messages" is $1/\mathsf{f}$.
- PIR Capacity: Optimal PIR rate when n, f are fixed but m is arbitrary.

$$C_{\text{classical}} = \sup R = \frac{1 - 1/\mathsf{n}}{1 - (1/\mathsf{n})^{\mathsf{f}}} \to_{\mathsf{n}\to\infty} 1.$$

Information-Theoretic Approach to PIR [Sun-Jafar16] (cont.)



- n = # servers, f = # messages, m = size of M_K (i.e., $M_i \in \{1, \ldots, \mathsf{m}\}$).
- PIR Rate: # of retrieved bits per 1-bit download.

$$\frac{1}{\mathsf{f}} \le R = \frac{\text{(Size of } M_K\text{)}}{\text{(Total download size)}} = \frac{\log \mathsf{m}}{\sum_{j=1}^{\mathsf{n}} \log |\mathcal{A}_i|} \le 1$$

  - $R \le 1$ from definition.
  - The rate of "downloading all messages" is $1/\mathsf{f}$.
- PIR Capacity: Optimal PIR rate when n, f are fixed but m is arbitrary.

$$C_{\text{classical}} = \sup R = \frac{1 - 1/\mathsf{n}}{1 - (1/\mathsf{n})^{\mathsf{f}}} \to_{\mathsf{n}\to\infty} 1.$$

Variants of PIR

Problem 1: In PIR, non-targeted messages may be leaked to the user.
(ex) In the trivial solution of "downloading all", the user knows all message.

- User secrecy: User's information K is not leaked to the servers.
- Server secrecy: Servers' information of non-targeted messages is not leaked to the user

Symmetric PIR is PIR with both user secrecy and server secrecy.

- Symmetric PIR is impossible,
  but it is possible with shared randomness between servers. [Gertner et al.00]
- Symmetric PIR capacity is $1 - \frac{1}{n}$ [Sun-Jafar17]

Problem 2: No communication between servers is too restrictive assumption.

t-**Private PIR** is PIR in which $\underbrace{\text{at most t servers}}_{\text{unknown to the user}}$ may collude to know the target index K.

- t-private PIR is possible for any $1 \leq t \leq n-1$.
- t-private PIR capacity is $\frac{1 - t/n}{1 - (t/n)^f}$ [Sun-Jafar16-2]

Existing Results on Quantum PIR (QPIR)

Quantum PIR (QPIR) is PIR with quantum communication.

Single-Server QPIR

1. Non-trivial QPIR protocol is possible. [Le Gall12], [Kerenidis et al.16]
2. QPIR with Specious Server: the server may deviate from the protocol but the malicious operation should not noticed by the user.
   - Trivial solution is optimal. [Baumeler-Broadbent15]
   - Trivial solution is optimal even with prior entanglement. [Aharonov et al.19]

Multi-Server QPIR

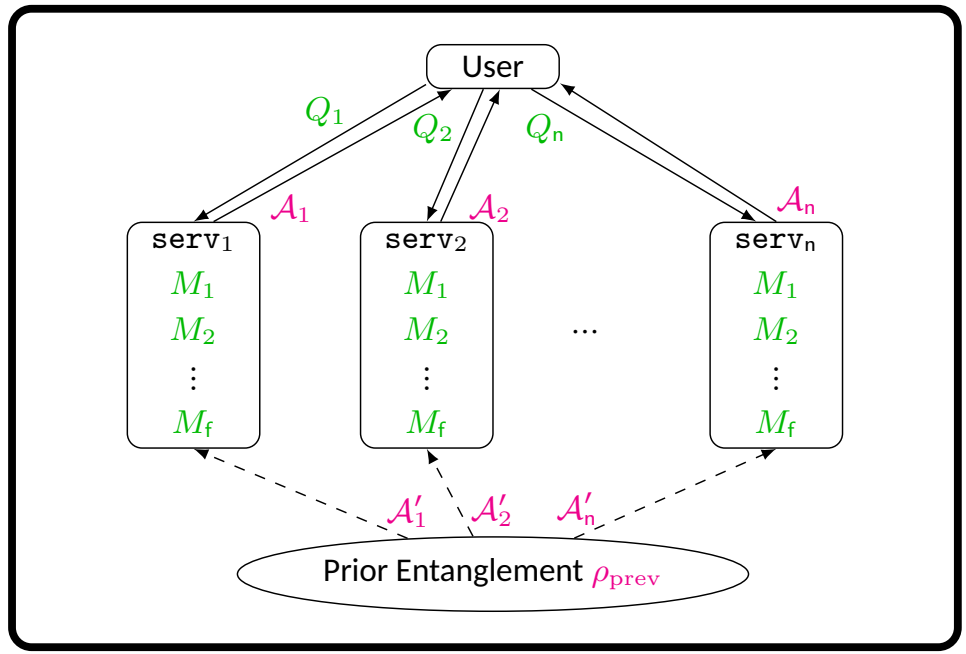
- Symmetric QPIR is possible without shared randomness. [Kerenidis-de Wolf04]

Summary of Results

As information-theoretic approach to QPIR, we derive the QPIR capacity.

Problem Setting

- Multi-server QPIR
- Communication model
  - query is classical,
  - download is quantum,
  - prior entanglement of servers are assumed.



(Green: classical, Magenta: quantum.)

Results

- QPIR capacities
  - QPIR capacity
  - Multi-round QPIR capacity
  - t-private QPIR capacity
  - Symmetric & non-symmetric cases.

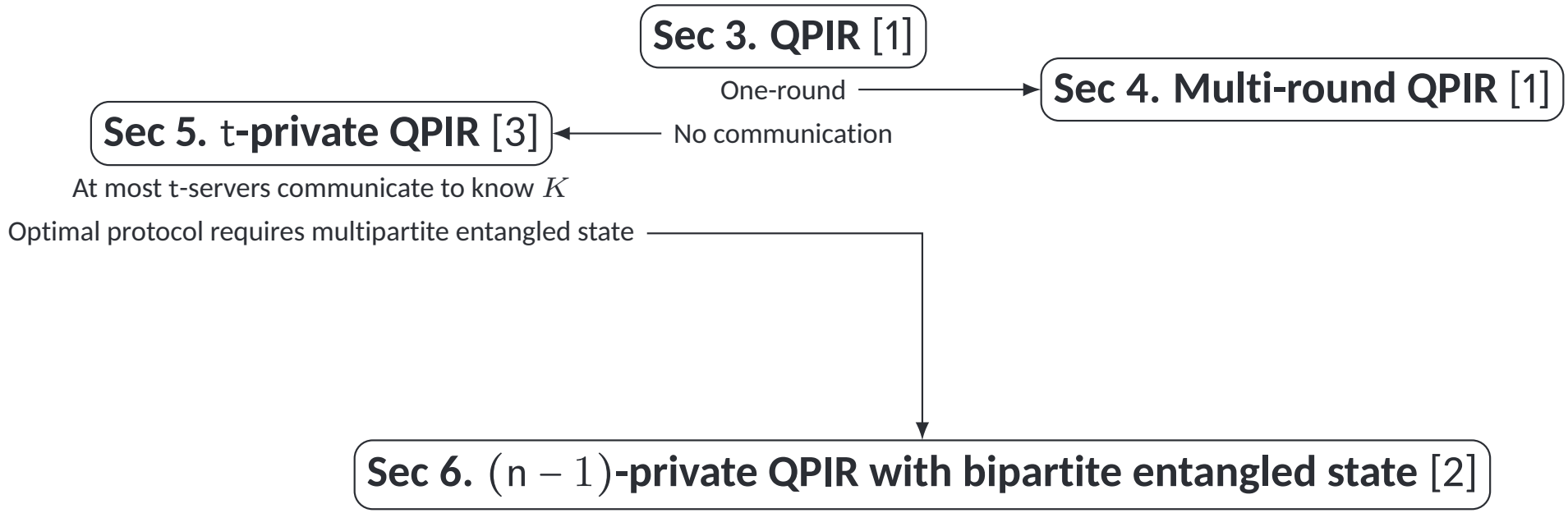
Classical PIR vs Quantum PIR Capacities (n servers, f messages, t colluding servers)

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 ‡
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1
Symmetric multi-round PIR	-	
t-Private PIR	$\frac{1-t/n}{1-(t/n)^f}$ [Sun-Jafar16-2]	1 for $t \leq \frac{n}{2}$, ‡ $2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ ‡
Symmetric t-private PIR	$\frac{n-t}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

Outline of Remaining Talk



Publications

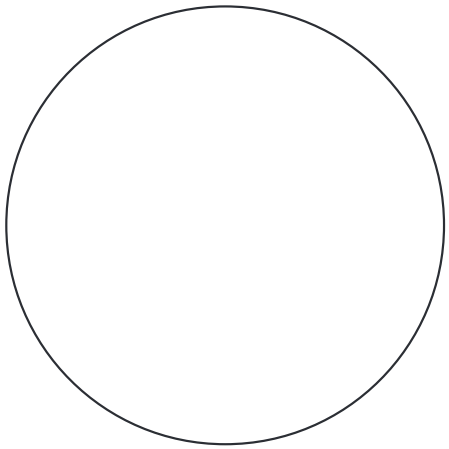
[1] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, accepted.

[2] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019 (submitted to *Journal on Selected Areas in Information Theory*).

[3] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1077–1082, 2020 (submitted to *IEEE Transactions on Information Theory*).

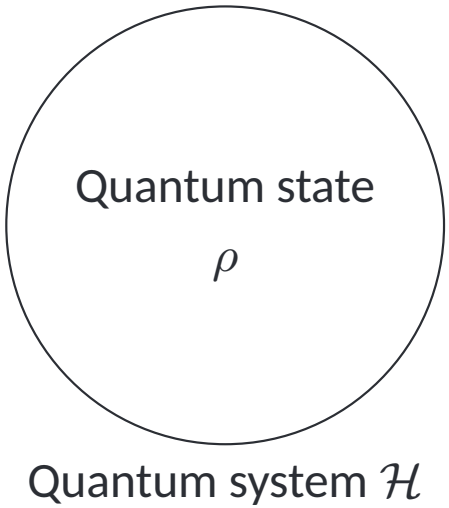
Contents

Framework of Quantum Information Theory

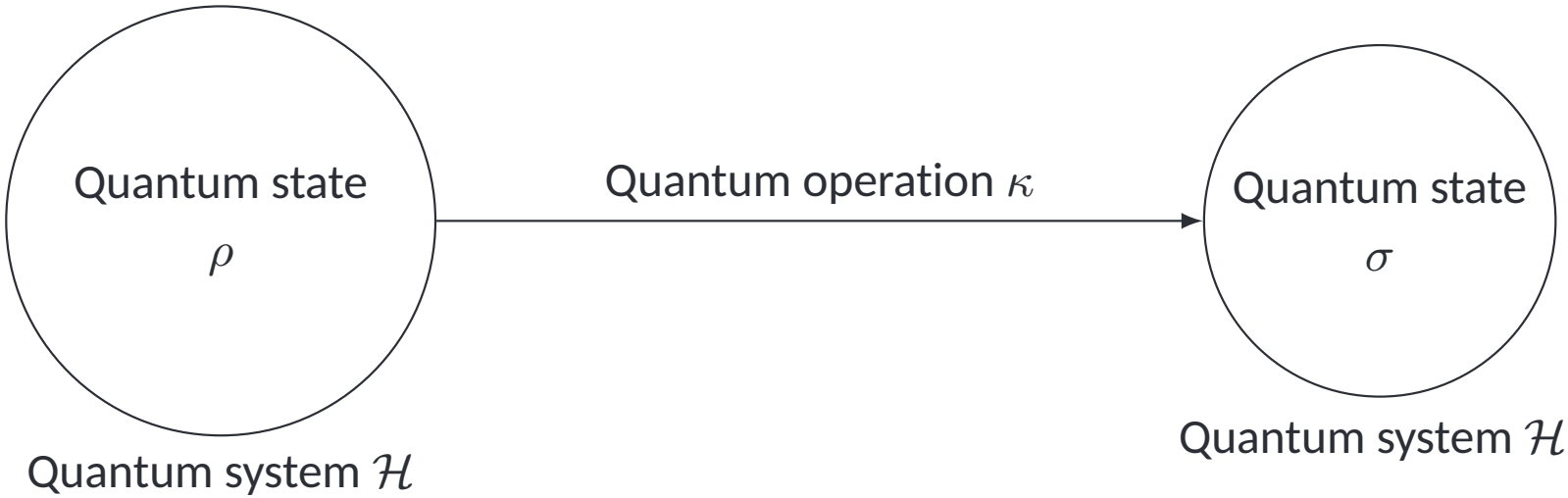


Quantum system $\mathcal{H}$

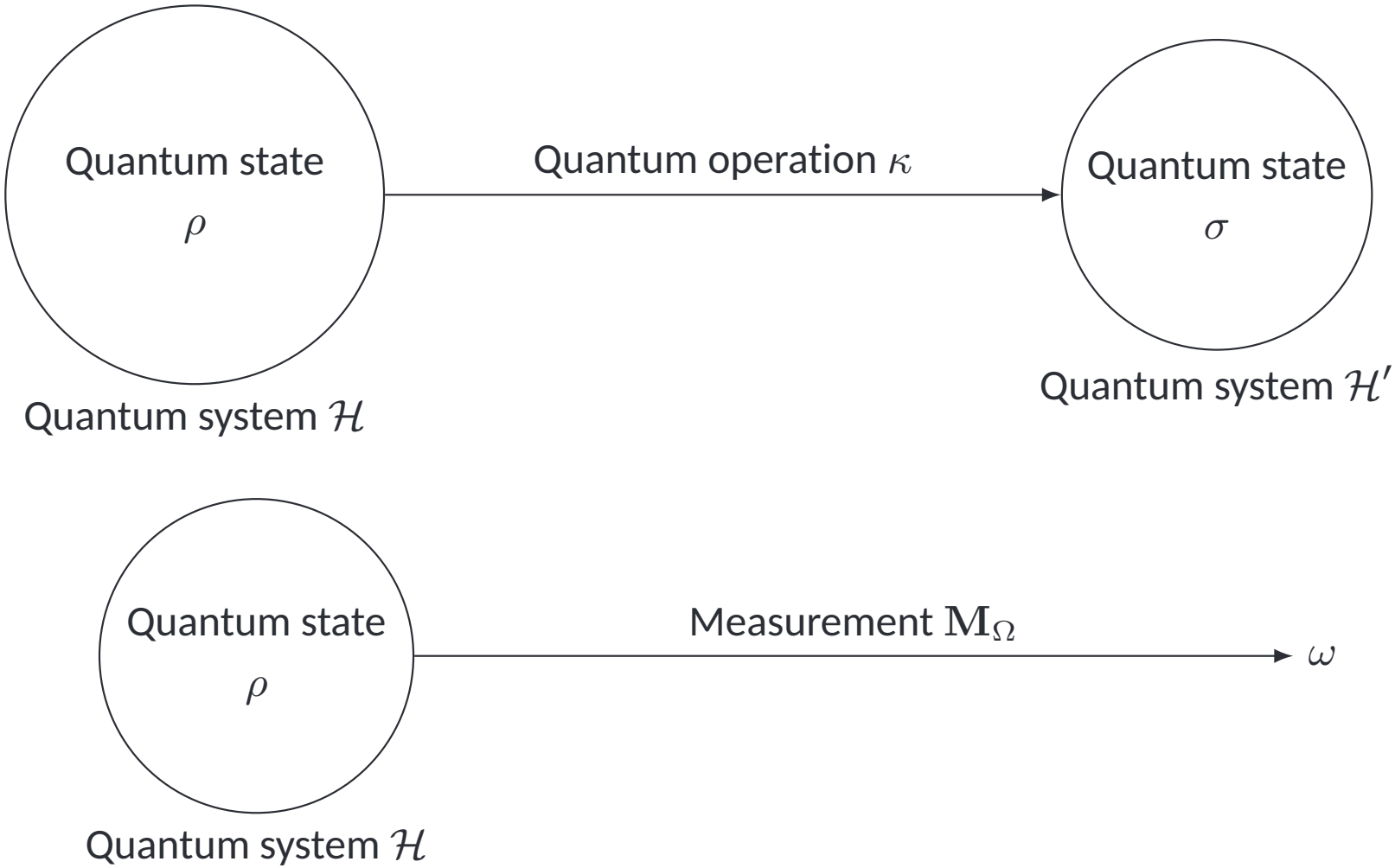
Framework of Quantum Information Theory



Framework of Quantum Information Theory



Framework of Quantum Information Theory



Quantum System and Quantum States

Quantum system

Any quantum system is described by a *finite-dimensional Hilbert space* $\mathcal{H}$.

- Multiple quantum systems are described by tensor products of the systems.

Quantum state

Any quantum state on a quantum system $\mathcal{H}$ is described by a *density matrix* on $\mathcal{H}$.

- A matrix ρ on $\mathcal{H}$ is called a *density matrix* on $\mathcal{H}$ if $\operatorname{Tr}\rho = 1 \quad$ and $\quad \rho \geq 0$.
- If $\rho = |x\rangle\langle x|$, the quantum state is represented by a unit vector $|x\rangle$.
- A state ρ on a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ is called *separable state* if

$$\rho = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i} \tag{1}$$

  for distribution p and states $\rho_{A,i}, \rho_{B,i}$.

- If ρ is not separable, it is called *entangled state*.

Quantum Operations and Quantum Measurements

Quantum Operation

Any quantum operation is described by a *completely positive trace-preserving (CPTP) linear map*.

- *Positive map* is a map from positive semidefinite matrices to positive semidefinite matrices.
- A map κ is a *completely positive* if $\kappa \otimes \iota_{\mathbb{C}_n}$ is a positive map for all $n \in \mathbb{N}$.
  - $\iota_{\mathbb{C}_n}$ is identity map on $\mathbb{C}^n$.

Measurement

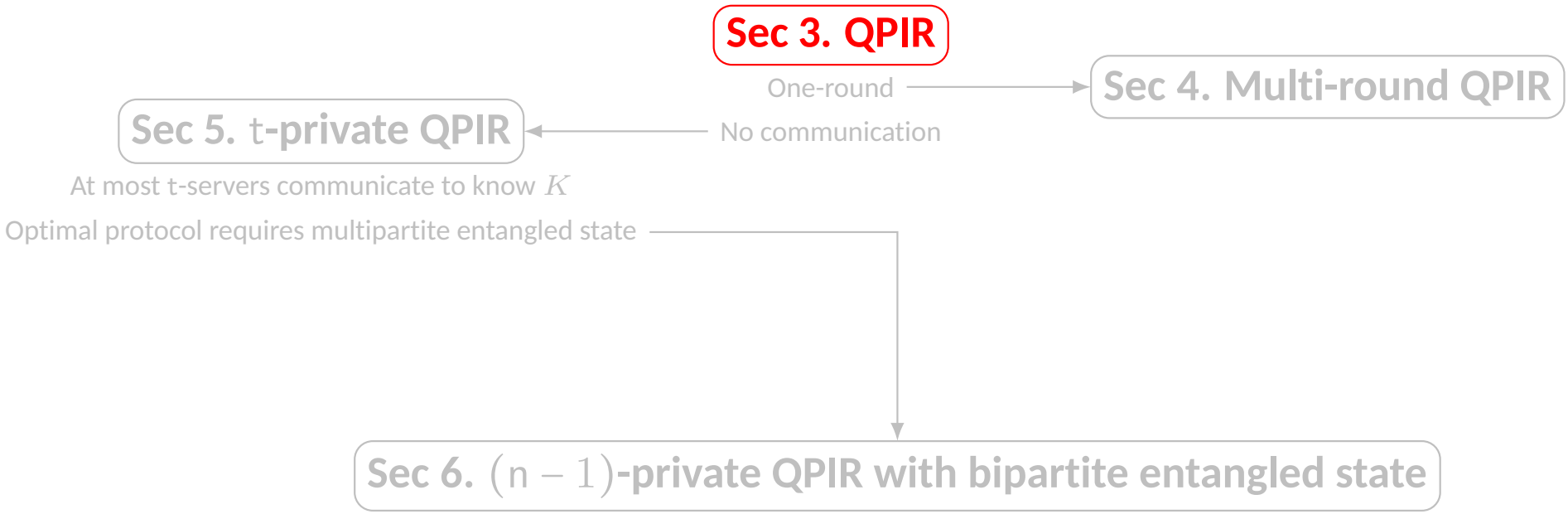
Any measurement on a quantum system $\mathcal{H}$ is described by a *positive operator-valued measure (POVM)*.

- A set of matrices $\mathbf{M}_\Omega \coloneqq \{M_\omega : \omega \in \Omega\}$ is called a *POVM* on $\mathcal{H}$ if

$$\sum_\omega M_\omega = I_\mathcal{H} \quad \text{and} \quad M_\omega \geq 0 \quad \text{for any } \omega \in \Omega.$$

- The probability for obtaining ω is $\operatorname{Tr} \rho M_\omega \in [0, 1]$. (c.f. $\sum_\omega \operatorname{Tr} \rho M_\omega = 1$)

Contents



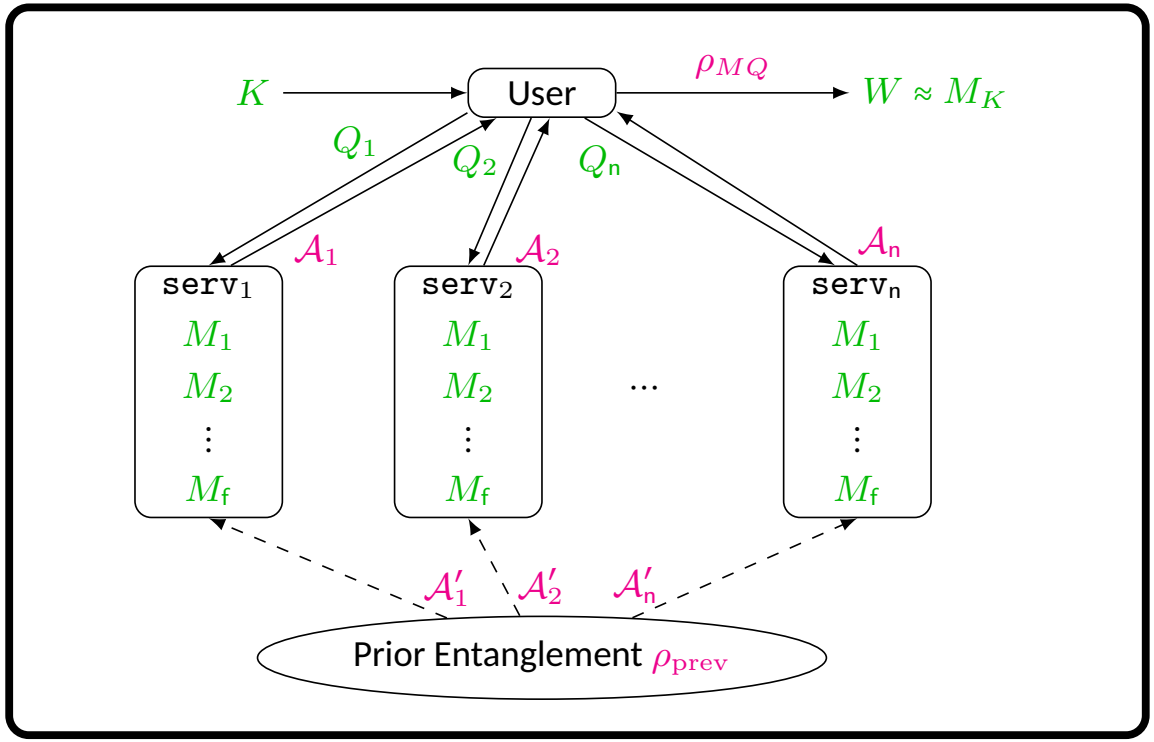
Publications

[1] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, accepted.

[2] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019 (submitted to *Journal on Selected Areas in Information Theory*).

[3] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1077–1082, 2020 (submitted to *IEEE Transactions on Information Theory*).

Formal Definition of QPIR Protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$



(Green: classical, Magenta: quantum.)

$M_i \in \{1, \ldots, \mathsf{m}\}$

$\mathcal{A}'_j, \mathcal{A}_j$: quantum systems

$\rho_{\mathrm{prev}}, \rho_{MQ}$: states

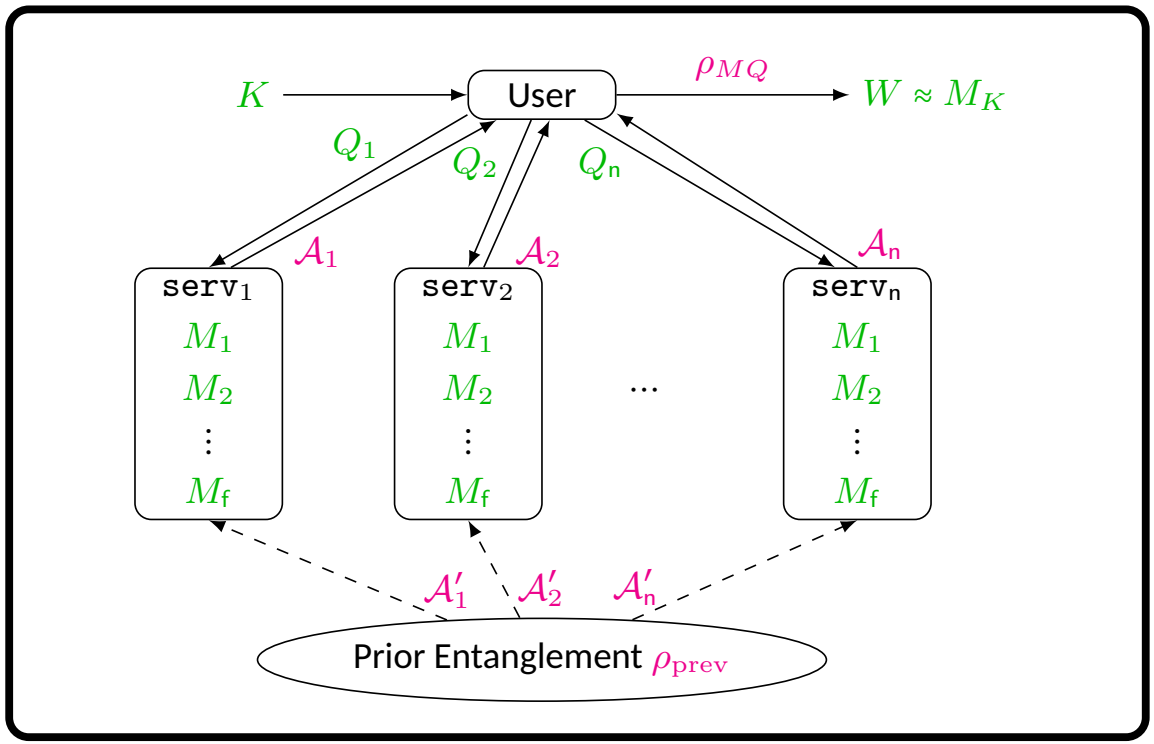
ρ_{prev} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}'_j$.

ρ_{MQ} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j$.

Security measures

- Error probability P_{err}
- Server secrecy S_{serv}
- User secrecy S_{user}

Formal Definition of QPIR Protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$



(Green: classical, Magenta: quantum.)

$M_i \in \{1, \ldots, \mathsf{m}\}$

$\mathcal{A}'_j, \mathcal{A}_j$: quantum systems

$\rho_{\mathrm{prev}}, \rho_{MQ}$: states

ρ_{prev} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}'_j$.

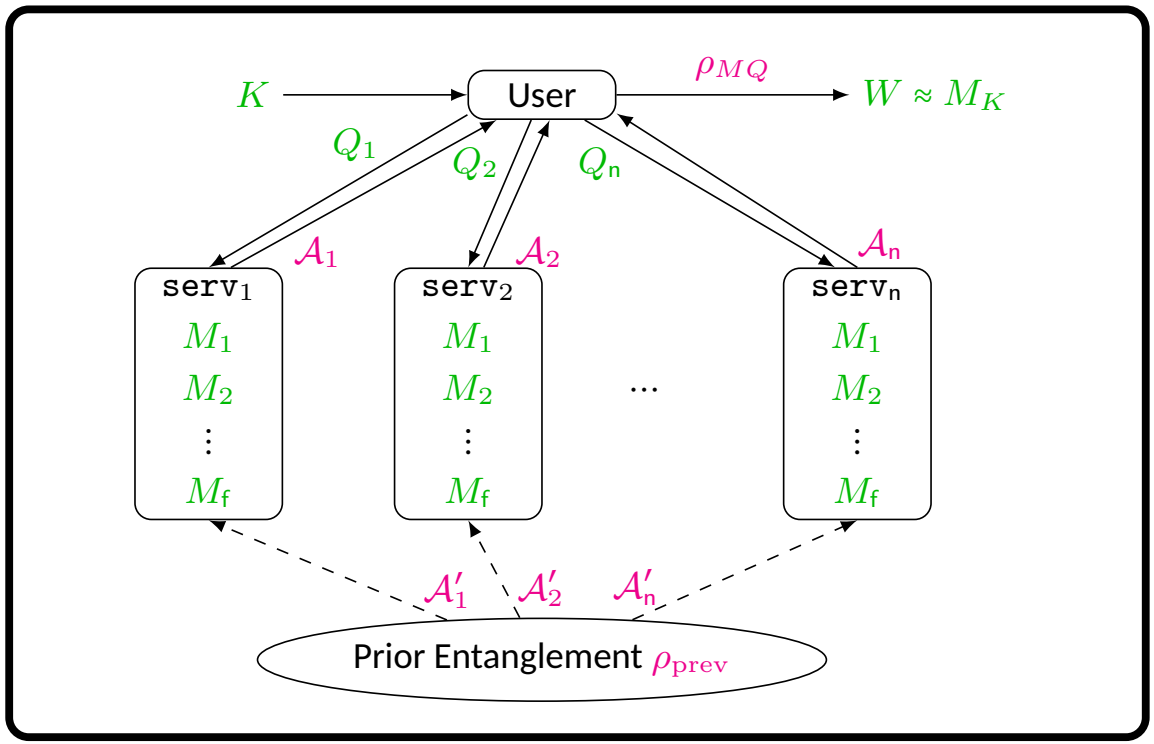
ρ_{MQ} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j$.

Security measures

- Error probability $P_{\mathrm{err}} := \Pr_W[W \neq M_K | MKQ] \in [0,1]$.
- Server secrecy $S_{\mathrm{serv}} := I(M_K^c; \mathfrak{user} | K) \geq 0$.
- User secrecy $S_{\mathrm{user}} := \max_{j \in \{1,\ldots,\mathsf{n}\}} I(K; \mathfrak{serv}_j) \geq 0$.

- If $(P_{\mathrm{err}}, S_{\mathrm{user}}) = (0,0)$, the protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$ is the *QPIR protocol*.
- If $(P_{\mathrm{err}}, S_{\mathrm{serv}}, S_{\mathrm{user}}) = (0,0,0)$, the protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$ is the *symmetric QPIR protocol*.

Formal Definition of QPIR Protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$



(Green: classical, Magenta: quantum.)

$M_i \in \{1, \ldots, \mathsf{m}\}$

$\mathcal{A}'_j, \mathcal{A}_j$: quantum systems

$\rho_{\mathrm{prev}}, \rho_{MQ}$: states

ρ_{prev} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}'_j$.

ρ_{MQ} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j$.

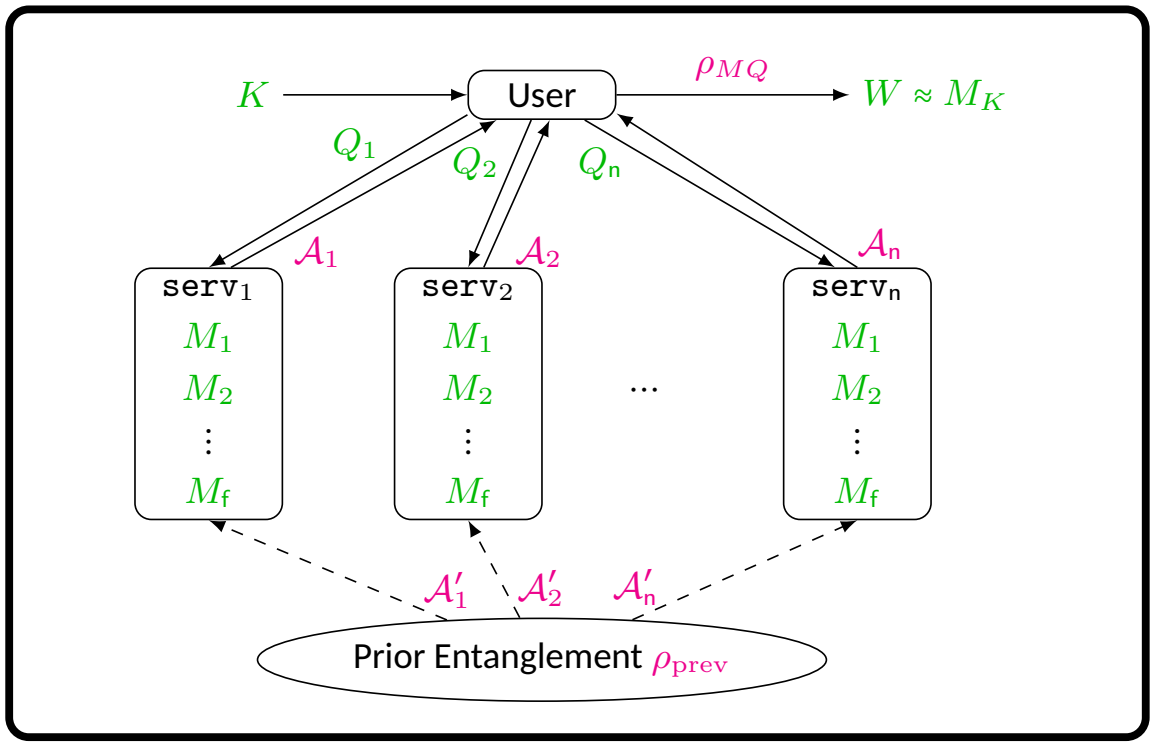
Security measures

- Error probability $P_{\mathrm{err}} := \Pr_W[W \neq M_K | MKQ] \in [0, 1]$.
- Server secrecy $S_{\mathrm{serv}} := I(M_K^c; \mathfrak{user} | K) \geq 0$.
- User secrecy $S_{\mathrm{user}} := \max_{j \in \{1,\ldots,\mathsf{n}\}} I(K; \mathfrak{serv}_j) \geq 0$.

QPIR rate is # of retrieved bits per 1-qubit download.

$$R := \frac{(\text{Size of } M_K)}{(\text{Total download size})} = \frac{\log \mathsf{m}}{\sum_{j=1}^{\mathsf{n}} \log \dim \mathcal{A}_j} \quad [\text{bit/qubit}].$$

Formal Definition of QPIR Protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$



(Green: classical, Magenta: quantum.)

$M_i \in \{1, \ldots, \mathsf{m}\}$

$\mathcal{A}'_j, \mathcal{A}_j$: quantum systems

$\rho_{\mathrm{prev}}, \rho_{MQ}$: states

ρ_{prev} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}'_j$.

ρ_{MQ} on $\bigotimes_{j=1}^{\mathsf{n}} \mathcal{A}_j$.

Security measures

- Error probability $P_{\mathrm{err}} := \Pr_W[W \neq M_K | MKQ] \in [0, 1]$.
- Server secrecy $S_{\mathrm{serv}} := I(M_K^c; \mathfrak{user} | K) \geq 0$.
- User secrecy $S_{\mathrm{user}} := \max_{j \in \{1,\ldots,\mathsf{n}\}} I(K; \mathfrak{serv}_j) \geq 0$.

QPIR rate is # of retrieved bits per 1-qubit download.

$$\frac{1}{\mathsf{f}} \leq R := \frac{(\text{Size of } M_K)}{(\text{Total download size})} = \frac{\log \mathsf{m}}{\sum_{j=1}^{\mathsf{n}} \log \dim \mathcal{A}_j} \leq 1 \ [\text{bit/qubit}].$$

QPIR Capacity

QPIR capacity is the optimal QPIR rate given the numbers of servers n and messages f.

Exact security-constrained capacity

$$C_{\text{exact}}^{\alpha,\beta,\gamma} \coloneqq \sup\left\{ R \;\middle|\; (*1) \right\},$$

$$(*1) = \begin{cases} P_{\text{err}} \le \alpha, \\ S_{\text{serv}} \le \beta, \\ S_{\text{user}} \le \gamma. \end{cases}$$

Asymptotic security-constrained capacity

$$C_{\text{asymp}}^{\alpha,\beta,\gamma} \coloneqq \sup_{\{\Psi_{\text{QPIR}}^{(\mathsf{m})}\}_{\mathsf{m}=1}^{\infty}} \left\{ \lim_{\mathsf{m}\to\infty} R^{(\mathsf{m})} \;\middle|\; (*2), \right\}$$

$$(*2) = \begin{cases} \limsup_{\mathsf{m}\to\infty} P_{\text{err}}^{(\mathsf{m})} \le \alpha, \\ \limsup_{\mathsf{m}\to\infty} S_{\text{serv}}^{(\mathsf{m})} \le \beta, \\ \limsup_{\mathsf{m}\to\infty} S_{\text{user}}^{(\mathsf{m})} \le \gamma. \end{cases}$$

From definitions,

$$C_{\text{exact}}^{0,0,0} \le C_{\text{exact}}^{\alpha,\beta,\gamma} \le C_{\text{asymp}}^{\alpha,\beta,\gamma} \le C_{\text{asymp}}^{\alpha,\infty,\infty}.$$

$C_{\text{exact}}^{0,\beta,0}, C_{\text{asymp}}^{0,\beta,0}$: QPIR capacity.
$C_{\text{exact}}^{0,0,0}, C_{\text{asymp}}^{0,0,0}$: symmetric QPIR capacity.

Main Theorem

Theorem 3.1: QPIR Capacity

The QPIR capacity with f ≥ 2 messages and n ≥ 2 servers is

$$C_{\text{exact}}^{\alpha,\beta,\gamma} = C_{\text{asymp}}^{\alpha,\beta,\gamma} = 1, \quad \forall \alpha \in [0,1) \text{ and } \forall \beta, \gamma \in [0,\infty].$$

(α: error bound, β: server secrecy bound, γ: user secrecy bound)

(Proof)

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

Classical PIR vs Quantum PIR Capacities (n servers, f messages, t colluding servers)

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 ‡
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1
Symmetric multi-round PIR	-	
t-Private PIR	$\frac{1-t/n}{1-(t/n)^f}$ [Sun-Jafar16-2]	1 for $t \leq \frac{n}{2}$, ‡ $2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ ‡
Symmetric t-private PIR	$\frac{n-t}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

Preliminaries for Protocol Construction

- Let $\mathcal{A} = \mathrm{span}\{|0\rangle, \ldots, |\ell - 1\rangle\}$ be an ℓ-dimensional Hilbert space.

Preliminaries for Protocol Construction

- Let $\mathcal{A} = \mathrm{span}\{|0\rangle, \ldots, |\ell - 1\rangle\}$ be an ℓ-dimensional Hilbert space.
- Maximally Entangled State

$$|\Phi\rangle \coloneqq \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A} \otimes \mathcal{A}\,.$$

Preliminaries for Protocol Construction

- Let $\mathcal{A} = \mathrm{span}\{|0\rangle, \ldots, |\ell - 1\rangle\}$ be an ℓ-dimensional Hilbert space.
- Maximally Entangled State

$$|\Phi\rangle \coloneqq \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A} \otimes \mathcal{A}\,.$$

- Pauli Operations on $\mathcal{A}$:

$$\mathsf{X} \coloneqq \sum_{i=0}^{\ell-1} |i+1\rangle\langle i|, \quad \mathsf{Z} \coloneqq \sum_{i=0}^{\ell-1} \omega^i |i\rangle\langle i|, \quad \mathsf{W}(a,b) \coloneqq \mathsf{X}^a \mathsf{Z}^b \quad \forall a, b \in \mathbb{Z}_\ell.$$

Preliminaries for Protocol Construction

- Let $\mathcal{A} = \mathrm{span}\{|0\rangle, \ldots, |\ell - 1\rangle\}$ be an ℓ-dimensional Hilbert space.
- Maximally Entangled State

$$|\Phi\rangle \coloneqq \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A} \otimes \mathcal{A}\,.$$

- Pauli Operations on $\mathcal{A}$:

$$\mathsf{X} \coloneqq \sum_{i=0}^{\ell-1} |i+1\rangle\langle i|, \quad \mathsf{Z} \coloneqq \sum_{i=0}^{\ell-1} \omega^i |i\rangle\langle i|, \quad \mathsf{W}(a,b) \coloneqq \mathsf{X}^a \mathsf{Z}^b \quad \forall\, a, b \in \mathbb{Z}_\ell.$$

- We have the relation

$$(\mathsf{W}(a,b) \otimes \overline{\mathsf{W}(c,d)})|\Phi\rangle = (\mathsf{W}(a-c, b-d) \otimes \mathsf{I})|\Phi\rangle.$$

Preliminaries for Protocol Construction

- Let $\mathcal{A} = \mathrm{span}\{|0\rangle, \ldots, |\ell-1\rangle\}$ be an ℓ-dimensional Hilbert space.
- Maximally Entangled State

$$|\Phi\rangle \coloneqq \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A} \otimes \mathcal{A}\,.$$

- Pauli Operations on $\mathcal{A}$:

$$\mathsf{X} \coloneqq \sum_{i=0}^{\ell-1} |i+1\rangle\langle i|, \quad \mathsf{Z} \coloneqq \sum_{i=0}^{\ell-1} \omega^i |i\rangle\langle i|, \quad \mathsf{W}(a,b) \coloneqq \mathsf{X}^a \mathsf{Z}^b \quad \forall a, b \in \mathbb{Z}_\ell.$$

- We have the relation

$$(\mathsf{W}(a,b) \otimes \overline{\mathsf{W}(c,d)})|\Phi\rangle = (\mathsf{W}(a-c, b-d) \otimes \mathsf{I})|\Phi\rangle.$$

- $\mathbf{M}_{\mathbb{Z}_\ell^2} \coloneqq \{(\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle \mid a, b \in \mathbb{Z}_\ell\}$ is a basis of $\mathcal{A} \otimes \mathcal{A}$.

Preliminaries for Protocol Construction

- Let $\mathcal{A} = \mathrm{span}\{|0\rangle, \ldots, |\ell-1\rangle\}$ be an ℓ-dimensional Hilbert space.
- Maximally Entangled State

$$|\Phi\rangle \coloneqq \frac{1}{\sqrt{\ell}} \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A} \otimes \mathcal{A}\,.$$

- Pauli Operations on $\mathcal{A}$:

$$\mathsf{X} \coloneqq \sum_{i=0}^{\ell-1} |i+1\rangle\langle i|, \quad \mathsf{Z} \coloneqq \sum_{i=0}^{\ell-1} \omega^i |i\rangle\langle i|, \quad \mathsf{W}(a,b) \coloneqq \mathsf{X}^a \mathsf{Z}^b \quad \forall a, b \in \mathbb{Z}_\ell.$$

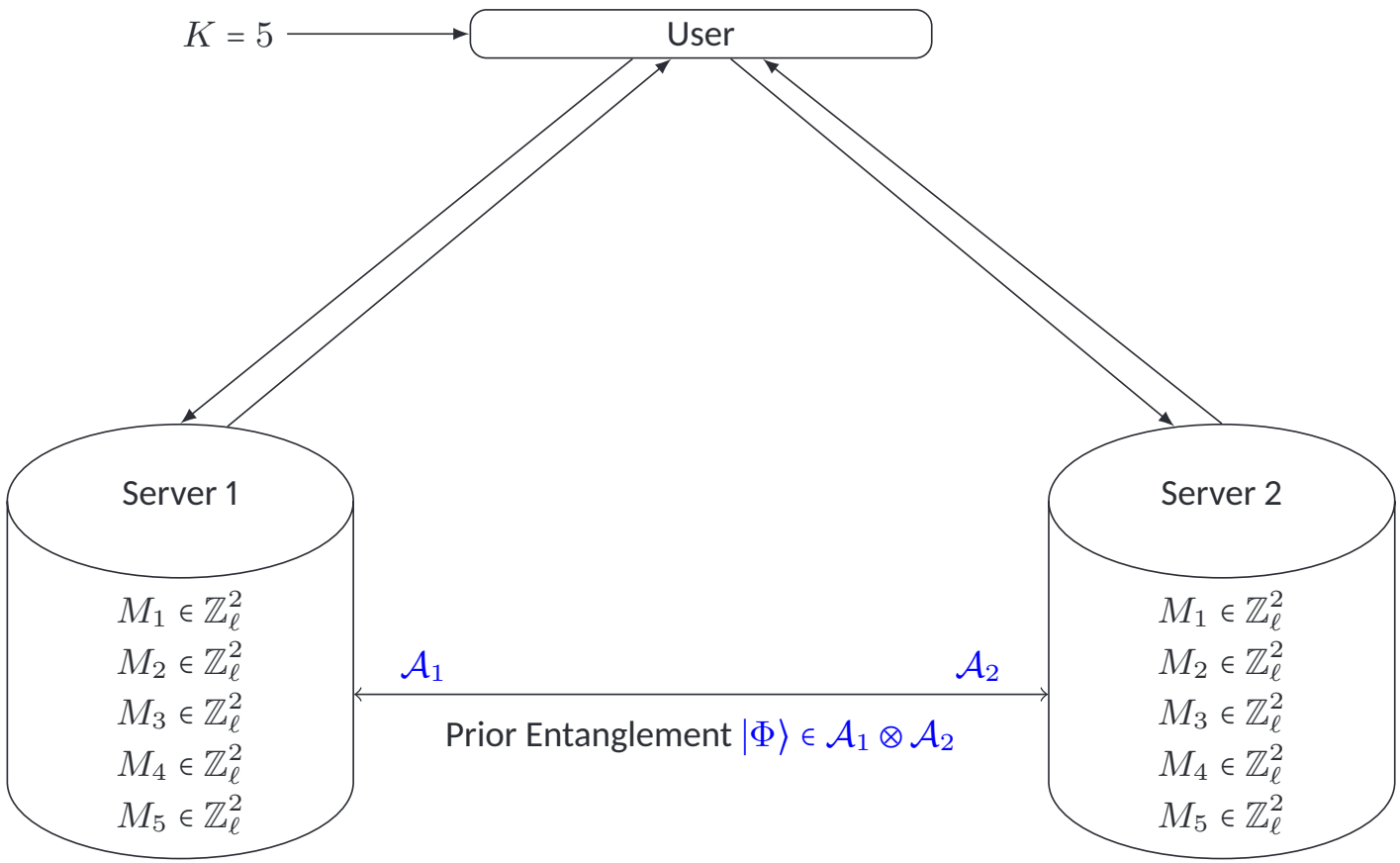
- We have the relation

$$(\mathsf{W}(a,b) \otimes \overline{\mathsf{W}(c,d)})|\Phi\rangle = (\mathsf{W}(a-c, b-d) \otimes \mathsf{I})|\Phi\rangle.$$

- $\mathbf{M}_{\mathbb{Z}_\ell^2} \coloneqq \{(\mathsf{W}(a,b) \otimes \mathsf{I})|\Phi\rangle \mid a, b \in \mathbb{Z}_\ell\}$ is a basis of $\mathcal{A} \otimes \mathcal{A}$.
- When the state is $(\mathsf{W}(x,y) \otimes \mathsf{I})|\Phi\rangle$ and the measurement $\mathbf{M}_{\mathbb{Z}_\ell^2}$ is applied, the measurement outcome is (x, y).

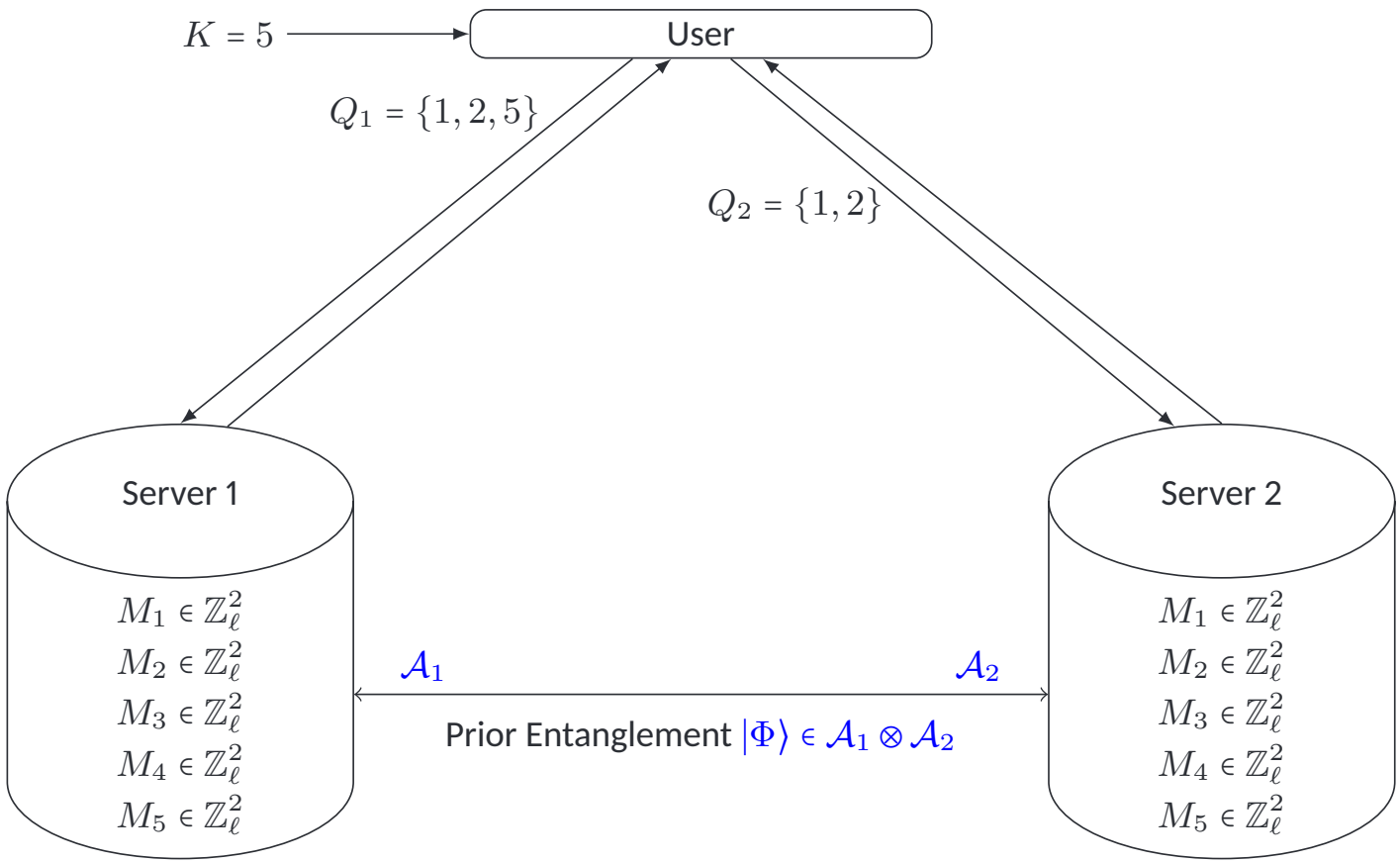
QPIR Protocol

1. Servers share maximally entangled state $|\Phi\rangle \coloneqq (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.



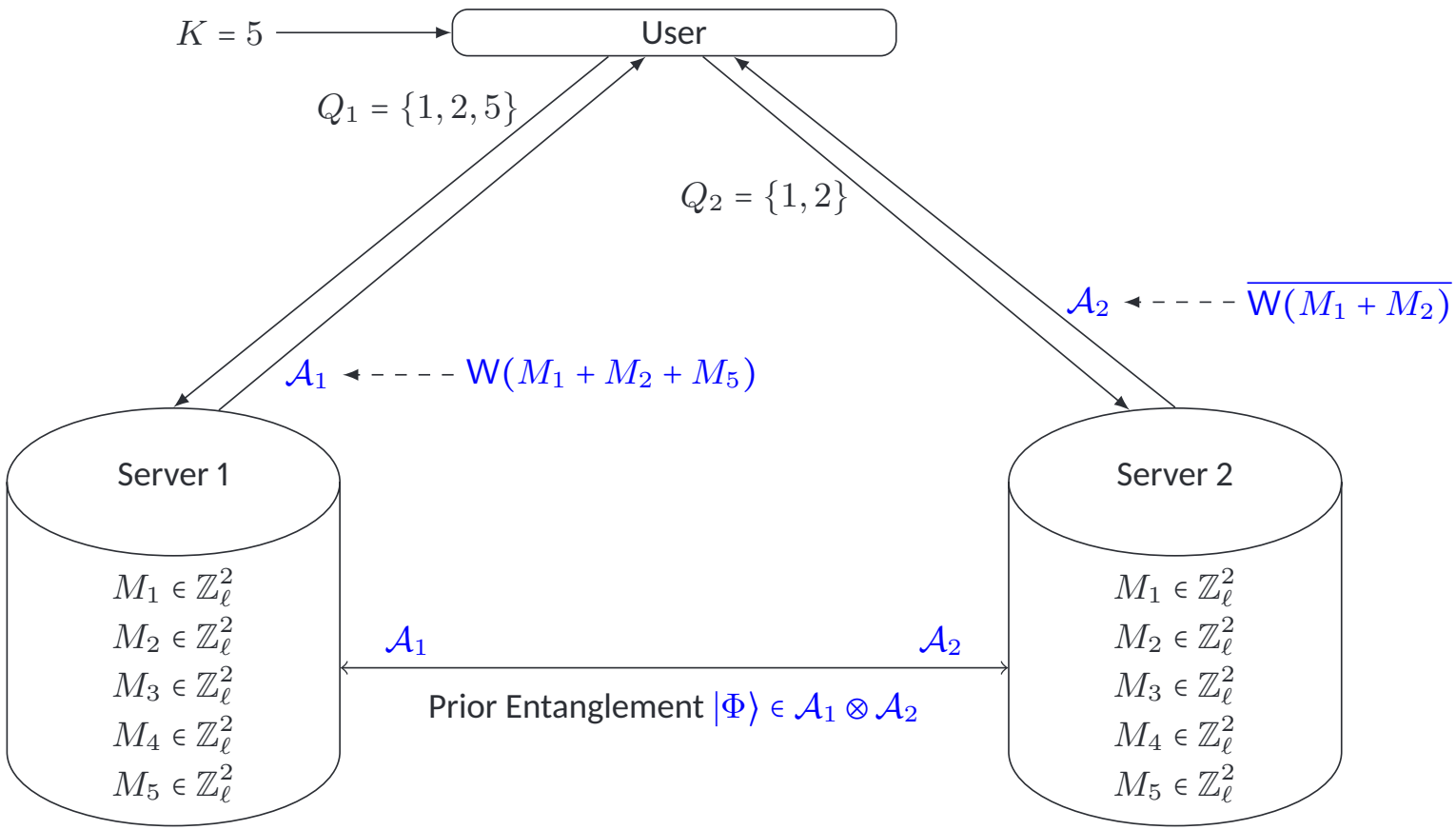
QPIR Protocol

1. Servers share maximally entangled state $|\Phi\rangle \coloneqq (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
2. Q_1: A random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.



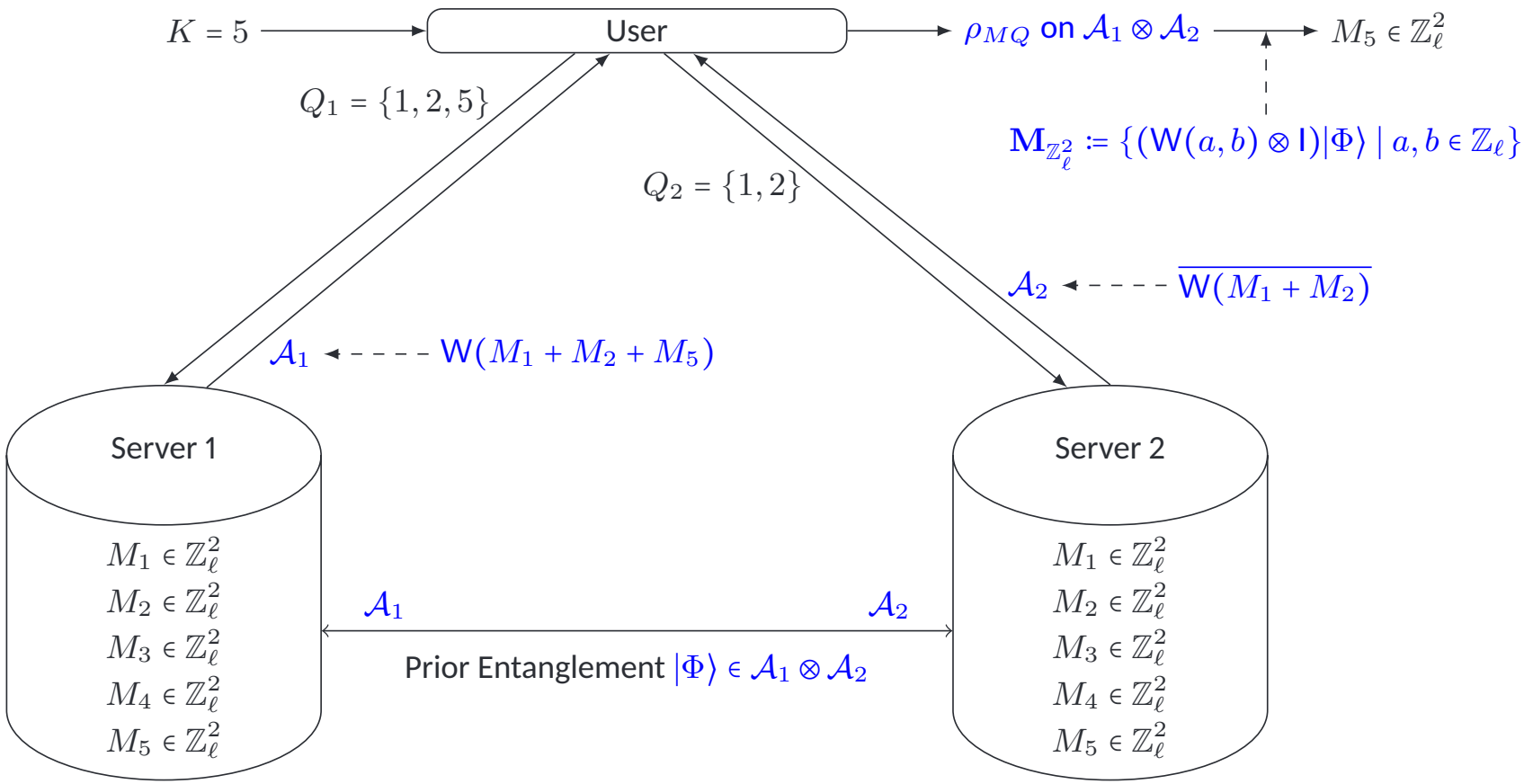
QPIR Protocol

1. Servers share maximally entangled state $|\Phi\rangle \coloneqq (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
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 $\mathsf{W}(\sum_{i \in Q_1} M_i)$ on $\mathcal{A}_1$ and Server 2 applies $\overline{\mathsf{W}(\sum_{i \in Q_2} M_i)}$ on $\mathcal{A}_2$.



QPIR Protocol

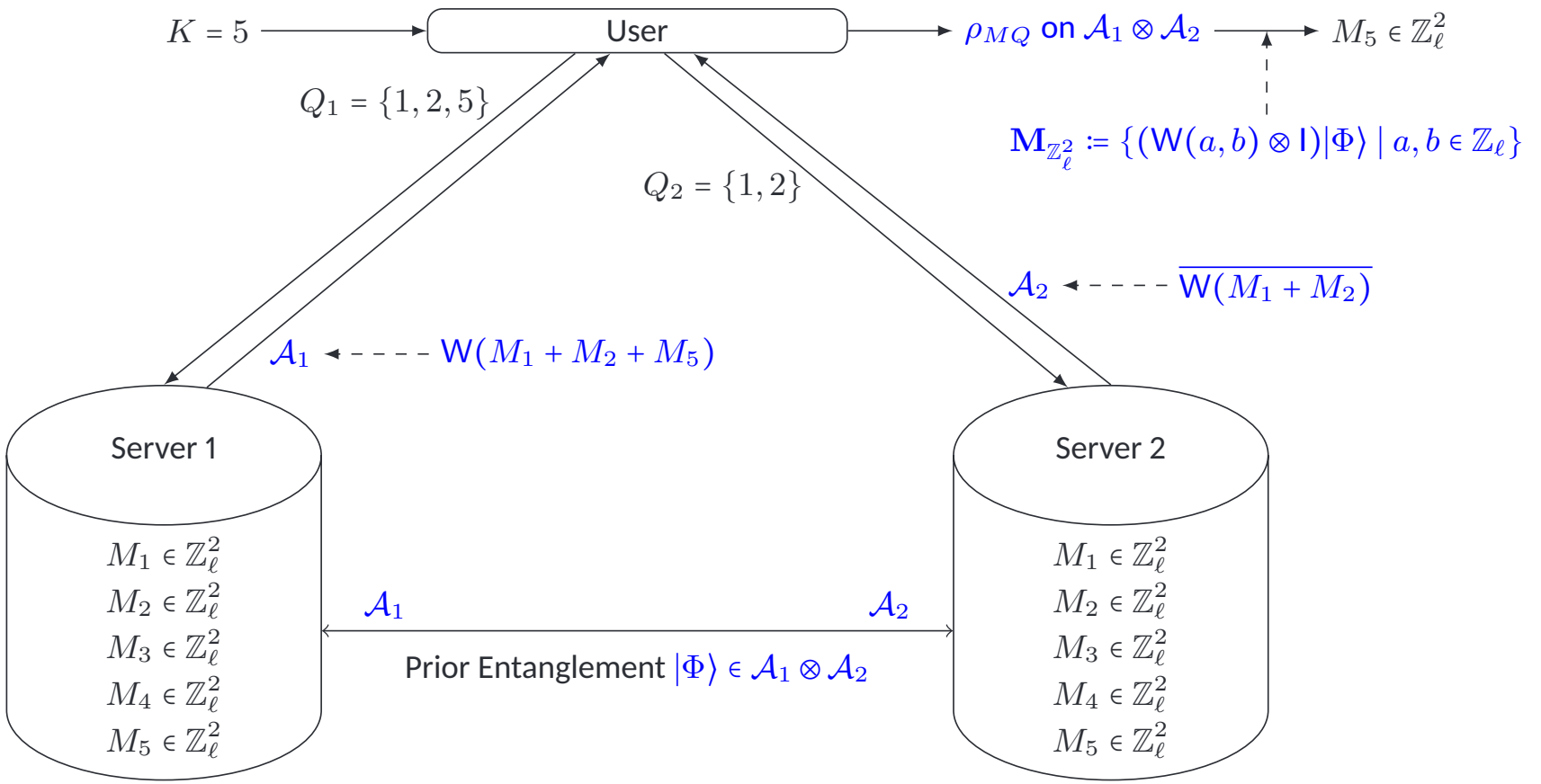
1. Servers share maximally entangled state $|\Phi\rangle \coloneqq (1/\sqrt{\ell}) \sum_{i=0}^{\ell-1} |i\rangle \otimes |i\rangle \in \mathcal{A}_1 \otimes \mathcal{A}_2$.
2. Q_1: A random subset of $\{1, \ldots, \mathsf{f}\}$.
   Q_2: a set satisfying $(Q_1 \cup Q_2) - (Q_1 \cap Q_2) = \{K\}$.
3. Server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



QPIR Protocol

Error Probability is 0 because

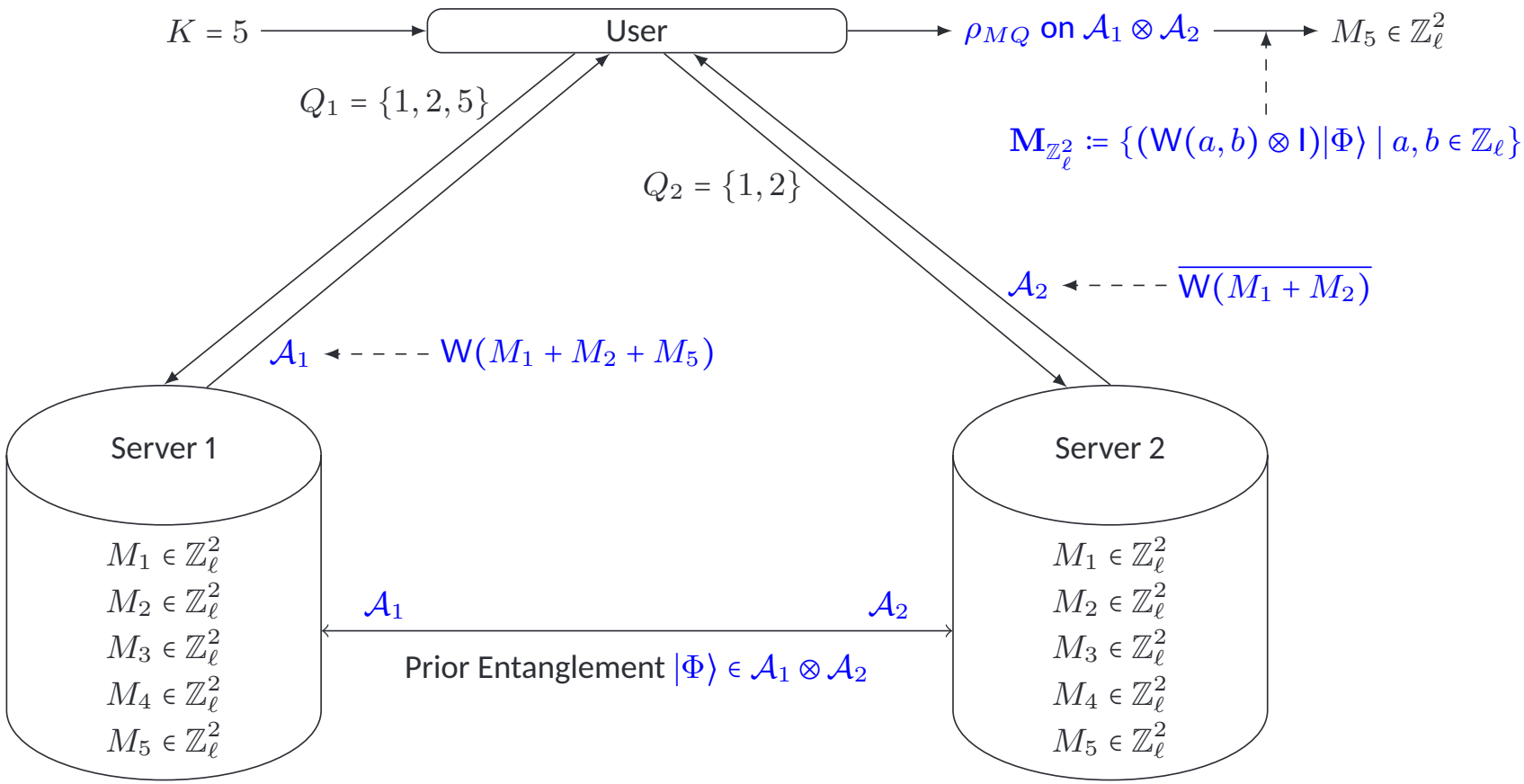
$$\rho_{MQ} = \left(\mathsf{W}\left(\sum_{i\in Q_1} M_i\right) \otimes \overline{\mathsf{W}\left(\sum_{i\in Q_2} M_i\right)}\right)|\Phi\rangle = \left(\mathsf{W}\left(\sum_{i\in Q_1} M_i - \sum_{i\in Q_2} M_i\right) \otimes \mathsf{I}\right)|\Phi\rangle = (\mathsf{W}(\pm M_K) \otimes \mathsf{I})|\Phi\rangle.$$



QPIR Protocol

User Secrecy: $I(K;Q_1) = I(K;Q_2) = 0$

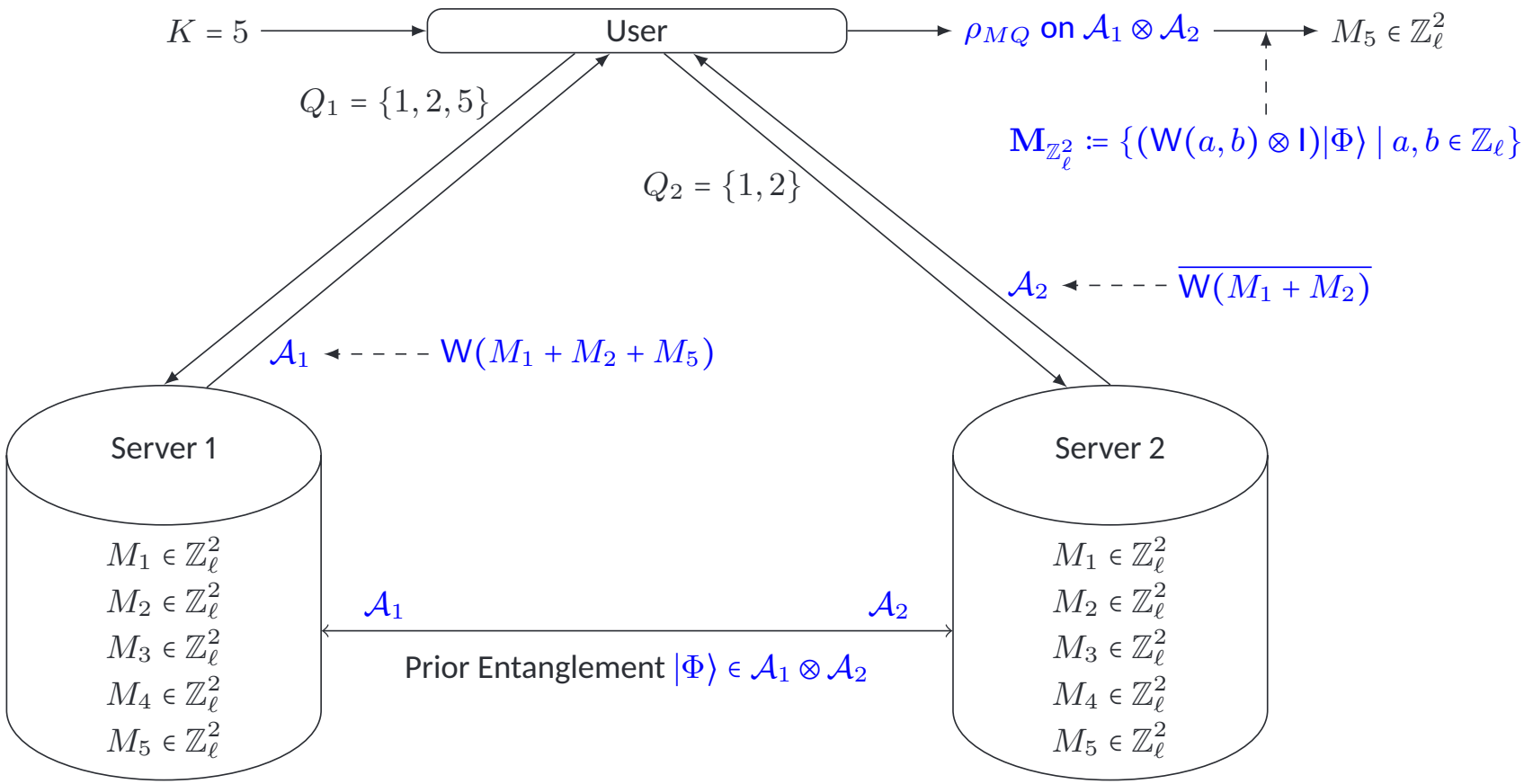
Server Secrecy: The received state $(\mathsf{W}(\pm M_K) \otimes \mathsf{I})|\Phi\rangle$ is independent of M_K^c.



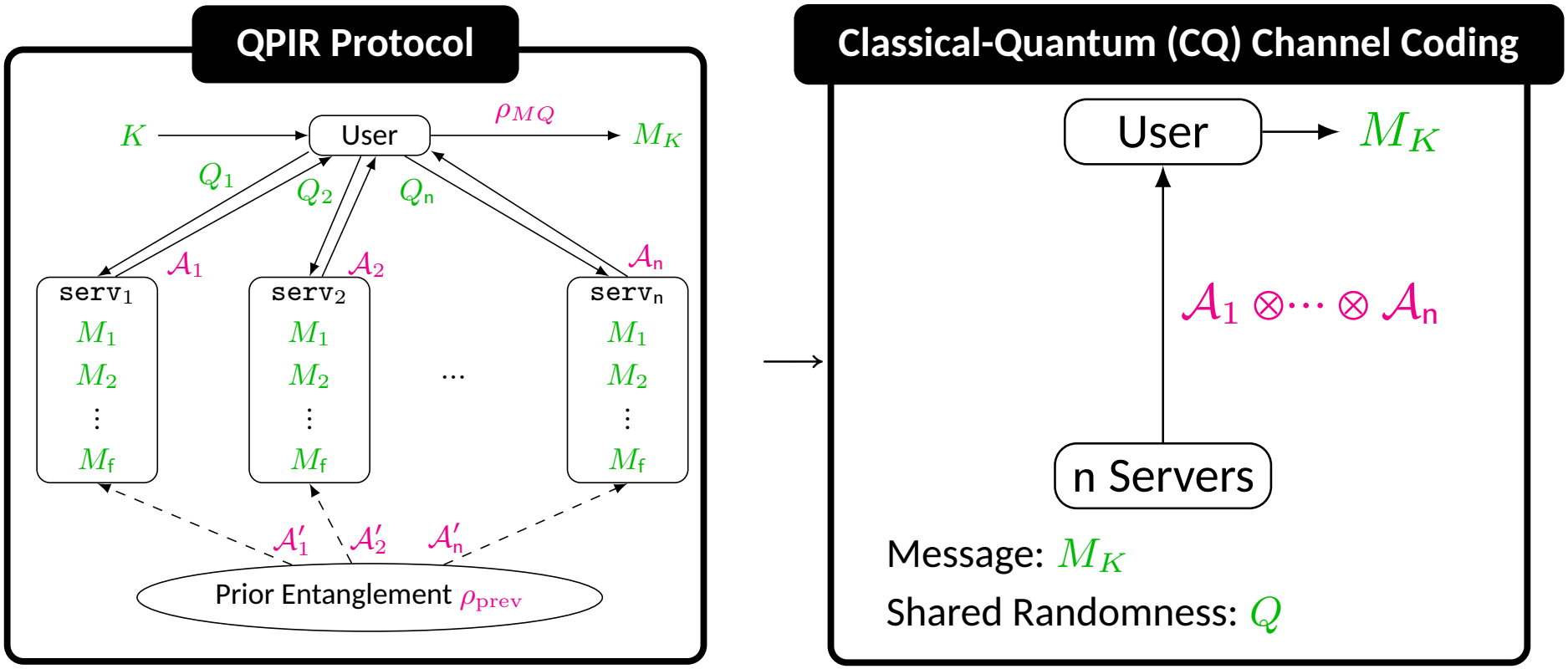
QPIR Protocol

Costs

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



Upper Bound $C \leq 1$

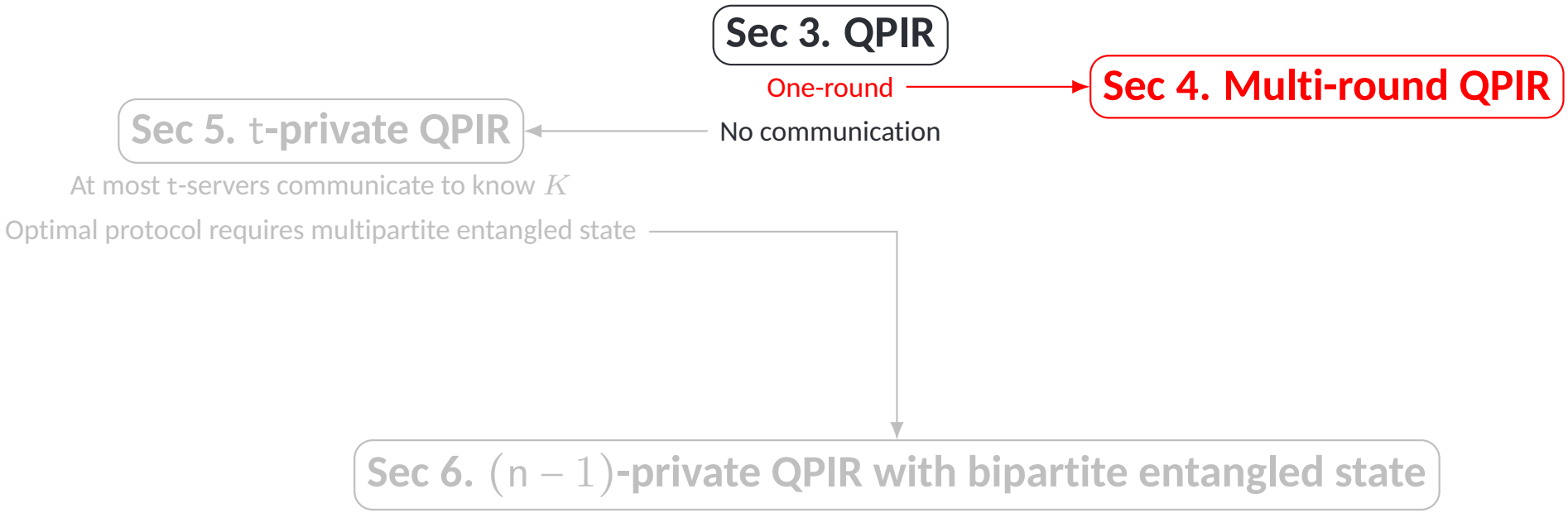


- Noting on the download step, QPIR protocol is reduced to the quantum channel coding.

$$\Longrightarrow \log(\text{Size of } M_K) \leq \log(\text{Dimension of } \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n)$$

$$\Longrightarrow C_{\text{asymp}}^{\alpha,\infty,\infty} = \sup \frac{\log(\text{Size of } M_K)}{\log(\text{Dimension of } \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n)} \leq 1.$$

Contents



Publications

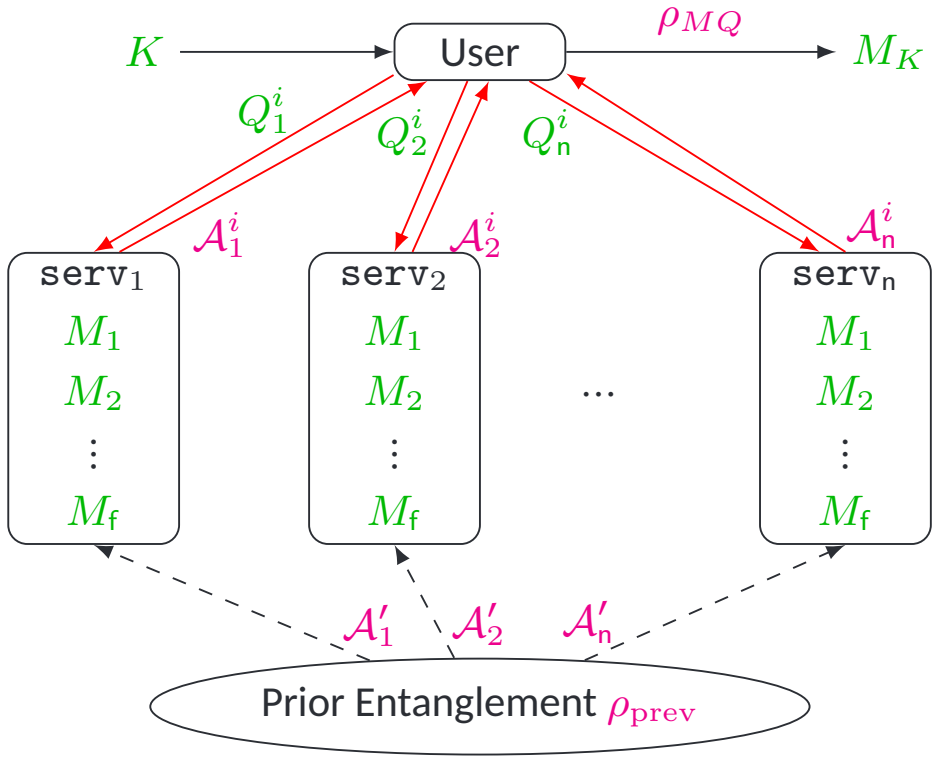
[1] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, accepted.

[2] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019 (submitted to *Journal on Selected Areas in Information Theory*).

[3] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1077–1082, 2020 (submitted to *IEEE Transactions on Information Theory*).

r-Round QPIR Protocol

r-Round QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m},\mathsf{r})}$: QPIR with querying and answering r times.



- Security measures
  - Error probability P_{err}
  - Server secrecy S_{serv}
  - User secrecy S_{serv}
- QPIR rate $R \coloneqq \dfrac{(\text{Size of } M_K)}{(\text{Total download size})} = \dfrac{\log \mathsf{m}}{\sum_{i=1}^{\mathsf{r}} \sum_{j=1}^{\mathsf{n}} \log \dim \mathcal{A}_j^i}$.

r-Round QPIR Capacity

r-Round QPIR capacities

$$C_{\text{exact}}^{\alpha,\beta,\gamma,(\mathsf{r})} \coloneqq \sup\left\{R \,\middle|\, P_{\text{err}} \le \alpha,\ S_{\text{serv}} \le \beta,\ S_{\text{serv}} \le \gamma\right\},$$

$$C_{\text{asymp}}^{\alpha,\beta,\gamma,(\mathsf{r})} \coloneqq \sup_{\{\Psi_{\text{QPIR}}^{(\mathsf{m},\mathsf{r})}\}_{\mathsf{m}=1}^{\infty}} \left\{ \lim_{\mathsf{m}\to\infty} R^{(\mathsf{m})} \,\middle|\, \lim_{\mathsf{m}\to\infty} (P_{\text{err}}^{(\mathsf{m})}, S_{\text{serv}}^{(\mathsf{m})}, S_{\text{serv}}^{(\mathsf{m})}) \le (\alpha,\beta,\gamma) \right\}.$$

- From definitions, $C_{\text{exact}}^{0,0,0,(\mathsf{r})} \le C_{\text{exact}}^{\alpha,\beta,\gamma,(\mathsf{r})} \le C_{\text{asymp}}^{\alpha,\beta,\gamma,(\mathsf{r})} \le C_{\text{asymp}}^{\alpha,\infty,\infty,(\mathsf{r})}$.
- $C_{\text{exact}}^{0,\beta,0,(\mathsf{r})}, C_{\text{asymp}}^{0,\beta,0,(\mathsf{r})}$: r-round QPIR capacity.
- $C_{\text{exact}}^{0,0,0,(\mathsf{r})}, C_{\text{asymp}}^{0,0,0,(\mathsf{r})}$: symmetric r-round QPIR capacity.
- Theorem 3.1 is written as

$$C_{\text{exact}}^{\alpha,\beta,\gamma,(1)} = C_{\text{asymp}}^{\alpha,\beta,\gamma,(1)} = 1 \quad (\forall \alpha,\beta,\gamma).$$

- For any $\mathsf{r} < \mathsf{r}'$,

$$C_{\text{exact}}^{\alpha,\beta,\gamma,(\mathsf{r})} \le C_{\text{exact}}^{\alpha,\beta,\gamma,(\mathsf{r}')}, \quad C_{\text{asymp}}^{\alpha,\beta,\gamma,(\mathsf{r})} \le C_{\text{asymp}}^{\alpha,\beta,\gamma,(\mathsf{r}')}$$

r-Round QPIR Capacity

(α: error bound, β: server secrecy bound, γ: user secrecy bound)

Theorem 4.1: Multi-round QPIR capacity

The r-round QPIR capacity for f ≥ 2 messages and n ≥ 2 servers is

$$C_{\text{exact}}^{0,\beta,\gamma,(\mathsf{r})} = C_{\text{asymp}}^{0,\beta,\gamma,(\mathsf{r})} = 1$$

for any $\beta, \gamma \in [0, \infty]$.

- For any r $<$ r$'$,

$$C_{\text{exact}}^{0,\beta,\gamma,(\mathsf{r})} = C_{\text{exact}}^{0,\beta,\gamma,(\mathsf{r}')} = 1,$$
$$C_{\text{asymp}}^{0,\beta,\gamma,(\mathsf{r})} = C_{\text{asymp}}^{0,\beta,\gamma,(\mathsf{r}')} = 1$$

(Proof)

$$\underbrace{1 = C_{\text{exact}}^{0,\beta,\gamma,(1)}}_{\text{Theorem 3.1}} \leq C_{\text{exact}}^{0,\beta,\gamma,(\mathsf{r})} \leq C_{\text{asymp}}^{0,\beta,\gamma,(\mathsf{r})} \leq \underbrace{C_{\text{asymp}}^{0,\infty,\infty,(\mathsf{r})} \leq 1}_{\text{Upper Bound}}$$

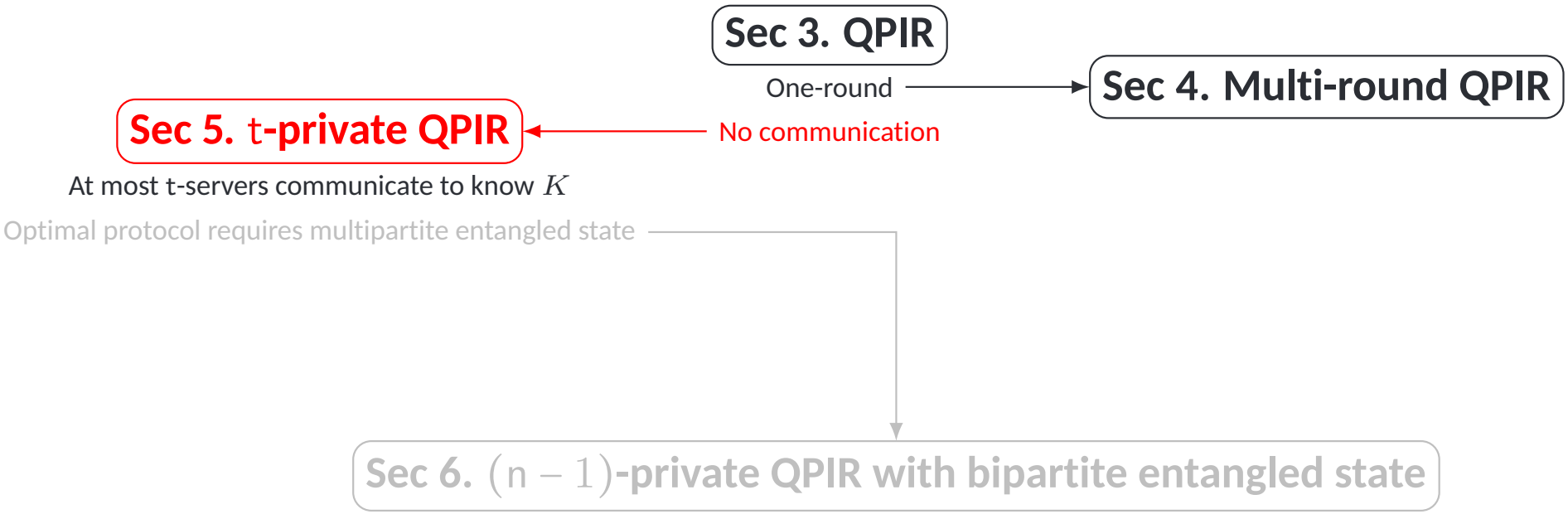
Classical PIR vs Quantum PIR Capacities (n servers, f messages, t colluding servers)

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 ‡
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1
Symmetric multi-round PIR	-	
t-Private PIR	$\frac{1-t/n}{1-(t/n)^f}$ [Sun-Jafar16-2]	1 for $t \leq \frac{n}{2}$, ‡ $2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ ‡
Symmetric t-private PIR	$\frac{n-t}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

Contents



Publications

[1] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, accepted.

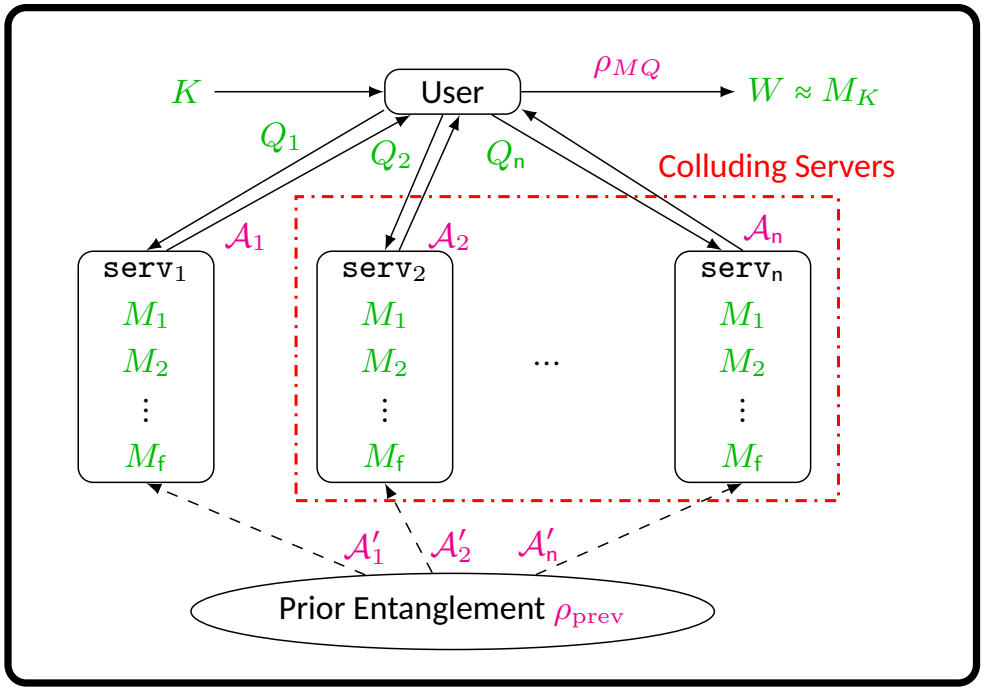
[2] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019 (submitted to *Journal on Selected Areas in Information Theory*).

[3] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1077–1082, 2020 (submitted to *IEEE Transactions on Information Theory*).

Formal Definition of t-Private QPIR Protocol $\Psi_{\text{QPIR}}^{(\mathsf{m})}$

t-Private QPIR

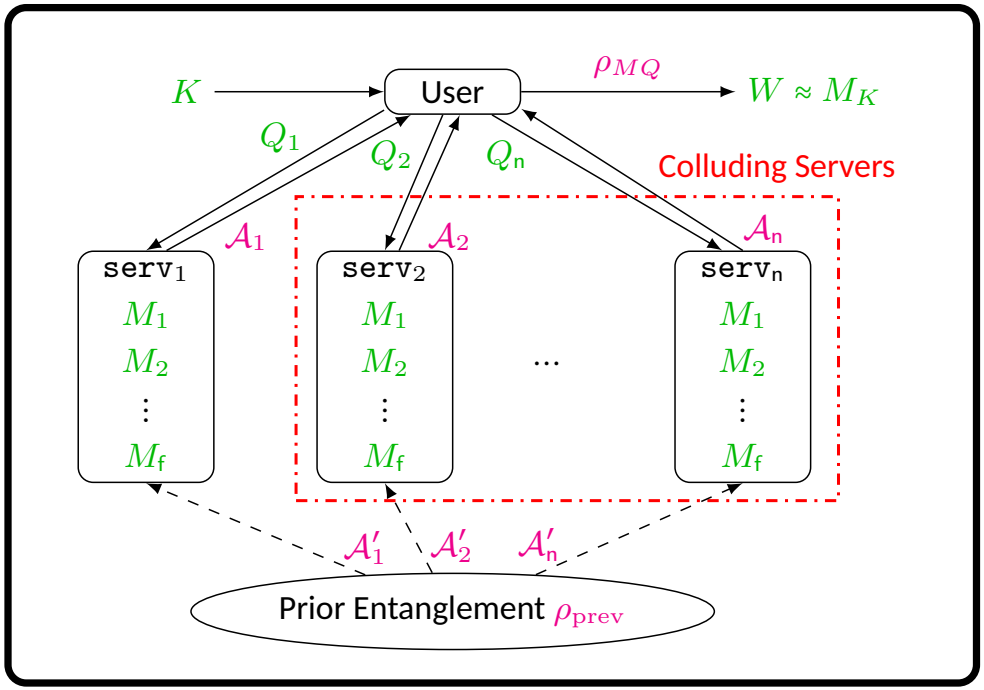
- At most t servers collude to know K.
- User doesn't know which servers are colluding.
- 1-Private QPIR is the QPIR in Section 3.



Formal Definition of t-Private QPIR Protocol $\Psi^{(\mathrm{m})}_{\mathrm{QPIR}}$

t-Private QPIR

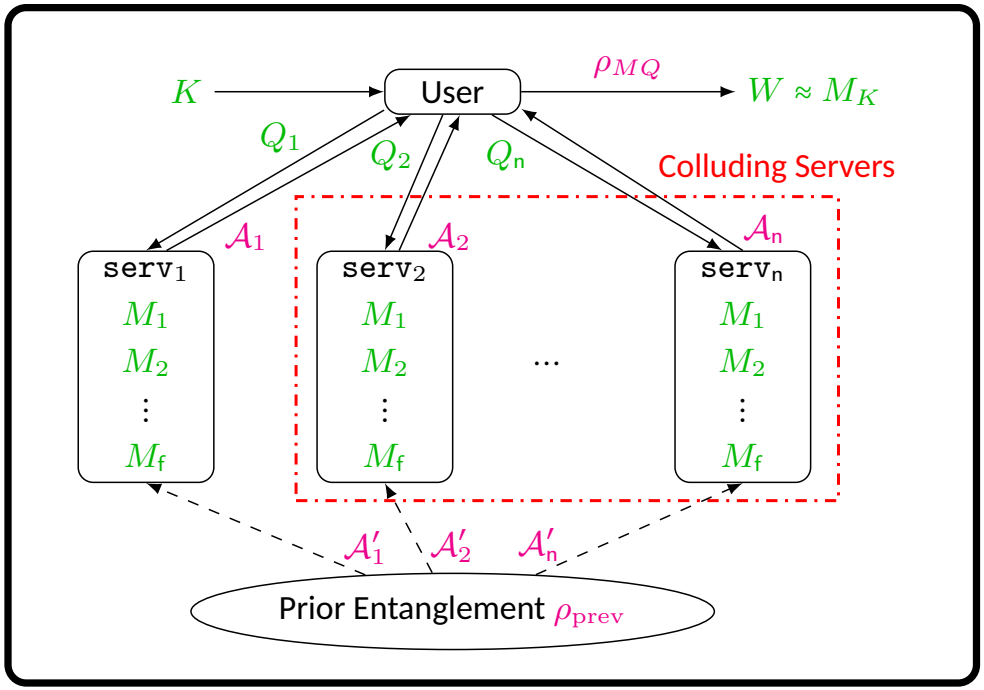
- At most t servers collude to know K.
- User doesn't know which servers are colluding.
- 1-Private QPIR is the QPIR in Section 3.



Security measures

- Error probability P_{err}
- Server secrecy S_{serv}
- User t-secrecy $S_{\mathrm{user,t}}$

Formal Definition of t-Private QPIR Protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$



t-Private QPIR

- At most t servers collude to know K.
- User doesn't know which servers are colluding.
- 1-Private QPIR is the QPIR in Section 3.

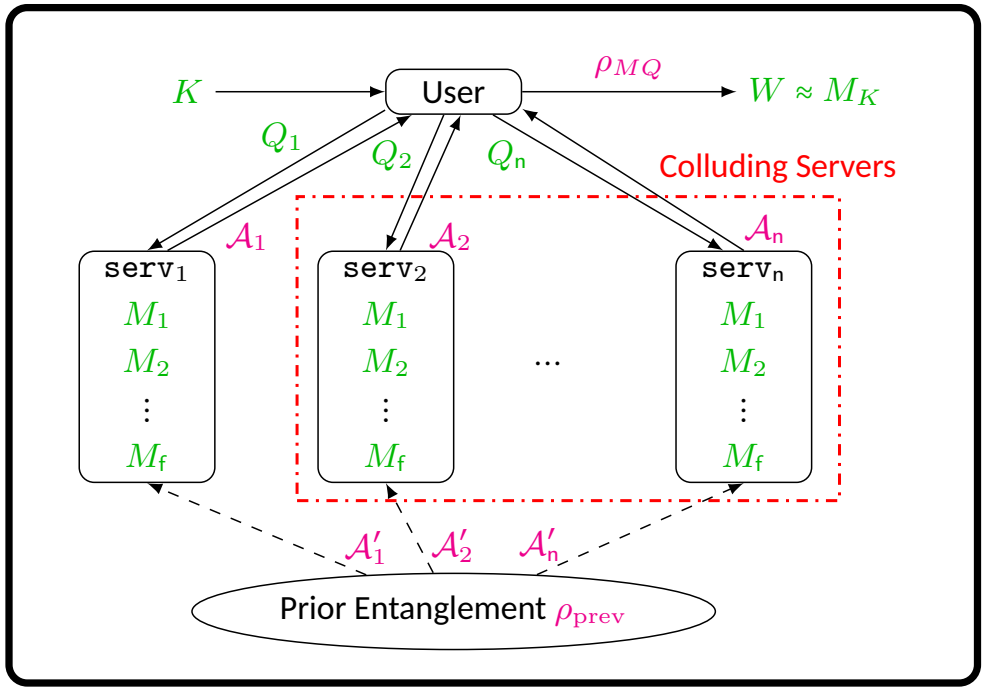
Security measures

- Error probability $P_{\mathrm{err}} \coloneqq \Pr_W[W \neq M_K | MKQ] \in [0,1]$.
- Server secrecy $S_{\mathrm{serv}} \coloneqq I(M_K^c; \mathfrak{user} | K) \geq 0$.
- User t-secrecy $S_{\mathrm{user},\mathsf{t}} \coloneqq \max_{\pi \in \mathrm{perm}(\mathsf{n})} I(K; Q_{\pi(1)} \dots Q_{\pi(\mathsf{t})}) \geq 0$.

Formal Definition of t-Private QPIR Protocol $\Psi^{(\mathsf{m})}_{\mathrm{QPIR}}$

t-Private QPIR

- At most t servers collude to know K.
- User doesn't know which servers are colluding.
- 1-Private QPIR is the QPIR in Section 3.



Security measures

- Error probability $P_{\mathrm{err}} \coloneqq \Pr_W[W \neq M_K | MKQ] \in [0,1]$.
- Server secrecy $S_{\mathrm{serv}} \coloneqq I(M_K^c; \mathfrak{user} | K) \geq 0$.
- User t-secrecy $S_{\mathrm{user},\mathsf{t}} \coloneqq \max_{\pi \in \mathrm{perm}(\mathsf{n})} I(K; Q_{\pi(1)} \dots Q_{\pi(\mathsf{t})}) \geq 0$.

QPIR rate is # of retrieved bits per 1-qubit download.

$$R \coloneqq \frac{(\text{Size of } M_K)}{(\text{Total download size})} = \frac{\log \mathsf{m}}{\sum_{j=1}^{\mathsf{n}} \log \dim \mathcal{A}_j} \ [\text{bit/qubit}].$$

t-Private QPIR Capacity

t-private QPIR capacity is the supremum of QPIR rate given the numbers of servers n and messages f.

Exact security-constrained capacity

$$C_{\text{exact,t}}^{\alpha,\beta,\gamma} \coloneqq \sup\left\{ R \,\middle|\, (*1) \right\},$$

$$(*1) = \begin{cases} P_{\text{err}} \le \alpha, \\ S_{\text{serv}} \le \beta, \\ S_{\text{user,t}} \le \gamma, \end{cases}$$

Asymptotic security-constrained capacity

$$C_{\text{asymp,t}}^{\alpha,\beta,\gamma} \coloneqq \sup_{\{\Psi_{\text{QPIR}}^{(m)}\}_{m=1}^{\infty}} \left\{ \lim_{m\to\infty} R^{(m)} \,\middle|\, (*2), \right\}$$

$$(*2) = \begin{cases} \limsup_{m\to\infty} P_{\text{err}}^{(m)} \le \alpha, \\ \limsup_{m\to\infty} S_{\text{serv}}^{(m)} \le \beta, \\ \limsup_{\ell\to m} S_{\text{user,t}}^{(m)} \le \gamma. \end{cases}$$

- From definitions, $C_{\text{exact,t}}^{0,0,0} \le C_{\text{exact,t}}^{\alpha,\beta,\gamma} \le C_{\text{asymp,t}}^{\alpha,\beta,\gamma} \le C_{\text{asymp,t}}^{\alpha,\infty,\infty}$.
- $C_{\text{exact,t}}^{0,\beta,0}, C_{\text{asymp}}^{0,\beta,0}$: t-private QPIR capacity.
- $C_{\text{exact,t}}^{0,0,0}, C_{\text{asymp}}^{0,0,0}$: symmetric t-private QPIR capacity.
- From Theorem 3.1, $C_{\text{exact,1}}^{\alpha,\beta,\gamma} = C_{\text{asymp,1}}^{\alpha,\beta,\gamma} = 1$.

Main Theorem

(α: error bound, β: server secrecy bound, γ: user secrecy bound)

Theorem 5.1: t-Private QPIR Capacity

The t-private QPIR capacity with $f \geq 2$ messages, $n \geq 2$ servers, and $1 \leq t < n$ colluding servers is

$$C_{\text{asymp,t}}^{\alpha,\beta,\gamma} = C_{\text{exact,t}}^{\alpha,\beta,\gamma} = 1 \qquad \text{if } 1 \leq t \leq \frac{n}{2}, \tag{2}$$

$$C_{\text{asymp,t}}^{0,\beta,0} = C_{\text{exact,t}}^{\alpha,0,0} = \frac{2(n-t)}{n} \qquad \text{if } \frac{n}{2} < t < n. \tag{3}$$

(Proof)

1. Optimal Protocol Construction

$$\min\left\{1, \frac{2(n-t)}{n}\right\} \leq C_{\text{exact,t}}^{0,0,0}.$$

2. Upper Bounds

$$C_{\text{asymp,t}}^{\alpha,\beta,\gamma} \leq 1 \qquad \text{if } 1 \leq t \leq \frac{n}{2},$$

$$C_{\text{exact,t}}^{\alpha,0,0} \leq \frac{2(n-t)}{n} \qquad \text{if } \frac{n}{2} < t < n,$$

$$C_{\text{asymp,t}}^{0,\beta,0} \leq \frac{2(n-t)}{n} \qquad \text{if } \frac{n}{2} < t < n.$$

Classical PIR vs Quantum PIR Capacities (n servers, f messages, t colluding servers)

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 ‡
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1
Symmetric multi-round PIR	-	
t-Private PIR	$\frac{1-t/n}{1-(t/n)^f}$ [Sun-Jafar16-2]	1 for $t \leq \frac{n}{2}$, ‡
Symmetric t-private PIR	$\frac{n-t}{n}$ [Wang-Skoglund17] †	$2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ ‡

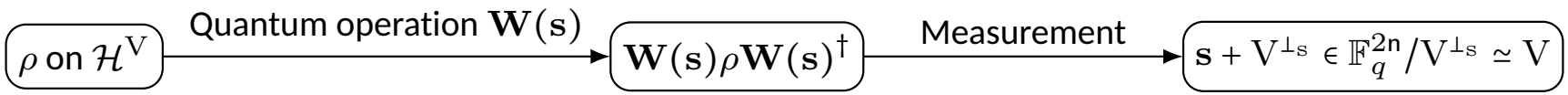
† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathrm{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathrm{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathrm{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_\mathrm{s}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathrm{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathrm{n}+1})\mathsf{Z}(v_{2\mathrm{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)



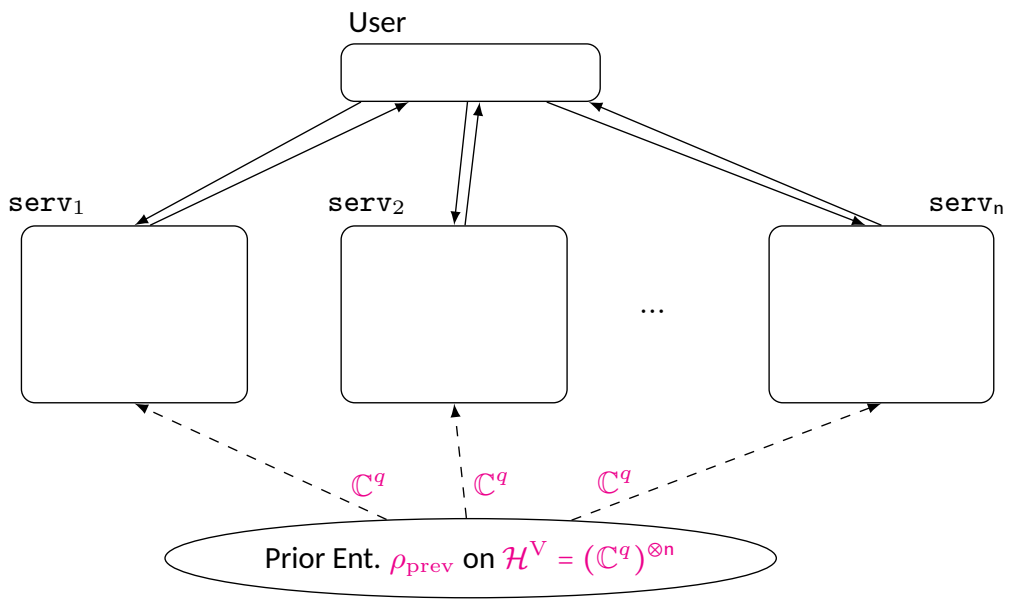
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathrm{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathrm{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathrm{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathrm{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathrm{n}+1})\mathsf{Z}(v_{2\mathrm{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → (Quantum operation $\mathbf{W}(\mathbf{s})$) → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → (Measurement) → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathrm{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



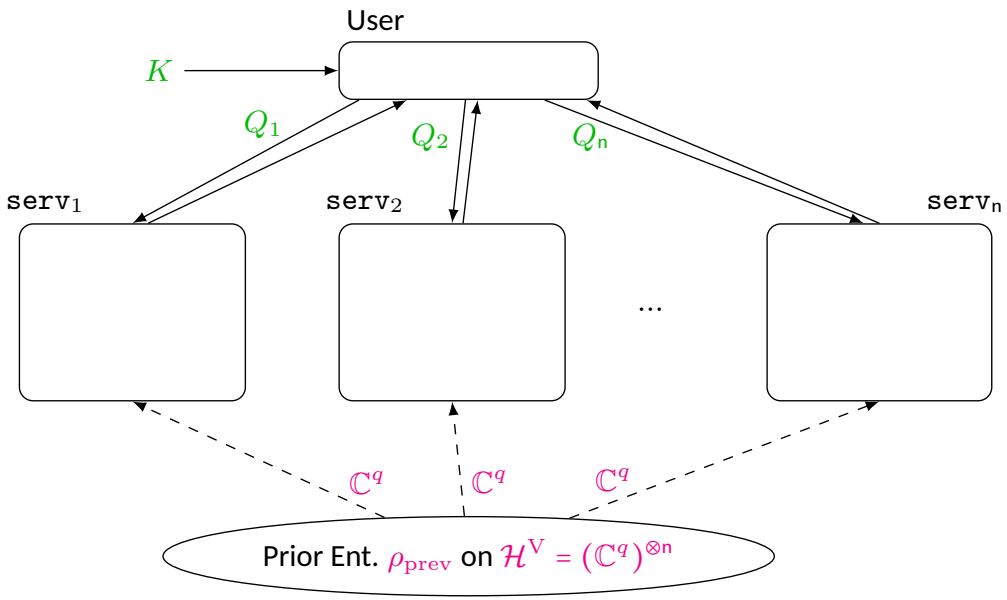
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → Quantum operation $\mathbf{W}(\mathbf{s})$ → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → Measurement → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



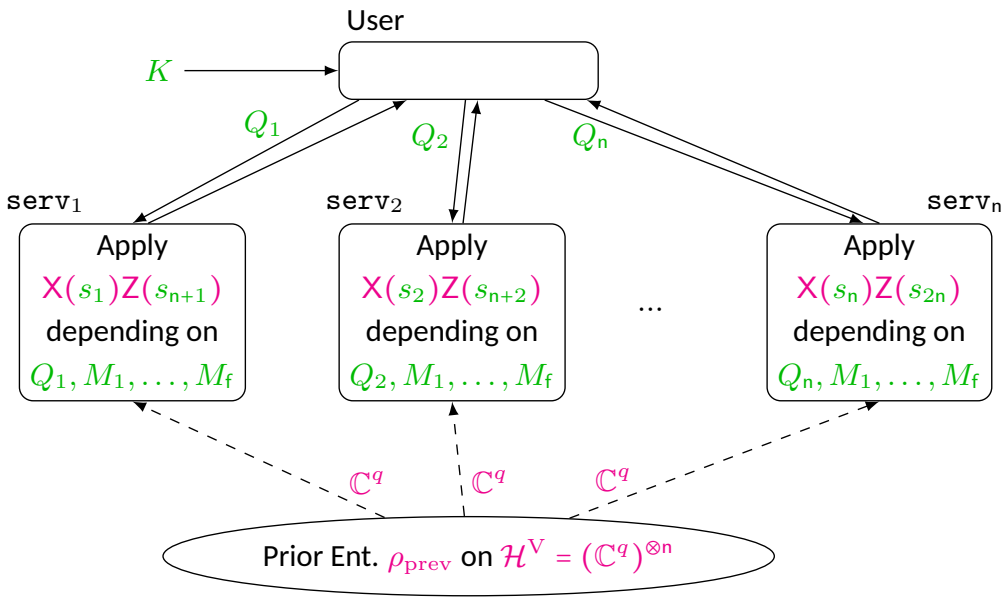
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → Quantum operation $\mathbf{W}(\mathbf{s})$ → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → Measurement → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



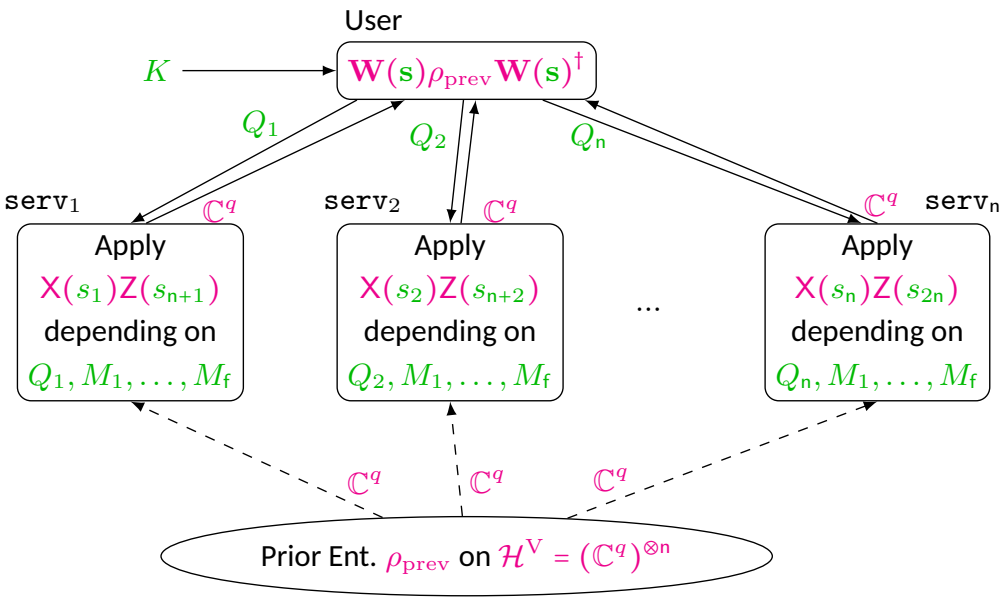
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → Quantum operation $\mathbf{W}(\mathbf{s})$ → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → Measurement → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



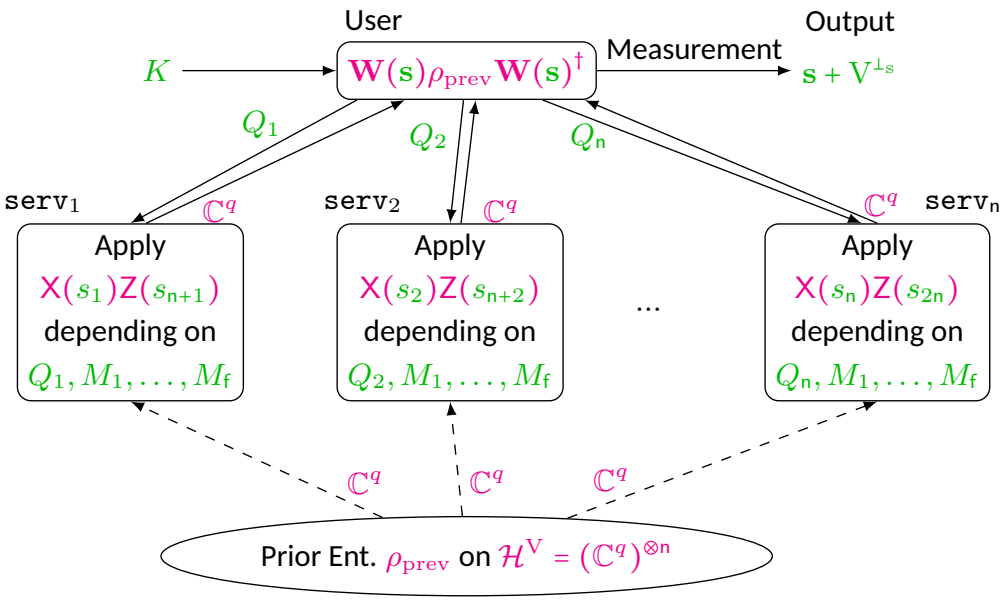
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → Quantum operation $\mathbf{W}(\mathbf{s})$ → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → Measurement → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



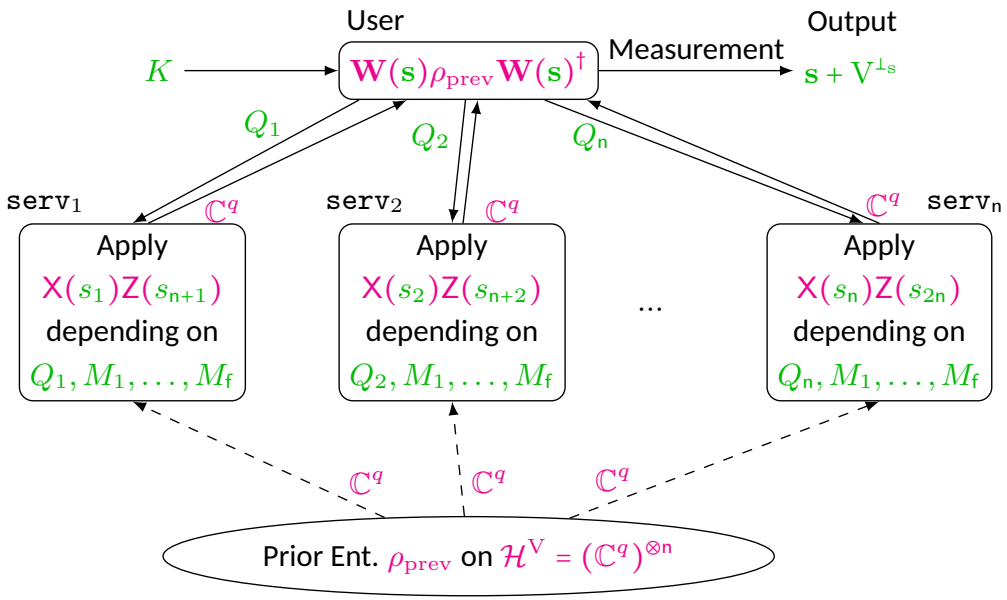
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → (Quantum operation $\mathbf{W}(\mathbf{s})$) → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → (Measurement) → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



← This is not yet QPIR protocol!

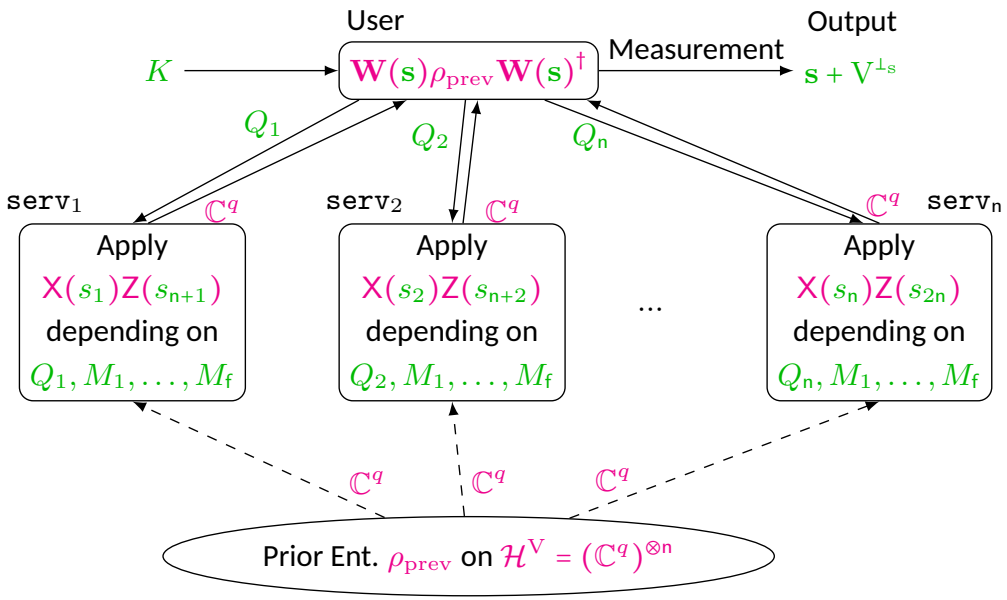
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → (Quantum operation $\mathbf{W}(\mathbf{s})$) → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → (Measurement) → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



← This is not yet QPIR protocol!

QPIR protocol should satisfy

i) $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \simeq M_K$,

ii) user secrecy and server secrecy.

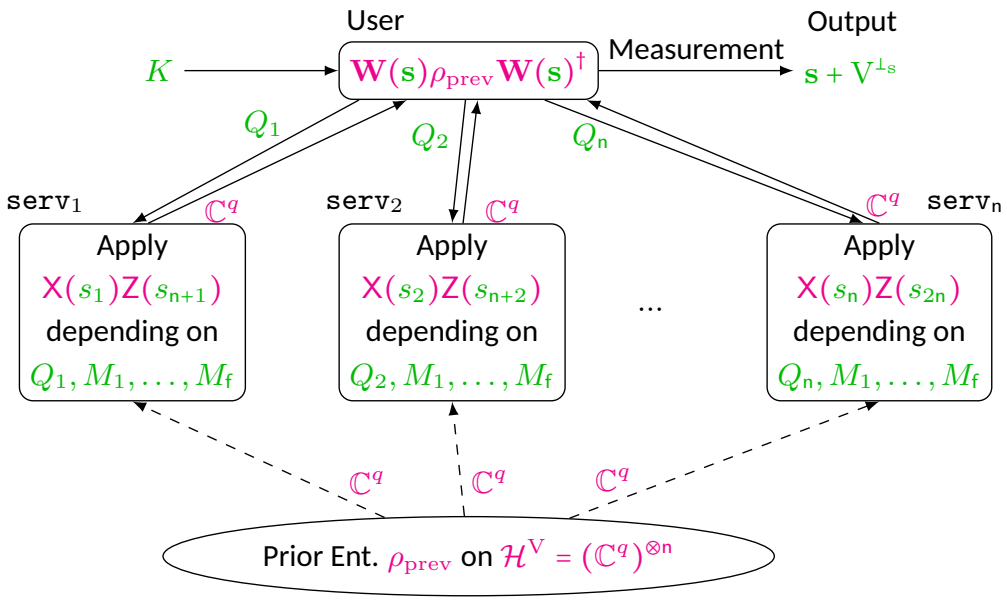
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

ρ on $\mathcal{H}^{\mathrm{V}}$ → (Quantum operation $\mathbf{W}(\mathbf{s})$) → $\mathbf{W}(\mathbf{s})\rho\mathbf{W}(\mathbf{s})^\dagger$ → (Measurement) → $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

t-Private QPIR Protocol



← This is not yet QPIR protocol!

QPIR protocol should satisfy

i) $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \simeq M_K$,

ii) user secrecy and server secrecy.

i), ii) are satisfied by *finding good* V.

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2\mathsf{n}}^\top)^\top \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{t}}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\}$, $\mathrm{V}^{\perp_\mathsf{s}} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_\mathsf{s}}$.

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{t})}, \mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are *linearly independent* for any $\pi \in \mathrm{perm}(\mathsf{n})$.

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2\mathsf{n}}^\top)^\top \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{t}}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\}$, $\mathrm{V}^{\perp_\mathsf{s}} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_\mathsf{s}}$.

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{t})}, \mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are *linearly independent* for any $\pi \in \mathrm{perm}(\mathsf{n})$.

- (a) defines *stabilizer*
- (b) is used for *secrecy* in our protocol.

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2\mathsf{n}}^\top)^\top \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{t}}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\}$, $\mathrm{V}^{\perp_{\mathrm{s}}} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{t})}, \mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are *linearly independent* for any $\pi \in \mathrm{perm}(\mathsf{n})$.

- (a) defines *stabilizer*
- (b) is used for *secrecy* in our protocol.

Classical Version of Lemma 5.2: (b') Any t rows of $D \in \mathbb{F}_q^{\mathsf{n}\times\mathsf{t}}$ are *linearly independent*.

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2\mathsf{n}}^\top)^\top \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{t}}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\}$, $\mathrm{V}^{\perp_{\mathrm{s}}} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{t})}, \mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are *linearly independent* for any $\pi \in \mathrm{perm}(\mathsf{n})$.

- (a) defines *stabilizer*
- (b) is used for *secrecy* in our protocol.

Classical Version of Lemma 5.2: (b') Any t rows of $D \in \mathbb{F}_q^{\mathsf{n}\times\mathsf{t}}$ are *linearly independent*.

- (b') has been used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(\mathsf{n}-\mathsf{t})$ symbols by using n symbols.

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \dots, \mathbf{v}_{2t}) = (\mathbf{w}_1^\top, \dots, \mathbf{w}_{2n}^\top)^\top \in \mathbb{F}_q^{2n \times 2t}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \dots, \mathbf{v}_{2n-2t}\}$, $\mathrm{V}^{\perp_s} = \mathrm{span}\{\mathbf{v}_1, \dots, \mathbf{v}_{2t}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_s}$.

(b) $\mathbf{w}_{\pi(1)}, \dots, \mathbf{w}_{\pi(t)}, \mathbf{w}_{\pi(1)+n}, \dots, \mathbf{w}_{\pi(t)+n}$ are *linearly independent* for any $\pi \in \mathrm{perm}(n)$.

- (a) defines *stabilizer*
- (b) is used for *secrecy* in our protocol.

Classical Version of Lemma 5.2: (b') Any t rows of $D \in \mathbb{F}_q^{n \times t}$ are *linearly independent*.

- (b') has been used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(n - t)$ symbols by using n symbols.

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = D \begin{pmatrix} r_1 \\ \vdots \\ r_t \end{pmatrix} + \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

When $\mathbf{r}$ is uniformly at random, any t coordinates of $\mathbf{y}$ are also uniformly at random.
If $\mathbf{r}$ is unknown but $\mathbf{y}$ is known, we can obtain $\mathbf{y} + \mathrm{Im}\, D \in \mathbb{F}_q^n / \mathrm{Im}\, D \simeq \mathbb{F}_q^{n-t}$.

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2\mathsf{n}}^\top)^\top \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{t}}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\}$, $\mathrm{V}^{\perp_{\mathrm{s}}} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{t})}, \mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are *linearly independent* for any $\pi \in \mathrm{perm}(\mathsf{n})$.

- (a) defines *stabilizer*
- (b) is used for *secrecy* in our protocol.

Classical Version of Lemma 5.2: (b') Any t rows of $D \in \mathbb{F}_q^{\mathsf{n}\times\mathsf{t}}$ are *linearly independent*.

- (b') has been used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(\mathsf{n}-\mathsf{t})$ symbols by using n symbols.
- In quantum case, we expect that $2(\mathsf{n}-\mathsf{t})$ symbols are transmitted.
  ($\because$ we can use both *bit* and *phase* information)

Outline of Protocol Construction: Finding Good V

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2\mathsf{n}}^\top)^\top \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{t}}$ satisfying the following conditions.

(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{n}-2\mathsf{t}}\}$, $\mathrm{V}^{\perp_\mathrm{s}} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2\mathsf{t}}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_\mathrm{s}}$.

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(\mathsf{t})}, \mathbf{w}_{\pi(1)+\mathsf{n}}, \ldots, \mathbf{w}_{\pi(\mathsf{t})+\mathsf{n}}$ are *linearly independent* for any $\pi \in \mathrm{perm}(\mathsf{n})$.

- (a) defines *stabilizer*
- (b) is used for *secrecy* in our protocol.

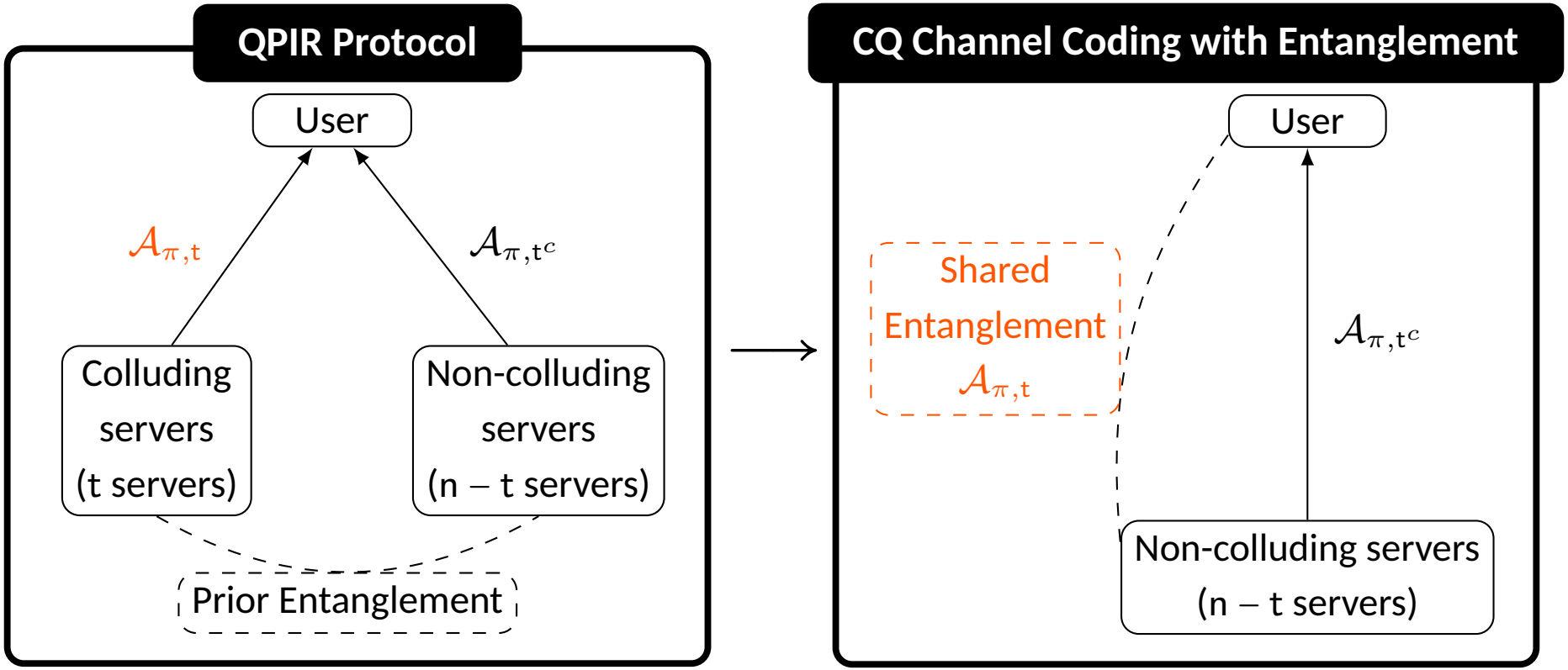
Classical Version of Lemma 5.2: (b') Any t rows of $D \in \mathbb{F}_q^{\mathsf{n}\times\mathsf{t}}$ are *linearly independent*.

- (b') has been used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(\mathsf{n}-\mathsf{t})$ symbols by using n symbols.
- In quantum case, we expect that $2(\mathsf{n}-\mathsf{t})$ symbols are transmitted.
  ($\because$ we can use both *bit* and *phase* information)
- We construct a QPIR protocol that achieves QPIR capacity $\frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}$.

Upper Bounds

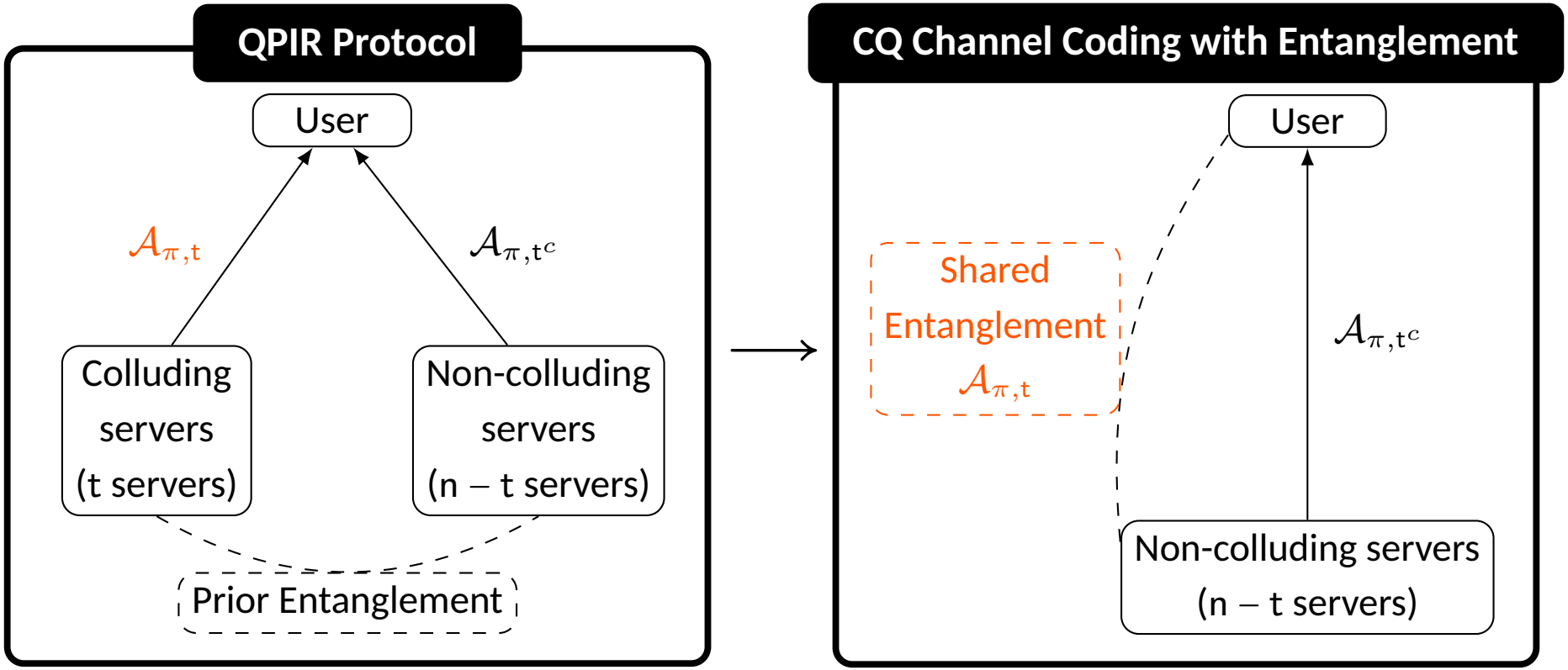
- Two upper bounds
  - $C_t \leq 1$ for $t < \frac{n}{2}$,
  - $C_t \leq \frac{2(n-t)}{n}$ for $t \geq \frac{n}{2}$.

Upper Bound for $t \geq n/2$: $C_t \leq \frac{2(n-t)}{n}$



- From secrecy conditions, $\mathcal{A}_{\pi,t}$ can be considered as shared entanglement.

Upper Bound for $t \geq n/2$: $C_t \leq \frac{2(n-t)}{n}$

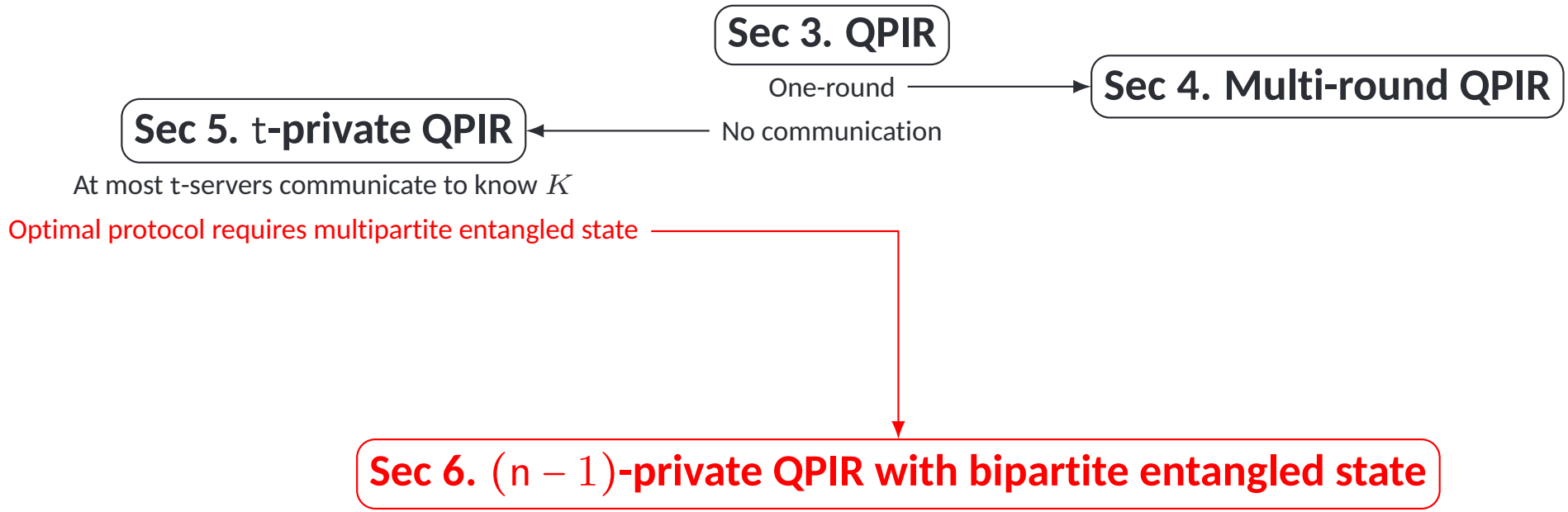


- From secrecy conditions, $\mathcal{A}_{\pi,t}$ can be considered as shared entanglement.

$$\Longrightarrow \log(\text{Size of } M_K) \leq 2\log(\text{Dimension of } \mathcal{A}_{\pi,t^c}) = 2(n-t)\log\dim\mathcal{A}_1$$

$$\Longrightarrow C_t = \sup \frac{\log(\text{Size of } M_K)}{\log(\text{Dim. of } \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n)} \leq \frac{2\log(\text{Dim. of } \mathcal{A}_{\pi,t^c})}{\log(\text{Dim. of } \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n)} = \frac{2(n-t)}{n}.$$

Contents



Publications

[1] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, accepted.

[2] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019 (submitted to *Journal on Selected Areas in Information Theory*).

[3] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Colluding Servers," *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1077–1082, 2020 (submitted to *IEEE Transactions on Information Theory*).

$(n-1)$-Private QPIR Protocol with Bipartite Entanglement

- t-Private QPIR protocol in the previous section requires sharing multipartite entangled state.
- The cost of sharing the multipartite entangled state is expensive.

- Bipartite entangled state $|\Phi\rangle := \frac{1}{2}(|00\rangle + |11\rangle)$
- *1 ebit*: one copy of the state $|\Phi\rangle$.

Theorem 6.1: $(n-1)$-Private QPIR Protocol with Bipartite Entanglement

There exists a ***symmetric*** $(n-1)$***-private QPIR protocol*** with

- **the rate** $\lceil n/2 \rceil^{-1}$**,**
- perfect security,
- nf-bit upload cost,
- 2ℓ-bit messages for any integer $\ell \geq 1$,
- $(\lfloor 3n/2 \rfloor - 2)$ **ebits as prior entanglement.**

Proof Idea: We use the quantum teleportation and dense coding repetitively in PIR.

$(n-1)$-Private QPIR Protocol with Bipartite Entanglement

- t-Private QPIR protocol in the previous section requires sharing multipartite entangled state.
- The cost of sharing the multipartite entangled state is expensive.

- Bipartite entangled state $|\Phi\rangle := \frac{1}{2}(|00\rangle + |11\rangle)$
- *1 ebit*: one copy of the state $|\Phi\rangle$.

Theorem 6.1: $(n-1)$-Private QPIR Protocol with Bipartite Entanglement

There exists a ***symmetric*** $(n-1)$***-private QPIR protocol*** with

- **the rate** $\lceil n/2 \rceil^{-1}$, **(← Achieves $(n-1)$-private QPIR capacity when n is even)**
- perfect security,
- nf-bit upload cost,
- 2ℓ-bit messages for any integer $\ell \geq 1$,
- $(\lfloor 3n/2 \rfloor - 2)$ **ebits as prior entanglement.**

Proof Idea: We use the quantum teleportation and dense coding repetitively in PIR.

Contents

Classical PIR vs Quantum PIR Capacities (n servers, f messages, t colluding servers)

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 ‡
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1
Symmetric multi-round PIR	-	
t-Private PIR	$\frac{1-t/n}{1-(t/n)^f}$ [Sun-Jafar16-2]	1 for $t \leq \frac{n}{2}$, ‡ $2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ ‡
Symmetric t-private PIR	$\frac{n-t}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

Conclusion

- QPIR Capacities
  - QPIR capacity
  - Multi-round QPIR capacity
  - t-private QPIR capacity
  - Symmetric & non-symmetric QPIR
- QPIR capacities are greater than classical PIR capacities.
- We constructed optimal protocols.

Open Problems

- QPIR without prior entanglement
- Trade-off between QPIR capacity and prior entanglement
- QPIR with noisy channels
- Quantum extension of many classical PIR
  - PIR with coded storage
  - Single-server PIR with side information
  - Distributed matrix multiplication
  - Private-set intersection
- QPIR for quantum messages