Capacity of Quantum Private Information Retrieval with Colluding Servers

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

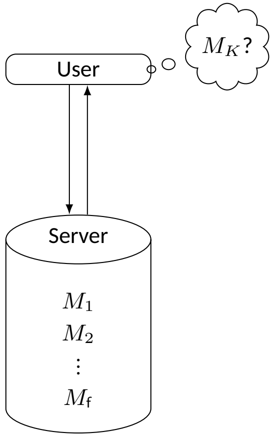
[1] Nagoya University,

[2] Southern University of Science and Technology

AQIS2020

Private Information Retrieval (PIR)

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

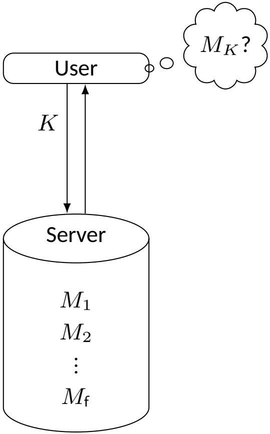


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

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

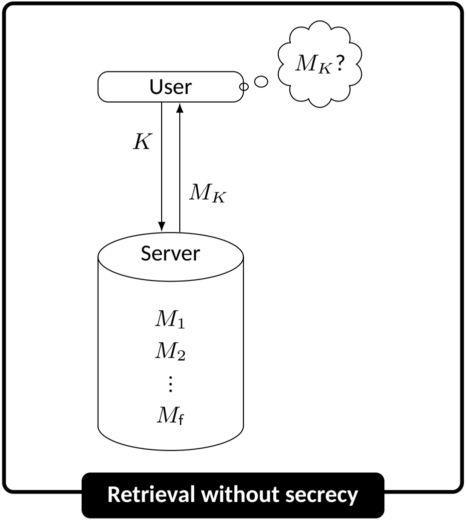


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

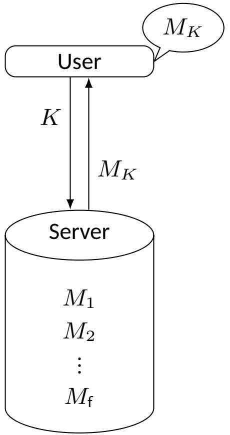
What is PIR? A retrieval protocol without revealing which message is requested. [Chor et al.95].



PIR

Private Information Retrieval (PIR)

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

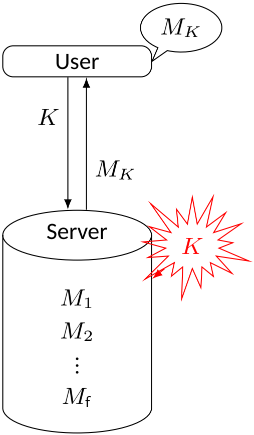


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

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

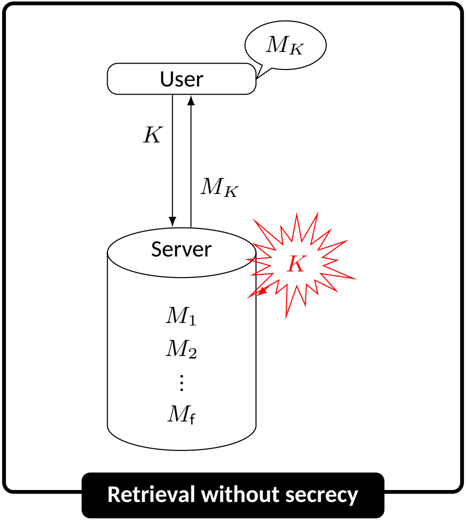


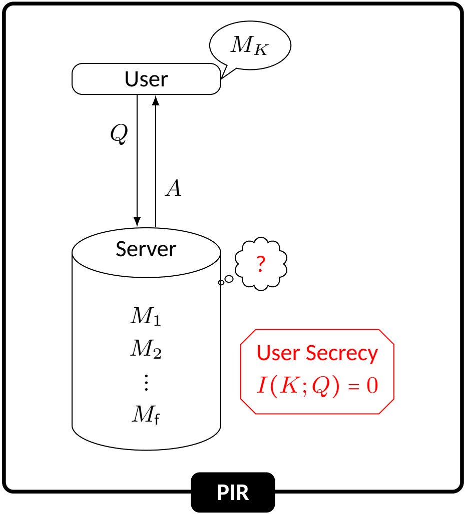
Retrieval without secrecy

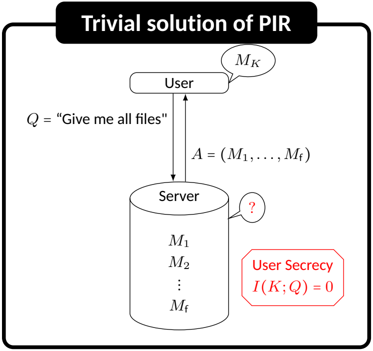
PIR

Private Information Retrieval (PIR)

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







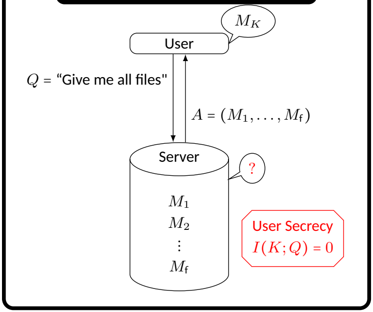
1. One-server PIR

- *PIR rate*

$$R = \frac{\text{(Size of } M_K)}{\text{(Total download size)}} \leq 1.$$

- *PIR rate* of trivial solution is $\frac{1}{f}$.
- *Trivial solution* is optimal [Chor et al.95].

Trivial solution of PIR

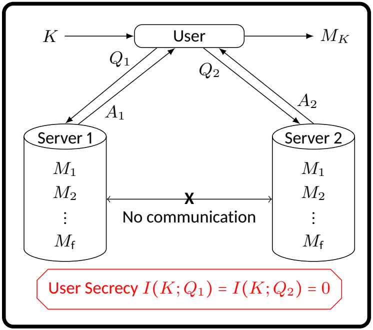


1. One-server PIR

- *PIR rate*

$$R = \frac{(\text{Size of } M_K)}{(\text{Total download size})} \leq 1.$$

- *PIR rate* of trivial solution is $\frac{1}{f}$.
- *Trivial solution* is optimal [Chor et al.95].



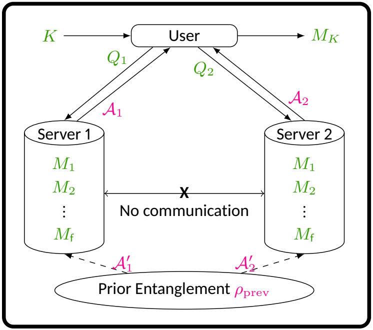
2. Multi-server PIR

- User Secrecy: K is not leaked to each server.

PIR capacity [Sun-Jafar16]

$$C := \sup R = \sup \frac{(\text{Size of } M_K)}{(\text{Total download size})}$$

$$= \frac{1 - n^{-1}}{1 - n^{-f}} \quad \text{for n servers and f files}$$



3. Multi-server QPIR [Song-Hayashi19]

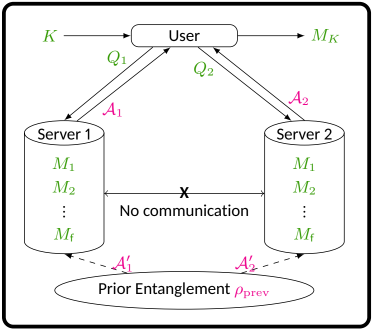
(Green: classical, Magenta: quantum.)

- User Secrecy: K is not leaked to each server.
- *Server Secrecy:* User only obtains M_K.

QPIR capacity [Song-Hayashi19]

$$C := \sup \frac{\text{(Size of } M_K\text{)}}{\text{(Total download size)}}$$

$= 1$ for n ≥ 2 servers and f files



3. Multi-server QPIR [Song-Hayashi19]

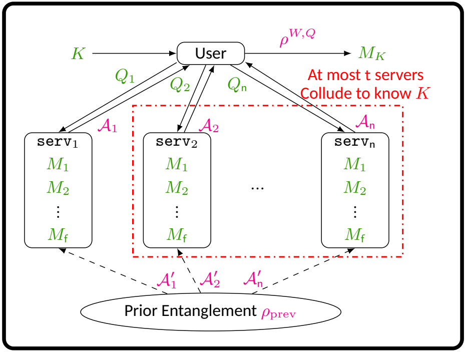
(Green: classical, Magenta: quantum.)

- User Secrecy: K is not leaked to each server.
- *Server Secrecy:* User only obtains M_K.

QPIR capacity [Song-Hayashi19]

$$C := \sup \frac{(\text{Size of } M_K)}{(\text{Total download size})}$$

$$= 1 \quad \text{for n} \geq 2 \text{ servers and f files}$$



4. t-Private QPIR [Our Result] $(1 \leq \mathsf{t} \leq \mathsf{n} - 1)$

- *User t-Secrecy:* K is secret to any t servers.
- Server Secrecy

t-Private QPIR capacity [This Work]

$$C_{\mathsf{t}} := \begin{cases} 1 & \text{if } \mathsf{t} \leq \frac{\mathsf{n}}{2}, \\ \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} & \text{if } \mathsf{t} > \frac{\mathsf{n}}{2}. \end{cases} \quad \text{for n servers}$$

PIR Capacities

(n servers, f files, t colluding servers)

	Secrecy Cond.	Classical Capacity	Quantum Capacity
PIR	User secrecy	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 ‡ [Song-Hayashi19]
Symmetric PIR	User secrecy, Server secrecy	$1-\frac{1}{n}$ [Sun-Jafar17] †	
t-Private PIR	User t-secrecy	$\frac{1}{1-(t/n)^f}\left(\frac{n-t}{n}\right)$ [Sun-Jafar16-2]	1 for $t \leq \frac{n}{2}$, ‡ $2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ ‡
t-Private symmetric PIR	User t-secrecy, Server secrecy	$\frac{n-t}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

‡ Capacities are derived with the strong converse bounds.

Construction of t-Private QPIR Protocol

Construction of t-Private QPIR Protocol

with optimal rate $\frac{2(n-t)}{n}$ for $t \geq \frac{n}{2}$

Are we skipping $t < \frac{n}{2}$? *No! It is automatically constructed.*

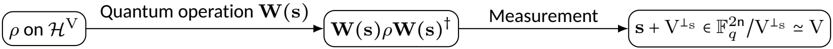
1) Our $\frac{n}{2}$-private protocol achieves the capacity 1.
2) $\frac{n}{2}$-private QPIR is also t-private QPIR for $t < \frac{n}{2}$.

$\Longrightarrow$ Our $\frac{n}{2}$-private protocol achieves t-private QPIR capacity 1 for $t < \frac{n}{2}$.

Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

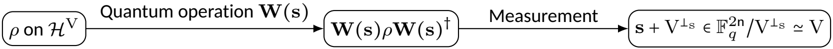
- Hilbert space $(\mathbb{C}^q)^{\otimes \mathsf{n}}$ is related to the finite field vector space $\mathbb{F}_q^{2\mathsf{n}}$.
- Stabilizer is defined from $\mathrm{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ s.t. $\mathrm{V} \subset \mathrm{V}^{\perp_{\mathrm{s}}}$.
- $\mathcal{H}^{\mathrm{V}}$: code space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



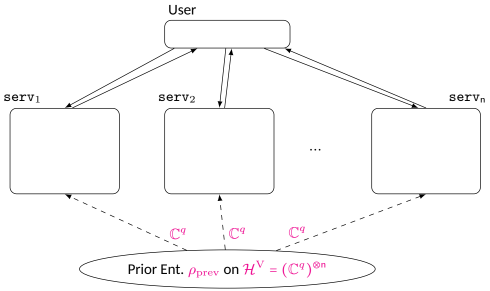
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

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



t-Private QPIR Protocol



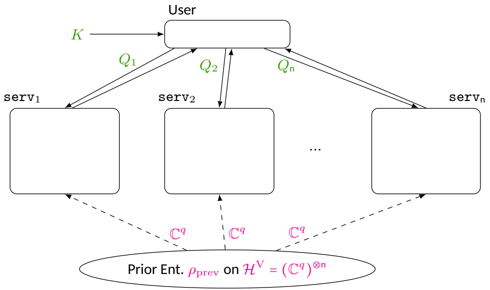
Outline of Protocol Construction (by stabilizer formalism)

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



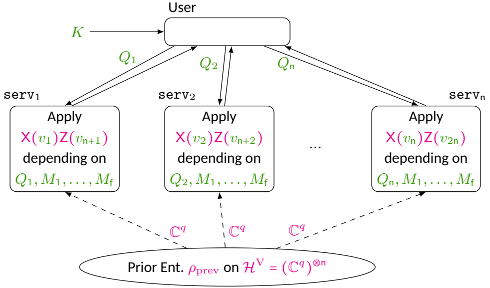
Outline of Protocol Construction (by stabilizer formalism)

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→ $\mathbf{s} + \mathrm{V}^{\perp_{\mathrm{s}}} \in \mathbb{F}_q^{2\mathsf{n}}/\mathrm{V}^{\perp_{\mathrm{s}}} \simeq \mathrm{V}$

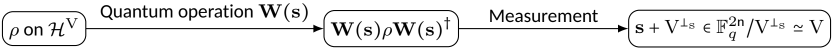
t-Private QPIR Protocol



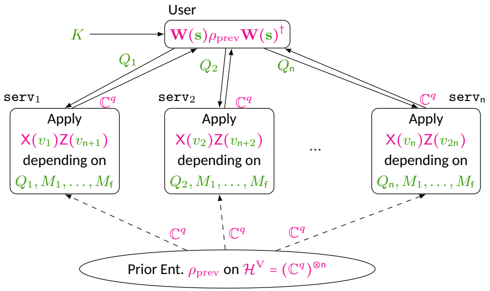
Outline of Protocol Construction (by stabilizer formalism)

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 $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)



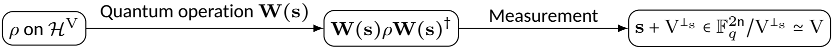
t-Private QPIR Protocol



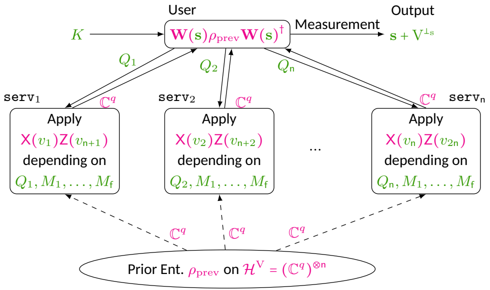
Outline of Protocol Construction (by stabilizer formalism)

Stabilizer Formalism

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



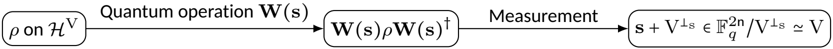
t-Private QPIR Protocol



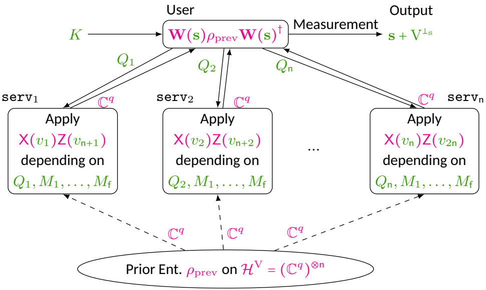
Outline of Protocol Construction (by stabilizer formalism)

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. $\mathrm{V} \subset \mathrm{V}^{\perp_s}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)



t-Private QPIR Protocol

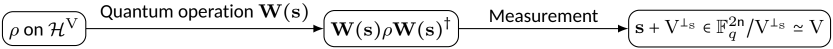


← This is not yet QPIR protocol!

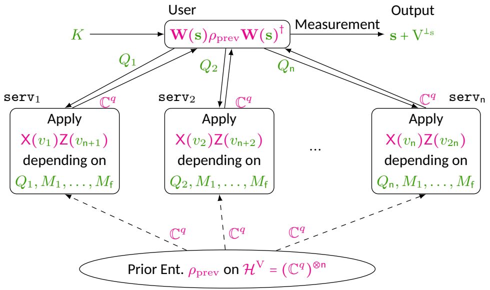
Outline of Protocol Construction (by stabilizer formalism)

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. $\mathrm{V} \subset \mathrm{V}^{\perp_s}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) \coloneqq \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)



t-Private QPIR Protocol



← This is not yet QPIR protocol!

QPIR protocol should satisfy

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

ii) user secrecy and server secrecy.

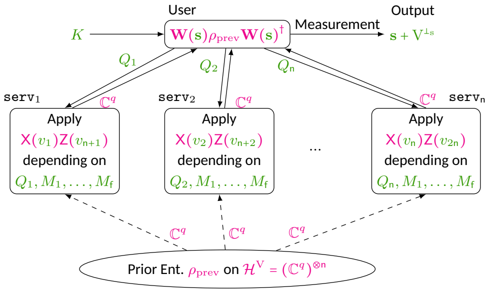
Outline of Protocol Construction (by stabilizer formalism)

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. $\mathrm{V} \subset \mathrm{V}^{\perp_s}$.
- $\mathcal{H}^{\mathrm{V}}$: code space (stabilized by $\mathbf{W}(\mathbf{v}) := \mathsf{X}(v_1)\mathsf{Z}(v_{\mathsf{n}+1}) \otimes \cdots \otimes \mathsf{X}(v_{\mathsf{n}+1})\mathsf{Z}(v_{2\mathsf{n}})$ $(\forall \mathbf{v} \in \mathrm{V})$)

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

t-Private QPIR Protocol



← This is not yet QPIR protocol!

QPIR protocol should satisfy

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

ii) user secrecy and server secrecy.

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

Outline of Protocol Construction: Finding Good V

Good stabilizer V is chosen by the following lemma.

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

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

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

Outline of Protocol Construction: Finding Good V

Good stabilizer V is chosen by the following lemma.

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

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

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

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

Outline of Protocol Construction: Finding Good V

Good stabilizer V is chosen by the following lemma.

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

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

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(t)}, \mathbf{w}_{\pi(1)+n}, \ldots, \mathbf{w}_{\pi(t)+n}$ 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*.

Outline of Protocol Construction: Finding Good V

Good stabilizer V is chosen by the following lemma.

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

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

(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(t)}, \mathbf{w}_{\pi(1)+n}, \ldots, \mathbf{w}_{\pi(t)+n}$ 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') is used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(n - t)$ symbols by using n symbols.

Outline of Protocol Construction: Finding Good V

Good stabilizer V is chosen by the following lemma.

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2t}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2n}^\top)^\top \in \mathbb{F}_q^{2n \times 2t}$ satisfying the following conditions.
(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2n-2t}\}$, $\mathrm{V}^{\perp_s} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2t}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_s}$.
(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(t)}, \mathbf{w}_{\pi(1)+n}, \ldots, \mathbf{w}_{\pi(t)+n}$ 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') is used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(n - t)$ symbols by using n symbols.
- In quantum case, we expect that $2(n - t)$ symbols are transmitted.
  ($\because$ we can use both *bit* and *phase* information)

Outline of Protocol Construction: Finding Good V

Good stabilizer V is chosen by the following lemma.

Lemma 5.2: There exists a matrix $D_1 = (\mathbf{v}_1, \ldots, \mathbf{v}_{2t}) = (\mathbf{w}_1^\top, \ldots, \mathbf{w}_{2n}^\top)^\top \in \mathbb{F}_q^{2n \times 2t}$ satisfying the following conditions.
(a) $\mathrm{V} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2n-2t}\}$, $\mathrm{V}^{\perp_s} = \mathrm{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{2t}\}$, and $\mathrm{V} \subset \mathrm{V}^{\perp_s}$.
(b) $\mathbf{w}_{\pi(1)}, \ldots, \mathbf{w}_{\pi(t)}, \mathbf{w}_{\pi(1)+n}, \ldots, \mathbf{w}_{\pi(t)+n}$ 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*.

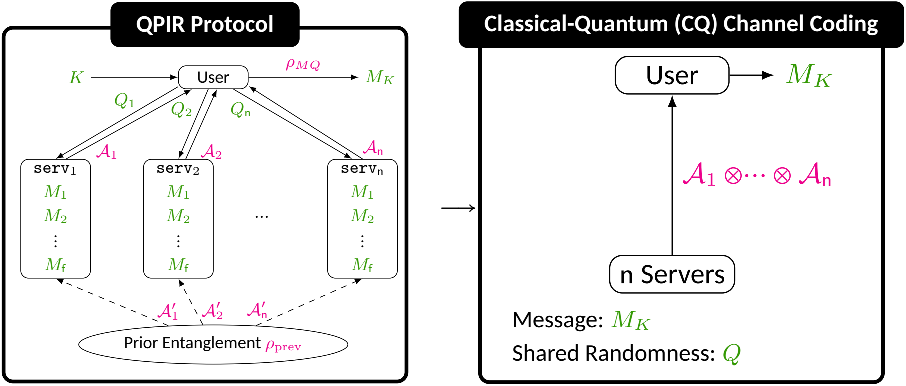
- (b') is used for crypto. protocols (e.g., PIR, secret sharing).
  These protocols transmits $(n - t)$ symbols by using n symbols.
- In quantum case, we expect that $2(n - t)$ symbols are transmitted.
  ($\because$ we can use both *bit* and *phase* information)
- We construct a QPIR protocol that achieves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

Converse Bounds

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

(n servers & t colluding servers)

Converse for $\mathsf{t} \leq \mathsf{n}/2$: $C_{\mathsf{t}} \leq 1$



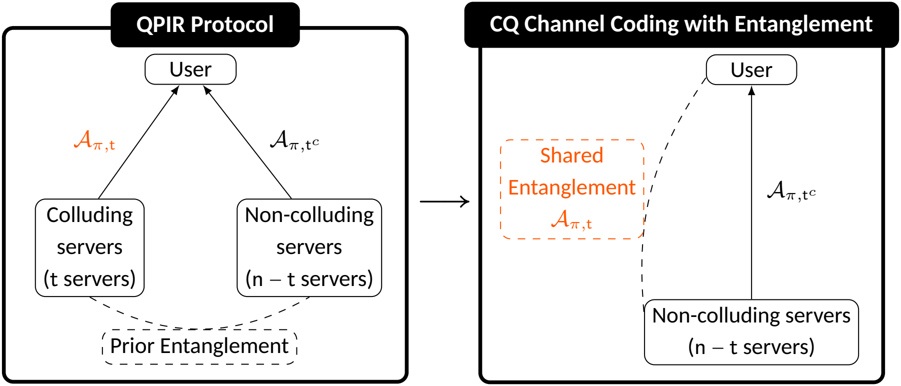
- Noting on the download step, QPIR protocol is reduced to the quantum channel coding.

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

$$\Longrightarrow C_\mathsf{t} = \sup \frac{\log(\text{Size of } M_K)}{\log(\text{Dimension of } \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_\mathsf{n})} \leq 1.$$

Converse for $t > n/2$: $C_t \le \frac{2(n-t)}{n}$

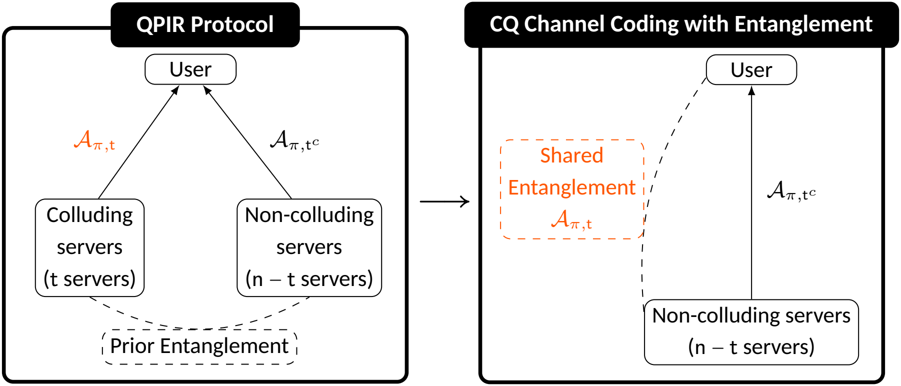
Give the user power to distinguish colluding servers.



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

Converse for $t > n/2$: $C_t \le \frac{2(n-t)}{n}$

Give the user power to distinguish colluding servers.



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

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

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

Conclusion

- t-private QPIR capacity is $\min\left\{1, \frac{2(n-t)}{n}\right\}$.
- We constructed an optimal QPIR protocol with colluding servers.

	Secrecy Cond.	Classical Capacity	Quantum Capacity
PIR	User secrecy	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 [Song-Hayashi19]
Symmetric PIR	User secrecy, Server secrecy	$1-\frac{1}{n}$ [Sun-Jafar17]	
t-**Private PIR**	User t-secrecy	$\frac{1}{1-(t/n)^f}\left(\frac{n-t}{n}\right)$ [Sun-Jafar16-2]	$\min\left\{1, 2\left(\frac{n-t}{n}\right)\right\}$
t-**Private symmetric PIR**	User t-secrecy, Server secrecy	$\frac{n-t}{n}$ [Wang-Skoglund17]	

Open Questions

- Trade-off between the QPIR capacity and the amount of entanglement.
- Quantum extensions of many classical PIR results.
- Application of QPIR to other problems.