Quantum Private Information Retrieval

Seunghoan Song

Nagoya University

SUSTech-Nagoya workshop on Quantum Science

June 22, 2021

Contents

1. Quantum Private Information Retrieval (QPIR) Capacity

2. Construction of QPIR protocol with colluding servers
   - Symplectic matrix over finite field with a certain condition: Existence & Minimum Field Size.

[1] S. Song and M. Hayashi, “Capacity of Quantum Private Information Retrieval with Multiple Servers,” *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 452–463, 2021.

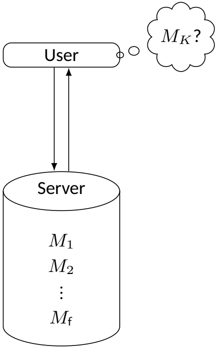
[2] S. Song and M. Hayashi, “Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers,” *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 380–390, 2021.

[3] S. Song and M. Hayashi, “Capacity of Quantum Private Information Retrieval with Colluding Servers,” *IEEE Transactions on Information Theory*, accepted.

[4] M. Allaix, S. Song, L. Holzbaur, T. Pllaha, M. Hayashi, and C. Hollanti, “On the Capacity of Quantum Private Information Retrieval from MDS-Coded and Colluding Servers,” arXiv preprint, 2021.

Private Information Retrieval (PIR)

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

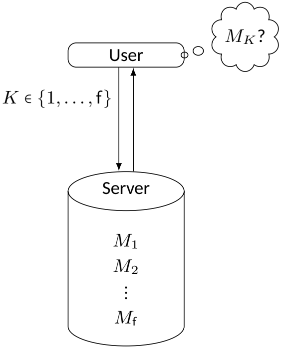


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

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

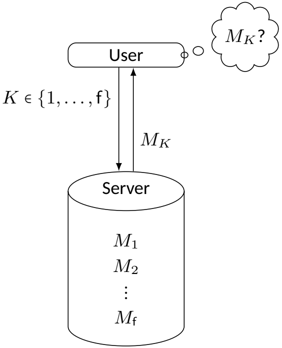


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

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

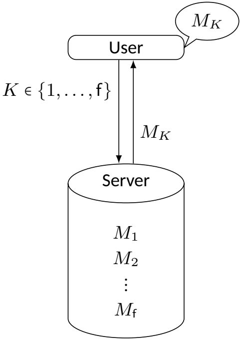


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

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

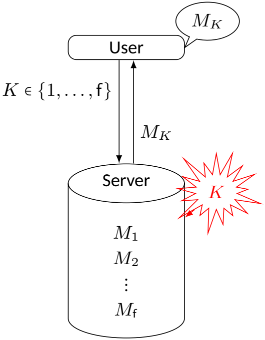


Retrieval without secrecy

PIR

Private Information Retrieval (PIR)

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



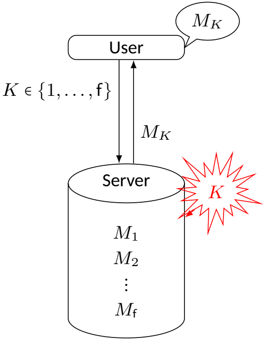
- Correctness: User retrieves M_K.

Retrieval without secrecy

PIR

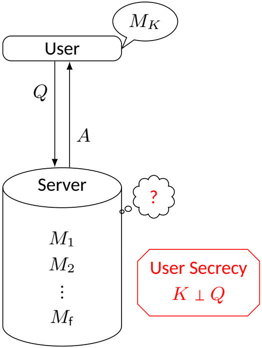
Private Information Retrieval (PIR)

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



- Correctness: User retrieves M_K.

Retrieval without secrecy

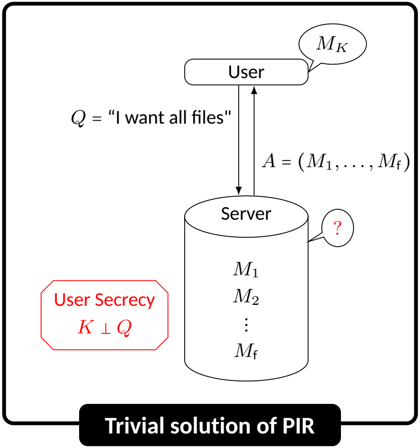


- Correctness: User retrieves M_K.
- User secrecy: Server does not know K.

PIR

Solutions for PIR

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

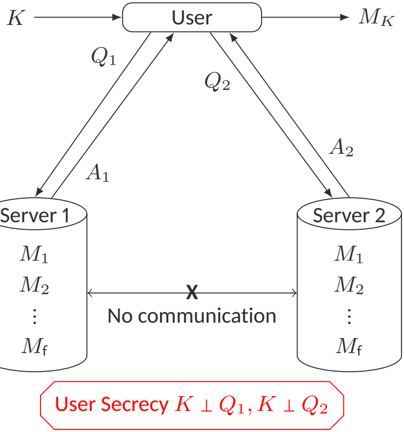


There have been two approaches to find efficient PIR protocols.

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

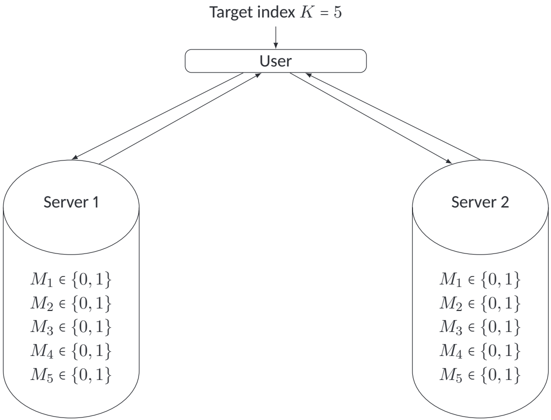
This talk only treats 2.

Multi-Server PIR



- Servers do not communicate with each other.
- User secrecy is $K \perp Q_j$ for all j.
- Most protocols are one-round protocols.

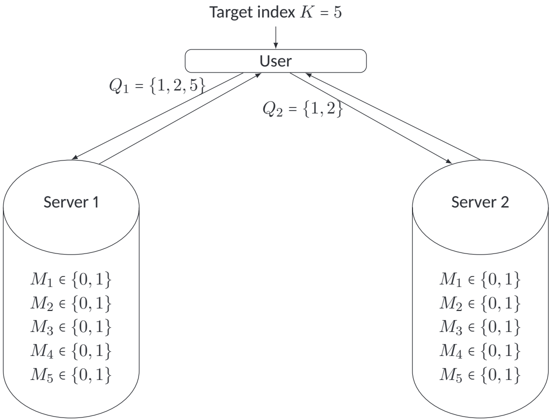
Example: Two-Server PIR Protocol [Chor et al.95]



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 $M_K = \pm(A_1 - A_2)$.

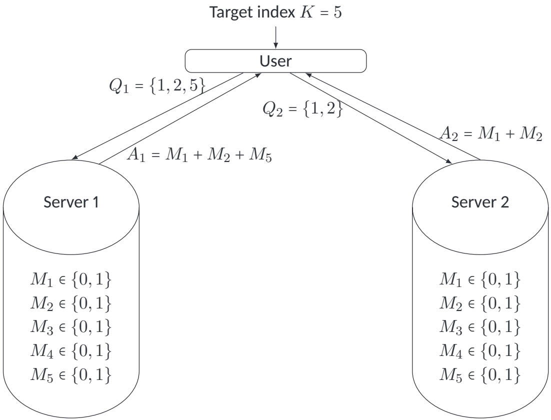
Example: Two-Server PIR Protocol [Chor et al.95]



Two-server PIR protocol

1. Q_1: a random subset of $\{1, \dots, \mathsf{f}\}$.
   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 $M_K = \pm(A_1 - A_2)$.

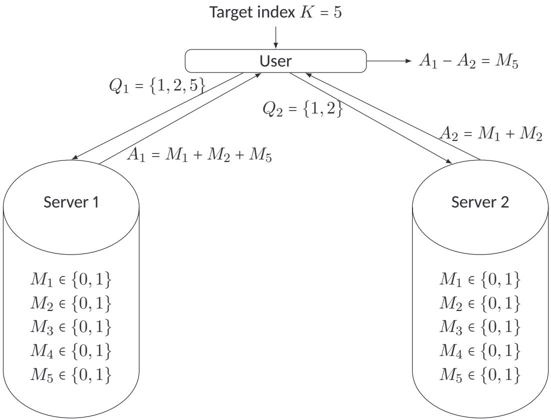
Example: Two-Server PIR Protocol [Chor et al.95]



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 $M_K = \pm(A_1 - A_2)$.

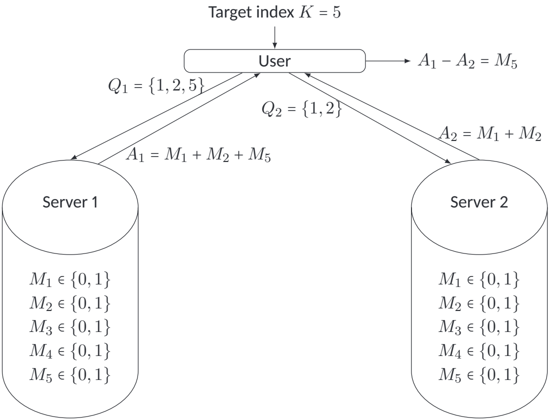
Example: Two-Server PIR Protocol [Chor et al.95]



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]

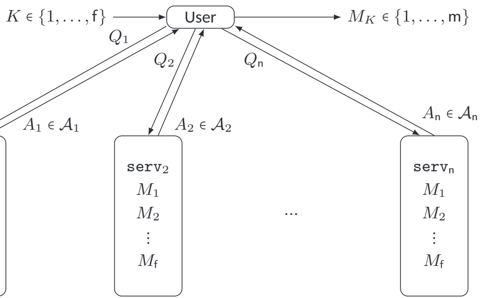


Two-server PIR protocol

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 $M_K = \pm(A_1 - A_2)$.

$$\begin{cases} Q_1 \perp K, Q_2 \perp K. \\ \text{2 bits are downloaded.} \end{cases}$$

PIR Capacity [Sun-Jafar16]



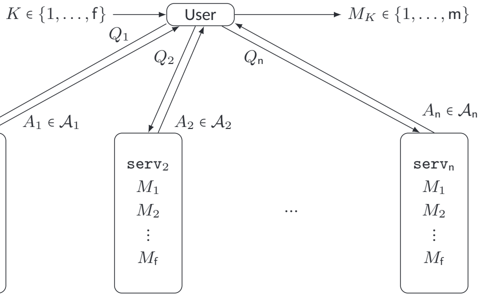
- n = # servers, f = # files, m = size of M_K (i.e., $M_i \in \{1,\ldots,\mathsf{m}\}$).
- PIR Rate: # of retrieved bits per 1-bit download.

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

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

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

PIR Capacity [Sun-Jafar16]



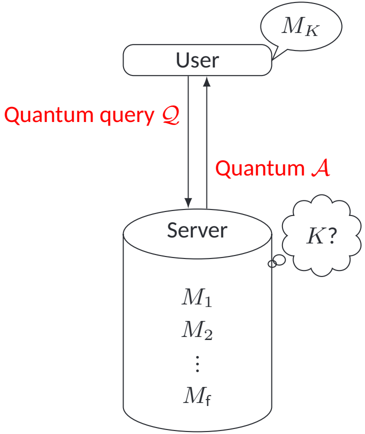
- n = # servers, f = # files, m = size of M_K (i.e., $M_i \in \{1, \ldots, \mathsf{m}\}$).
- PIR Rate: # of retrieved bits per 1-bit download.

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

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

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

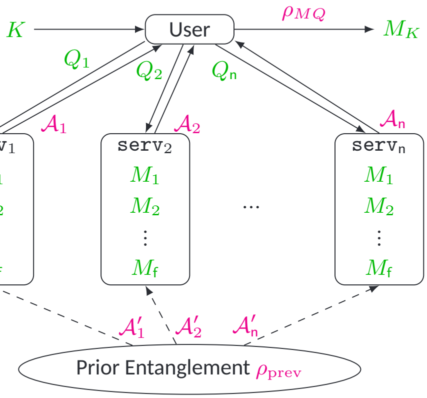
Quantum Private Information Retrieval (QPIR)



1. Efficient QPIR protocol is possible. [Le Gall12], [Kerenidis et al.16]
   = requires less cost than "downloading all"

2. QPIR with Specious Server: the server may deviate from the protocol but the malicious operation should not noticed by the user.
   - "Downloading all" is optimal. [Baumeler-Broadbent15]
   - "Downloading all" is optimal even with prior entanglement. [Aharonov et al.19]

QPIR Capacity [Song-Hayashi19]



(Green: classical, Magenta: quantum.)

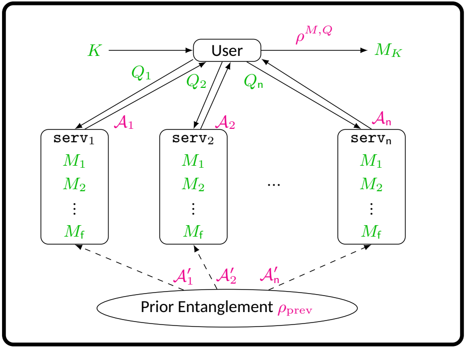
- n = # servers, f = # files, m = size of M_K (i.e., $M_i \in \{1, \dots, \mathsf{m}\}$).
- QPIR Rate: # of retrieved bits per 1-*qubit* download.

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

- PIR Capacity: Optimal PIR rate when n, f are fixed and m is arbitrary.

$$C_{\text{quantum}} = \sup R = 1.$$

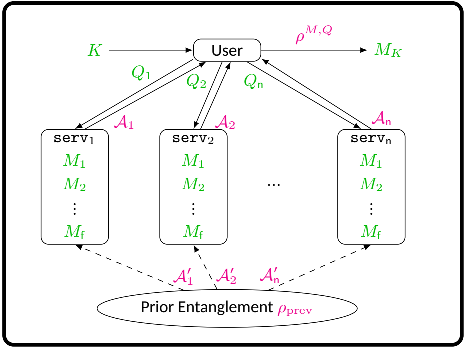
Variants of PIR/QPIR



Symmetric QPIR

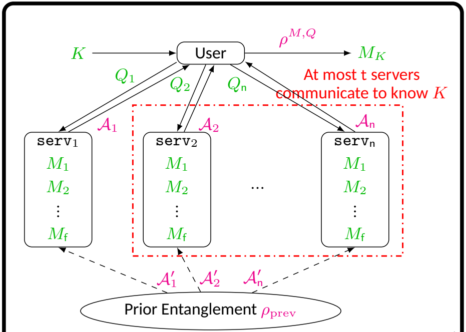
- Correctness: The user retrieves M_K.
- User Secrecy: K is not leaked to each server.
- *Server Secrecy*: The user only obtains M_K.

Variants of PIR/QPIR



Symmetric QPIR

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



t-Private QPIR $(1 \leq t \leq n-1)$

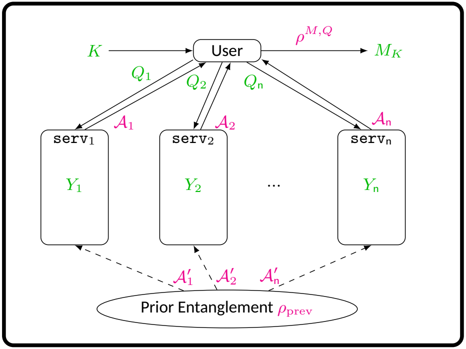
- Correctness.
- *User t-Secrecy*: K is secret to any t servers.

Variants of PIR/QPIR

QPIR with distributed storage system

- Correctness.
- User Secrecy.
- *The files are coded and distributed:*

$$(M_1, \dots, M_{\mathsf{f}}) \mapsto (Y_1, \dots, Y_{\mathsf{n}}).$$



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

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 [Song-Hayashi19]
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	
Symmetric multi-round PIR	-	
t**-Private PIR**	$\frac{1-t/n}{1-(t/n)^{f}}$ [Sun-Jafar16-2]	1 for $t \le \frac{n}{2}$, $2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$ [Song-Hayashi20]
Symmetric t**-private PIR**	$\frac{n-t}{n}$ [Wang-Skoglund17] †	
t**-private PIR with** $[n,k]$ **MDS coded storage**	$\frac{1-(t+k-1)/n}{1-((t+k-1)/n)^{f}}$ [Sun-Jafar16-2]	1 for $t+k-1 \le \frac{n}{2}$, $2\left(\frac{n-(t+k-1)}{n}\right)$ for $t > \frac{n}{2}$ [Allaix et al.21]
Symmetric t**-private PIR with** $[n,k]$ **MDS coded storage**	$\frac{n-(t+k-1)}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

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

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]	1 [Song-Hayashi19]
Symmetric PIR	$1-\frac{1}{n}$ [Sun-Jafar17] †	
Multi-round PIR	$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]	1 [Song-Hayashi19]
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 $t > \frac{n}{2}$ [Song-Hayashi20]
Symmetric t-private PIR	$\frac{n-t}{n}$ [Wang-Skoglund17] †	
t-private PIR with $[n,k]$ MDS coded storage	$\frac{1-(t+k-1)/n}{1-((t+k-1)/n)^f}$ [Sun-Jafar16-2]	1 for $t+k-1 \leq \frac{n}{2}$, $2\left(\frac{n-(t+k-1)}{n}\right)$ for $t > \frac{n}{2}$ [Allaix et al.21]
Symmetric t-private PIR with $[n,k]$ MDS coded storage	$\frac{n-(t+k-1)}{n}$ [Wang-Skoglund17] †	

† Shared randomness among servers is necessary.

Proof Steps of QPIR Capacities

- QPIR capacity is the supremum of QPIR rates. ($C_{\mathrm{quantum}} = \sup R$)
- Our proof of QPIR capacity consists of the achievability part and the converse part.
  - In the achivability part, we construct the capacity-achieving QPIR protocol.
  - In the converse part, we prove the tight upper bound of the QPIR capacity by entropic inequalities.

Achievablity of t-private QPIR capacity

Theorem 1: Achievability of t-private QPIR capacity

Suppose there exists a matrix $A = (\mathbf{a}_1, \ldots, \mathbf{a}_{2n}) \in \mathbb{F}_q^{2n \times 2n}$ satisfying the following properties.

(i) A is symplectic over $\mathbb{F}_q$, i.e.,

$$A^\top \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} A = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

(ii) Let $A' \coloneqq (\mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{a}_{3n-2t+1}, \ldots, \mathbf{a}_{2n}) = (\mathbf{r}_1^\top, \ldots, \mathbf{r}_{2n}^\top)^\top \in \mathbb{F}_q^{2n \times 2t}$.
For any permutation π of $\{1, \ldots, n\}$, the $2t$ rows $\mathbf{r}_{\pi(1)}, \ldots, \mathbf{r}_{\pi(t)}$, $\mathbf{r}_{\pi(1)+n}, \ldots, \mathbf{r}_{\pi(t)+n}$ are linearly independent.

Then, there exists a symmetric t-private QPIR protocol with n-servers that achieves the QPIR capacity $2(n-t)/n$.

We discuss **Existence** & **Minimum field size** of the matrix $A \in \mathbb{F}_q^{2n \times 2n}$ satisfying the properties (i) and (ii).

Classical Version of Theorem 1

Proposition 1: Achievability of t-private classical PIR capacity

Suppose there exists a matrix $B = (\mathbf{b}_1, \ldots, \mathbf{b}_\mathsf{n}) \in \mathbb{F}_q^{\mathsf{n}\times\mathsf{n}}$ satisfying the following properties.

(i') B is invertible.

(ii') Let $B' := (\mathbf{b}_1, \ldots, \mathbf{b}_\mathsf{t}) \in \mathbb{F}_q^{\mathsf{n}\times\mathsf{t}}$. Any t rows of B' are linearly independent.

Then, there exists a symmetric t-private classical PIR protocol with n-servers that achieves the PIR capacity $(\mathsf{n}-\mathsf{t})/\mathsf{n}$.

If we find B' *satisfying* (ii'), *then we can trivially extend* B' *to satisfy* (i').

Methods to find B' with condition (ii')

- Choose all elements of B' randomly on $\mathbb{F}_q$. If q is sufficiently large, (ii') is satisfied with high probability.
- Vandermonde type matrix: for any distinct elements $\alpha_1, \ldots, \alpha_\mathsf{t} \neq 0 \in \mathbb{F}_q$,

$$B' = \begin{pmatrix} \alpha_1 & \cdots & \alpha_\mathsf{t} \\ \alpha_1^2 & \cdots & \alpha_\mathsf{t}^2 \\ \vdots & \ddots & \vdots \\ \alpha_1^\mathsf{n} & \cdots & \alpha_\mathsf{t}^\mathsf{n} \end{pmatrix}. \quad (1)$$

- Maximum distance separable (MDS) code ($\stackrel{\text{def}}{=} \operatorname{Im} B'$).

Existence of Matrix A with Conditions (i) and (ii)

Theorem 2

Let $q = p^{2^{n+2t-2}}$ for a prime number p. There exists a matrix $A = (\mathbf{a}_1, \ldots, \mathbf{a}_{2n}) \in \mathbb{F}_q^{2n\times 2n}$ satisfying the following conditions:

(i) A is symplectic over $\mathbb{F}_q$, i.e., $A^\top \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} A = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$.

(ii) Let $A' := (\mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{a}_{3n-2t+1}, \ldots, \mathbf{a}_{2n}) = (\mathbf{r}_1^\top, \ldots, \mathbf{r}_{2n}^\top)^\top \in \mathbb{F}_q^{2n\times 2t}$.
For any permutation π of $\{1, \ldots, n\}$, the $2t$ rows $\mathbf{r}_{\pi(1)}, \ldots, \mathbf{r}_{\pi(t)}$, $\mathbf{r}_{\pi(1)+n}, \ldots, \mathbf{r}_{\pi(t)+n}$ are linearly independent.

Proof Idea

1. For symmetric matrices $X, Y \in \mathbb{F}_q^{n\times n}$, the matrices $\begin{pmatrix} I_n & X \\ 0 & I_n \end{pmatrix}$, $\begin{pmatrix} I_n & 0 \\ Y & I_n \end{pmatrix} \in \mathbb{F}_q^{2n\times 2n}$ are symplectic.
2. Let $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \ldots, \alpha_{n+2t-2})$, where $\alpha_i \notin \mathbb{F}_p(\alpha_1, \ldots, \alpha_{i-1})$ for any i, and

$$X = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_n & \cdots & \alpha_{2n-2} \end{pmatrix}, \quad Y = \begin{pmatrix} \alpha_{2t-n} & \alpha_{2t-n+1} & \cdots & \alpha_{2t-1} \\ \alpha_{2t-n+1} & \alpha_{2t-n+2} & \cdots & \alpha_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{2t-1} & \alpha_{2t} & \cdots & \alpha_{n+2t-2} \end{pmatrix} \in \mathbb{F}_q^{n\times n}.$$

3. Then, $S = \begin{pmatrix} I_n & X \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ Y & I_n \end{pmatrix}$ satisfies the conditions (i) and (ii).

Minimum Size of Finite Field for Matrix A with Conditions (i) and (ii)

Theorem 3

Let $\mathsf{n}/2 \le \mathsf{t} \le \mathsf{n}$. The following two conditions are equivalent.

1. There exists a matrix $A \in \mathbb{F}_q^{2\mathsf{n}\times 2\mathsf{n}}$ satisfying the conditions (i) and (ii).
2. There exists a $[\mathsf{n}, 2\mathsf{t}-\mathsf{n}]_q$ quantum MDS code.

Definition: Quantum Code

- $[\mathsf{n},\mathsf{k}]_q$ quantum code is the subspace $\mathcal{V} \subset \mathbb{F}_q^{2\mathsf{n}}$ such that $\mathcal{V} \subset \mathcal{V}^{\perp_{\mathbb{S}}}$ and $\dim \mathcal{V} = \mathsf{n}-\mathsf{k}$.
- Quantum Singleton Bound: Any quantum code satisfies

$$d := \min\{\mathrm{wt}_{\mathbb{S}}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{V}\} \le (\mathsf{n}-\mathsf{k})/2 + 1, \tag{2}$$

  where $\mathrm{wt}_{\mathbb{S}}(v_1,\ldots,v_{2\mathsf{n}}) := \#\{i \in \{1,\ldots,\mathsf{n}\} \mid (v_i, v_{i+\mathsf{n}}) \neq (0,0)\}$.
- Quantum Maximum Distance Separable (QMDS) code is the quantum code satisfying (2) with equality.

Conjecture: QMDS Conjecture [Ketkar06] (cf. MDS conjecture [Segre55])

Any $[\mathsf{n},\mathsf{k}]_q$ QMDS code satisfy $q \ge \begin{cases} \sqrt{\mathsf{n}-2} & \text{if } q \text{ is even and } \mathsf{k} \in \{3, q-1\}, \\ \sqrt{\mathsf{n}-1} & \text{otherwise.} \end{cases}$.

The equality of the MDS-conjecture is achieved for several cases [Jin-Xing13, Grassl-Rotteler15, Ball19]

Classical MDS Conjecture

MDS Conjecture [Segre55]

Let $B' \in \mathbb{F}_q^{n \times t}$ be the matrix s.t. any t rows are linearly independent. Then

$$q \geq \begin{cases} n-2 & \text{if } q \text{ is even and } k \in \{3, q-1\}, \\ n-1 & \text{otherwise.} \end{cases} . \tag{3}$$

- Proved for prime fields [Ball10].
- Proved for $k \leq 2p-2$ [Chowdhury16].

Conclusion

- QPIR Capacities

<table>
<tr><th></th><th>Classical PIR Capacity</th><th>Quantum PIR Capacity</th></tr>
<tr><td>PIR</td><td>$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar16]</td><td rowspan="4">1 [Song-Hayashi19]</td></tr>
<tr><td>Symmetric PIR</td><td>$1-\frac{1}{n}$ [Sun-Jafar17] †</td></tr>
<tr><td>Multi-round PIR</td><td>$\frac{1-n^{-1}}{1-n^{-f}}$ [Sun-Jafar18]</td></tr>
<tr><td>Symmetric multi-round PIR</td><td>-</td></tr>
<tr><td>t-Private PIR</td><td>$\frac{1-t/n}{1-(t/n)^f}$ [Sun-Jafar16-2]</td><td rowspan="2">1 for $t \leq \frac{n}{2}$,
$2\left(\frac{n-t}{n}\right)$ for $t > \frac{n}{2}$
[Song-Hayashi20]</td></tr>
<tr><td>Symmetric t-private PIR</td><td>$\frac{n-t}{n}$ [Wang-Skoglund17] †</td></tr>
<tr><td>t-private PIR with $[n,k]$ MDS coded storage</td><td>$\frac{1-(t+k-1)/n}{1-((t+k-1)/n)^f}$ [Sun-Jafar16-2]</td><td rowspan="2">1 for $t+k-1 \leq \frac{n}{2}$,
$2\left(\frac{n-(t+k-1)}{n}\right)$ for $t > \frac{n}{2}$
[Allaix et al.21]</td></tr>
<tr><td>Symmetric t-private PIR with $[n,k]$ MDS coded storage</td><td>$\frac{n-(t+k-1)}{n}$ [Wang-Skoglund17] †</td></tr>
</table>

† Shared randomness among servers is necessary.

- Construction of t-private QPIR protocol
  - Existence and minimum field size of a symplectic matrix over finite field.