Quantum Private Information Retrieval

A New Approach

Tefjol Pllaha

Department of Mathematics
University of Nebraska - Lincoln

The Power of Classical-Quantum Computation

Utilizing quantum resources to:

- increase performance, by boosting existing protocols.
- prove theoretical results, by leveraging new tools at disposal.

The Power of Classical-Quantum Computation

Utilizing quantum resources to:

- increase performance, by boosting existing protocols.
- prove theoretical results, by leveraging new tools at disposal.

Distributed computations is a form of ***many-to-one*** communication.

- Suffer from high communication cost, but various coding techniques help.

The Power of Classical-Quantum Computation

Utilizing quantum resources to:

- increase performance, by boosting existing protocols.
- prove theoretical results, by leveraging new tools at disposal.

Distributed computations is a form of ***many-to-one*** communication.

- Suffer from high communication cost, but various coding techniques help.

What about ***quantum*** many-to-one communication?

- Quantum entanglement gives superdense coding gains.
- Readily available only to quantum experts.

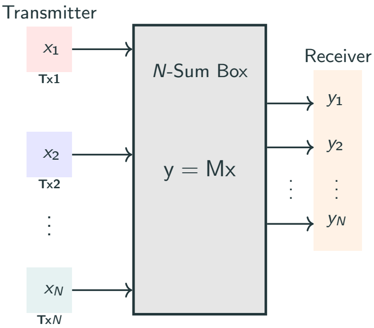
Objectives

Objective 1: Convenient abstraction for ***linear computation*** over quantum many-to-one networks.

Objective 2: Explore its scope and limitations.

Objectives

Objective 1: Convenient abstraction for ***linear computation*** over quantum many-to-one networks.
Objective 2: Explore its scope and limitations.

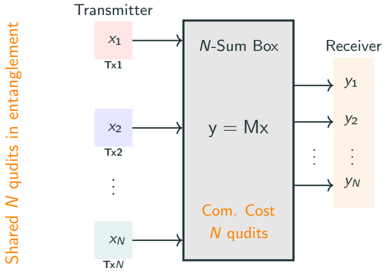


$$\mathrm{y} = (y_1, y_2, \cdots, y_N)^\top$$
$$\mathrm{x} = (x_1, x_2, \cdots, x_N)^\top$$

Objectives

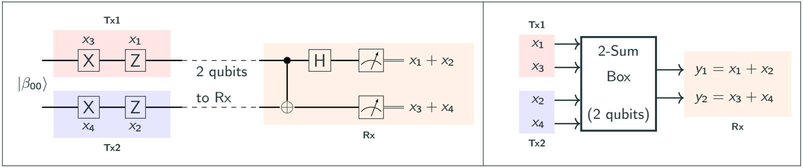
Objective 1: Convenient abstraction for ***linear computation*** over quantum many-to-one networks.

Objective 2: Explore its scope and limitations.

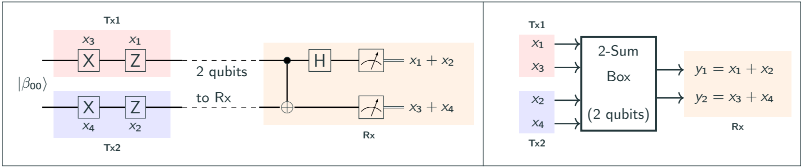


$$\mathrm{y} = (y_1, y_2, \cdots, y_N)^\top$$
$$\mathrm{x} = (x_1, x_2, \cdots, x_N)^\top$$

Example - The Two-Sum Protocol

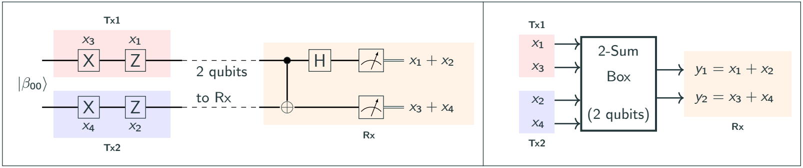


Example - The Two-Sum Protocol



$$Mx = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_3 + x_4 \end{pmatrix}.$$

Example - The Two-Sum Protocol



$$\mathrm{Mx} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_3 + x_4 \end{pmatrix}.$$

Reason: M is the stabilizer of the Bell state

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

N-Sum Boxes

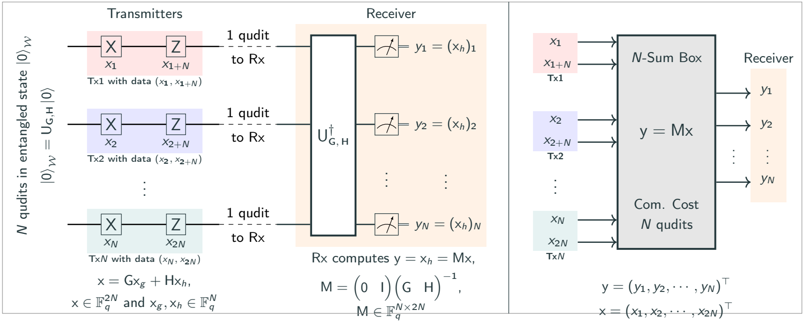
Theorem

Let $\mathsf{M} \in \mathbb{F}_q^{N\times 2N}$. Then there exists and N-Sum Box with transfer matrix M if and only if

$$\mathsf{M}\begin{pmatrix} 0 & -\mathsf{I}_n \\ \mathsf{I}_n & 0 \end{pmatrix}\mathsf{M}^T = 0,$$

that is, if and only if M is “self-dual”.

N-Sum Boxes



Transmitters
Receiver
N qudits in entangled state $|0\rangle_{\mathcal{W}}$
$|0\rangle_{\mathcal{W}} = U_{G,H}|0\rangle$
X
Z
x_1
x_{1+N}
Tx1 with data (x_1, x_{1+N})
x_2
x_{2+N}
Tx2 with data (x_2, x_{2+N})
x_N
x_{2N}
TxN with data (x_N, x_{2N})
1 qudit
to Rx
$U^{\dagger}_{G,H}$
$y_1 = (x_h)_1$
$y_2 = (x_h)_2$
$y_N = (x_h)_N$
$x = Gx_g + Hx_h$,
$x \in \mathbb{F}_q^{2N}$ and $x_g, x_h \in \mathbb{F}_q^N$
Rx computes $y = x_h = Mx$,
$M = \begin{pmatrix} 0 & I \end{pmatrix} \begin{pmatrix} G & H \end{pmatrix}^{-1}$,
$M \in \mathbb{F}_q^{N \times 2N}$
Tx1
Tx2
TxN
N-Sum Box
$y = Mx$
Com. Cost
N qudits
Receiver
y_1
y_2
y_N
$y = (y_1, y_2, \cdots, y_N)^\top$
$x = (x_1, x_2, \cdots, x_{2N})^\top$

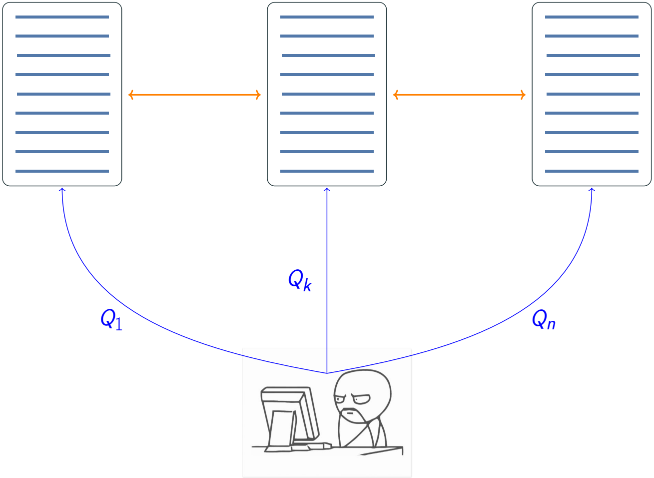
Coded Storage

m files $x^1, \dots, x^m \in \mathbb{F}_q^{\beta \times k}$ are encoded and stored on n servers by a $[n, k]$ storage code $\mathcal{C}$.

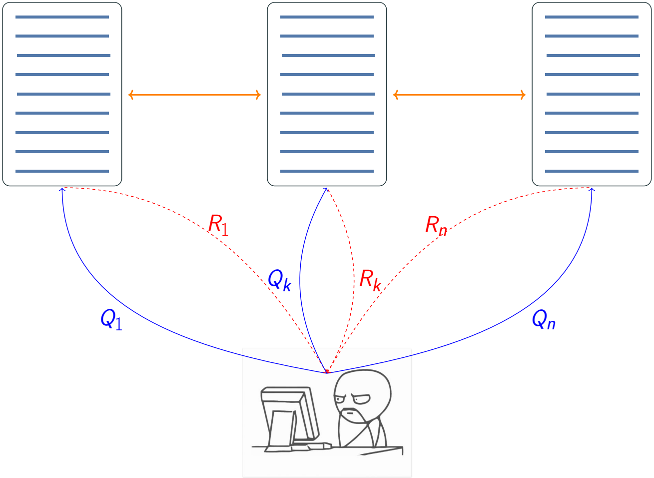
$$
\begin{matrix} \text{file } 1 \\ \\ \text{file } m \end{matrix}
\begin{pmatrix}
x^1_{1,1} & \cdots & x^1_{1,k} \\
\vdots & \ddots & \vdots \\
x^1_{\beta,1} & \cdots & x^1_{\beta,k} \\
\vdots & \vdots & \vdots \\
x^m_{1,1} & \cdots & x^m_{1,k} \\
\vdots & \ddots & \vdots \\
x^m_{\beta,1} & \cdots & x^m_{\beta,k}
\end{pmatrix}
\cdot \mathsf{G}_{\mathcal{C}} =
\begin{pmatrix}
y^1_{1,1} & \cdots & y^1_{1,n} \\
\vdots & \ddots & \vdots \\
y^1_{\beta,1} & \cdots & y^1_{\beta,n} \\
\vdots & \vdots & \vdots \\
y^m_{1,1} & \cdots & y^m_{1,n} \\
\vdots & \ddots & \vdots \\
y^m_{\beta,1} & \cdots & y^m_{\beta,n}
\end{pmatrix}
$$

SERVER_1 $\quad$ SERVER_n

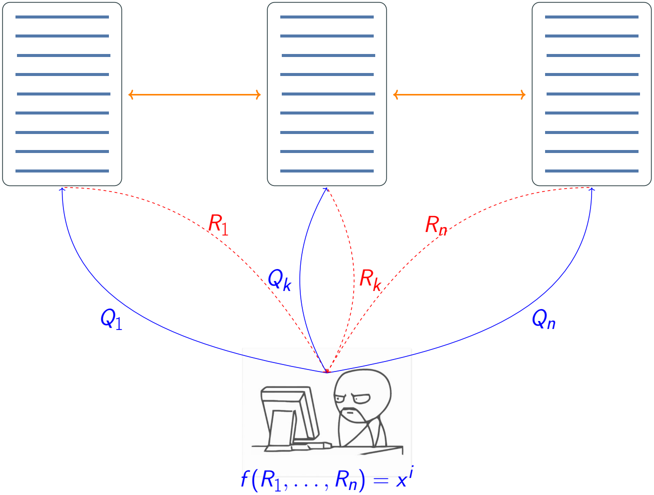
Private Information Retrieval (PIR)



Private Information Retrieval (PIR)



Private Information Retrieval (PIR)



PIR with t-collusion (t-PIR)

Definition (t-PIR).

User privacy: Any set of at most t colluding nodes learns no information about the index i of the desired file, *i.e.*, the mutual information

$$I(i; Q_{\mathcal{T}}^K, R_{\mathcal{T}}^K, y_{\mathcal{T}}) = 0, \quad \forall\, \mathcal{T} \subset [n], |\mathcal{T}| \leq t\ .$$

Server privacy: The user does not learn any information about the files other than the requested one, *i.e.*,

$$I(x^j; Q^K, R^K, K) = 0, \quad \forall j \neq K\ .$$

A scheme with both user and server privacy is called *symmetric*.

PIR with t-collusion (t-PIR)

Definition (Rate and Capacity).

For a PIR scheme the **rate** is the number of information bits of the requested file retrieved per downloaded bits, *i.e.*,

$$R_{\text{PIR}} = \frac{\text{Number of bits in a file}}{\text{Number of downloaded bits}} \, .$$

The PIR **capacity** is the supremum of PIR rates of all possible PIR schemes, for a fixed parameter setting.

PIR with t-collusion (t-PIR)

Definition (Rate and Capacity).

For a PIR scheme the rate is the number of information bits of the requested file retrieved per downloaded bits, *i.e.*,

$$R_{\text{PIR}} = \frac{\text{Number of bits in a file}}{\text{Number of downloaded bits}} \; .$$

The PIR capacity is the supremum of PIR rates of all possible PIR schemes, for a fixed parameter setting.

Convention

QPIR is PIR with "*entangled servers*" and "*quantum answers*".

Ingredients for QPIR

- Quantum adaptation of existing schemes.

Ingredients for QPIR

- Quantum adaptation of existing schemes.
- Generalized Reed-Solomon codes

$$\mathrm{GRS}_k(\alpha, v) = \{(v_i f(\alpha_i))_{1 \leq i \leq n} \mid f(x) \in \mathbb{F}_q^{<k}[x]\}.$$

Ingredients for QPIR

- Quantum adaptation of existing schemes.
- Generalized Reed-Solomon codes

$$\mathsf{GRS}_k(\alpha, v) = \{(v_i f(\alpha_i))_{1 \le i \le n} \mid f(x) \in \mathbb{F}_q^{<k}[x]\}.$$

- Quantum Computation.

A High-Rate Scheme for t-QPIR

Theorem [1]

There exists a t-QPIR scheme with rate

$$R_{\text{QPIR}} = \frac{2(n - k - t + 1)}{n}.$$

1. M. Allaix, L. Holzbaur, T. Pllaha, C. Hollanti. "High-Rate Quantum Private Information Retrieval with Weakly Self-Dual Star Product Codes," *In 2021 IEEE International Symposium on Information Theory*, 1046-1051.

Capacity [2]

Capacities	PIR	ref.	SPIR	ref.	QPIR	ref.
Replicated storage, no collusion	$1-\frac{1}{n}$	[3]	$1-\frac{1}{n}$	[6]	1	[21]
Replicated storage, t-collusion	$1-\frac{t}{n}$	[4]	$1-\frac{t}{n}$	[25]	$\min\{1, \frac{2(n-t)}{n}\}$	[23]
$[n,k]$-MDS coded storage, no collusion	$1-\frac{k}{n}$	[5]	$1-\frac{k}{n}$	[7]	$\min\{1, \frac{2(n-k)}{n}\}$	–
$[n,k]$-MDS coded storage, t-collusion	$1-\frac{k+t-1}{n}$	[12]	$1-\frac{k+t-1}{n}$	[7]	$\min\{1, \frac{2(n-k-t+1)}{n}\}$	–

2. 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," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 3, pp. 885-898, March 2022.

(s, t)-PIR with Byzantine Servers

Definition

A scheme is called s-secure if any set of s colluding servers learn nothing about the messages.

(s,t)-PIR with Byzantine Servers

Definition

A scheme is called s-secure if any set of s colluding servers learn nothing about the messages.

Theorem

For MDS-(s,t)-PIR (s-secure, t-private information retrieval from $[N, K_c]$ MDS coded storage among $N > X + T + K_c - 1$ distributed servers), there exists a scheme with rate

$$R = \min\left\{1, 2\left(1 - \left(\frac{X + T + K_c - 1}{N}\right)\right)\right\}.$$

Idea of Proof

$$\underbrace{\begin{bmatrix} A_1(i) \\ \vdots \\ A_N(i) \end{bmatrix}}_{\boldsymbol{A}(i)} = \underbrace{\left[\begin{array}{ccc|cccc} \frac{1}{f_1-\alpha_1} & \cdots & \frac{1}{f_L-\alpha_1} & 1 & \alpha_1 & \cdots & \alpha_1^{N-L-1} \\ \frac{1}{f_1-\alpha_2} & \cdots & \frac{1}{f_L-\alpha_2} & 1 & \alpha_2 & \cdots & \alpha_2^{N-L-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{f_1-\alpha_N} & \cdots & \frac{1}{f_L-\alpha_N} & 1 & \alpha_N & \cdots & \alpha_N^{N-L-1} \end{array}\right]}_{\mathrm{CSA}_{N,L(\boldsymbol{\alpha},\boldsymbol{f})}} \underbrace{\begin{bmatrix} \delta_1(i) \\ \vdots \\ \delta_L(i) \\ \nu_1(i) \\ \vdots \\ \nu_{N-L}(i) \end{bmatrix}}_{\boldsymbol{X}_{\delta\nu}(i)}$$

Secure Distributed Batch Matrix Multiplication

Theorem

Let $A_1, \cdots, A_L \in \mathbb{F}_q^{\lambda\times\eta}$ be L matrices X_A-securely shared among N servers and let $B_1, \cdots, B_L \in \mathbb{F}_q^{\eta\times\mu}$ another set of L matrices X_B-securely shared among the same N servers. The user wants to compute the products $A_1B_1, A_2B_2, \cdots, A_LB_L \in \mathbb{F}_q^{\lambda\times\mu}$ by querying the $N > X_A + X_B$ servers. There exists a scheme with rate

$$R = \min\left\{1, 2\left(1 - \left(\frac{X_A + X_B}{N}\right)\right)\right\}.$$

References:

- M. Allaix, Y. Lu, Y. Yao, T. Pllaha, C. Hollanti, S. Jafar. "Quantum N-Sum Boxes from Stabilizer Formalism." Submitted.
- 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," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 3, pp. 885-898, March 2022.
- M. Allaix, L. Holzbaur, T. Pllaha, C. Hollanti. "High-Rate Quantum Private Information Retrieval with Weakly Self-Dual Star Product Codes," *In 2021 IEEE International Symposium on Information Theory*, 1046-1051.
- M. Allaix, L. Holzbaur, T. Pllaha, C. Hollanti. "Quantum Private Information Retrieval from Coded and Colluding Servers," *IEEE Journal on Selected Areas in Information Theory*, 1(2), 599-610, August 2020.
- M. Allaix, L. Holzbaur, T. Pllaha, C. Hollanti. "Quantum Private Information Retrieval from MDS-coded and Colluding Servers," *In 2020 IEEE International Symposium on Information Theory*, 1059–1064.

Thank You!