Private Information Retrieval and Quantum Information

ABHISHEK MITTAL[2], ZEESHAN AHMED[2], ALAPAN CHAUDHURI[3, 1]

Dec 9, 2021

INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

CONTENTS

[1] with Prof. Prasad Krishnan, *SPCRC, IIITH*

[2] *SPCRC, IIITH*

[3] *CQST & CSTAR, IIITH*

PREFACE

This document serves as an update and report for my independent study (ongoing) on Quantum Private Information Retrieval (Monsoon 2021). Here, I formulate the problem of Private Information Retieval (PIR) and lay down the setup for the Quantum PIR problem.

This work is done in collaboration with **Prof. Prasad Krishnan** to whom we are deeply indebted for his guidance.

1 PRIVATE INFORMATION RETRIEVAL

1.1 Definition

Private Information Retrieval (PIR) refers to the problem of "privately" retrieving a file out of M messages from N distributed databases (or servers) in such a way that no individual database can tell which file has been retrieved. Thus, the goal of such as a system is to protect the privacy of the query (the file we are interested in retrieving). Each database can only tell that a file has been requested and the response time, but they do not know exactly which one we were interested in retrieving.

There are two fields of study within PIR, namely - information theoretic PIR (ITPIR) and computational PIR (CPIR). ITPIR is faster since it uses cheap cryptographic operations and is information theoretically secure. But, it assumes non-collusion and requires a minimum of 2 databases.

CPIR, on the other hand, is much slower but we can use it for colluding servers as well as just a single server (or database).

1.2 Major motivations for QPIR

- Protecting our online query privacy.
- PIR for replicated and MSD coded storage as well as for colluding servers has gained a lot of interest recently.
- Promise of better rates of transmission are possible with quantum communication.

1.3 Chor's Theorem and more on PIR

Theorem 1. *If the data is stored on only one server (or equivalently, if all servers are colluding), then the only thing we can do to achieve perfect privacy is to download the entire database.*

- On the other hand, if the database is replicated or coded on multiple servers that are not all communicating, then we can do better.
- Upload cost ignored: *the number of bits in the files (∼ download cost) is assumed to be much bigger than the number of files on the servers (∼ upload cost).*
- Symmetric PIR (SPIR): *the user is only able to decode the file that he has requested, and learns nothing about the other files, i.e., privacy is guaranteed also for the server.*

1.4 Definitions within PIR

- Correctness: there exists a functional D such that $D(A^K, Q^K, K) = x^K, \forall K$.
- t-collusion: any t servers may collude, i.e., exchange their received queries.
- t-PIR scheme: a scheme that protects against t-collusion, i.e., any set of at most t colluding nodes learns no information about the index K of the desired file.
- PIR rate: $R = \frac{\text{number of bits in a file}}{\text{number of received bits}}$ and in case of QPIR we have number of received qubits as the denominator.
- Capacity: supremum of PIR rates of all possible PIR schemes, for a fixed parameter setting.

1.5 Coding Theory: a recap

- A linear code C is a subspace of $\mathbb{F}_q^n$.
- We call n the length and $k = \dim(C)$ the dimension of C.
- The minimum distance of C is $d = \min\{wt_H(c) : c \in C\{0\}\}$, where $wt_H(c)$ is the Hamming weight of c, i.e., the number of non zero coordinates in c.
- When $d = n - k + 1$, C is called a maximum distance separable (MDS) code.
- The dual code C' is the dual vector space of C.
- The dual codes of MDS codes are also MDS.
- We call $G_C \in \mathbb{F}_q^{k\times n}$ is a generator matrix for C if rank $G_C = k$ and its k rows span C.
- A message $m \in \mathbb{F}_q^n$ is encoded into a codeword c by $c = mG_C$.
- m files $x_1, \cdots, x_m \in F_q^{\beta\times k}$ are encoded and stored on n servers by a storage code C.

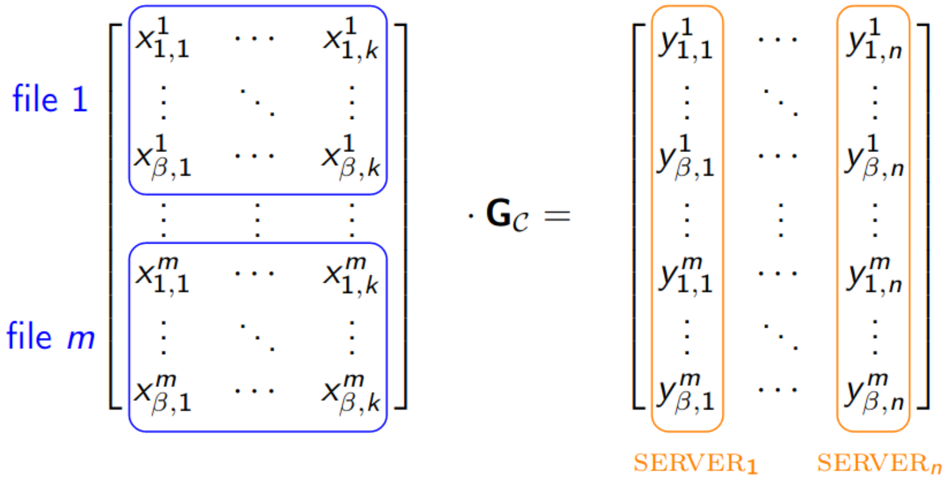
file 1
file m
$x^1_{1,1}$ $\cdots$ $x^1_{1,k}$
$x^1_{\beta,1}$ $\cdots$ $x^1_{\beta,k}$
$x^m_{1,1}$ $\cdots$ $x^m_{1,k}$
$x^m_{\beta,1}$ $\cdots$ $x^m_{\beta,k}$
$\cdot \mathbf{G}_C =$
$y^1_{1,1}$ $\cdots$ $y^1_{1,n}$
$y^1_{\beta,1}$ $\cdots$ $y^1_{\beta,n}$
$y^m_{1,1}$ $\cdots$ $y^m_{1,n}$
$y^m_{\beta,1}$ $\cdots$ $y^m_{\beta,n}$
SERVER$_1$
SERVER$_n$

Figure 1: Generator

1.6 Classical PIR Model

Let us consider the classical PIR setup with respect to multiple replicated servers. Now, if $N = 1$, i.e., we have only a single server then all that we can do is download all the files $W_1, W_2, \ldots, W_M$ and the related rate of this trivial PIR scheme is $1/M$.

The first interesting scheme that we come across is when $N = 2$.

- Given: two replicated databases, as shown in the figure, with M one-bit messages. And, we are trying to retrieve the message W_i.
- Consider a random vector $\vec{h} \in \mathcal{L}(\{0,1\}^M)$.

$$\vec{h} = \begin{bmatrix} h_1 & h_2 & \ldots & h_M \end{bmatrix}$$

- Our queries are based on $\vec{h}$ and $\vec{W}$.
- We have two queries in this scheme. The first one is made to server 1 ($Q_1^{[i]}$) and the last one is made to server 2 ($Q_2^{[i]}$).
- $Q_1^{[i]}$: retrieve dot product of $\vec{h}$ and $\vec{W}$.
- Thus, $A_1^{[i]} = \sum_{j=1}^{M} h_j W_j$.
- $Q_2^{[i]}$: retrieve dot product of $\vec{h}'$ and $\vec{W}$ where $\vec{h}' = \begin{bmatrix} h_1 & h_2 & \ldots & h_i + 1 & \ldots & h_M \end{bmatrix}$
- Thus, $A_2^{[i]} = \sum_{j=1}^{M} h_j W_j + W_i$.
- Therefore, we have $W_i = A_2^{[i]} - A_1^{[i]}$ and the retrieval rate is given by $1/2$.

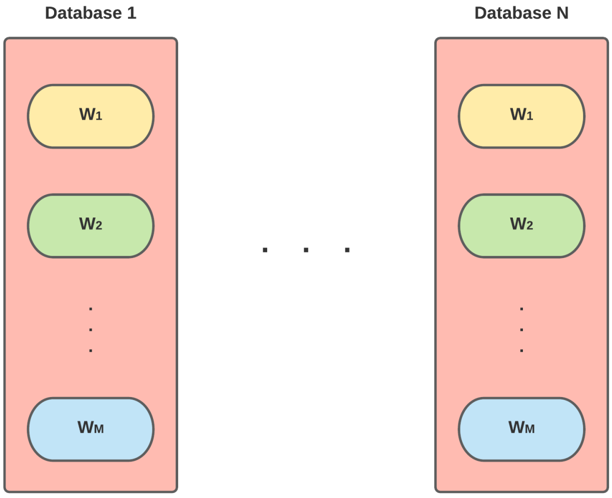

Figure 2: Replicated databases or servers

1.7 N-server system with M-multibit messages

- Given: N replicated databases, as shown in the figure, with M multi-bit ($L = N - 1$) messages. And, we are trying to retrieve the message W_i.

- Consider a random vector $\vec{h} \in \mathcal{L}(\{0,1\}^{M\times L})$.

$$\vec{h} = \begin{bmatrix} \vec{h_1} \\ \vec{h_2} \\ \vdots \\ \vec{h_M} \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,L} \\ h_{2,1} & h_{2,2} & \dots & h_{2,L} \\ \vdots & \vdots & & \vdots \\ h_{M,1} & h_{M,2} & \dots & h_{M,L} \end{bmatrix}$$

- Our queries are based on $\vec{h}$ and $\vec{W}$.

- We have two queries in this scheme. The first one is made to server 1 ($Q_1^{[i]} \rightarrow A_1^{[i]}$) and the last one is made to server N ($Q_N^{[i]} \rightarrow A_N^{[i]}$).

$$A_1^{[i]} = \sum\sum h_{j,k} W_{j,k}$$

$$A_2^{[i]} = \sum\sum h_{j,k} W_{j,k} + W_{i,1}$$

$$A_N^{[i]} = \sum\sum h_{j,k} W_{j,k} + W_{i,N-1}$$

- Therefore, we can obtain $\vec{W_i}$ from $\vec{A^{[i]}}$ and the rate of retrieval is $R = \frac{N-1}{N}$.

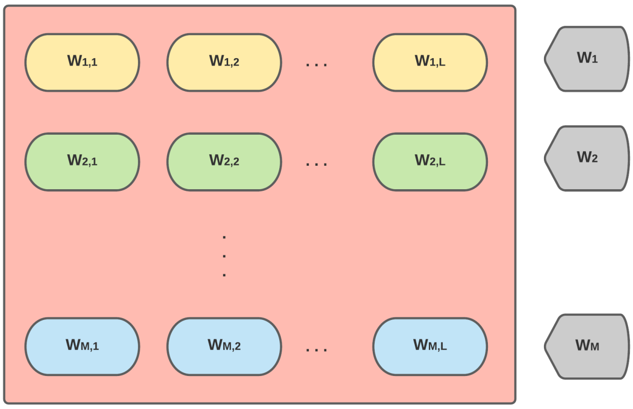

Figure 3: N replicated databases

1.8 Formulating PIR

- Queries and files or messages are independent and have zero mutual information.

$$I(Q_1^{[i]}, \dots, Q_N^{[i]}; W_1, \dots, W_M) = 0$$

- Answers are fully determined by messages and queries.

$$H(A_n^{[i]} | Q_n^{[i]}, W_1, \dots, W_M) = 0, \ n \in \{1, \dots, N\}$$

- Constraint of Reliability: $H(W_i | A_1^{[i]}, \dots, A_N^{[i]}, Q_1^{[i]}, \dots, Q_N^{[i]}) = o(L)$

- Constraint of Privacy: $I(Q_n^{[i]}; i) = 0, \ n \in \{1, \dots, N\}$

- Retrieval rate of PIR is given by the following.

$$R = \frac{H(W_i)}{\sum_{n=1}^{N} H(A_n^{[i]})}$$

- Capacity of PIR is given by the supremum of PIR rates of all possible PIR schemes, for a fixed parameter setting.

1.9 Capacity of Classical PIR

The capacity of classical PIR is given by C_{PIR}.

$$C_{\text{PIR}} = \frac{1 - 1/N}{1 - (1/N)^M}$$

We can construct the C_{PIR} scheme by making sure that we maximally utilize interference or interference alignment.

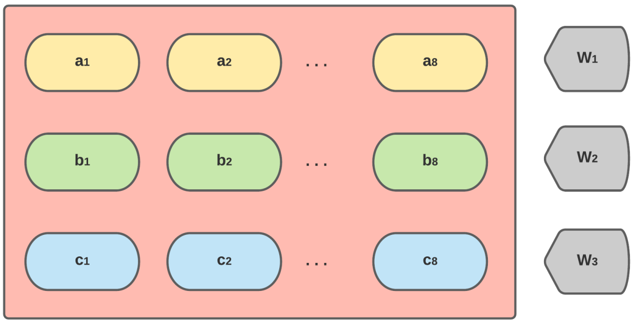

Figure 4: Database

Let us understand the scheme via the example shown above. Here, we have 2 servers and 3 multibit files ($N = 2,\ M = 3$).

Server			
DB_1	a_1	b_1	c_1
DB_2	a_2	b_2	c_2
DB_1	$a_3 + b_2$	$a_4 + c_2$	$b_3 + c_3$
DB_2	$a_5 + b_1$	$a_6 + c_1$	$b_4 + c_4$
DB_1		$a_7 + b_3 + c_3$	
DB_2		$a_8 + b_4 + c_4$	

Table 1: Query results

Rate of this above scheme is given as follows.

$$R = \frac{8}{14} = C_{\text{PIR}}(N = 2, M = 3)$$

2 PROBABILISTIC PIR

Now, let us look into some probabilistic schemes. This approach is used to construct queries with asymmetric lengths.

$$R = \frac{L}{\sum_{n=1}^{N} \mathbb{E}[l_n]}$$

The retrieval rate of such a scheme is constructed as given above. And, in this case too we have objectives such as:

- Obtain optimal retrieval rate for probabilistic PIR $= C_{\text{PIR}}$
- Minimize message length
- Minimize upload cost

2.1 $N=2,\ M=2$ probablistic PIR scheme

Probability	Requesting W_1	
	DB_1	DB_2
1/2	ϕ	W_1
1/2	W_1+W_2	W_2

$$\text{Retrieval Rate } = \frac{1}{1/2\times 1+1/2\times 2}=\frac{2}{3}=C_{PIR}(N=2,M=2)$$

Probability	Requesting W_2	
	DB_1	DB_2
1/2	ϕ	W_2
1/2	W_1+W_2	W_1

3 CAPACITY OF DIFFERENT PIR SCHEMES

- Classical PIR
$$C_{PIR}=\frac{1-1/N}{1-(1/N)^M}$$
- T-colluding PIR
$$C_{COL}=\frac{1-T/N}{1-(T/N)^M}$$
- U-robust PIR
$$C_{ROB}=\frac{1-\frac{T}{N-U}}{1-(\frac{T}{N-U})^M}$$
- B-byzantine PIR
$$C_{BYZ}=\frac{1-\frac{T}{N-2B}}{1-(\frac{T}{N-2B})^M}$$
- Symmetric PIR
$$C_{SPIR}=1-\frac{1}{N}$$
- (N,K) MDS-coded PIR
$$C_{MDS}=\frac{1-\frac{K}{N}}{1-(\frac{K}{N})^M}$$

3.1 Tabulated results for important cases

Capacities	**PIR**	**SPIR**	**QPIR**
Replicated (non-colluding)	$1-1/N$	$1-1/N$	1
Replicated (T-collusion)	$1-T/N$	$1-T/N$	$\geqslant 2/(T+2)$
(N,K) MDS-coded (T-collusion)	$1-(K+T-1)/N$ *	$1-(K+T-1)/N$	$\geqslant 2/(K+T-1)$

* *conjectured to be true by Freij-Hollanti et. al.*

4 INTRODUCTION TO QUANTUM INFORMATION

4.1 On the Formulations of Quantum Mechanics

Today, Quantum Mechanics is amongst the foundational bedrocks of Modern Physics. As a result, there is no surprise that the field comes across as some strange physical theory and we are taught of how it grew rather than what it truly stands for.

Quantum Theory, in its essence, is as much an extension of Classical Probability Theory, as it is a physical theory that descrives the universe. Moreover, just as Classical Probability Theory, Quantum Mechanics can too be formulated via pure thought alone without any particular appeal to experiment.

To formally state it, quantum mechanics is what we arrive at upon conserving the L_2 norm rather than the L_1 norm (as in Classical Probability) along with addition of the continuity axiom and the concept of measurement. Basedon the same, we can propose the following axiomatic formulation of Quantum Mechanics.

- The state of a system encodes probability of outcomes in a vector, say $[\alpha_1, \alpha_2, \dots \alpha_n]$, such that $\sum_{\forall i} |\alpha_i|^2 = 1$, or that the L_2 norm is preserved.
- There exists a continuous reversible transformation on a system between any two pure states of that system. This is called the axiom of continuity.
- Measurement in a standard basis results in a collapse of the state to whatever outcome is obtained. The outcome is governed by the probability distribution.
- Associated with every system, exists degree of freedom and dimension.
- Degree of Freedom of a system (K) denotes the minimum number of probability measurements needed to determine the state.
- Dimension of a system (N) denotes the maximum number of states that can be reliably distinguished from one another in a single shot measurement.
- A composite system consisting of two subsystems A and B having dimension N_A and N_B respectively, and number of degrees of freedom K_A and K_B respectively, has dimension $N = N_A N_B$ and number of degrees of freedom $K = K_A K_B$.

These axioms can be revised and restated as the following, under the state-vector and density matrix representations, respectively.

4.1.1 *State is a vector*

1. Isolated physical system is given by its state vector operating on a certain Hilbert space.
2. Evolution of a closed quantum system is given by a unitary transformation. In its physical interpretation we have this postulate governed by the Schrodinger Equation, as stated.
$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$
The Hamiltonian is a hermitian operator and has a spectral decomposition, $H = \sum E|E\rangle\langle E|$.
3. The state space of a composite physical system is the tensor product of the state spaces of the component systems.
$$|\psi\rangle = |\psi_1\rangle \otimes ... \otimes |\psi_n\rangle$$

4. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the state space of the system. Probability that upon measurement the outcome is $m = p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ and the state of the system becomes as follows.

$$|\psi\rangle \xrightarrow{\text{on measuring}} \frac{M_m|\psi\rangle}{\sqrt{p(m)}} = \frac{M_m|\psi\rangle}{||M_m|\psi\rangle||}$$

Measurement operators also follow the completeness equation, described as follows.

$$\sum_m M_m^\dagger M_m = I$$

4.1.2 *State is a density matrix*

1. Isolated physical system is given by its density matrix operating on a certain Hilbert space. A matrix ρ is a density matrix if and only if it is both positive $(\rho = \rho^\dagger)$ and $tr(\rho) = 1$.
2. Evolution of a closed quantum system is given by a unitary transformation as $\rho \xrightarrow{U} U\rho U^\dagger$.
3. The state space of a composite physical system is the tensor product of the state spaces of the component systems.

$$\rho = \rho_1 \otimes ... \otimes \rho_n$$

4. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the state space of the system. Probability that upon measurement the outcome is $m = p(m) = tr(M_m^\dagger M_m \rho)$ and the state of the system becomes as follows.

$$\rho \xrightarrow{\text{on measuring}} \frac{M_m \rho M_m^\dagger}{p(m)}$$

Measurement operators follow the completeness equation, $\sum_m M_m^\dagger M_m = I$.

4.2 Unitarity, complex numbers and linearity

- **Why is quantum computing reversible?** Any quantum gate must thus be implemented as a unitary operator and is therefore reversible.
- **Why are transformations in Quantum Mechanics and Quantum Computing unitary?** In case of Quantum Mechanics, all transformations are required to be L_2 norm preserving and the matrices which possess this property, upon introducing complex numbers as well, are unitary matrices (provided that we are operating in the same Hilbert Space).
- **Why do we use complex numbers, instead of real numbers?** The axiom of continuity requires us to operate on a field which is algebraically closed. Thus, we need complex numbers. In simpler terms, if you want every unitary operation to have a square root, then you have to go to the complex numbers.
- **Why Linearity?** When, we stated out our axioms – linearity was implied in the idea of state transformation. However, let us move out of our formulation and think about why linearity might be necessary.
  The first compelling argument for linearity was made by Wigner and Bargmann who proved that quantum dynamics must be linear if it does not change absolute values of inner products of state vectors.

However, the assumption – upon which this argument stands – is not strong enough. In fact, Steven Weinberg among others have indeed come up with non-linear formulations of Quantum Mechanics.
So, can we come up with an argument that is stronger? Fortunately, we can! And, guess what? It is inherently based on Computational Complexity. If quantum mechanics were non-linear, then one could build a computer to solve **NP**-complete problems in polynomial time.

- **What about theories based on any L_p norm where** $p \in \mathbb{N},\ p \neq 1, 2$**?** Let T be a linear transformation such that it preserves L_p. Then, if T is a non-trivial transformation such that it doesn't involve re-shuffling of the elements of the vector – then $p = 1$ or $p = 2$.

5 QUANTUM PRIVATE INFORMATION RETRIEVAL

In the QPIR problem with multiple servers, the objective is for a user to retrieve a classical file by downloading (entangled) quantum systems from multiple replicated servers, while maintaining the privacy constraint that identity of the downloaded file remains unknown to each server.

In the quantum counterpart for the classical PIR problem, we shall be dealing with non-colluded replicated servers.

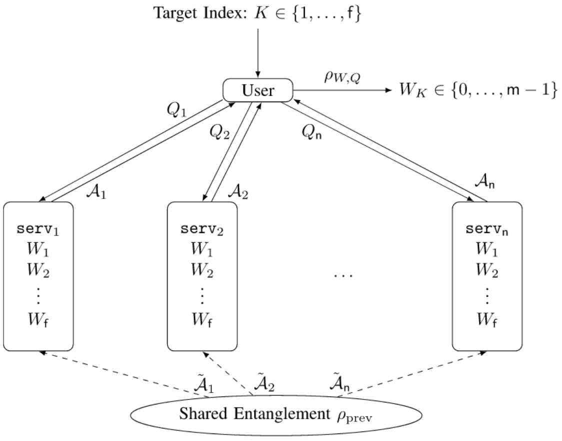
Target Index: $K \in \{1, \dots, f\}$
User
$\rho_{W,Q}$
$W_K \in \{0, \dots, m-1\}$
Q_1
Q_2
Q_n
$\mathcal{A}_1$
$\mathcal{A}_2$
$\mathcal{A}_n$
$\mathtt{serv}_1$ W_1 W_2 ⋮ W_f
$\mathtt{serv}_2$ W_1 W_2 ⋮ W_f
…
$\mathtt{serv}_n$ W_1 W_2 ⋮ W_f
$\tilde{\mathcal{A}}_1$
$\tilde{\mathcal{A}}_2$
$\tilde{\mathcal{A}}_n$
Shared Entanglement ρ_{prev}

Figure 5: QPIR protocol showing the composite system of the servers initialized to an entangled state ρ_{perv}.

5.1 Description of the QPIR scheme

QPIR protocol, for n-servers and f-files with m-bits each, is given by the 4-tuple $\Phi^{(}m)_{QPIR} = (\rho_{prev}, Enc_{user}, Enc_{serv}, Dec)$ where Enc_{user} denotes the user encoder, $Enc_{serv} := (Enc_{serv_1}, ..., Enc_{serv_n})$ denotes the collection of the server encoders, and Dec denotes the decoder.

To retrieve the W_K , the user encodes queries by user encoder given below. $Enc_{user}(K, R_{user}) = (Q_1, ..., Q_n)$ where Q_t is the set of query symbols to the t-th server for any $t \in \{1, \dots, n\}$. The n queries $Q1, \dots, Q_n$ are sent to the servers $serv_1, \dots, serv_n$, respectively.

Finally, each server $serv_t$ applies a CPTP map Λ_t depending on $Q_t, W_1, \ldots, W_f$. The final received state of the user is given above.

$$\rho_{W,Q} := \Lambda_1, \ldots, \Lambda_n(\rho_{prev})$$

5.2 Tools for QPIR

Consider multiple 2-qubit systems $\mathcal{H}_i \otimes \mathcal{H}_j$ in maximally entangled state ϕ.

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

We then define an unitary operator $W(a, b)$, where $a, b \in \mathbb{F}_2$, over the system.

$$W(a, b) = (-1)^{ab} \sum_{i=0}^{l-1} (-1)^{ai} |i + b\rangle \langle i|$$

Theorem 2. *The set* $\mathcal{B}_{\mathbb{F}_2^2} := \{B_{(a,b)} := W(a, b) |\phi\rangle \langle\phi| W(a, b)^T \mid a, b \in \mathcal{F}_2\}$ *is a projection valued measure. And, the measurement defined by the POVM* $\mathcal{B}_{\mathbb{F}_2^2}$ *is called the Bell measurement.*

5.2.1 *Two sum transmission protocol*

- Alice and Bob prepare qubits $\mathcal{H}_A$ and $\mathcal{H}_B$ in the maximally entangled state $|\phi\rangle$.
- Alice and Bob apply the unitaries $W_A(a_1, a_2)$ on $\mathcal{H}_A$ and $W_B(b_1, b_2)$ on $\mathcal{H}_B$, respectively.
- Alice and Bob send their qubits (respectively $\mathcal{H}_A, \mathcal{H}_B$) to Carol through two quantum channels.
- Carol performs a Bell measurement on the system $\mathcal{H}_A \otimes \mathcal{H}_B$ and obtains $(a_1 + b_1, a_2 + b_2)$ as the protocol output.

6 RATE-ONE QPIR PROTOCOL

In this section, we propose a $R_{QPIR} = 1$ 2-server QPIR protocol with the perfect security and negligible upload cost. This protocol is constructed from the idea of the classical two-server PIR protocol.

- To retrieve: W_K
- In each server: $W_1, \ldots, W_f \in \{0, \ldots, l^2 - 1 =: m_l - 1\}$
- We assume that $serv_1$ and $serv_2$ possess the l-dimensional quantum systems $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively.
- The maximally entangled state $|\phi\rangle$ in $\mathcal{A}_1 \otimes \mathcal{A}_2$ is shared at the beginning of the protocol.

The QPIR protocol for retrieving W_K is described as follows.

1. Depending on the target file index K, the user chooses a subset R_{user} of $\{1, , f\}$ uniformly. Let $Q_1 := R_{user}$ and we have:

$$Q_2 = \begin{cases} Q_1 - K, \text{ if } \{K\} \in Q_1 \\ Q_1 \cup K, \text{ if } \{K\} \notin Q_1 \end{cases}$$

2. The user sends the queries Q_1 and Q_2 to $serv_1$ and $serv_2$, respectively.
3. $serv_1$ calculates $H_1 := \sum_{i \in Q_1} W_i \in \mathbb{Z}_l^2$ and applies $W(H_1)$ on the quantum system $\mathcal{A}_1$.
4. Similarly, $serv_2$ calculates $H_2 := \sum_{i \in Q_2} W_i \in \mathbb{Z}_l^2$ and applies $W(H_2)$ on the quantum system $\mathcal{A}_2$.
5. The state on $\mathcal{A}_1 \otimes \mathcal{A}_2$ is $(W(H_1) \otimes W(H_2)) \left|\phi\right\rangle$.
6. $serv_1$ and $serv_2$ send the quantum systems $\mathcal{A}_1$ and $\mathcal{A}2$ to the user, respectively.
7. The user performs a POVM $\mathcal{B}_{\mathbb{F}_2^2}$ where each POVM element is given by the following.

$$B_{(a,b)} := (W(a,b) \otimes I) \left|\phi\right\rangle \left\langle\phi\right| (W(a,b)^\dagger \otimes I), \quad \text{if } K \in Q_1$$

$$B_{(a,b)} := (W(-a,-b) \otimes I) \left|\phi\right\rangle \left\langle\phi\right| (W(-a,-b)^\dagger \otimes I), \quad \text{otherwise}$$

The user obtains the measurement outcome (a,b) as the retrieval result.

7 CONCLUSION

As described above, we have mostly explored Classical PIR schemes and topics in Quantum Shannon Theory during the extent of my study. Future work involves looking into different QPIR protocols, so as to come up with new novel schemes or results on capacity under different scenarios and settings.

REFERENCES

1. Song et. al. Capacity of Quantum Private Information Retrieval With Multiple Servers
2. Susana F. Huelga Angel Rivas and Martin B. Plenio. Entanglement and Non-Markovianity of Quantum Evolutions
3. Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information
4. B. Chor et. al. Private Information Retrieval
5. Alliax et. al. Quantum private information retrieval from mds-coded and colluding servers