Quantum Private Information Retrieval from MDS-coded and Colluding Servers

Matteo Alliax *, Lukas Holzbaur †, Tefjol Plaha ‡, Camilla Hollanti ¶

* University of Genoa, Italy. E-mail: matteo.alliax95@gmail.com
† Technical University of Munich, Germany. E-mail: lukas.holzbaur@tum.de
‡ Aalto University, Finland. E-mails: {tefjol.plaha, camilla.hollanti}@aalto.fi

Abstract—In the classical private information retrieval (PIR) setup, a user wants to retrieve a file from a database or a distributed storage system (DSS) without revealing the file identity to the servers holding the data. In the quantum PIR (QPIR) setting, a user privately retrieves a classical file by downloading quantum systems from the servers. The QPIR problem has been treated by Song et al. in the case of replicated servers, both without collusion and with all but one servers colluding. In this paper, the QPIR setting is extended to account for MDS-coded servers. The proposed protocol works for any \( [n,k] \)-MDS code and \( t \)-collusion with \( t \leq n-k \). Similarly to the previous cases, the rates achieved are better than those known or conjectured in the classical counterparts.

I. INTRODUCTION

Private information retrieval (PIR), a problem initially introduced by Chor et al. [11], enables a user to download a data item from a database without revealing the identity of the retrieved item to the database owner. During the past few years, PIR has gained renewed interest in the setting of distributed storage systems (DSSs), where the servers are storing possibly large files that may be encoded, e.g., by an MDS code. The capacity of PIR is already known in a variety of settings [2], [3], [4], [5], [6], but is still open for coded and colluding servers [7], [8]. Progress towards the general coded colluding PIR capacity was recently made in [9], [10].

More recently, Song et al. have considered a similar problem in a quantum setting. They consider a replicated storage system with classical files, where the servers respond to user’s (classical) queries by sending quantum systems. The user is then able to privately retrieve the file by measuring the quantum systems. The servers are assumed to share some maximally entangled states, while the user and the servers are not entangled. The non-colluding case was considered in [11], and was shown to have capacity equal to one. This is in contrast to the classical replicated (asymptotic) PIR capacity \( 1 - \frac{1}{n} \) for \( n \) servers. The case of all but one servers colluding

L. Holzbaur was supported by TU Munich – Institute for Advanced Study, funded by the German Excellence Initiative and EU 7th Framework Programme under Grant Agreement No. 291763 and the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) under Grant No. WA3907/1-1. T. Plaha was partially supported by Academy of Finland, under the Grant No. 319578. C. Hollanti was supported by the Academy of Finland, under Grants No. 303819 and 318937, and by the TU Munich – Institute for Advanced Study, funded by the German Excellence Initiative and the EU 7th Framework Programme under Grant Agreement No. 291763, via a Hans Fischer Fellowship.

was considered in [12], again achieving higher capacity than the classical counterpart. In this case, the QPIR capacity is \( \frac{1}{n} \), while classically (and asymptotically) it is \( \frac{1}{n} \).

A. Contributions

We adapt the QPIR protocol for replicated storage systems protecting against collusion of all but one servers [12] to the case of \( [n,k] \) MDS coded servers and arbitrary \( t \)-collusion.

That is, from the case \( t = n - 1 \) to \( t = n - k \). This can be seen as trading off collusion protection for reduced storage overhead. The achieved rate \( \frac{1}{n} \) is higher than the conjectured asymptotic rate in the classical coded and colluding PIR [7], giving \( \frac{1}{n} \).

The setup is very similar to [13], which provides an optimal classical PIR scheme for the case \( t = n - k \). This was extended to cover non-maximal collusion \( (t < n - k) \) in [7] by considering the queries as coming from another code via the star product scheme. With this interpretation, the query code in [13] is the dual of the storage code — similarly as in the QPIR protocol presented here — while [7] enables it to be any \( [n,t] \) MDS code for \( t \leq n-k \). One may wonder why we do not do this generalization here, but merely use the dual as the query code. This is simply due to the limitation imposed by quantum measurement, see the discussion in Remark 2.

II. BASICS ON PIR AND QUANTUM COMPUTATION

A. Notation

For any two vectors \( \alpha = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \) of the same length \( n \) we denote their inner product by \( \langle \alpha | v \rangle = u_1v_1 + \cdots + u_nv_n \). We will denote by \( [n] \) the set \{1, 2, \ldots, n\}, and by \( F_q \) the finite field of \( q \) elements. In this paper, we only consider characteristic two, i.e., \( q = 2^E \) for some positive integer \( E \).

Let \( \Gamma = \{ \gamma_1, \ldots, \gamma_E \} \) be a basis of \( \mathbb{F}_2^n \) over \( \mathbb{F}_2 \). For \( \alpha \in \mathbb{F}_q \) denote by \( \varphi \) the bijective, \( \mathbb{F}_2 \)-linear map

\[
\varphi : \mathbb{F}_2^E \rightarrow \mathbb{F}_2^E \n
\alpha \mapsto \sum_{i=1}^E \alpha_i \gamma_i \mapsto (\alpha_1, \ldots, \alpha_E). \tag{1}
\]

Note that this mapping preserves addition, i.e., \( \varphi(\alpha + \alpha') = \varphi(\alpha) + \varphi(\alpha') \forall \alpha, \alpha' \in \mathbb{F}_2^E \).
B. Private Information Retrieval

Consider a storage system storing $m$ files $x^i$, $i \in [m]$, where each server stores a share $y^i$, $i \in [m]$ of each (encoded) file (for replication $y^i = x^i$). In a PIR protocol a user desiring the $K$-th file $X^K$ chooses a query $Q^K$ from a query space $Q$ and transmits it to the servers. The servers’ response $A_i^i$ is a function of the received queries and the shares of the (encoded) files they store. By query and response here we mean the overall matrix containing all the individual queries and responses. Below, $Q^K_i$ denotes the matrix of queries sent to a subset $T_i$.

**Definition 1 (Correctness).** There exists a function $D$ such that

\[ D(A^K, Q^K, K) = x^K, \forall K \in [m]. \]

As usual, we assume honest-but-curious servers who follow the assigned protocol, but might try to determine the index $i$ of the file desired by the user.

**Definition 2 (Privacy with $t$-Collusion).** 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

\[ I(i; Q^K_i, A^K, y_T) = 0, \quad \forall T \subset [n], |T| \leq t. \]

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

\[ I(x^i; Q^K_i, A^K, K) = 0, \quad \forall j \neq K. \]

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

As customary, we assume that the size of the query vectors is negligible compared to the size of the files. Hence, we ignore the upload cost and define the PIR rate as follows:

**Definition 3 (PIR Rate and Capacity).** For a PIR scheme the rate is the number of information bits of the requested file retrieved per downloaded answer bits, i.e.,

\[ R_{\text{PIR}} = \frac{\text{Number of bits in a file}}{\text{Number of received bits}}. \]

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

**Remark 1.** As the user and the servers do not share any entanglement in this model, the number of bits obtained when receiving a qubit, i.e., the number of bits that can be communicated by transmitting a qubit from a server to the user without privacy considerations, is the dimension of the qubit.

C. Quantum Computation

In this section we introduce the notation to be used later on. For details we refer the reader to [12].

A qubit is a 2-dimensional Hilbert space $H$ along with a computational basis, that is, a prespecified orthonormal basis $B = \{ |0\rangle, |1\rangle \}$. One typically takes $H = \mathbb{C}^2$. A state of $H$ is a unit vector $|\psi\rangle \in H$, while $\langle \psi |$ denotes the adjoint of $|\psi\rangle$,

that is, $\langle \psi | = |\psi\rangle^\dagger$. Thus, $\langle \phi | \psi \rangle$ and $|\phi\rangle \langle \psi |$ define inner and outer products respectively.

We will work with 2-qubit systems $H = H_1 \otimes H_2$. In this case the computational basis is $B^{\otimes 2} = \{|a\rangle | a \in F_2^2\}$, where $|a\rangle = |a_1\rangle \otimes |a_2\rangle$. We will also use the maximally entangled state

\[ |\Phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \]

We denote by $|\Phi\rangle_i$ the $i$-th qubit of $|\Phi\rangle$.

For $a, b \in F_2$, the Weyl operator is defined as

\[ W(a, b) = (-1)^{ab} W(a, b), \]

\[ W(a_1, b_1) W(a_2, b_2) = (-1)^{a_2 b_1} W(a_1 + a_2, b_1 + b_2), \]

\[ W(a, b)^\dagger W(a, b) = W(a, b)^2 = I_2, \]

\[ W_2(a, b) \langle \Phi | = (-1)^{ab} W_1(a, b) |\Phi\rangle. \]

**Lemma 1. The set**

\[ B_{2^2} = \{ B(a, b) = W_1(a, b) |\Phi\rangle \langle \Phi | W_1(a, b)^\dagger \} | a, b \in F_2^2 \}

**is a projection-valued measure (PVM), that is, the matrix**

\[ B(a, b) \]

**is a Hermitian projector for any**

\[ | a, b \in F_2^2 \]

**and satisfies the completeness equation.**

**Proof. Straightforward.**

**Definition 4. The Bell measurement is the measurement defined by the PVM $B_{2^2}$ described in Lemma 1.**

In the following we will require the two-sum transmission protocol [12].

Two-sum transmission protocol: This protocol allows to send the sum of two pairs of classical bits by communicating two qubits. Suppose that Alice and Bob possess a qubit $H_A$ and $H_B$, respectively, and share the maximally entangled state $|\Phi\rangle \in H_A \otimes H_B$. They would like to send the sum of Alice’s information $(a_1, a_2) \in F_2^2$ and Bob’s information $(b_1, b_2) \in F_2^2$ to Carol through two quantum channels. The protocol is given as follows:

1. Alice and Bob apply the unitaries $W(a_1, a_2)$ on $H_A$ and $W(b_1, b_2)$ on $H_B$, respectively;
2. Alice and Bob send the qubits $H_A$ and $H_B$, respectively, over noiseless quantum channels;
3. Carol performs a Bell measurement on the system $H_A \otimes H_B$ and obtains $(a_1 + b_1, a_2 + b_2)$ as the protocol output.

III. $[n, k]$-MDS CODED QPIR WITH $t$-COLLUSION

Let $n$ be the number of servers, $L = \min \{ l \in \mathbb{N} : 4^l \geq n \}$ and $F_{4^L}$ be the finite field with $4^L$ elements. We present a protocol with user and server secrecy, in which the user retrieves a file $x^K$ from a DSS of $n$ servers coded with an $[n, k]$-MDS storage code $C$. We denote the $k \times n$ generator
A coded QPIR scheme

Preparation Step. For each \( p \in [k] \) the servers prepare the following qubits and states. Server \( s \in \{2, \ldots, n-1\} \) possesses \( 3L\beta \) qubits \( H_{s}^{(l, b, p)} \), where \( l \in [L] \), \( b \in [\beta] \). The first and the last server possess \( L\beta \) qubits \( H_{1}^{(l, b, p)} \) and \( H_{n}^{(l, b, p)} \) respectively. If \( n \) is odd, server \( n-1 \) possesses \( L\beta \) additional qubits \( H_{n-1}^{(l, b, p)} \).

The maximally entangled state \( |\Phi\rangle^{(l, b, p)} \) is shared between each pair \( H_{s}^{(l, b, p)} \) and \( H_{s+1}^{(l, b, p)} \) for any \( s \in [n-1] \) and \( H_{2c}^{(l, b, p)} H_{2c+1}^{(l, b, p)} \) for any \( c \in \left[ \left\lfloor \frac{n}{2} \right\rfloor - 1 \right] \). If \( n \) is odd, then an additional \( |\Phi\rangle^{(l, b, p)} \) is shared between \( H_{n-1}^{(l, b, p)} \) and \( H_{n}^{(l, b, p)} \).

The protocol for querying the \( K \)-th file is depicted in Figure 1 and described as follows:

1. Suppose the user wants to retrieve the symbol \( y_{p}^{K} \) stored in server \( p \in [k] \). Then, he generates \( n-k \) independent and uniformly random vectors \( Z_{1}^{(p)}, \ldots, Z_{n-k}^{(p)} \in (\mathbb{F}_4^L)^{m} \), and encodes them as codewords of the dual code \( C \), i.e.,

\[
\begin{bmatrix}
Z_{1}^{(p)} \\
\vdots \\
Z_{n-k}^{(p)}
\end{bmatrix} = G_{C} \cdot \xi_{K,p},
\]

where \( \xi_{K,p} \) is the null matrix with a 1 in position \((K,p)\).

2. The user sends query \( Q_{s}^{(p)} \) to each server \( s \in [n] \).

3. In round \( b \), server \( s \in [n] \) computes \( H_{s}^{(l, b, p)} = \langle Q_{s}^{(p)} | y_{s,b} \rangle \in \mathbb{F}_4^L \) and divides it into \( L \) elements \( H_{1s}^{(l, b, p)}, \ldots, H_{Ls}^{(l, b, p)} \) of \( \mathbb{F}_4 \) by the bijection \( \varphi \) defined in Figure 1. For each \( l \in [L] \), the servers perform these steps:

a. server 1 and server \( n \) apply \( W(H_{1s}^{(l, b, p)}) \) and \( W(H_{n}^{(l, b, p)}) \) to the qubits \( H_{1}^{(l, b, p)} \) and \( H_{n}^{(l, b, p)} \), respectively;

b. server \( s \in \{2, \ldots, n-1\} \) applies \( W(H_{s}^{(l, b, p)}) \) to the qubits \( H_{s}^{(l, b, p)} \) and performs a Bell measurement on \( H_{s}^{Ls} \otimes H_{s}^{Rs} \) the outcome of which is denoted by \( G_{s}^{(l, b, p)} \). Then, server \( s \) applies \( W(G_{s}^{(l, b, p)}) \) to the qubits \( H_{s}^{(l, b, p)} \).

4. Each server sends its \( L \) qubits \( H_{s}^{(l, b, p)} \) to the user. If \( n \) is odd, server \( n-1 \) sends its additional \( L \) qubits \( H_{n-1}^{(l, b, p)} \).

5. For each \( l \in [L] \), the user performs the following steps:

a. If \( n \) is even, he performs a Bell measurement on each \( H_{2c}^{(l, b, p)} \) to retrieve \( G_{2c}^{(l, b, p)} \) via the two-sum transmission protocol (cf. Sec. 11-A) for every \( c \in \left[ \frac{n}{2} \right] - 1 \), and computes

\[
G_{l}^{(l, b, p)} = \sum_{c=1}^{n-2} \left( G_{2c}^{(l, b, p)} + G_{2c+1}^{(l, b, p)} \right).
\]

b. If \( n \) is odd, he also performs a Bell measurement on the pair \( H_{n-1}^{(l, b, p)} \otimes H_{n}^{(l, b, p)} \) to retrieve \( G_{n-1}^{(l, b, p)} \) and computes

\[
G_{l}^{(l, b, p)} = \sum_{c=1}^{n-2} \left( G_{2c}^{(l, b, p)} + G_{2c+1}^{(l, b, p)} \right) + G_{n-1}^{(l, b, p)}.
\]

Finally, he depacketizes \( y_{p,b}^{K} \) from the \( L \) outcomes through the bijection \( \varphi^{-1} \).

(6) Repeat Steps 3, 4 and 5 for every round \( b \in [\beta] \).

(7) Repeat all the previous steps for every piece \( p \in [k] \).

(8) Now the user possesses \( \{ y_{p,b}^{K} \} : b \in [\beta], p \in [k] \). First, he depacketizes \( y_{K}^{p} \) from the \( \beta \) elements of \( (\mathbb{F}_4)^{m} \) for each \( p \in [k] \) and builds \( y_{K} := \left( y_{K}^{1}, \ldots, y_{K}^{k} \right) \). Then, he computes the desired file \( x_{K}^{p} \), the bijection \( \varphi \) in the figure denotes \( |\Phi\rangle^{(l, b, p)} \), where \( G_{C}^{o} \) is the \( k \times k \) submatrix of \( G_{C} \) constructed with its first \( k \) columns.

B. Properties of the coded QPIR scheme

**Lemma 2.** The scheme of Section 11-A is correct, i.e., fulfills Definition 7.

**Proof.** The final state before the measurement performed by the user is reached in the same way as the one of the QPIR...
protocol in [12] for each $p \in [k]$. Thus, during round $b \in [\beta]$ and for packet $l \in [L]$, that final state is
\begin{equation}
(−1)^{\tilde{\phi}_{n}} \mathcal{W}_{n} \left( \sum_{a=1}^{n} H_{a} \right) |\Phi\rangle,
\end{equation}
where $\tilde{\phi}_{n} \in \mathbb{F}_{2}$ is determined upon measurement $H_{1}, \ldots, H_{n}$, $G_{1}, \ldots, G_{n−1}$ and $G$.

We need to prove that the outcome of the measurement performed on the system $\mathcal{H}_{1}^{1(b,p)} \otimes \mathcal{H}_{n}^{1(b,p)}$ is $y_{p,b}^{K,1}$ for every $b \in [\beta]$, $p \in [k]$ and $l \in [L]$. Suppose $L = 1$ and fixed $b, p$. We have $H_{s}^{1(b,p)} = \langle Q_{s}^{(p)} | y_{s,b} \rangle$. Denoting $e_{p}^{n}$ the zero vector with length $n$ and $a$ in position $p$, $\delta_{i,K} e_{p}^{n}$ is the $i$-th row of $\xi_{K,p}$. Therefore,
\begin{equation}
\sum_{s=1}^{n} H_{s}^{1(b,p)} = \sum_{s=1}^{n} \langle Q_{s}^{(p)} | y_{s,b} \rangle = \sum_{s=1}^{n} \sum_{i=1}^{m} Q_{i}^{(p)} y_{s,b}^{i,n} = \sum_{i=1}^{m} y_{b}^{i} \left( Q_{i}^{(p)} \right)^{T} T = \sum_{i=1}^{m} y_{b}^{i} \left( G_{C}^{(i−p)} \right)^{T} + \delta_{i,K} e_{p}^{n} \right)^{T} = \sum_{i=1}^{m} x_{b}^{i} G_{C} \left( G_{C}^{(i−p)} \right)^{T} + x_{b}^{K} G_{C} \left( e_{p}^{n} \right)^{T}
\end{equation}
where (a) holds because the dual of a code is its nullspace. If $L > 1$, we have that $H_{s}^{1(b,p)}$ is the $l$-th entry of the index $K$ and generated by encoding random vectors by the dual code $C_{s}^{⊥}$. Since the dual code is MDS, every set of $n−k$ positions in these codewords is independent and hence at least $n−k+1$ servers are needed in order to determine the file requested. Thus, user privacy is achieved. For each $l \in [L]$, server secrecy is achieved because in every round $b$ the received state of the user is independent of the fragments $y_{p,b}^{i,1}$ with $i \neq K$ and the measurement outcomes $C_{s}^{(1(b,p))}$ are mutually independent and independent of any file for all $s \in \{2, \ldots, n\}$.

Lemma 3. The scheme of Section III-A is symmetric and protects against t-collusion in the sense of Definition 2.

Proof. For any $p$ the queries $Q_{1}^{(p)} \ldots, Q_{n}^{(p)}$ are independent of the index $K$ and generated by encoding random vectors by the dual code $C_{s}^{⊥}$. Since the dual code is MDS, every set of $n−k$ positions in these codewords is independent and hence at least $n−k+1$ servers are needed in order to determine the file requested. Thus, user privacy is achieved. For each $l \in [L]$, server secrecy is achieved because in every round $b$ the received state of the user is independent of the fragments $y_{p,b}^{i,1}$ with $i \neq K$ and the measurement outcomes $C_{s}^{(1(b,p))}$ are mutually independent and independent of any file for all $s \in \{2, \ldots, n\}$.

Theorem 1. The PIR rate of the scheme in Section III-A is
\begin{equation}
R_{\text{PIR}} = \left\{ \begin{array}{ll}
\frac{2}{n}, & \text{if } n \text{ is even}, \\
\frac{n}{2n+1}, & \text{if } n \text{ is odd},
\end{array} \right.
\end{equation}
in which $n = k + t$.

Proof. The upload cost is $U_{\text{PIR}} = k n |Q| = k m n$ and $\lim_{\beta \rightarrow \infty} \frac{U_{\text{PIR}}}{R_{\text{PIR}}} = \lim_{\beta \rightarrow \infty} \frac{k m n}{k L \beta} = 0$. Hence, we consider the upload cost to be negligible compared to the download cost for a large file size $F$. As discussed in Remark 1, every qubit carries 1 bit of information. The download cost is $L n$ or $L (n+1)$ qubits per round and piece, i.e., $D_{\text{PIR}} = k L n \beta$ or $D_{\text{PIR}} = k L (n+1) \beta$ bits, if $n$ is even or odd, respectively. The information retrieved is a symbol of $\mathbb{F}_{2}L$ per round and piece, i.e., $I_{\text{PIR}} = k \beta L (4L) = 2 k L \beta$ bits. Thus, the rate is $R_{\text{PIR}} = \frac{2 k L \beta}{2 k L \beta} = \frac{2}{2} = \frac{n}{n+1}$ if $n$ is even and $R_{\text{PIR}} = \frac{2 k L \beta}{4 k L \beta} = \frac{n}{2n+1}$ if $n$ is odd.

IV. [4,2]-CODED QPIR EXAMPLE

Let us consider $n = 4$ servers. Then $L = 1$, and the base field is $\mathbb{F}_{4} = \{0, 1, \alpha, \alpha^{2}\}$ where $\alpha$ is a primitive element that satisfies
\begin{equation}
\alpha^{2} + \alpha + 1 = 0.
\end{equation}

1 It is well-known that the dual of an MDS code is also an MDS code.
Suppose also $\beta = 1$, hence the set of files $x^i = (x_1^i, x_2^i)$ is given by $X = \{ x^i \in (\mathbb{F}_2)^2 : i \in [m] \}$. The files are encoded with a $[4, 2]$-Reed–Solomon storage code with generator matrix

$$G_C = \begin{bmatrix} 1 & 0 & \alpha^2 & \alpha \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix}.$$ 

Hence, the codewords are

$$y^i = x^i G_C = \begin{bmatrix} x_1^i \\ x_2^i \end{bmatrix} 2 \alpha^2 x_1^i + \alpha x_2^i \alpha x_1^i + \alpha^2 x_2^i.$$

Server $s \in [4]$ stores the $s$-th column of $y^i$, namely $y^i_s$.

**Preparation Step.** For each $p \in [2]$ the servers prepare the following qubits and states. Server $s \in \{2, 3\}$ possesses 3 qubits $H_s^{L(p)}$, $H_s^{R(p)}$ and $H_s^{4(p)}$. The first and the last server possess qubits $H_1^{L(p)}$ and $H_3^{R(p)}$, respectively. The maximally entangled state $|\Phi\rangle^{(p)}$ is shared between the pairs $(H_1^{(p)}, H_2^{L(p)})$, $(H_2^{R(p)}, H_3^{L(p)})$, $(H_3^{R(p)}, H_4^{(p)})$ and $(H_4^{2(p)}, H_3^{3(p)})$.

The protocol for querying the $K$-th file $x^K$ is depicted in Figure 2 and is described as follows:

1. The user wants to retrieve the symbol $y^K_p$ stored in server $p \in [2]$. He generates two independent and uniformly random vectors $Z_1 \in (\mathbb{F}_2)^m$ and $Z_2 \in (\mathbb{F}_2)^n$, and encodes them as codewords of the dual code of $\mathcal{C}$.

2. The user sends query $Q_s(p)$ to each server $s \in [4]$.

3. Server $s \in \{4\}$ computes $H_s^{l(p)} = (Q_s(p)) | y_s \rangle \in \mathbb{F}_2$. For bijection (1) each $H_s^{l(p)}$ can be written as an element of $\mathbb{F}_2^4$. Then, the first and the last server apply $W(H_1^{p})$ and $W(H_4^{p})$ to the qubits $H_1^{L(p)}$ and $H_4^{R(p)}$, respectively.

4. Server $s \in \{2, 3\}$ applies $W(H_2^{p})$ to the qubit $H_2^{L(p)}$ and performs a Bell measurement on $H_s^{L(p)} \otimes H_s^{R(p)}$ whose outcome is denoted by $G_s^{(p)} \in \mathbb{F}_2^2$. Finally, server $s$ applies $W(G_s^{(p)})$ to the qubit $H_s^{4(p)}$.

5. Each server sends its qubit $H_s^{4(p)}$ to the user.

6. The user performs a Bell measurement to the pair $H_2^{p} \otimes H_2^{p}$ to retrieve $G^{(p)} = G_2^{(p)} + G_3^{(p)}$ via the two-sum transmission protocol (cf. Sec II-C). He applies $W(G^{(p)})$ to the qubit $H_4^{4(p)}$ and performs a Bell measurement on $H_4^{4(p)} \otimes H_4^{4(p)}$, whose outcome is $y^K_p$ with probability 1.

7. Repeat all the previous steps for every piece $p \in [2]$.

The operations performed by the servers and the download step (Step 4) are visualized in Figure 3. After these steps, the user possesses the entangled pairs of qubits $H_2^{2(p)} \otimes H_2^{3(p)}$ and $H_4^{4(p)} \otimes H_4^{4(p)}$ for each $p \in [2]$. The states of those two pairs are, respectively,

$$W_2(G_2^{(p)}) W_3(G_3^{(p)}) |\Psi\rangle \equiv W_3(G^{(p)}) |\Phi\rangle,$$

$$(-1)^{\delta_4^{(p)}} W_4 \left( \sum_{s = 1}^{4} H_s^{(p)} + G^{(p)} \right) |\Phi\rangle,$$

where $\sum_{s = 1}^{4} H_s^{(p)} = x^K_p$. The proof is straightforward is for every $p \in [2]$. Performing a Bell measurement on the first pair, the user retrieves $G^{(p)}$ and then applies $W(G^{(p)})$ to the qubit $H_4^{4(p)}$. Doing so, the state of the second pair becomes

$$(-1)^{\delta_4^{(p)}} W_4(G^{(p)}) W_4(x^K_p + G^{(p)}) |\Phi\rangle$$

and

$$(-1)^{\delta_4^{(p)}} W_4(x^K_p) |\Phi\rangle.$$
Performing now the Bell measurement on the second pair, the user retrieves $x^K_p$ with probability 1. After retrieving $x^K_1$ and $x^K_2$, the user depacketizes the requested file $x^K$.

User and server secrecy are achieved for $\frac{3}{2}$. The rate is $R_{\text{PIR}} = \frac{2 \cdot 2}{4} = \frac{1}{2}$, since we recovered four bits and downloaded eight qubits each carrying one bit over two rounds.

ACKNOWLEDGMENTS

The authors would like to thank Prof. M. Hayashi and S. Song for helpful discussions.

REFERENCES

[1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” in Proceedings of IEEE 36th Annual Foundations of Computer Science. IEEE, 1995, pp. 41–50.

[2] H. Sun and S. A. Jafar, “The capacity of robust private information retrieval with colluding databases,” IEEE Transactions on Information Theory, vol. 64, no. 4, pp. 2361–2370, 2017.

[3] ———, “The capacity of symmetric private information retrieval,” IEEE Transactions on Information Theory, vol. 65, no. 1, pp. 322–329, 2018.

[4] K. Banawan and S. Ulukus, “The capacity of private information retrieval from coded databases,” IEEE Transactions on Information Theory, vol. 64, no. 3, pp. 1945–1956, 2018.

[5] Q. Wang and M. Skoglund, “Symmetric private information retrieval for MDS coded distributed storage,” in 2017 IEEE International Conference on Communications (ICC). IEEE, 2017, pp. 1–6.

[6] K. Banawan and S. Ulukus, “The capacity of private information retrieval from Byzantine and colluding databases,” IEEE Transactions on Information Theory, vol. 65, no. 2, pp. 1206–1219, Feb 2019.

[7] R. Freij-Hollanti, O. W. Gnilke, C. Hollanti, and D. A. Karpuk, “Private information retrieval from coded databases with colluding servers,” SIAM Journal on Applied Algebra and Geometry, vol. 1, no. 1, pp. 647–664, 2017.

[8] H. Sun and S. A. Jafar, “Private information retrieval from mds coded data with colluding servers: Settling a conjecture by Freij-Hollanti et al.” IEEE Transactions on Information Theory, vol. 64, no. 2, pp. 1000–1022, Feb 2018.

[9] L. Holzbaur, R. Freij-Hollanti, J. Li, and C. Hollanti, “On the capacity of private information retrieval from coded, colluding, and adversarial servers,” in 2019 IEEE Inf. Theory Workshop (ITW), 2019.

[10] ———, “On the capacity of private information retrieval from coded, colluding, and adversarial servers,” arXiv preprint arXiv:1903.12552v3, 2019.

[11] S. Song and M. Hayashi, “Capacity of quantum private information retrieval with multiple servers,” arXiv preprint arXiv:1903.10209. 2019.

[12] ———, “Capacity of quantum private information retrieval with collusion of all but one of servers,” arXiv preprint arXiv:1903.12556, 2019.

[13] R. Tajeddine, O. W. Gnilke, and S. El Rouayheb, “Private information retrieval from MDS coded data in distributed storage systems,” IEEE Transactions on Information Theory, vol. 64, no. 11, pp. 7081–7093, 2018.

[14] M. A. Nielsen and I. L. Chuang, “Quantum computation and quantum information,” Phys. Today, vol. 54, pp. 60–2, 2001.

[15] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes. Elsevier, 1977, vol. 16.