A New Approach to Harnessing Side Information in Multi-Server Private Information Retrieval

Ningze Wang, Anoosheh Heidarzadeh, and Alex Sprintson

***Abstract*—This paper presents new solutions for Private Information Retrieval (PIR) with side information. This problem is motivated by PIR settings in which a client has side information about the data held by the servers and would like to leverage this information in order to improve the download rate. The problem of PIR with side information has been the subject of several recent studies that presented achievability schemes as well as converses for both multi-server and single-server settings. However, the solutions for the multi-server settings adapted from the solutions for the single-server setting in a rather straightforward manner, relying on the concept of *super-messages*. Such solutions require an exponential degree of sub-packetization (in terms of the number of messages).**

This paper makes the following contributions. First, we revisit the PIR problem with side information and present a new approach to leverage side information in the context of PIR. The key idea of our approach is a randomized algorithm to determine the linear combinations of the sub-packets that need to be recovered from each server. In addition, our approach takes advantage of the fact that the identity of the side information messages does not need to be kept private, and, as a result, the information retrieval scheme does not need to be symmetric. Second, we present schemes for PIR with side information that achieve a higher rate than previously proposed solutions and require a significantly lower degree of sub-packetization (linear in the number of servers). Our scheme not only achieves the highest known download rate for the problem at hand but also invalidates a previously claimed converse bound on the maximum achievable download rate.

I. Introduction

Private Information Retrieval (PIR) is a fundamental problem in information security and privacy. The goal of the PIR is to retrieve data from one or more remote servers while protecting the identity of the retrieved data items. The problem has attracted significant attention within the computer science community since the 1990s (see, e.g., [1]) and more recently has become a very active research topic in the information theory community (see, e.g., [2]–[6] and references therein). This research has produced many interesting results on several important variations of the PIR problem, including PIR in the presence of colluding servers [6]–[12], PIR from coded data [13]–[15], as well as multi-message PIR [16], [17].

This paper presents new approaches for the design of multi-server PIR schemes that leverage prior side information. The problem is inspired by PIR scenarios where a user has prior information about the data stored on the servers and would like to leverage it to maximize the download rate.

The PIR setting with side information was initially studied in single-server scenarios (refer to, e.g., [18]–[30]). This line of work has been extended to multi-server settings, including cache-aided PIR [31]–[33], PIR with side information [34]–[36], PIR with private side information [37]–[39], PIR with private coded side information [40], and multi-message PIR with private side information [41]. In PIR problems with private side information, it is required to prevent any server from identifying the side information messages. This requirement results in a lower rate than in scenarios where the side information messages do not need to be kept private.

The most relevant to our work are the papers by Kadhe *et al.* [35] and Li and Gastpar [36]. In particular, [35] extends the PIR scheme developed for the single-server PIR problem for the more general multi-server setting. Later, [36] claimed a converse bound on the maximum achievable download rate for the multi-server PIR in the presence of side information.

In this work, we make the following contributions. First, we revisit the PIR problem with side information and present a new technique to leverage side information for the construction of more efficient multi-server PIR schemes. Our approach generalizes the probabilistic method due to Tian *et al.* [4] for settings with side information. The key idea is that since the identity of the side information messages does not need to be kept private, the information retrieval scheme does not need to be symmetric. In particular, the information requested from a server does not need to have an equal probability across different sets of demand and side information. This offers more flexibility in designing the retrieval scheme, enabling us to achieve higher rates compared to symmetric schemes.

Second, we use this approach to construct an efficient randomized algorithm that determines the linear combinations of sub-packets that need to be recovered from each server. Our scheme achieves the highest known download rate for this problem. In particular, the rate of our scheme is higher than that of the scheme in [35] when $M+1$ does not divide K, where M is the number of side information messages and K is the total number of messages stored at the servers. In addition, our scheme requires a much lower sub-packetization level of $N-1$, compared to the sub-packetization level of N^K required by the existing solutions, where N is the number of servers. A lower degree of sub-packetization has many practical advantages, including reduced complexity. Moreover, the rate achieved by our scheme invalidates the converse bound on the maximum achievable download rate claimed in [36].

Ningze Wang and Alex Sprintson are with the Department of Electrical and Computer Engineering, Texas A&M University (E-mail: {ningzewang, spalex}@tamu.edu). Anoosheh Heidarzadeh is with the Department of Electrical and Computer Engineering, Santa Clara University, (E-mail: aheidarzadeh@scu.edu).

979-8-3503-8284-6/24/$31.00 ©2024 IEEE

II. Problem Setup

We use bold-face symbols to represent random variables and regular symbols for their realizations. For an integer $i \geq 1$, we denote the set $\{1, \ldots, i\}$ by $[i]$, and denote the set $\{0\} \cup [i]$ by $[0 : i]$. For any set, we refer to its subsets of size k as k-subsets. We denote the ith component of a vector v by $\mathrm{v}(i)$, and denote its support, which refers to the index set of its nonzero components, by $\mathrm{supp}(\mathrm{v})$.

In this work, we revisit the problem of *Private Information Retrieval with Side Information (PIR-SI)*, which was initially introduced in [35] and subsequently studied in [36]. For completeness, the problem formulation is presented below.

For a prime power q and an integer $L \geq 1$, let $\mathbb{F}_q$ be a finite field of order q, and $\mathbb{F}_q^L$ be the L-dimensional vector space over $\mathbb{F}_q$.

Consider $N > 1$ non-colluding servers each of which stores an identical copy of $K > 1$ messages $\mathrm{X}_1, \ldots, \mathrm{X}_K$, where each message X_i is a vector in $\mathbb{F}_q^L$. That is, each message X_i consists of L sub-packets $\mathrm{X}_{i,1}, \ldots, \mathrm{X}_{i,L}$, where each sub-packet $\mathrm{X}_{i,j}$ is a symbol from $\mathbb{F}_q$. We refer to L as the *sub-packetization level* and q as the *field size*. Consider a scenario where a user wants to retrieve the message X_{W} for some $\mathrm{W} \in [K]$, and the user has prior knowledge of M messages $\mathrm{X}_{\mathrm{S}} := \{\mathrm{X}_i : i \in \mathrm{S}\}$ for some M-subset $\mathrm{S} \subseteq [K] \setminus \{\mathrm{W}\}$. We refer to X_{W} as the *user's demand* and W as the *demand's index*. In addition, we refer to X_{S} as the *user's side information*, S as the *side information's index set*, and M as the *number of side information messages*.

In line with prior work, we make the following assumptions in this work: (i) $\mathbf{X}_1, \ldots, \mathbf{X}_K$ are independent uniform random variables over $\mathbb{F}_q^L$; (ii) $\mathbf{W}$ is a uniform random variable over $[K]$, and $\mathbf{S}$ is a uniform random variable over all M-subsets of $[K] \setminus \{\mathrm{W}\}$ given $\mathbf{W} = \mathrm{W}$; (iii) The random variables $(\mathbf{W}, \mathbf{S})$ and $(\mathbf{X}_1, \ldots, \mathbf{X}_K)$ are independent; (iv) The distribution of $(\mathbf{W}, \mathbf{S})$ is known in advance to all servers; and (v) The realization (W, S) is not initially known to any server.

For each $n \in [N]$, the user generates a query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$, which is a (deterministic or stochastic) function of (W, S), and sends the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$ to server n. For each $n \in [N]$, it is required that the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$ does not reveal any information about the demand's index W to server n. That is, for all $n \in [N]$, it must hold that

$$I(\mathbf{W}; \mathbf{Q}_n^{[\mathbf{W},\mathbf{S}]}) = 0,$$

or equivalently,

$$\mathbb{P}(\mathbf{Q}_n^{[\mathbf{W},\mathbf{S}]} = \mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]} | \mathbf{W} = \mathrm{W}^*) = \mathbb{P}(\mathbf{Q}_n^{[\mathbf{W},\mathbf{S}]} = \mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]})$$

for all $\mathrm{W}^* \in [K]$. We refer to this requirement as the *privacy condition*. It should be noted that the privacy condition does not imply the privacy of the side information's index set S. That is, the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$ may leak some information about S to server n, while satisfying the privacy condition. This differs from the Private Information Retrieval with Private Side Information (PIR-PSI) setting considered in [37]–[39], where both the demand's index W and the side information's index set S must be kept private from each server.

Upon receiving the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$, server n generates an answer $\mathrm{A}_n^{[\mathrm{W},\mathrm{S}]}$, and sends it back to the user. The answer $\mathrm{A}_n^{[\mathrm{W},\mathrm{S}]}$ is a deterministic function of $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$ and $\mathrm{X}_1, \ldots, \mathrm{X}_K$. That is, $H(\mathbf{A}_n^{[\mathrm{W},\mathrm{S}]} | \mathbf{Q}_n^{[\mathrm{W},\mathrm{S}]}, \mathbf{X}_1, \ldots, \mathbf{X}_K) = 0$. The user must be able to recover their demand X_{W} given the collection of answers $\mathrm{A}^{[\mathrm{W},\mathrm{S}]} := \{\mathrm{A}_n^{[\mathrm{W},\mathrm{S}]} : n \in [N]\}$, the collection of queries $\mathrm{Q}^{[\mathrm{W},\mathrm{S}]} := \{\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]} : n \in [N]\}$, the side information X_{S}, and the realizations W and S. That is,

$$H(\mathbf{X}_{\mathrm{W}} | \mathbf{A}^{[\mathrm{W},\mathrm{S}]}, \mathbf{Q}^{[\mathrm{W},\mathrm{S}]}, \mathbf{X}_{\mathrm{S}}) = 0.$$

We refer to this requirement as the *recoverability condition*.

The PIR-SI problem is to design a protocol for generating a collection of queries $\mathrm{Q}^{[\mathrm{W},\mathrm{S}]}$ and the corresponding collection of answers $\mathrm{A}^{[\mathrm{W},\mathrm{S}]}$ for any given (W, S) such that both the privacy and recoverability conditions are satisfied.

We define the *rate* of a PIR-SI scheme as the ratio of the number of bits required by the user, i.e., $H(\mathbf{X}_{\mathrm{W}}) = B := L \log_2 q$, to the total number of bits downloaded from all servers, i.e., $\sum_{n=1}^{N} H(\mathbf{A}_n^{[\mathrm{W},\mathrm{S}]} | \mathbf{Q}_n^{[\mathrm{W},\mathrm{S}]})$. Note that the number of bits downloaded from each server n, i.e., $H(\mathbf{A}_n^{[\mathrm{W},\mathrm{S}]} | \mathbf{Q}_n^{[\mathrm{W},\mathrm{S}]})$, is given by

$$\sum \mathbb{P}(\mathbf{Q}_n^{[\mathrm{W},\mathrm{S}]} = \mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}) H(\mathbf{A}_n^{[\mathrm{W},\mathrm{S}]} | \mathbf{Q}_n^{[\mathrm{W},\mathrm{S}]} = \mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}),$$

where the summation is over all query realizations $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$.

It is important to highlight that we define rate based on the conditional entropy of each server's answer given the user's query sent to that server, i.e., $H(\mathbf{A}_n^{[\mathrm{W},\mathrm{S}]} | \mathbf{Q}_n^{[\mathrm{W},\mathrm{S}]})$. This metric accurately captures the expected number of bits downloaded from server n, because the user's query sent to server n is known to both the user and server n. In contrast, the (unconditional) entropy of the answer from each server, i.e., $H(\mathbf{A}_n^{[\mathrm{W},\mathrm{S}]})$, which was used in previous works, e.g., in [2] and [3], for rate calculation, takes also into account the randomness of the query. This can potentially introduce excessive uncertainty, which is irrelevant to the expected number of downloaded bits. It should be noted that, regardless of which rate definition is used, the rate of the PIR-SI scheme presented in [35] remains unchanged. This is because, in this scheme, the length of the answer (i.e., the number of bits downloaded) from each server is the same for all query realizations. As a consequence, the entropy of the answer and the conditional entropy of the answer given the query are equal. However, this equivalence may not hold for PIR-SI schemes in which the answer length varies across different query realizations.

In this work, our goal is to characterize the *capacity* of PIR-SI, defined as the maximum achievable rate among all PIR-SI schemes, in terms of the number of servers N, the number of messages K, the number of side information messages M, the sub-packetization level L, and the field size q. We consider all values of $N > 1$, $K > 1$, $1 \leq M \leq K - 1$, and $q \geq 2$. Additionally, we focus on cases with $1 \leq L \leq N - 1$. Such small values of L are particularly interesting when considering schemes that utilize linear operations at the sub-packet level and require a low sub-packetization level.

III. Main Results

In this section, we present our main results and discuss the existing bounds on the capacity of PIR-SI for all admissible values of N, K, M, L, and q.

To simplify the notation, we define $g := \lceil \frac{K}{M+1} \rceil$, and $r_k := \prod_{j=1}^{k} \frac{K/(M+1)-j}{j}$ for all $k \in [g-1]$.

Theorem 1. *The capacity of PIR-SI with N servers, K messages, M side information messages, the sub-packetization level $L = N-1$, and the field size q, is lower bounded by*

$$R := (N-1)\left(N - \left(1 + \sum_{k=1}^{g-1} r_k (N-1)^k\right)^{-1}\right)^{-1}. \quad (1)$$

To establish this result, we present a novel PIR-SI scheme that achieves the rate R defined in (1). The retrieval process in our scheme relies on linear operations at the sub-packet level, and requires recovering no more than one linear combination of message sub-packets from each server. The distinctive aspect of our scheme lies in its randomized strategy to identify the message sub-packets to be combined and determine the specific linear combination to be recovered from each server. This strategy is carefully designed to ensure both the privacy and recoverability conditions, while taking advantage of the fact that the side information messages do not require privacy.

Theorem 2. *With R defined in* (1) *and R^* defined as*

$$R^* := \frac{N^g - N^{g-1}}{N^g - 1}, \quad (2)$$

it follows that $R \geq R^*$ for all values of N, K, and M. In particular, we have $R = R^*$ when K is divisible by $M+1$, and $R > R^*$ when K is not divisible by $M+1$.

Theorem 3. *The capacity of PIR-SI with the same parameters as in Theorem 1, except when $L < N-1$, is lower bounded by R_L defined as in* (1)*, except when N is replaced by $L+1$.*

The proof follows from a simple two-step application of our PIR-SI scheme, and is omitted for brevity. Here, we outline the key steps of the proof. First, the user chooses $L+1$ servers arbitrarily. Then, the user employs the proposed scheme designed for the case with $L+1$ servers, K messages, M side information messages, and the sub-packetization level L, to privately retrieve the demand message with the help of the side information messages. This achieves the rate R_L defined similarly to R as in (1) when N is replaced by $L+1$.

Remark 1. Our PIR-SI scheme serves as a nontrivial extension of the PIR scheme presented in [4] to incorporate side information. In the PIR scheme of [4], the space of query realizations includes a linear combination of any subset of messages, or more generally, a linear combination of their respective sub-packets with one sub-packet per message. However, in the PIR-SI setting, not all of these query realizations are necessary, and excluding certain query realizations can potentially increase the rate. Specifically, it is unnecessary to retrieve any side information message or any linear combination of any subset of side information messages. However, excluding only these query realizations can compromise privacy. This implies the need to exclude additional query realizations beyond those specifically related to side information messages. Moreover, in the PIR scheme of [4], privacy is ensured by employing a uniform probability distribution over all query realizations. However, when some query realizations are excluded, it may be necessary to introduce a non-uniform probability distribution over the remaining ones to maintain privacy. Our PIR-SI scheme maximizes the rate while ensuring privacy by identifying query realizations to exclude and optimizing the probability distribution over the remaining ones.

Remark 2. The best previously-known achievable rate for PIR-SI was reported in [35]. The PIR-SI scheme presented in [35] is based on the following approach: (i) forming g linear combinations of messages, referred to as the *coded messages*, each of which is the sum of a distinct subset of messages, where one of these subsets contains only the demand message and a subset of the side information messages, and (ii) privately retrieving one of these g coded messages, namely, the one containing the demand message, through the application of a capacity-achieving PIR scheme. As shown in [35], this scheme achieves the rate R^* defined in (2). As evident from the result of Theorem 2, our scheme and the one in [35] achieve the same rate when $M+1$ divides K, yet remarkably, our scheme achieves a higher rate when $M+1$ does not divide K. The main difference between these schemes lies in determining which sub-packets of which messages must be combined in each query realization. In the scheme of [35], the query realizations are linear combinations of only g coded messages, each corresponding to a specific subset of messages. This is while our scheme incorporates many more subsets of messages to construct query realizations. Moreover, the scheme of [35] operates exclusively on the sub-packets of the underlying coded messages, where the lth sub-packet of each coded message is the sum of the lth sub-packet of the corresponding messages. In contrast, our scheme goes beyond this limitation by allowing the combination of sub-packets with different indices for any subset of messages. While this flexibility does not result in a rate increase when K is divisible by $M+1$, its advantage becomes apparent when K is not divisible by $M+1$. Specifically, this flexibility allows for utilizing a more efficient probability distribution over query realizations, leading to an improved rate performance.

Remark 3. The capacity of PIR-SI is obviously upper bounded by 1, which coincides with the achievable rate R when $M = K-1$. However, a nontrivial upper bound remains unknown for cases where $1 \leq M \leq K-2$. It was reported in [36] that the capacity is upper bounded by R^*. While R^* matches R when K is divisible by $M+1$, R^* is strictly less than R when K is not divisible by $M+1$. This shows that R^* is not a valid upper bound on the capacity in non-divisible cases. Moreover, it remains unknown whether R^* is indeed the capacity in divisible cases or there exists a scheme that can achieve a rate higher than R^* in such cases.

IV. Proof of Theorem 1

In this section, we present a new PIR-SI scheme that achieves the rate R defined in (1) for any admissible set of values of N, K, M, and q, when $L = N-1$.

The proposed scheme consists of two steps as outlined below.

Step 1: Given the demand's index W and the side information's index set S, the user generates N queries $\mathrm{Q}_1^{[\mathrm{W},\mathrm{S}]},\ldots,\mathrm{Q}_N^{[\mathrm{W},\mathrm{S}]}$, and sends the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$ to server n.

The user's query to each server must specify which sub-packets of which messages are to be combined and what specific combination coefficients are to be used to generate the corresponding answer. In the proposed scheme, each server's answer is either *null*, meaning that the server does not send an answer back to the user, or composed of a *sum* that includes exactly one sub-packet of every message within a designated subset of messages. Thus, the user's query to each server can be represented by a vector $\mathrm{v} \in [0:N-1]^K$, where an all-zero vector corresponds to a null answer, and any nonzero vector corresponds to a specific sum. Specifically, if $\mathrm{v}(i)$ is zero, it means that none of the sub-packets $\mathrm{X}_{i,1},\ldots,\mathrm{X}_{i,N-1}$ contributes to the sum that forms the server's answer, and if $\mathrm{v}(i)$ is equal to $j \neq 0$, it means that the sub-packet $\mathrm{X}_{i,j}$ contributes to the sum forming the answer of the server.

To generate the queries $\mathrm{Q}_1^{[\mathrm{W},\mathrm{S}]},\ldots,\mathrm{Q}_N^{[\mathrm{W},\mathrm{S}]}$, the user employs a randomized algorithm—which depends on W and S—to construct N vectors $\mathrm{v}_1,\ldots,\mathrm{v}_N \in [0:N-1]^K$, and sends the vector $\tilde{\mathrm{v}}_n := \mathrm{v}_{\pi(n)}$ to server n as the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]}$, where $\pi:[N]\to[N]$ is a randomly chosen permutation of $[N]$. The algorithm for constructing $\mathrm{v}_1,\ldots,\mathrm{v}_N$ is described below.

Let $g := \lceil K/(M+1)\rceil$, and $r_k := \prod_{j=1}^{k} \frac{K/(M+1)-j}{j}$ for all $k \in [g-1]$. First, the user randomly selects an integer, denoted by I, from $[0:g-1]$, where the probability of selecting each $k \in [0:g-1]$ is equal to P_k, where

$$P_0 = \left(1+\sum_{k=1}^{g-1} r_k (N-1)^k\right)^{-1}$$

and $P_k = P_0(N-1)^k r_k$ for all $k \in [g-1]$. Given the value of I, the user then proceeds as follows:

1) $I \neq g-1$: First, the user randomly selects a vector $\mathrm{a} \in [0:N-1]^K$ with $\mathrm{supp}(\mathrm{a}) \subset [K]\setminus\{\mathrm{W}\}\cup\mathrm{S}$ and $|\mathrm{supp}(\mathrm{a})| = I(M+1)$. If $I=0$, the vector a is all-zero. Otherwise, if $I \neq 0$, the vector a corresponds to a sum of $I(M+1)$ sub-packets, each belonging to one message from the set of interference messages, i.e., messages that are neither demand nor side information.

Next, the user randomly selects a vector $\mathrm{b} \in [0:N-1]^K$ with $\mathrm{supp}(\mathrm{b}) = \mathrm{S}$. The vector b corresponds to a sum of M sub-packets, each belonging to one side information message. Then, the user forms the vectors $\mathrm{v}_1,\ldots,\mathrm{v}_N$ by setting

$$\mathrm{v}_1 = \mathrm{a}, \text{ and } \mathrm{v}_{n+1} = \mathrm{a}+\mathrm{b}+\mathrm{c}_n, \quad \forall n \in [N-1],$$

where $\mathrm{c}_j \in [0:N-1]^K$ represents the vector corresponding to the jth sub-packet of the demand message X_{W}. That is, $\mathrm{c}_j(i) = 0$ for $i \in [K]\setminus\{\mathrm{W}\}$, and $\mathrm{c}_j(\mathrm{W}) = j$.

2) $I = g-1$: First, the user randomly selects a vector $\mathrm{a} \in [0:N-1]^K$ with $\mathrm{supp}(\mathrm{a}) = [K]\setminus\{\mathrm{W}\}\cup\mathrm{S}$. The vector a corresponds to a sum of $K-M-1$ sub-packets, each belonging to one interference message.

Next, the user randomly selects a vector $\mathrm{b}_1 \in [0:N-1]^K$ with $\mathrm{supp}(\mathrm{b}_1) \subseteq \mathrm{S}$ and $|\mathrm{supp}(\mathrm{b}_1)| = g(M+1)-K$. The user then randomly selects a vector $\mathrm{b}_2 \in [0:N-1]^K$ with $\mathrm{supp}(\mathrm{b}_2) = \mathrm{S}\setminus\mathrm{supp}(\mathrm{b}_1)$. Note that $|\mathrm{supp}(\mathrm{b}_2)| = K-(g-1)(M+1)-1$. The vectors b_1 and b_2 respectively correspond to a sum of $g(M+1)-K$ and $K-(g-1)(M+1)-1$ sub-packets, each belonging to one side information message. Then, the user forms the vectors $\mathrm{v}_1,\ldots,\mathrm{v}_N$ by setting

$$\mathrm{v}_1 = \mathrm{a}+\mathrm{b}_1, \text{ and } \mathrm{v}_{n+1} = \mathrm{a}+\mathrm{b}_1+\mathrm{b}_2+\mathrm{c}_n, \quad \forall n \in [N-1],$$

where $\mathrm{c}_1,\ldots,\mathrm{c}_{N-1}$ are defined as before.

Step 2: Upon receiving the query $\mathrm{Q}_n^{[\mathrm{W},\mathrm{S}]} = \tilde{\mathrm{v}}_n$ $(= \mathrm{v}_{\pi(n)})$, if the vector $\tilde{\mathrm{v}}_n$ is nonzero, server n computes the sum

$$\tilde{\mathrm{Y}}_n := \sum_{i\in\mathrm{supp}(\tilde{\mathrm{v}}_n)} \mathrm{X}_{i,\tilde{\mathrm{v}}_n(i)},$$

and sends back $\tilde{\mathrm{Y}}_n$ to the user as the answer $\mathrm{A}_n^{[\mathrm{W},\mathrm{S}]}$. Otherwise, if the vector $\tilde{\mathrm{v}}_n$ is all-zero, server n does not send back any answer to the user, and the user sets $\tilde{\mathrm{Y}}_n = 0$.

Lemma 1. *The proposed scheme satisfies both the privacy and recoverability conditions and achieves the rate R in* (1).

Proof: The proof can be found in the extended version of this work, [42]. □

V. Proof of Theorem 2

We need to show that (i) $R = R^*$ when K is divisible by $M+1$, and (ii) $R > R^*$ when K is not divisible by $M+1$, where R and R^* are defined in (1) and (2), respectively.

First, consider the case (i). In this case, $g = K/(M+1)$. Thus, $r_k = \prod_{j=1}^{k}\frac{g-j}{j} = \binom{g-1}{k}$ for all $k \in [g-1]$. Moreover, by the binomial theorem, $1+\sum_{k=1}^{g-1}\binom{g-1}{k}(N-1)^k = N^{g-1}$. Thus, it follows that $P_0 = N^{1-g}$, which implies that

$$R = \frac{N-1}{N-P_0} = \frac{N-1}{N-N^{1-g}} = \frac{N^g-N^{g-1}}{N^g-1} = R^*.$$

Now, consider the case (ii). In this case, $g > K/(M+1)$. Thus, $r_k = \prod_{j=1}^{k}\frac{K/(M+1)-j}{j} < \prod_{j=1}^{k}\frac{g-j}{j} = \binom{g-1}{k}$ for all $k \in [g-1]$. This implies that $\sum_{k=1}^{g-1} r_k(N-1)^k < \sum_{k=1}^{g-1}\binom{g-1}{k}(N-1)^k$, and consequently,

$$P_0 = \left(1+\sum_{k=1}^{g-1} r_k(N-1)^k\right)^{-1} > \left(1+\sum_{k=1}^{g-1}\binom{g-1}{k}(N-1)^k\right)^{-1} = N^{1-g},$$

implying that

$$R = \frac{N-1}{N-P_0} > \frac{N-1}{N-N^{1-g}} = \frac{N^g-N^{g-1}}{N^g-1} = R^*.$$

VI. An Illustrative Example

Consider $N = 3$ servers, each storing $K = 3$ messages $\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3$, where each message X_i consists of $L = N - 1 = 2$ sub-packets $\mathrm{X}_{i,1}$ and $\mathrm{X}_{i,2}$. Suppose that a user wants to retrieve one message, say, X_1, and the user knows $M = 1$ other message, say, X_2. That is, $\mathrm{W} = 1$ and $\mathrm{S} = \{2\}$.

To generate the $N = 3$ queries, one for each server, the user proceeds as follows to construct $N = 3$ vectors $\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3 \in [0 : N-1]^K = [0:2]^3$, each of length $K = 3$ with components from $[0 : N-1] = \{0, 1, 2\}$.

Noting that $g = \lceil K/(M+1) \rceil = 2$, the user begins by randomly selecting $I \in [0 : g-1] = \{0, 1\}$, where the probability of $I = 0$ (or $I = 1$) is P_0 (or P_1). In this example, $P_0 = (1 + \sum_{k=1}^{g-1} r_k (N-1)^k)^{-1} = \frac{1}{2}$ and $P_1 = 1 - P_0 = \frac{1}{2}$.

If $I = 0$, the user sets $\mathrm{a} = [0, 0, 0]$ and randomly selects $\mathrm{b} \in \{[0, 1, 0], [0, 2, 0]\}$. Note that (i) $\mathrm{supp}(\mathrm{a}) = \emptyset$, and (ii) $\mathrm{supp}(\mathrm{b}) = \mathrm{S} = \{2\}$. Otherwise, if $I = 1$, the user randomly selects $\mathrm{a} \in \{[0, 0, 1], [0, 0, 2]\}$ and $\mathrm{b}_1 \in \{[0, 1, 0], [0, 2, 0]\}$, and sets $\mathrm{b}_2 = [0, 0, 0]$. Note that (i) $\mathrm{supp}(\mathrm{a}) = [K] \setminus \{\mathrm{W}\} \cup \mathrm{S} = \{3\}$, (ii) $\mathrm{supp}(\mathrm{b}_1) \subseteq \mathrm{S} = \{2\}$ and $|\mathrm{supp}(\mathrm{b}_1)| = g(M+1) - K = 1$, and (iii) $\mathrm{supp}(\mathrm{b}_2) = \mathrm{S} \setminus \mathrm{supp}(\mathrm{b}_1) = \emptyset$.

Given the vectors a and b (or b_1 and b_2) and the $N - 1 = 2$ vectors $\mathrm{c}_1 = [1, 0, 0]$ and $\mathrm{c}_2 = [2, 0, 0]$ with $\mathrm{supp}(\mathrm{c}_1) = \mathrm{supp}(\mathrm{c}_2) = \{\mathrm{W}\} = \{1\}$, the user constructs the vectors $\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3$ by using the algorithm described in Step 1. In this example, there are six feasible sets of vectors $\{\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3\}$ in total, with two sets for $I = 0$ and the remaining four sets for $I = 1$. The table presented below enumerates all six sets of vectors $\{\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3\}$ along with their corresponding probabilities $P_{\{\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3\}}$, where the first two rows correspond to $I = 0$, and the last four rows correspond to $I = 1$.

v_1	v_2	v_3	$P_{\{\mathrm{v}_1,\mathrm{v}_2,\mathrm{v}_3\}}$
$[0,0,0]$	$[1,1,0]$	$[2,1,0]$	$P_0/2$
$[0,0,0]$	$[1,2,0]$	$[2,2,0]$	$P_0/2$
$[0,1,1]$	$[1,1,1]$	$[2,1,1]$	$P_1/4$
$[0,2,1]$	$[1,2,1]$	$[2,2,1]$	$P_1/4$
$[0,1,2]$	$[1,1,2]$	$[2,1,2]$	$P_1/4$
$[0,2,2]$	$[1,2,2]$	$[2,2,2]$	$P_1/4$

Followed by constructing $\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3$, the user randomly selects a permutation $\pi : [3] \to [3]$, and sends the query vector $\mathrm{v}_{\pi(n)}$ to server n. Upon receiving $\mathrm{v}_{\pi(n)}$, if $\mathrm{v}_{\pi(n)}$ is nonzero, server n sends back the answer sum $\mathrm{Y}_{\pi(n)} = \sum_{i \in \mathrm{supp}(\mathrm{v}_{\pi(n)})} \mathrm{X}_{i, \mathrm{v}_{\pi(n)}(i)}$; otherwise, if $\mathrm{v}_{\pi(n)}$ is all-zero, no answer is sent back, and $\mathrm{Y}_{\pi(n)} = 0$. In this example, there are six feasible sets of sums $\{\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3\}$, one for each set of vectors $\{\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3\}$. Table I lists all six sets of sums $\{\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3\}$ and their probabilities $P_{\{\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3\}}$. For completeness, we also present Table II which lists all six sets of sums $\{\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3\}$ and their probabilities $P_{\{\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3\}}$, for the general case of $\mathrm{W} = i$, $\mathrm{S} = \{j\}$, and $[K] \setminus \{\mathrm{W}\} \cup \mathrm{S} = [3] \setminus \{i, j\} = \{k\}$, where $\{i, j, k\}$ is an arbitrary permutation of $[3]$.

TABLE I
$\mathrm{W} = 1, \mathrm{S} = \{2\}$

Y_1	Y_2	Y_3	$P_{\{\mathrm{Y}_1,\mathrm{Y}_2,\mathrm{Y}_3\}}$
0	$\mathrm{X}_{1,1} + \mathrm{X}_{2,1}$	$\mathrm{X}_{1,2} + \mathrm{X}_{2,1}$	$P_0/2$
0	$\mathrm{X}_{1,1} + \mathrm{X}_{2,2}$	$\mathrm{X}_{1,2} + \mathrm{X}_{2,2}$	$P_0/2$
$\mathrm{X}_{2,1} + \mathrm{X}_{3,1}$	$\mathrm{X}_{1,1} + \mathrm{X}_{2,1} + \mathrm{X}_{3,1}$	$\mathrm{X}_{1,2} + \mathrm{X}_{2,1} + \mathrm{X}_{3,1}$	$P_1/4$
$\mathrm{X}_{2,2} + \mathrm{X}_{3,1}$	$\mathrm{X}_{1,1} + \mathrm{X}_{2,2} + \mathrm{X}_{3,1}$	$\mathrm{X}_{1,2} + \mathrm{X}_{2,2} + \mathrm{X}_{3,1}$	$P_1/4$
$\mathrm{X}_{2,1} + \mathrm{X}_{3,2}$	$\mathrm{X}_{1,1} + \mathrm{X}_{2,1} + \mathrm{X}_{3,2}$	$\mathrm{X}_{1,2} + \mathrm{X}_{2,1} + \mathrm{X}_{3,2}$	$P_1/4$
$\mathrm{X}_{2,2} + \mathrm{X}_{3,2}$	$\mathrm{X}_{1,1} + \mathrm{X}_{2,2} + \mathrm{X}_{3,2}$	$\mathrm{X}_{1,2} + \mathrm{X}_{2,2} + \mathrm{X}_{3,2}$	$P_1/4$

TABLE II
$\mathrm{W} = i, \mathrm{S} = \{j\}$

Y_1	Y_2	Y_3	$P_{\{\mathrm{Y}_1,\mathrm{Y}_2,\mathrm{Y}_3\}}$
0	$\mathrm{X}_{i,1} + \mathrm{X}_{k,1}$	$\mathrm{X}_{i,2} + \mathrm{X}_{k,1}$	$P_0/2$
0	$\mathrm{X}_{i,1} + \mathrm{X}_{k,2}$	$\mathrm{X}_{i,2} + \mathrm{X}_{k,2}$	$P_0/2$
$\mathrm{X}_{j,1} + \mathrm{X}_{k,1}$	$\mathrm{X}_{i,1} + \mathrm{X}_{j,1} + \mathrm{X}_{k,1}$	$\mathrm{X}_{i,2} + \mathrm{X}_{j,1} + \mathrm{X}_{k,1}$	$P_1/4$
$\mathrm{X}_{j,2} + \mathrm{X}_{k,1}$	$\mathrm{X}_{i,1} + \mathrm{X}_{j,2} + \mathrm{X}_{k,1}$	$\mathrm{X}_{i,2} + \mathrm{X}_{j,2} + \mathrm{X}_{k,1}$	$P_1/4$
$\mathrm{X}_{j,1} + \mathrm{X}_{k,2}$	$\mathrm{X}_{i,1} + \mathrm{X}_{j,1} + \mathrm{X}_{k,2}$	$\mathrm{X}_{i,2} + \mathrm{X}_{j,1} + \mathrm{X}_{k,2}$	$P_1/4$
$\mathrm{X}_{j,2} + \mathrm{X}_{k,2}$	$\mathrm{X}_{i,1} + \mathrm{X}_{j,2} + \mathrm{X}_{k,2}$	$\mathrm{X}_{i,2} + \mathrm{X}_{j,2} + \mathrm{X}_{k,2}$	$P_1/4$

Consider an arbitrary $n \in [3]$, and suppose that server n receives the query vector v^* from the user. To verify that the privacy condition is met, we need to show that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = \mathrm{W}^*) = \mathbb{P}(\mathbf{Q}_n = \mathrm{v}^*)$ for all $\mathrm{W}^* \in [3]$. As an example, consider the case of $\mathrm{v}^* = [0, 2, 1]$. In this case, server n sends the answer $\mathrm{Y}^* = \mathrm{X}_{2,2} + \mathrm{X}_{3,1}$ to the user.

First, consider $\mathrm{W}^* = 1$. From the table corresponding to the case of $(\mathrm{W}, \mathrm{S}) = (1, \{2\})$, it follows that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 1, \mathbf{S} = \{2\}) = \frac{1}{3} \times \frac{P_1}{4} = \frac{1}{24}$. Similarly, in the table for the case of $(\mathrm{W}, \mathrm{S}) = (1, \{3\})$, we observe that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 1, \mathbf{S} = \{3\}) = \frac{1}{3} \times \frac{P_1}{4} = \frac{1}{24}$. Since $\mathbb{P}(\mathbf{S} = \{2\} | \mathbf{W} = 1) = \mathbb{P}(\mathbf{S} = \{3\} | \mathbf{W} = 1) = \frac{1}{2}$, it follows that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 1) = \frac{1}{2} \times \frac{1}{24} + \frac{1}{2} \times \frac{1}{24} = \frac{1}{24}$.

Next, consider $\mathrm{W}^* = 2$. From the tables corresponding to the cases of $(\mathrm{W}, \mathrm{S}) = (2, \{1\})$ and $(\mathrm{W}, \mathrm{S}) = (2, \{3\})$, it follows that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 2, \mathbf{S} = \{1\}) = \frac{1}{3} \times \frac{P_0}{2} = \frac{1}{12}$ and $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 2, \mathbf{S} = \{3\}) = 0$. Since $\mathbb{P}(\mathbf{S} = \{1\} | \mathbf{W} = 2) = \mathbb{P}(\mathbf{S} = \{3\} | \mathbf{W} = 2) = \frac{1}{2}$, we find that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 2) = \frac{1}{2} \times \frac{1}{12} + \frac{1}{2} \times 0 = \frac{1}{24}$.

Lastly, consider $\mathrm{W}^* = 3$. In the tables for the cases of $(\mathrm{W}, \mathrm{S}) = (3, \{1\})$ and $(\mathrm{W}, \mathrm{S}) = (3, \{2\})$, we observe that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 3, \mathbf{S} = \{1\}) = 0$ and $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 3, \mathbf{S} = \{2\}) = \frac{1}{3} \times \frac{P_0}{2} = \frac{1}{12}$. Since $\mathbb{P}(\mathbf{S} = \{1\} | \mathbf{W} = 3) = \mathbb{P}(\mathbf{S} = \{2\} | \mathbf{W} = 3) = \frac{1}{2}$, we find that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = 3) = \frac{1}{2} \times 0 + \frac{1}{2} \times \frac{1}{12} = \frac{1}{24}$.

By the above results, $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = \mathrm{W}^*) = \frac{1}{24}$ for all $\mathrm{W}^* \in [3]$. Since $\mathbb{P}(\mathbf{W} = \mathrm{W}^*) = \frac{1}{3}$ for all $\mathrm{W}^* \in [3]$, it follows that $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^*) = 3 \times \frac{1}{3} \times \frac{1}{24} = \frac{1}{24}$. Thus, $\mathbb{P}(\mathbf{Q}_n = \mathrm{v}^* | \mathbf{W} = \mathrm{W}^*) = \mathbb{P}(\mathbf{Q}_n = \mathrm{v}^*)$ for all $\mathrm{W}^* \in [3]$, implying that the privacy condition is met for the case of $\mathrm{v}^* = [0, 2, 1]$. Similarly, it can be shown that the privacy condition is met for all other cases of v^*.

For this example, the proposed scheme achieves the rate $R = (N-1)/(N-P_0) = 4/5$, which is higher than the rate $R^* = (N^g - N^{g-1})/(N^g - 1) = 3/4$ achieved by the scheme presented in [35].

REFERENCES

[1] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private Information Retrieval," *Journal of the ACM (JACM)*, vol. 45, no. 6, pp. 965–981, 1998.

[2] H. Sun and S. A. Jafar, "The Capacity of Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4075–4088, July 2017.

[3] ——, "Optimal download cost of private information retrieval for arbitrary message length," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2920–2932, 2017.

[4] C. Tian, H. Sun, and J. Chen, "Capacity-Achieving Private Information Retrieval Codes with Optimal Message Size and Upload Cost," *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7613–7627, 2019.

[5] S. Vithana, K. Banawan, and S. Ulukus, "Semantic Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2635–2652, 2022.

[6] 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, 2018.

[7] 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, 2019.

[8] Z. Zhang and J. Xu, "The Optimal Sub-Packetization of Linear Capacity-Achieving PIR Schemes with Colluding Servers," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 2723–2735, 2019.

[9] X. Yao, N. Liu, and W. Kang, "The Capacity of Private Information Retrieval Under Arbitrary Collusion Patterns," in *IEEE International Symposium on Information Theory*, 2020, pp. 1041–1046.

[10] Y. Lu, Z. Jia, and S. A. Jafar, "Double Blind T-Private Information Retrieval," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 428–440, 2021.

[11] L. Holzbaur, R. Freij-Hollanti, J. Li, and C. Hollanti, "Toward the Capacity of Private Information Retrieval From Coded and Colluding Servers," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 517–537, 2022.

[12] R. Zhou, C. Tian, H. Sun, and J. S. Plank, "Two-level private information retrieval," *IEEE Journal on Selected Areas in Information Theory*, vol. 3, no. 2, pp. 337–349, 2022.

[13] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, C. Hollanti, and S. E. Rouayheb, "Private Information Retrieval Schemes for Coded Data with Arbitrary Collusion Patterns," in *IEEE International Symposium on Information Theory*, June 2017, pp. 1908–1912.

[14] 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, March 2018.

[15] K. Banawan, B. Arasli, Y.-P. Wei, and S. Ulukus, "The Capacity of Private Information Retrieval From Heterogeneous Uncoded Caching Databases," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3407–3416, 2020.

[16] K. Banawan and S. Ulukus, "Multi-Message Private Information Retrieval: Capacity Results and Near-Optimal Schemes," *IEEE Transactions on Information Theory*, vol. 64, no. 10, pp. 6842–6862, Oct 2018.

[17] N. Wang, A. Heidarzadeh, and A. Sprintson, "Multi-Message Private Information Retrieval: A Scalar Linear Solution," in *2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2022, pp. 1–8.

[18] S. Kadhe, B. Garcia, A. Heidarzadeh, S. E. Rouayheb, and A. Sprintson, "Private Information Retrieval with Side Information: The Single Server Case," in *55th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2017, pp. 1099–1106.

[19] S. Li and M. Gastpar, "Single-Server Multi-Message Private Information Retrieval with Side Information," in *56th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2018.

[20] A. Gomez-Leos and A. Heidarzadeh, "Single-Server Private Information Retrieval with Side Information Under Arbitrary Popularity Profiles," in *2022 IEEE Information Theory Workshop (ITW)*, 2022, pp. 101–106.

[21] A. Heidarzadeh, F. Kazemi, and A. Sprintson, "Capacity of Single-Server Single-Message Private Information Retrieval with Coded Side Information," in *IEEE Information Theory Workshop*, Nov 2018.

[22] ——, "Capacity of Single-Server Single-Message Private Information Retrieval with Private Coded Side Information," in *IEEE International Symposium on Information Theory*, July 2019, pp. 1662–1666.

[23] A. Heidarzadeh, S. Kadhe, S. E. Rouayheb, and A. Sprintson, "Single-Server Multi-Message Individually-Private Information Retrieval with Side Information," in *IEEE International Symposium on Information Theory*, July 2019, pp. 1042–1046.

[24] F. Kazemi, E. Karimi, A. Heidarzadeh, and A. Sprintson, "Single-Server Single-Message Online Private Information Retrieval with Side Information," in *IEEE International Symposium on Information Theory*, July 2019, pp. 350–354.

[25] A. Heidarzadeh, F. Kazemi, and A. Sprintson, "The Role of Coded Side Information in Single-Server Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 25–44, 2021.

[26] S. Kadhe, A. Heidarzadeh, A. Sprintson, and O. O. Koyluoglu, "Single-Server Private Information Retrieval Schemes are Equivalent to Locally Recoverable Coding Schemes," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 391–402, 2021.

[27] A. Heidarzadeh and A. Sprintson, "Single-Server Individually-Private Information Retrieval: A Combinatorial Approach," in *IEEE Information Theory Workshop*, 2021.

[28] ——, "The Role of Reusable and Single-Use Side Information in Private Information Retrieval," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 414–419.

[29] Y. Lu and S. A. Jafar, "On Single Server Private Information Retrieval With Private Coded Side Information," *IEEE Transactions on Information Theory*, vol. 69, no. 5, pp. 3263–3284, 2023.

[30] A. Heidarzadeh, S. Kadhe, B. Garcia, S. E. Rouayheb, and A. Sprintson, "On the Capacity of Single-Server Multi-Message Private Information Retrieval with Side Information," in *56th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2018.

[31] R. Tandon, "The Capacity of Cache Aided Private Information Retrieval," in *55th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2017, pp. 1078–1082.

[32] Y. Wei, K. Banawan, and S. Ulukus, "Cache-Aided Private Information Retrieval with Partially Known Uncoded Prefetching: Fundamental Limits," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 6, pp. 1126–1139, June 2018.

[33] Y.-P. Wei, K. Banawan, and S. Ulukus, "Fundamental Limits of Cache-Aided Private Information Retrieval with Unknown and Uncoded Prefetching," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 3215–3232, 2019.

[34] F. Kazemi, E. Karimi, A. Heidarzadeh, and A. Sprintson, "Multi-Server Private Information Retrieval with Coded Side Information," in *Canadian Workshop on Information Theory*, 2019.

[35] S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb, and A. Sprintson, "Private Information Retrieval with Side Information," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2032–2043, 2020.

[36] S. Li and M. Gastpar, "Converse for Multi-Server Single-Message PIR with Side Information," in *54th Annual Conference on Information Sciences and Systems*, 2020, pp. 1–6.

[37] Z. Chen, Z. Wang, and S. A. Jafar, "The Capacity of T-Private Information Retrieval with Private Side Information," *IEEE Transactions on Information Theory*, vol. 66, no. 8, pp. 4761–4773, 2020.

[38] M. Krishnan K. H. and J. Harshan, "On the Existence of XOR-Based Codes for Private Information Retrieval with Private Side Information," *Entropy*, vol. 23, no. 10, 2021.

[39] L. Erhili and A. Heidarzadeh, "Achieving Capacity of PIR with Private Side Information with Low Sub-packetization and without MDS Codes," Jan 2024. [Online]. Available: arXiv:2401.16630

[40] F. Kazemi, E. Karimi, A. Heidarzadeh, and A. Sprintson, "Private Information Retrieval with Private Coded Side Information: The Multi-Server Case," in *57th Annual Allerton Conference on Communication, Control, and Computing*, 2019, pp. 1098–1104.

[41] S. P. Shariatpanahi, M. J. Siavoshani, and M. A. Maddah-Ali, "Multi-Message Private Information Retrieval with Private Side Information," in *IEEE Information Theory Workshop*, 2018.

[42] N. Wang, A. Heidarzadeh, and A. Sprintson, "A New Approach to Harnessing Side Information in Multi-Server Private Information Retrieval," Jan 2024. [Online]. Available: arXiv:2401.16628