

Weakly Private Information Retrieval with Heterogeneity in Servers' Trustfulness

Wenyuan Zhao, Yu-Shin Huang, Ruida Zhou, and Chao Tian

June 20, 2025

Abstract

We study the problem of weakly private information retrieval (PIR) when there is heterogeneity in servers' trustworthiness under the maximal leakage (Max-L) metric and mutual information (MI) metric. A user wishes to retrieve a desired message from N non-colluding servers efficiently, such that the identity of the desired message is not leaked in a significant manner; however, some servers can be more trustworthy than others. We propose a code construction for this setting and optimize the probability distribution for this construction. For the Max-L metric, it is shown that the optimal probability allocation for the proposed scheme essentially separates the delivery patterns into two parts: a completely private part that has the same download overhead as the capacity-achieving PIR code, and a non-private part that allows complete privacy leakage but has no download overhead by downloading only from the most trustful server. The optimal solution is established through a sophisticated analysis of the underlying convex optimization problem and a reduction between the homogeneous setting and the heterogeneous setting. For the MI metric, the homogeneous case is studied first for which the code can be optimized with an explicit probability assignment, while a closed-form solution becomes intractable for the heterogeneous case. Numerical results are provided for both cases to corroborate the theoretical analysis.

1 Introduction

Private information retrieval (PIR) systems [1], initiated by Chor et al. in 1995, were motivated by the necessity to safeguard user privacy during information retrieval. In the standard PIR framework, a user aims to retrieve a specific message from N independent servers, each holding a complete set of K messages. The critical challenge here is to prevent the servers from deducing which message the user is accessing. Typically, messages are quite large, making the download from the servers the dominant communication cost. The efficiency of a PIR system is measured in terms of its PIR capacity: the highest possible information bits per downloaded bit, which was definitively established by Sun and Jafar [2]. Subsequently, an alternative optimal code, known as the TSC code, was introduced by Tian et al. in 2019 [3], featuring the smallest possible message length and query set. Many variations and extensions of the canonical PIR problem have been studied, such as PIR with colluding servers [4–6], storage-constrained PIR [7–18], PIR with symmetric privacy requirement [19–21], and PIR with side information [22–29]; a more comprehensive literature survey can be found in [30].

In certain scenarios, absolute privacy may not be a critical requirement. In these cases, users might tolerate a scenario in which servers can guess the identity of the desired message with low confidence. This leads to the concept of Weakly Private Information Retrieval (W-PIR), which imposes a more relaxed privacy constraint [31–40]. In exchange for loss of privacy, a higher retrieval rate can be achieved. The assessment of privacy leakage in W-PIR has been approached through several different metrics. Differential privacy was used in [32, 33]; conditional entropy was used in [34]; mutual information (MI) was used in [35]; and the maximal leakage (Max-L) metric (see [41]) was adopted in [36, 37, 42]. The W-PIR code in [36] was obtained by breaking the uniform distribution on the retrieval patterns in the TSC code, which increasingly favors the direct download pattern in the code as the privacy requirement is relaxed. The improved construction in [42] is based on the observation that in the high leakage regime, the direct retrieval of the desired message becomes increasingly efficient, effectively reducing the overall cost of the retrieval process in scenarios with higher permissible leakage levels.

In this work, we consider the setting where there is heterogeneity in the trustfulness of the servers, that is, some of the servers may be more trustworthy than others. To address this, we propose a general version of the improved W-PIR code [42], which we designate as the W-PIR[#] code. Our focus is on fine-tuning the probability allocation within this W-PIR[#] framework. Our findings reveal that the optimal strategy for the Max-L metric is surprisingly straightforward: it is essentially a probabilistic sharing between the original TSC code and a direct download from the most trustworthy server. This optimal solution emerges from an intricate examination of a convex optimization problem, initially framed in the context of homogeneously trusted servers. A key aspect of our analysis is that the Max-L setting facilitates a natural transition from a homogeneous trust environment to one that is heterogeneous. For the MI metric, an explicit probability allocation is given in the homogeneous case first, which requires a delicate analysis of the property of the entropy and mutual information. However, a closed-form solution becomes intractable for the heterogeneous setting under the MI metric, for which numerical results are provided to corroborate the theoretical analysis.

The remainder of the paper is organized as follows. In Section 2, we introduce the notation and briefly review the maximal leakage metric, the mutual information metric, and the TSC scheme. The proposed optimal code scheme and a motivating example are presented in section 3. Sections 4 and 5 are devoted to the main results under the Max-L and MI settings, respectively, and Section 6 concludes this paper.

2 Preliminaries

We present a formal introduction to the Weakly Private Information Retrieval (W-PIR) problem, considering both Max-L and MI metrics, with homogeneously and heterogeneously trusted servers. Then we review the TSC code proposed in [3], followed by a discussion on a particular variant of this code tailored to construct W-PIR codes.

2.1 Information Retrieval Systems

There are a total of K mutually independent messages $W_{1:K} := (W_1, W_2, \dots, W_K)$, each of which consists of L i.i.d. symbols uniformly distributed in a finite set \mathcal{X} :

$$\begin{aligned} W_k &:= (W_k[1], W_k[2], \dots, W_k[L]), \quad k \in [1 : K], \\ L &= H(W_1) = H(W_2) = \dots = H(W_K), \end{aligned}$$

where $[1 : K]$ is used to denote the set $\{k : k = 1, 2, \dots, K\}$ in the sequel, and the entropy is calculated using the logarithm of base $|\mathcal{X}|$. Without loss of generality, we assume $K \geq 2$, and an independent copy of all the messages $W_{1:K}$ is stored in a total of N non-colluding servers, respectively. An information retrieval code comprises specific component functions of queries, answers, and decoders. When a user seeks to retrieve a message W_k , $k \in [1 : K]$, from N servers without disclosing the identity of k to any individual server, a private random key $F^* \in \mathcal{F}^*$ is firstly used to generate the queries

$$Q_n^{[k]} := \phi_n(k, F^*), \quad n \in [1 : N], \quad (1)$$

where $Q_n^{[k]} \in \mathcal{Q}_n$, the union of all possible queries $Q_n^{[k]}$ over all k . Upon receiving $Q_n^{[k]}$, the server- n generates an answer $A_n^{(q)}$ as a function of the query $Q_n^{[k]}$ and stored messages $W_{1:K}$, which is produced as

$$A_n^{(q)} := \varphi_n(q, W_{1:K}), \quad n \in [1 : N]. \quad (2)$$

In this work, we assume that the answer symbols are distributed in a finite set \mathcal{Y} which is the same as message symbols, i.e., $\mathcal{X} = \mathcal{Y}$. The length of the answer is denoted as $\ell_n^{(q)}$, which may vary according to the query but not to the messages.

For simplicity of notation, we denote $A_n^{(Q_n^{[k]})}$ by $A_n^{[k]}$ and $\ell_n^{(Q_n^{[k]})}$ as $\ell_n^{[k]}$, both of which are random variables. Using all the answers from N servers, the user intends to decode the message \hat{W}_k with the function

$$\hat{W}_k := \psi(A_{1:N}^{[k]}, k, F^*). \quad (3)$$

An information retrieval code is said to be valid only when the desired message is recovered accurately, that is, $\hat{W}_k = W_k$.

The normalized (worst-case) average download cost is then defined as

$$D := \max_{k \in [1:K]} \mathbb{E} \left[\frac{1}{L} \sum_{n=1}^N \ell_n^{[k]} \right], \quad (4)$$

where the expectation is taken over the set of all random keys F^* . Note that D is determined solely by queries and query distribution, without being influenced by the realization of specific messages or the selection of the desired message index k .

2.2 Maximal Leakage and MI Leakage Metric

We consider *weakly private information retrieval* (W-PIR) where the user intends to control the amount of information leakage that a database can infer from queries. The privacy leakage in the identity of the desired message, represented as the index M of W_M , is due to the query $Q_n^{[M]}$ sent by the user and must be measured for control. We adopted two metrics to study this leakage: Max-L and MI metric.

The Max-L metric $\mathcal{L}(M \rightarrow Q_n^{[M]})$: The Max-L leakage on the message M to the n -th server is defined in [36] and [41] as

$$\mathcal{L}(M \rightarrow Q_n^{[M]}) = \log_2 \left(\sum_{q \in \mathcal{Q}_n} \max_{k \in [1:K]} \mathbb{P}(Q_n^{[k]} = q) \right), \quad (5)$$

which in fact does not depend on the probability distribution of M . The server can estimate M more accurately from $Q_n^{[M]}$ in the sense that $\mathcal{L}(M \rightarrow Q_n^{[M]})$ is large; on the other hand, the retrieval is completely private when $\mathcal{L}(M \rightarrow Q_n^{[M]}) = 0$, and the distribution of $Q_n^{[k]}$ and $Q_n^{[k']}$ is identical for any $k, k' \in [1:K]$. In [41], it was suggested that the exponential of leakage can also be viewed as a measure of information leakage. We can measure the overall privacy leakage under the Max-L metric as $\rho_{(\text{Max-L})}$ by the weighted sum of the exponential leakage amounts to the individual servers

$$\rho_{(\text{Max-L})} \triangleq \sum_{n=1}^N \gamma_n 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})},$$

where $\gamma_n > 0$. Here, the exponential is taken for simplifying the analysis. Without loss of generality, we assume $\gamma_1 \leq \gamma_2 \leq \dots \leq \gamma_N$. In most cases, we shall choose to normalize the weights so that $\sum_{n=1}^N \gamma_n = 1$, however, this is not critical, and we shall utilize this fact in subsequent derivations. Note that the γ_n 's are strictly positive, as otherwise the problem becomes trivial since the optimal strategy is to directly retrieve all messages from this completely trusted server. For the homogeneous trust setting, we simply set $\gamma_n = 1/N$.

The MI metric $MI(M \rightarrow Q_n^{[M]})$: The MI leakage on the message M to the n -th server is defined as

$$MI(M \rightarrow Q_n^{[M]}) := I(M; Q_n), \quad (6)$$

where Q_n is the random variable which represents the query induced jointly by the random key F^* and the random message index M . We assume the message index M is uniformly distributed in $[1:K]$ in this work, and the overall leakage under the MI metric is similarly defined as the weighted sum of the leaked MI to the individual servers

$$\rho_{(\text{MI})} \triangleq \sum_{n=1}^N \gamma_n MI(M \rightarrow Q_n^{[M]}). \quad (7)$$

A *valid* code for W-PIR with K messages and N servers under the download cost constraint d is a collection of functions $(\{\phi_n\}_{n \in [1:N]}, \{\varphi_n\}_{n \in [1:N]}, \psi)$ that can correctly retrieve the desired message and additionally satisfies the download constraint $D \leq d$. A leakage ρ is called achievable for the download cost constraint d , if there exists a valid code such that the leakage $\mathcal{L} \leq \rho$ under the download constraint d . The closure of the collection of these (ρ, d) pairs is called the achievable (ρ, d) region, denoted by $\mathcal{G}_{\text{Max-L}}$ and \mathcal{G}_{MI} under the Max-L metric and the MI metric, respectively.

2.3 The TSC Code and its Permuted Variant

We briefly review the TSC code in [3], and propose one permuted variant of this code that is suitable for our cases where limited information leakage is allowed. In the TSC code, each message consists of symbols $L = N - 1$, i.e.,

$$W_k = (W_k[1], W_k[2], \dots, W_k[N - 1]), \quad k \in [1 : K],$$

where a dummy symbol $W_k[0] = 0$ is prepended at the beginning of all messages. To better facilitate the construction of the new code, especially in a heterogeneous setting, we provide a variation of the original construction, which can be viewed as probabilistic sharing between all permutations (over N servers) of the PIR code in [3].

Define a random vector $F \triangleq (F_1, F_2, \dots, F_{K-1})$ of length- $(K - 1)$, which is uniformly distributed in $[0 : N - 1]^{K-1}$ and a random bijective mapping $\pi : [1 : N] \rightarrow [0 : N - 1]$ (a permutation on the set $[1 : N]$ but downshifted by 1). The random key F^* is defined as the concatenation of F and π :

$$F^* := (F, \pi) = (F_1, F_2, \dots, F_{K-1}, \pi), \quad (8)$$

where F_1, \dots, F_{K-1}, π are mutually independent random variables, and the distribution of π will be specified later. We shall use f to denote a specific realization of the random vector F , and use \mathcal{F} to denote the set of $[0 : N - 1]^{K-1}$, i.e., the set of possible values of the partial random key F .

The function $\phi_n^*(k, F^*)$ to generate the query $Q_n^{[k]}$ for retrieving message- k from server- n is defined as

$$\phi_n^*(k, F^*) \triangleq \left(F_1, F_2, \dots, F_{k-1}, \left(\pi(n) - \sum_{j=1}^{K-1} F_j \right)_N, F_k, F_{k+1}, \dots, F_{K-1} \right), \quad (9)$$

where $(\cdot)_N$ denotes the modulo N operation. Each query is a length- K vector, and we denote the m -th symbol of $Q_n^{[k]}$ as $Q_{n,m}^{[k]}$. Upon receiving the query, the answer $A_n^{[k]}$ is returned from server- n generated by the function

$$\begin{aligned} \varphi_n^*(q, W_{1:K}) &\triangleq W_1[Q_{n,1}^{[k]}] \oplus W_2[Q_{n,2}^{[k]}] \oplus \dots \oplus W_K[Q_{n,K}^{[k]}] \\ &= W_k[(\pi(n) - \sum_{j=1}^{K-1} F_j)_N] \oplus \mathcal{I}, \end{aligned} \quad (10)$$

where \oplus is addition in the given finite field. As a result, \mathcal{I} is the interference signal given by

$$\mathcal{I} = W_1[F_1] \oplus \dots \oplus W_{k-1}[F_{k-1}] \oplus W_{k+1}[F_k] \oplus \dots \oplus W_K[F_{K-1}]. \quad (11)$$

Given the existence of an $n^* \in [1 : N]$ such that $(\pi(n^*) - \sum_{j=1}^{K-1} F_j)_N = 0$, it implies that $A_{n^*}^{[k]} = \mathcal{I}$. Consequently, the user can retrieve the desired message W_k by subtracting \mathcal{I} from $A_n^{[k]}$ for all $n \neq n^*$. It should be noted that with a probability of $N^{-(K-1)}$, the interference signal \mathcal{I} may only consist of dummy symbols, which eliminates the need for its download entirely. In such cases, direct retrieval can be achieved by accessing the desired message from $N - 1$ servers, one symbol per server. The download cost is therefore

$$D^* = \frac{N}{N-1} \left(1 - \frac{1}{N^{K-1}} \right) + \frac{1}{N^{K-1}} = \frac{1 - N^{-K}}{1 - N^{-1}}, \quad (12)$$

matching the capacity result given in [2]. It can be shown that there is no privacy leakage regardless of the distribution of the random permutation π , since for each fixed permutation the resultant code is private. An example of the code (with adjusted probabilities for W-PIR) is given in Section 3 (Tables 1, the lower halves without the # parts); more details can be found in [3].

2.4 Weakly PIR: Reassigned Probabilities in TSC

In the permuted variant of the generalized TSC code, we can reduce the download cost by assigning a higher probability to random keys when $F_1 = F_2 = \dots = F_{K-1} = 0$, i.e. the pattern for which the retrieval downloads the messages without interference at the cost of L . If the probabilities of these random keys are very high, then the messages will be more likely to be downloaded directly from the $N - 1$ servers, resulting in privacy leakage but a lower download cost. If the probabilities of these random keys are the same as for all other keys, then we have the original permuted variant of the TSC code, resulting in completely private retrieval. By adjusting these probability assignments, we obtain a range of weakly private information retrieval codes achieving different trade-offs between the download cost and the privacy leakage. Almost all existing W-PIR code constructions essentially utilize this approach in some manner [35–38].

3 W-PIR[#]: Generalized TSC Code with Escape Retrieval Symbols

3.1 The Proposed Code Construction

For high-leakage situations, the weakly private information retrieval code given above by reassigning probabilities in the TSC code does not perform well. To see this, consider the extreme case of the minimum download cost point, this code will download the messages directly from $N - 1$ servers, resulting in a privacy leakage to all these servers. However, we can instead directly download the message from a single server, therefore, leaking the message index to only one server. This motivates the addition of such direct download patterns in our proposed new code, and these download patterns are denoted as $\#$.

We next present the W-PIR[#] code, which is essentially a probabilistic sharing scheme between the generalized TSC code and the direct retrieval patterns from individual servers. In this code, we again set $L = N - 1$. The random key F^* is generated from the set \mathcal{F}^* with a probability distribution $\mathbb{P}_k(F^*)$, where $\mathcal{F}^* = ([0 : N - 1]^{K-1} \times \mathcal{P}) \cup [1 : N]$ for which $\mathcal{P} = \{\pi\}$ is the set of all bijective mappings $[1 : N] \rightarrow [0 : N - 1]$. This probability distribution of requesting message k is denoted as

$$\mathbb{P}_k(F^*) = \begin{cases} p_{(\#)}^{k, F^*}, & F^* \in [1 : N] \\ p_{(f)}^{k, \pi}, & F^* = (f, \pi) \in [0 : N - 1]^{K-1} \times \mathcal{P} \end{cases}, \quad (13)$$

which needs to satisfy

$$\sum_{n=1}^N p_{(\#)}^{k, n} + \sum_{f \in \mathcal{F}} \sum_{\pi \in \mathcal{P}} p_{(f)}^{k, \pi} = 1, \quad k = 1, 2, \dots, K. \quad (14)$$

The query $Q_n^{[k]}$ to server- n is produced as:

$$Q_n^{[k]} = \begin{cases} \#_k, & F^* = n \\ \underline{0}_K, & F^* \in [1 : N], F^* \neq n, \\ \phi_n^*(k, F^*), & F^* \notin [1 : N] \end{cases}, \quad (15)$$

where $\underline{0}_K$ is the length- K all-zero vector. The answer $A_n^{[k]}$ from server- n is generated as

$$A_n^{[k]} = \begin{cases} W_k, & q = \#_k \\ \varphi^*(q, W_{1:K}), & q \notin \{\#_k : k \in [1 : K]\}. \end{cases} \quad (16)$$

The decoding procedure follows directly from the original generalized TSC code when $F^* \notin [1 : N]$ and does not require decoding when $F^* \in [1 : N]$. We will refer to this code as W-PIR[#]. A simpler version of W-PIR[#], which does not allow all permutations, was first presented in [42].

Table 1: Proposed code for $N = 3, K = 2$

(a) Retrieval of W_1									(b) Retrieval of W_2								
Requesting Message $k = 1$									Requesting Message $k = 2$								
Prob.	F	π or n	Server 1		Server 2		Server 3		Prob.	F	π or n	Server 1		Server 2		Server 3	
			$Q_1^{[1]}$	A_1	$Q_2^{[1]}$	A_2	$Q_3^{[1]}$	A_3				$Q_1^{[2]}$	A_1	$Q_2^{[2]}$	A_2	$Q_3^{[2]}$	A_3
$p_{(\#)}^{1,1}$	#	1	# ₁	a_1, a_2	00	\emptyset	00	\emptyset	$p_{(\#)}^{2,1}$	#	1	# ₂	b_1, b_2	00	\emptyset	00	\emptyset
$p_{(\#)}^{1,2}$	#	2	00	\emptyset	# ₁	a_1, a_2	00	\emptyset	$p_{(\#)}^{2,2}$	#	2	00	\emptyset	# ₂	b_1, b_2	00	\emptyset
$p_{(\#)}^{1,3}$	#	3	00	\emptyset	00	\emptyset	# ₁	a_1, a_2	$p_{(\#)}^{2,3}$	#	3	00	\emptyset	00	\emptyset	# ₂	b_1, b_2
$p_{(0)}^{1,[2,1,0]}$	0	(2, 1, 0)	20	a_2	10	a_1	00	\emptyset	$p_{(0)}^{2,[2,1,0]}$	0	(2, 1, 0)	02	b_2	01	b_1	00	\emptyset
$p_{(0)}^{1,[2,0,1]}$	0	(2, 0, 1)	20	a_2	00	\emptyset	10	a_1	$p_{(0)}^{2,[2,0,1]}$	0	(2, 0, 1)	02	b_2	00	\emptyset	01	b_1
$p_{(0)}^{1,[1,2,0]}$	0	(1, 2, 0)	10	a_1	20	a_2	00	\emptyset	$p_{(0)}^{2,[1,2,0]}$	0	(1, 2, 0)	01	b_1	02	b_2	00	\emptyset
$p_{(0)}^{1,[1,0,2]}$	0	(1, 0, 2)	10	a_1	00	\emptyset	20	a_2	$p_{(0)}^{2,[1,0,2]}$	0	(1, 0, 2)	01	b_1	00	\emptyset	02	b_2
$p_{(0)}^{1,[0,2,1]}$	0	(0, 2, 1)	00	\emptyset	20	a_2	10	a_1	$p_{(0)}^{2,[0,2,1]}$	0	(0, 2, 1)	00	\emptyset	02	b_2	01	b_1
$p_{(0)}^{1,[0,1,2]}$	0	(0, 1, 2)	00	\emptyset	10	a_1	20	a_2	$p_{(0)}^{2,[0,1,2]}$	0	(0, 1, 2)	00	\emptyset	01	b_1	02	b_2
$p_{(1)}^{1,[2,1,0]}$	1	(2, 1, 0)	11	$a_1 \oplus b_1$	01	b_1	21	$a_2 \oplus b_2$	$p_{(1)}^{2,[2,1,0]}$	1	(2, 1, 0)	11	$a_1 \oplus b_1$	10	a_1	12	$a_1 \oplus b_2$
$p_{(1)}^{1,[2,0,1]}$	1	(2, 0, 1)	11	$a_1 \oplus b_1$	21	$a_2 \oplus b_2$	01	b_1	$p_{(1)}^{2,[2,0,1]}$	1	(2, 0, 1)	11	$a_1 \oplus b_1$	12	$a_1 \oplus b_2$	10	a_1
$p_{(1)}^{1,[1,2,0]}$	1	(1, 2, 0)	01	b_1	11	$a_1 \oplus b_1$	21	$a_2 \oplus b_2$	$p_{(1)}^{2,[1,2,0]}$	1	(1, 2, 0)	10	a_1	11	$a_1 \oplus b_1$	12	$a_1 \oplus b_2$
$p_{(1)}^{1,[1,0,2]}$	1	(1, 0, 2)	01	b_1	21	$a_2 \oplus b_2$	11	$a_1 \oplus b_1$	$p_{(1)}^{2,[1,0,2]}$	1	(1, 0, 2)	10	a_1	12	$a_1 \oplus b_2$	11	$a_1 \oplus b_1$
$p_{(1)}^{1,[0,2,1]}$	1	(0, 2, 1)	21	$a_2 \oplus b_2$	11	$a_1 \oplus b_1$	01	b_1	$p_{(1)}^{2,[0,2,1]}$	1	(0, 2, 1)	12	$a_1 \oplus b_2$	11	$a_1 \oplus b_1$	10	a_1
$p_{(1)}^{1,[0,1,2]}$	1	(0, 1, 2)	21	$a_2 \oplus b_2$	01	b_1	11	$a_1 \oplus b_1$	$p_{(1)}^{2,[0,1,2]}$	1	(0, 1, 2)	12	$a_1 \oplus b_2$	10	a_1	11	$a_1 \oplus b_1$
$p_{(2)}^{1,[2,1,0]}$	2	(2, 1, 0)	02	b_2	22	$a_2 \oplus b_2$	12	$a_1 \oplus b_2$	$p_{(2)}^{2,[2,1,0]}$	2	(2, 1, 0)	20	a_2	22	$a_2 \oplus b_2$	21	$a_2 \oplus b_1$
$p_{(2)}^{1,[2,0,1]}$	2	(2, 0, 1)	02	b_2	12	$a_1 \oplus b_2$	22	$a_2 \oplus b_2$	$p_{(2)}^{2,[2,0,1]}$	2	(2, 0, 1)	20	a_2	21	$a_2 \oplus b_1$	22	$a_2 \oplus b_2$
$p_{(2)}^{1,[1,2,0]}$	2	(1, 2, 0)	22	$a_2 \oplus b_2$	02	b_2	12	$a_1 \oplus b_2$	$p_{(2)}^{2,[1,2,0]}$	2	(1, 2, 0)	22	$a_2 \oplus b_2$	20	a_2	21	$a_2 \oplus b_1$
$p_{(2)}^{1,[1,0,2]}$	2	(1, 0, 2)	22	$a_2 \oplus b_2$	12	$a_1 \oplus b_2$	02	b_2	$p_{(2)}^{2,[1,0,2]}$	2	(1, 0, 2)	22	$a_2 \oplus b_2$	21	$a_2 \oplus b_1$	20	a_2
$p_{(2)}^{1,[0,2,1]}$	2	(0, 2, 1)	12	$a_1 \oplus b_2$	02	b_2	22	$a_2 \oplus b_2$	$p_{(2)}^{2,[0,2,1]}$	2	(0, 2, 1)	21	$a_2 \oplus b_1$	20	a_2	22	$a_2 \oplus b_2$
$p_{(2)}^{1,[0,1,2]}$	2	(0, 1, 2)	12	$a_1 \oplus b_2$	22	$a_2 \oplus b_2$	02	b_2	$p_{(2)}^{2,[0,1,2]}$	2	(0, 1, 2)	21	$a_2 \oplus b_1$	20	$a_2 \oplus b_2$	20	a_2

The correctness of the code is obvious, and the download cost D can be simply computed as

$$p_d^k \triangleq \sum_{n=1}^N p_{(\#)}^{k,n} + \sum_{\pi \in \mathcal{P}} p_{(0)_{(K-1)}}^{k,\pi}, k \in [1 : K], \quad (17)$$

$$D = \max_k \left(p_d^k + \frac{N}{N-1} (1 - p_d^k) \right), \quad (18)$$

where p_d^k is the overall probability of using a direct download to retrieve message k , either by retrieving from $(N-1)$ servers, or by retrieving from only 1 servers. We defer the analysis of privacy to Sections 4 and 5.

3.2 An Example When $K = 2$ and $N = 3$

We provide an example of more explicit code construction in Table 1. Consider the case with $K = 2$ messages and $N = 3$ servers. Here the dummy symbols a_0 and b_0 are omitted for conciseness. The random key F^* has a total of 21 possible realizations, each is either associated with a random key and the downshifted permutation function (F, π) , or a direct retrieval specified by the server index. The message length is $L = N - 1 = 2$, and we write the two messages $W_1 = (a_1, a_2)$, $W_2 = (b_1, b_2)$. The queries and answers are given in Table 1. The queries in the top three rows of the two tables directly request the full message from a single server denoted by #₁ and #₂, while the remaining rows are essentially the TSC code with different probabilities for the queries, assigned according to their interference signals and the permutation functions. Note that the interference signal is controlled by the first $(K-1)$ entries F of the random key F^* . Let us denote $\|F\|$ as the *size* of the interference corresponding to the random key F , which is also its Hamming weight; in this example, $\|F\|$ can only be 0 or 1. Note that $|\mathcal{F}|$ is used to denote the *cardinality* of the set \mathcal{F} , different from $\|F\|$.

3.3 The Reduced W-PIR[#] Code

A simpler scheme can in fact be as good as the general W-PIR[#] code in some cases, and this reduced version plays an instrumental role for us to establish the optimal probability allocation for W-PIR[#]. In this reduced version, we set the probability as follows.

$$\mathbb{P}_k(F^*) = \begin{cases} p_{\#}, & F^* \in [1 : N] \\ p_j, & F^* = (F, \pi) \in [0 : N-1]^{K-1} \times \mathcal{P} \\ & : \pi \text{ is cyclic and } \|F\| = j \\ 0, & \text{otherwise} \end{cases}, \quad (19)$$

where $\|F\|$ is the Hamming weight of the first part of the random key (F, π) when $F^* \notin [1 : N]$. In other words, only cyclic permutations are allowed, instead of the full set of permutations; moreover, F 's with the same Hamming weight are assigned the same probability. We say π is *cyclic* when π is in the set of $\{\pi : \pi(n+1) = (\pi(n) + 1)_N, \forall n \in [1 : N]\}$. Note that this reduced W-PIR[#] is *symmetric* even when used in the heterogeneous setting.

The query $Q_n^{[k]}$ can take any possible values in \mathcal{Q} . Denote $t_j \triangleq |\{q \in \mathcal{Q} : \|q\| = j\}|$, which is calculated as

$$t_j = \binom{K}{j} (N-1)^j, \quad \forall j \in [0 : K]. \quad (20)$$

For notational simplicity, let $p_{-1} = p_K = 0$. Similarly, we use s_j to denote $|\mathcal{F}_j|$, that is, the number of random keys f that have Hamming weight j , given by

$$s_j = \binom{K-1}{j} (N-1)^j, \quad \forall j \in [0 : K-1]. \quad (21)$$

The download cost and the corresponding privacy of the reduced W-PIR[#] code under the Max-L and MI metric are discussed in Section 4 and Section 5, respectively.

4 WPIR: The Maximal Leakage Setting

4.1 Main Result

We summarize the main result with *heterogeneous* trustfulness of the servers under the Max-L metric in Theorem 1.

Theorem 1. *An optimal probability assignment for W-PIR[#] under the Max-L metric is given by*

$$p_{(\#)}^{k,1} = \frac{N^K(1-D+D/N)-1}{N^{K-1}-1} := \hat{p}_{\#}, \quad k \in [1 : K];$$

$$p_{(f)}^{k,\pi^*} = \frac{1-\hat{p}_{\#}}{N^{K-1}}, \quad k \in [1 : K], \quad f \in \mathcal{F},$$

where π^* is the mapping $\pi^*(n) = n+1$, and other $p_{(\#)}^{k,n}$ and $p_{(f)}^{k,\pi}$ are assigned value zero. Without loss of generality, let $\gamma_1 \leq \gamma_2 \leq \dots \leq \gamma_n$. As a consequence, with download cost $D \in [1, D^*]$, we have the optimal surrogate leakage for the W-PIR[#] code as

$$\rho_{(Max-L)}^*(D) = \gamma_1 \frac{(K-1)[N^{K-1}(N-(N-1)D)-1]}{N^{K-1}-1} + \sum_{n=1}^N \gamma_n. \quad (22)$$

Theorem 1 implies that without loss of optimality for the W-PIR[#] code, we can directly use probabilistic sharing between a direct download from the most trustworthy server and the original TSC strategy without any permutation. In other words, it consists of a completely public part (to the most trusted server) and

a completely private part, and the proportion of the mixture determines the exact leakage in this trade-off. Intuitively, this strategy makes perfect sense, since the most trusted server will induce the least amount of leakage, and we might as well prefer to retrieve the whole message from it. Note that the probability assignment given in Theorem 1 for the heterogeneous W-PIR[#] is also an optimal probability assignment for the homogeneous setting under this metric.

The proof of Theorem 1 is however quite sophisticated: first, we establish that without the loss of optimality, we can restrict our attention to a special type of probability allocation strategy corresponding to the reduced W-PIR[#] code for the *homogeneous* setting; then we show that a particular probability allocation for the reduced W-PIR[#] code is in fact optimal for the *homogeneous* setting; lastly, we make a reduction based on a special property in the reduced W-PIR[#] code, to yield the optimal probability allocation for the *heterogeneous* setting.

The download cost and maximal leakage of the reduced W-PIR[#] code are given in the following proposition. The proof is relatively straightforward, and we omit it here for brevity.

Proposition 1. *The reduced W-PIR[#] scheme induces the download cost and Max-L pair $(\rho_{(\text{Max-L})}, D)$ given by*

$$D = \frac{N - (Np_{\#} + Np_0)}{N - 1}, \quad (23)$$

$$\begin{aligned} \rho_{(\text{Max-L})} &= \sum_{n=1}^N \gamma_n 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} \\ &= \sum_{n=1}^N \gamma_n \left(\sum_{j=1}^K t_j \max\{p_{j-1}, p_j\} + p_0 + (N + K - 1)p_{\#} \right), \end{aligned} \quad (24)$$

for $p_{\#} \in [0, 1/N]$.

4.2 Homogeneous Trustfulness: Reduced W-PIR[#] is Optimal

Let us consider the homogeneous case under the Max-L metric where $\gamma_1 = \gamma_2 = \dots = \gamma_N = \gamma$, which we shall refer to as problem *P1*:

$$\begin{aligned} &\underset{\substack{p_{(\#)}^{k,n}, p_{(f)}^{k,\pi}}}{\text{minimize}} && \rho_{(\text{Max-L})} = \sum_{n=1}^N \gamma_n 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} \\ &\text{subject to} && p_{(\#)}^{k,n} \geq 0, \quad \forall k, n, \\ &&& p_{(f)}^{k,\pi} \geq 0, \quad \forall k, \pi, f, \\ &&& \sum_{n=1}^N p_{(\#)}^{k,n} + \sum_f \sum_{\pi} p_{(f)}^{k,\pi} = 1, \quad \forall k, \\ &&& p_d^k + \frac{N}{N-1}(1 - p_d^k) \leq D, \quad \forall k. \end{aligned} \quad (25)$$

Recall that $p_{(\#)}^{k,n}$ is the probability of requesting the server- n only for the entire k^{th} message, and $p_{(f)}^{k,\pi}$ is the probability of querying for the k^{th} message under the random key (f, π) . For simplicity, we will write $p_{(0, \frac{0_{K-1}}{0})}^{k,\pi}$ as $p_{(0)}^{k,\pi}$ in the sequel.

We first show that the optimal value of the optimization problem (*P1*) above, which is achieved under the optimal probability distribution in W-PIR[#] code, is the same as the optimal value of the optimization

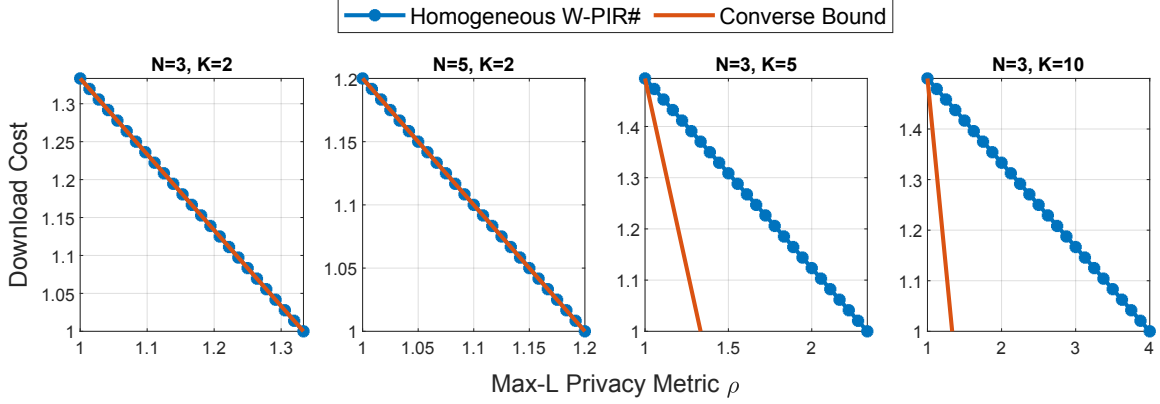


Figure 1: W-PIR[#] v.s. Converse Bound in [37] for the Max-L metric.

problem (P2) below, which is achieved by the optimal probability allocation for the reduced W-PIR[#]:

$$\begin{aligned}
& \underset{p_{\#}, p_0, p_1, \dots, p_{K-1}}{\text{minimize}} && \sum_{j=1}^K t_j \max\{p_{j-1}, p_j\} \\
& && + (p_0 + (N-1)p_{\#}) + Kp_{\#} \\
& \text{subject to} && p_{\#}, p_0, p_1, \dots, p_{K-1} \geq 0, \\
& && Np_{\#} + \sum_{j=0}^{K-1} Ns_j p_j = 1, \\
& && \frac{N - (Np_{\#} + Np_0)}{N-1} \leq D.
\end{aligned} \tag{26}$$

For simplicity of notation, we have taken the convention that $p_{-1} = p_K = 0$. The following proposition establishes the optimality of the reduced W-PIR[#] code.

Proposition 2. *In the homogeneous setting, (P1) = (P2).*

The proof is given in Appendix A by carefully constructing a sequence of inequalities based mainly on the convexity of the maximum function. The optimality of the probabilistic sharing solution of the reduced W-PIR[#] code in the homogeneous setting is established in Theorem 2.

Theorem 2. *With download cost $D \in [1, D^*]$ and homogeneous trustfulness γ , the optimal surrogate leakage under the Max-L metric is given as*

$$\begin{aligned}
\hat{\rho}_{(\text{Max-L})}^*(D) &= \gamma \sum_{n=1}^N 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} \\
&= N\gamma \left(1 + \frac{(K-1) [N^{K-1} (N - (N-1)D) - 1]}{N^K - N} \right),
\end{aligned} \tag{27}$$

which is achieved using the allocation in Theorem 1.

This theorem is proved in Appendix B by analyzing the KKT conditions [43] of the given convex optimization problem and constructing primal and dual solutions satisfying these conditions.

Remark 1. *(Connections to the reduced W-PIR[#] in [42]). We first remark that Theorem 2 is a special case of the heterogeneous setting, when we set $\gamma_1 = \dots = \gamma_n = \gamma$. The optimal probability allocation is achieved using the same strategy as W-PIR[#]. Without loss of generality, when $\gamma = 1/N$, the optimal pair (ρ, D) is equivalent to the reduced W-PIR[#] proposed in [42]. However, if $\gamma \neq 1/N$, there exists a multiplicative ratio between $\hat{\rho}_{(\text{Max-L})}^*$ and the optimal ρ in the reduced W-PIR[#].*

Remark 2. (Connections to the converse bound in [37]). Consider an (N, K) W-PIR scheme with download cost $D \in [1, D^*]$. Under the assumption that the query size does not grow unbounded and the downloaded answer size per server is lower than or equal to the entire retrieved file size, the converse result for the Max-L metric in [37] can be written as

$$\rho_{(\text{Max-L})} \geq 1 + \frac{1}{N} - \frac{(D-1)(1-N^{-1})}{1-N^{-(K-1)}}. \quad (28)$$

The optimal $\hat{\rho}_{(\text{Max-L})}^*$ in Theorem 2 in fact matches this outer bound when $K = 2$ for any number of servers¹. However, for $K > 2$, there exists a discrepancy between W-PIR[#] and the converse result, which is shown in Fig. 1.

4.3 Heterogeneous Trustfulness: Proof of Theorem 1

We are now ready to prove Theorem 1.

Proof. Recall that the loss function, i.e., the objective function, in the *heterogeneous* Max-L setting is

$$\rho_{(\text{Max-L})} = \sum_{n=1}^N \gamma_n 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})}. \quad (29)$$

We can alternatively consider an equivalent loss function ρ_o defined as

$$\rho_o = \sum_{n=1}^N \gamma_n \left(2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} - 1 \right). \quad (30)$$

We shall denote the optimal value under download cost constraint D as $\rho_{(\text{Max-L})}^*(D)$ for the loss function $\rho_{(\text{Max-L})}$, and similarly for other loss functions in the sequel. It is clear that the optimal value $\rho_{(\text{Max-L})}^*(D)$ and the optimal value $\rho_o^*(D)$ are related as

$$\rho_o^*(D) = \rho_{(\text{Max-L})}^*(D) - \sum_{n=1}^N \gamma_n. \quad (31)$$

Next consider a *homogeneous* setting, with the same download cost constraint D and the corresponding surrogate loss function

$$\hat{\rho}_{(\text{Max-L})} = \gamma_1 \sum_{n=1}^N 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})}, \quad (32)$$

as well as the corresponding equivalent loss function $\hat{\rho}_o$

$$\hat{\rho}_o = \gamma_1 \sum_{n=1}^N (2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} - 1). \quad (33)$$

In a similar manner, the optimal $\hat{\rho}_{(\text{Max-L})}^*(D)$ and the optimal $\hat{\rho}_o^*(D)$ are related as

$$\hat{\rho}_o^*(D) = \hat{\rho}_{(\text{Max-L})}^*(D) - N\gamma_1. \quad (34)$$

It is clear that the optimal value of the homogeneous setting $\hat{\rho}_o^*(D)$ is less than or equal to the optimal value of the heterogeneous setting $\rho_o^*(D)$, i.e. $\hat{\rho}_o^*(D) \leq \rho_o^*(D)$, because $\gamma_1 \leq \gamma_2 \leq \dots \leq \gamma_N$ and $2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} \geq$

¹We are grateful to one of the reviewers for bringing this fact to our attention.

1 for any n due to the non-negativity of the maximal leakage metric. Since under this new surrogate loss function the problem is homogeneous, Theorem 2 implies that

$$\begin{aligned} \hat{\rho}_o^*(D) &= \hat{\rho}_{(\text{Max-L})}^*(D) - N\gamma_1 \\ &= N\gamma_1 \left(\frac{(K-1) [N^{K-1}(N - (N-1)D) - 1]}{N^K - N} \right), \end{aligned} \quad (35)$$

which is therefore a lower bound for $\rho_o^*(D)$. It follows that

$$\begin{aligned} \rho_{(\text{Max-L})}^*(D) &= \rho_o^*(D) + \sum_{n=1}^N \gamma_n \geq \hat{\rho}_o^*(D) + \sum_{n=1}^N \gamma_n \\ &= \gamma_1(K-1) \frac{N^{K-1}(N - (N-1)D) - 1}{N^{K-1} - 1} + \sum_{n=1}^N \gamma_n. \end{aligned} \quad (36)$$

However, this lower bound is indeed achieved by the probability distribution assignment in Theorem 1 by assigning

$$\hat{p}_\# = \frac{N^K(1 - D + D/N) - 1}{N^{K-1} - 1}. \quad (37)$$

The proof is thus complete. \square

4.4 Heterogeneous Trustfulness: Numerical Results

The numerical results shown in Fig. 2 compare W-PIR[#] with TSC (without $p_\#$), reduced W-PIR[#] and numerically optimized W-PIR[#]. Our newly proposed code (referred to as W-PIR[#]) establishes a new benchmark point of minimum download cost and privacy leakage trade-offs, which is validated by numerically solving W-PIR[#] with convex programming tools. The numerical results in both homogeneous and heterogeneous settings corroborate the result established in Theorem 1: the optimal (ρ, D) trade-offs under the Max-L metric can be achieved by employing a probabilistic sharing of direct download from the most trustworthy server and the original TSC strategy without any permutation. The balance between the fully public segment to the most trustworthy server and the completely private segment is crucial, as it precisely dictates the level of privacy leakage involved under this trade-off. This is logical, as using the most trusted server minimizes leakage, suggesting that retrieving the entire message from this server is a viable strategy. We further note that the probability allocation of W-PIR[#] in the heterogeneous setting is equally optimal in the homogeneous setting. Although the reduced W-PIR[#] is as good as the W-PIR[#] in the homogeneous setting, it is no longer optimal in the heterogeneous setting. As the number of servers and messages increases, W-PIR[#] achieves the most favorable (ρ, D) trade-offs compared to other schemes with an increasing divergence.

5 WPIR: The Mutual Information Setting

5.1 Main Result

Under the MI metric, the analytical probability allocation for W-PIR[#] in a *heterogeneous* setting is quite sophisticated. Therefore, we first present the main result with *homogeneous* trustfulness of the servers under the MI metric in Theorem 3.

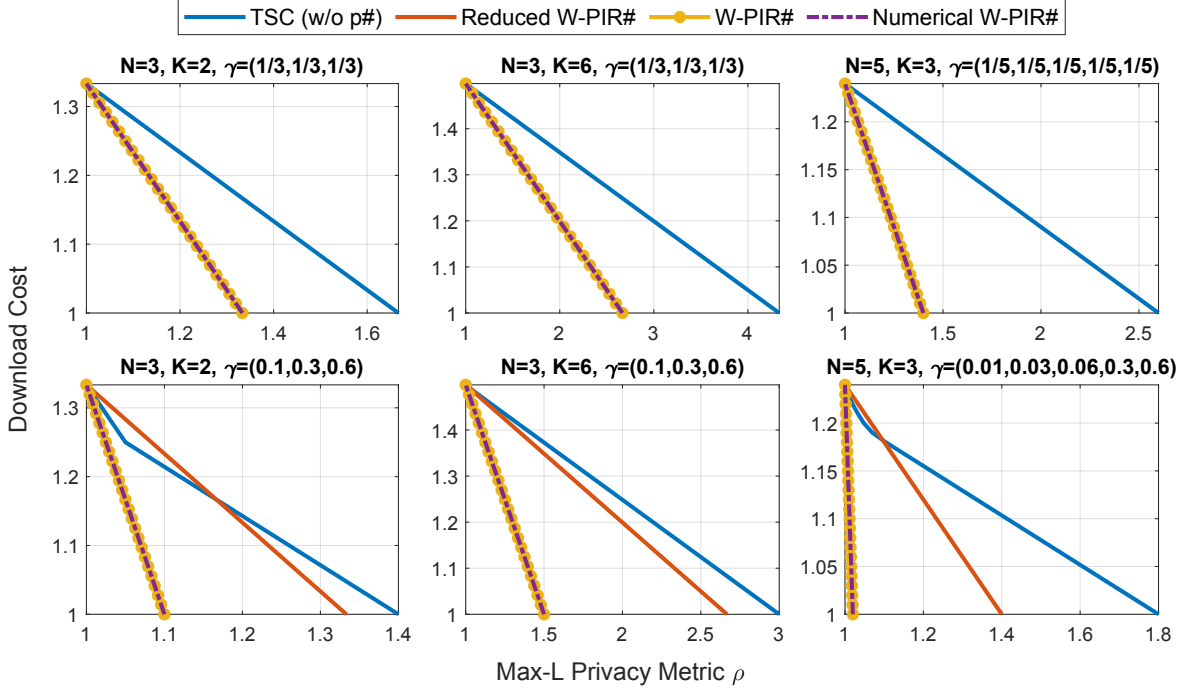


Figure 2: Numerical comparisons between the proposed code and existing codes under the Max-L metric.

Theorem 3. An optimal probability allocation for homogeneous W-PIR# under the MI metric is given by

$$\begin{aligned}
 p_{(\#)}^{k,1} &= Np_{\#} = N(1 - p_0) - (N - 1)D, \quad k \in [1 : K], \\
 p_{(0)}^{k,\pi^*} &= p_0 = (N - 1)(D - 1) \left(\sum_{j=1}^{K-1} Ns_j \prod_{i=1}^j \frac{1}{x_i} \right)^{-1}, \\
 p_{(f)}^{k,\pi^*} &= p_j = p_0 \prod_{i=1}^j \frac{1}{x_i}, \quad (f, \pi) \in \{(f, \pi^*) : \|f\| = j > 0\},
 \end{aligned}$$

where $\pi^* \in \{\pi : \pi(n+1) = (\pi(n) + 1)_N, \forall n\}$, i.e., π^* is cyclic, and other $p_{(\#)}^{k,n}$ and $p_{(f)}^{k,\pi}$ are assigned value zero. $\mathbf{x} = (x_1, x_2, \dots, x_{K-1})$ are defined by the following sequence with $x_1 = \frac{K-1}{K^{\frac{N-1}{N-1}} - 1}$:

$$\begin{aligned}
 \log \frac{(K-j)x_{K-j} + j}{K} &= \sum_{i=0}^{j-1} (1-N)^i \log \frac{(K-1)x_{K-1} + 1}{K} \\
 &\quad - \sum_{i=1}^{j-1} (1-N)^i \log x_{K-j+i}.
 \end{aligned} \tag{38}$$

As a consequence, with download cost $D \in [1, D^*]$, the optimal surrogate leakage for homogeneous W-PIR# under the MI metric is

$$\begin{aligned}
 \rho_{(MI)}^*(D) = I(\mathbf{p}) &:= p_{\#} \log K + \frac{1}{K} \sum_{j=1}^K \binom{K}{j} (N-1)^j \left\{ jp_{j-1} \log p_{j-1} + (K-j)p_j \log p_j \right. \\
 &\quad \left. - [jp_{j-1} + (K-j)p_j] \log \frac{jp_{j-1} + (K-j)p_j}{K} \right\}.
 \end{aligned} \tag{39}$$

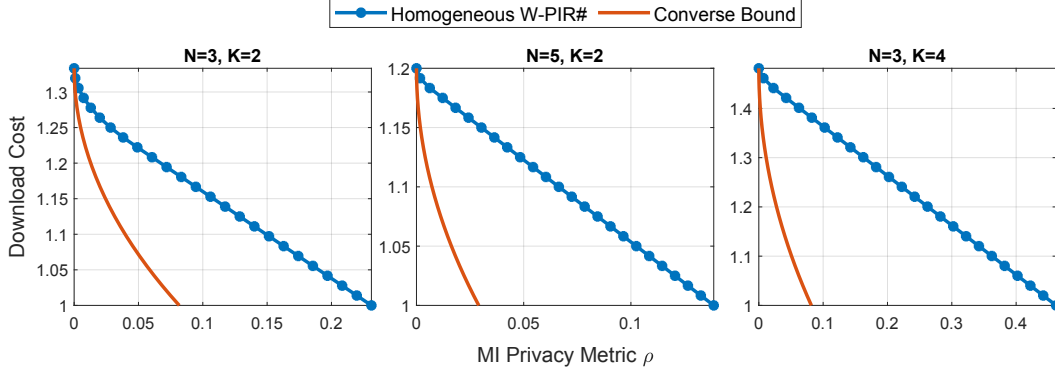


Figure 3: W-PIR[#] v.s. Converse Bound in [37] for the MI metric.

Theorem 3 implies that under the MI metric, we can achieve the optimal \mathcal{G}_{MI} for *homogeneous* W-PIR[#] using the similar reduction in the Max-L setting: a public part (to the most trusted server) and a private part. Note that in homogeneous cases, our proposed probability allocation is equivalent to the reduced symmetric code proposed in [42], where only cyclic permutations are required instead of the entire set of permutations. This allocation strategy has the property of time sharing between the public and the private parts, as shown in Proposition 3. We also compared $\rho_{(\text{MI})}^*$ with the outer bound in [37], which is shown in Fig. 3.

The construction of probability allocation under the MI metric given above is much more sophisticated than that under the Max-L metric. The auxiliary sequence \mathbf{x} is well defined by the above recursive equations when x_1 is specified. It is evident that $\mathbf{p} = (p_{\#}, p_0, p_1, \dots, p_{K-1})$ generates a probability distribution given to the relevant combinatorial coefficients.

We shall show later that the optimality of this structure is broken down in the *heterogeneous* cases, where a *closed-form* solution becomes intractable. We also present numerical results to illustrate the discrepancy between our proposed homo W-PIR[#] allocation and the numerically optimized region \mathcal{G}_{MI} in a *heterogeneous* setting.

To prove Theorem 3, we first establish the reduced W-PIR[#] with a special probability assignment strategy in Proposition 4. We then show that such a reduced W-PIR[#] strategy is, in fact, optimal by carefully investigating the properties of MI and the log sum inequality. Lastly, we construct an explicit probability allocation by carefully solving the KKT conditions of the reduced W-PIR[#] optimization problem. We defer the complete proof of Theorem 3 to Section 5.3.

Proposition 3. *Denote the achievable region of the clean TSC scheme under the MI metric as $\hat{\mathcal{G}}_{\text{MI}}$. In the homogeneous case, the optimal W-PIR[#] strategy under the MI metric is time-sharing between the clean TSC scheme and the extreme point using the direct retrieval pattern # only, i.e., $\mathcal{G}_{\text{MI}} = \text{conv}(\hat{\mathcal{G}}_{\text{MI}} \cup \{(\gamma_1 \log K, 1)\})$.*

Proof. One direction $\text{conv}(\hat{\mathcal{G}}_{\text{MI}} \cup \{(\gamma_1 \log K, 1)\}) \subseteq \mathcal{G}_{\text{MI}}$ is trivial because the time-sharing region can be viewed as \mathcal{G}_{MI} under the additional constraints. In the other direction, we need to show that with the same download cost D , the time-sharing strategy provides a lower bound of MI leakage $\rho_{(\text{MI})}$. Without loss of generality, we set $\gamma_1 = \dots = \gamma_N = \gamma = \frac{1}{N}$ in the homogeneous case. Given the optimal surrogate leakage for homogeneous W-PIR[#] shown by Theorem 3,

$$\rho_{(\text{MI})} = \sum_{n=1}^N \gamma_n \text{MI}(M \rightarrow Q_n^{[M]}) = \sum_{n=1}^N \frac{1}{N} I(Q_n; M) \quad (40)$$

$$\begin{aligned} &\geq p_{\#} \log K + \frac{1}{K} \sum_{j=0}^{K-1} \binom{K}{j} (N-1)^j \left\{ j p_{j-1} \log p_{j-1} + (K-j) p_j \log p_j \right. \\ &\quad \left. - [j p_{j-1} + (K-j) p_j] \log \frac{j p_{j-1} + (K-j) p_j}{K} \right\} \quad (41) \end{aligned}$$

$$\begin{aligned}
&= \alpha \frac{\log K}{N} + (1 - \alpha) \frac{1}{K} \sum_{j=0}^{K-1} \binom{K}{j} (N-1)^j \left\{ j p'_{j-1} \log p'_{j-1} + (K-j) p'_j \log p'_j \right. \\
&\quad \left. - [j p'_{j-1} + (K-j) p'_j] \log \frac{j p'_{j-1} + (K-j) p'_j}{K} \right\}, \tag{42}
\end{aligned}$$

where

$$\alpha = N p_{\#}, \tag{43}$$

$$1 - \alpha = \sum_{j=0}^{K-1} N s_j p_j, \tag{44}$$

$$p'_j = \frac{p_j}{1 - \alpha}. \tag{45}$$

The first term $\log(K)/N$ is achieved by the extreme point using escape pattern $\#$ only to retrieve the whole message from the most trustworthy server. For the second term, note that the probability vector $\mathbf{p}' = (p'_0, p'_1, \dots, p'_{K-1})$ induces a valid probability space since

$$\sum_{j=0}^{K-1} N s_j p'_j = \frac{\sum_{j=0}^{K-1} N s_j p_j}{1 - \alpha} = 1. \tag{46}$$

The optimal probability allocation of clean TSC scheme without the escape retrieval symbol $\#$ can be induced from W-PIR $^{\#}$ by setting $p_{(\#)}^{k,1}$ as zero [42]:

$$\begin{aligned}
\hat{I}(\mathbf{p}) &= \frac{1}{K} \sum_{j=0}^{K-1} \binom{K}{j} (N-1)^j \left\{ j p_{j-1} \log p_{j-1} + (K-j) p_j \log p_j \right. \\
&\quad \left. - [j p_{j-1} + (K-j) p_j] \log \frac{j p_{j-1} + (K-j) p_j}{K} \right\}, \tag{47}
\end{aligned}$$

where $\mathbf{p} = (p_0, p_1, \dots, p_{K-1})$ is obtained by using the same allocation strategy in Theorem 3 but setting $p_{(\#)}^{k,1}$ as zero. The rigorous proof of $\hat{I}(\mathbf{p})$ can be found in Appendix C.

Therefore, we have the other direction $\text{conv}(\hat{\mathcal{G}}_{\text{MI}} \cup \{(\gamma_1 \log K, 1)\}) \supseteq \mathcal{G}_{\text{MI}}$, i.e., the optimal W-PIR $^{\#}$ strategy under the MI metric is time-sharing between the extreme point (using the direct retrieval $p_{(\#)}^{k,1}$ only) and the clean TSC scheme (using $p_{(f)}^{k,\pi}$ only). \square

Note that this equivalence to the time-sharing (probabilistic sharing) solution is based on one particular structure of the optimal solution in the homogeneous setting. More precisely, it essentially relies on the fact that in the optimal solution, the “request-for-nothing” query does not induce any privacy leakage.

5.2 Homogeneous Trustfulness: Reduced W-PIR $^{\#}$ is Optimal

Given the parameters of the server trustworthy $\gamma_n, n \in [1 : N]$, the heterogeneous W-PIR $^{\#}$ objective under the MI metric is shown in the following optimization problem (P3):

$$\begin{aligned}
& \underset{p_{(\#)}^{k,n}, p_{(f)}^{k,\pi}}{\text{minimize}} && \rho_{(\text{MI})} = \sum_{n=1}^N \gamma_n \text{MI} \left(M \rightarrow Q_n^{[M]} \right) \\
& \text{subject to} && p_{(\#)}^{k,n} \geq 0, \quad \forall k, n, \\
& && p_{(f)}^{k,\pi} \geq 0, \quad \forall k, \pi, f, \\
& && \sum_{n=1}^N p_{(\#)}^{k,n} + \sum_f \sum_{\pi} p_{(f)}^{k,\pi} = 1, \quad \forall k, \\
& && p_d^k + \frac{N}{N-1} (1 - p_d^k) \leq D, \quad \forall k.
\end{aligned} \tag{48}$$

Proposition 4. *The above optimization problem (P3) in the homogeneous setting, where $\gamma_1 = \gamma_2 = \dots = \gamma_N = \gamma = 1/N$, has the same optimal value as the following reduced problem (P4):*

$$\begin{aligned}
& \underset{p_{\#}, p_0, \dots, p_{K-1}}{\text{minimize}} && I(\mathbf{p}) \\
& \text{subject to} && p_{\#}, p_0, p_1, \dots, p_{K-1} \geq 0, \\
& && Np_{\#} + \sum_{j=0}^{K-1} Ns_j p_j = 1, \\
& && \frac{N - N(p_{\#} + p_0)}{N-1} \leq D.
\end{aligned} \tag{49}$$

We prove this proposition in Appendix C mainly based on the properties of mutual information and log sum inequality. The optimal probability assignment in Proposition 4 is established by the scheme in Theorem 3, which is proved in Section 5.3.

Before the proof of Theorem 3, we further specify that the download cost constraint $p_0 + p_{\#} \geq 1 - D + D/N$ under the homogeneous MI setting can always be achieved by letting $p_0 + p_{\#} = 1 - D + D/N$ in Lemma 1.

Lemma 1. *Given a legal solution $\mathbf{p} = (p_{\#}, p_0, \dots, p_{K-1})$ of (P4) satisfying $p_0 + p_{\#} = \hat{p}^* \geq \hat{p} = 1 - D + D/N$, we can explicitly construct a new vector $\mathbf{p}' = (p'_{\#}, p'_0, \dots, p'_{K-1})$ by setting*

$$\begin{aligned}
p'_j &= \frac{1 - N\hat{p}}{1 - N\hat{p}^*} p_j, \quad j \in [0, K-1], \\
p'_{\#} &= \hat{p} - p'_0,
\end{aligned}$$

such that this newly constructed assignment has lower MI leakage $I(\mathbf{p}') \leq I(\mathbf{p})$.

The proof of Lemma 1 is given in Appendix D by carefully computing the difference between the new constructed assignment $I(\mathbf{p}')$ and the original $I(\mathbf{p})$.

5.3 Homogeneous Trustfulness: Proof of Theorem 3

Now we are ready to prove Theorem 3.

Proof. Using a similar manner in Max-L, we define $\hat{p} = 1 - D + D/N$, where $\hat{p} \in [N^{-K}, N^{-1}]$. Without loss of optimality, a feasible download cost $D \in [1, D^*]$ in (P4) can be achieved by setting $p_0 + p_{\#} = \hat{p}$, which is established in Lemma 1. Therefore, the optimization problem under the homogeneous MI setting can be written as (P4'):

$$\begin{aligned}
& \underset{p_{\#}, p_0, p_1, \dots, p_{K-1}}{\text{minimize}} && I(\mathbf{p}) \\
& \text{subject to} && p_{\#}, p_0, p_1, \dots, p_{K-1} \geq 0, \\
& && Np_{\#} + \sum_{j=0}^{K-1} Ns_j p_j = 1, \\
& && p_0 + p_{\#} = \hat{p}
\end{aligned} \tag{50}$$

The Lagrangian function is

$$\begin{aligned} \mathcal{L} = I(\mathbf{p}) &- \sum_{j=0}^{K-1} \lambda_j p_j - \eta_{\#} p_{\#} \\ &+ \nu \left(N p_{\#} + \sum_{j=0}^{K-1} N s_j p_j - 1 \right) \\ &+ \mu (\hat{p} - p_0 - p_{\#}) \end{aligned} \quad (51)$$

We introduce the two sets of auxiliary variables for $j = 1, 2, \dots, K-1$:

$$x_j \triangleq p_{j-1}/p_j, \quad (52)$$

$$y_j \triangleq \log \frac{j x_j + K - j}{K}. \quad (53)$$

Then the KKT condition can be derived as follows:

1. stationarity:

$$\begin{cases} \log K - \eta_{\#} + N\nu - \mu = 0 \\ s_j \left(-y_j + (N-1)(\log x_{j+1} - y_{j+1}) \right. \\ \left. + N\nu \right) - \lambda_j = 0, j \in [1 : K-2] \\ (N-1)^{K-1} [-y_{K-1} + N\nu] - \lambda_{K-1} = 0 \\ (N-1)(\log x_1 - y_1) + N\nu - \lambda_0 - \mu = 0 \end{cases} \quad (54)$$

2. primal feasibility:

$$\begin{cases} N p_{\#} + N \sum_{j=0}^{K-1} s_j p_j - 1 = 0 \\ p_j \geq 0, p_{\#} \geq 0, j \in [0 : K-1] \\ p_0 + p_{\#} = \hat{p} \end{cases} \quad (55)$$

3. dual feasibility:

$$\begin{cases} \eta_{\#} \geq 0 \\ \lambda_j \geq 0, j \in [0 : K-1] \end{cases} \quad (56)$$

4. complementary slackness:

$$\begin{cases} \eta_{\#} p_{\#} = 0 \\ \lambda_j p_j = 0 \\ \mu (\hat{p} - p_0 - p_{\#}) = 0 \end{cases} \quad (57)$$

We give the solution to the KKT conditions as the following variable assignments:

1) primal variables:

$$\begin{cases} p_{\#} = \hat{p} - p_0 \\ p_0 = (N-1)(D-1) \left(\sum_{j=1}^{K-1} N s_j \prod_{i=1}^j \frac{1}{x_i} \right)^{-1} \\ p_j = p_0 \prod_{i=1}^j \frac{1}{x_i}, j \in [1 : K-1] \end{cases} \quad (58)$$

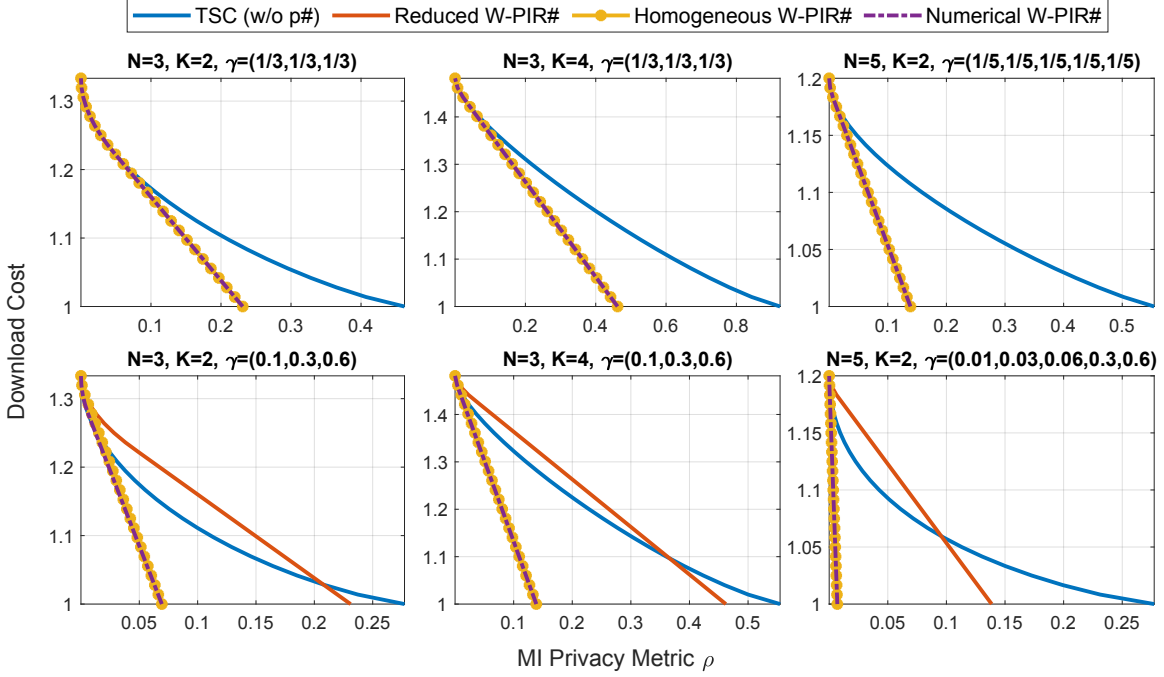


Figure 4: Numerical comparisons between the proposed code and existing codes under the MI metric.

where $\mathbf{x} = (x_1, x_2, \dots, x_{K-1})$ is defined as the following sequence with $x_1 = \frac{K-1}{K^{\frac{N-2}{N-1}-1}}$:

$$\log \frac{(K-j)x_{K-j} + j}{K} = \sum_{i=0}^{j-1} (1-N)^i y_{K-1} - \sum_{i=1}^{j-1} (1-N)^i \log x_{K-j+i}. \quad (59)$$

2) dual variables:

$$\begin{cases} \eta_{\#} = 0 \\ \lambda_j = 0, j \in [0 : K-1] \\ \nu = \frac{y_{K-1}}{N} \\ \mu = \log K + y_{K-1} \end{cases} \quad (60)$$

It can be verified that the solution given above satisfies all KKT conditions. Firstly with $\lambda_j = 0$ for $j = 0, 1, \dots, K-1$, x_j and y_j assigned by (38), with y_j 's eliminated, can properly satisfy stationarity and primal feasibility conditions. The dual feasibility and complementary slackness can be easily verified by simply plugging the variables, and this completes the proof. \square

5.4 Heterogeneous Trustfulness: Numerical Results

The optimal regions \mathcal{G}_{MI} under different allocation strategies are illustrated in Fig. 4. In homogeneous settings, our proposed allocation (WPIR $\#$ - optimized for homogeneity) in Theorem 3 provides the least MI privacy leakage under the same download cost constraint, which indeed matches the result numerically solved by convex programming tools. However, in the heterogeneous case, the WPIR $\#$ optimized for homogeneity is no longer optimal, and a closed-form solution for heterogeneous settings becomes intractable. Therefore,

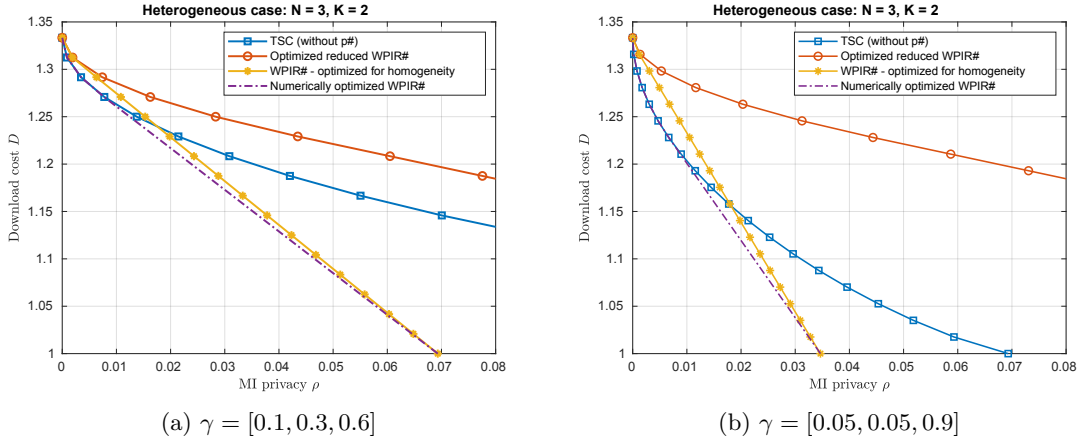


Figure 5: Numerical comparisons with different trustworthy weights γ under the MI metric.

a numerically optimized WPIR[#] with convex programming tools is provided to corroborate the theoretical analysis. With an increasing number of servers and messages, the WPIR[#] achieves better (ρ, D) trade-offs than other PIR schemes. Although the analytical allocation in Theorem 3 may not be optimal in the heterogeneous setting, it appears to be quite close to the numerical solution when N and K are large.

We compared the W-PIR schemes with different weights on the trustworthiness of the servers in Fig. 5. The allocation of W-PIR[#] in Theorem 3 approaches the numerical solution as the value of $\Delta\gamma \triangleq \gamma_N - \gamma_1$ becomes smaller, that is, there do not exist extremely trustworthy and extremely untrustworthy servers. When $\Delta\gamma \rightarrow 0$, the analytical allocation of W-PIR[#] converges to the numerical solution, as shown in homogeneous settings. It is also observed that the original TSC code and the optimized reduced WPIR[#] suffer in a heterogeneous setting because they do not take into account the more trustworthy server.

The structure of the probabilistic sharing mechanism becomes more intricate in the context of MI metric than in the Max-L metric. In particular, it is observed that when the leakage parameter ρ falls below a certain threshold, these new direct download patterns become ineffective, implying that they are not used in the retrieval process. This numerical result also validates the correctness of Proposition 3: the optimal W-PIR[#] is time-sharing between the extreme point of direct retrieval pattern and the clean TSC scheme without the # pattern for the homogeneous setting, and appears to even hold for the heterogeneous case, though we are not able to establish this conjecture rigorously. However, we can still apply the allocation in Theorem 3, which is optimal for the homogeneous setting, which appears to be quite close to the optimal \mathcal{G}_{MI} numerically computed in this setting, as shown in Fig. 4.

6 Conclusion

We studied the problem of weakly private information retrieval when there is heterogeneity in the servers' trustfulness, and identified the optimal probability allocation of a general class of W-PIR code, which we refer to as the W-PIR[#] code. This optimal distribution is notably straightforward, essentially being a probabilistic sharing of a capacity-achieving PIR code and a direct download from the most reliable server. Intriguingly, we found that a specific optimal code designed for a homogeneous trust environment is equally effective in a heterogeneous trust scenario, particularly under the Max-L metric. Further explorations in our subsequent work delved into the W-PIR[#] code within the context of the MI metric, examining both homogeneous and heterogeneous settings, where the optimal solutions for the two settings showed significant divergence.

References

- [1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” in *IEEE 36th Annual Foundations of Computer Science*, Milwaukee, WI, USA, Oct. 1995, pp. 41–50.
- [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, 2017.
- [3] 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.
- [4] 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.
- [5] 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, Apr. 2018.
- [6] 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.
- [7] R. Zhou, C. Tian, H. Sun, and T. Liu, “Capacity-achieving private information retrieval codes from MDS-coded databases with minimum message size,” *IEEE Transactions on Information Theory*, vol. 66, no. 8, pp. 4904–4916, Aug. 2020.
- [8] T. Guo, R. Zhou, and C. Tian, “New results on the storage-retrieval tradeoff in private information retrieval systems,” *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 403–414, Mar. 2021.
- [9] C. Tian, “On the storage cost of private information retrieval,” *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7539–7549, Dec. 2020.
- [10] C. Tian, H. Sun, and J. Chen, “A Shannon-theoretic approach to the storage–retrieval trade-off in pir systems,” *Information*, vol. 14, no. 1, p. 44, 2023.
- [11] H. Sun and C. Tian, “Breaking the MDS-PIR capacity barrier via joint storage coding,” *Information*, vol. 10, no. 9, Aug. 2019.
- [12] 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, Mar. 2018.
- [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, Nov. 2018.
- [14] 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, Nov. 2017.
- [15] 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.
- [16] S. Kumar, H.-Y. Lin, E. Rosnes, and A. Graell i Amat, “Achieving maximum distance separable private information retrieval capacity with linear codes,” *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4243–4273, Jul. 2019.
- [17] J. Zhu, Q. Yan, C. Qi, and X. Tang, “A new capacity-achieving private information retrieval scheme with (almost) optimal file length for coded servers,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1248–1260, 2019.

- [18] A. Vardy and E. Yaakobi, “Private information retrieval without storage overhead: Coding instead of replication,” *IEEE Journal on Selected Areas in Information Theory*, vol. 4, pp. 286–301, Jul. 2023.
- [19] T. Guo, R. Zhou, and C. Tian, “On the information leakage in private information retrieval systems,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2999–3012, Mar. 2020.
- [20] H. Sun and S. A. Jafar, “The capacity of symmetric private information retrieval,” *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 322–329, Jan. 2019.
- [21] Z. Wang, K. Banawan, and S. Ulukus, “Private set intersection: A multi-message symmetric private information retrieval perspective,” *IEEE Transactions on Information Theory*, vol. 68, no. 3, pp. 2001–2019, 2021.
- [22] R. Tandon, “The capacity of cache aided private information retrieval,” in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, USA, Oct. 2017, pp. 1078–1082.
- [23] 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, May 2019.
- [24] 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, Apr. 2020.
- [25] 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, Aug. 2020.
- [26] Y.-P. Wei and S. Ulukus, “The capacity of private information retrieval with private side information under storage constraints,” *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2023–2031, Apr. 2020.
- [27] S. Li and M. Gastpar, “Single-server multi-message private information retrieval with side information: the general cases,” in *2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 1083–1088.
- [28] Z. Wang and S. Ulukus, “Symmetric private information retrieval with user-side common randomness,” in *2021 IEEE International Symposium on Information Theory (ISIT)*, Melbourne, Victoria, Australia, Jul. 2021, pp. 2119–2124.
- [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, Mar. 2023.
- [30] S. Ulukus, S. Avestimehr, M. Gastpar, S. A. Jafar, R. Tandon, and C. Tian, “Private retrieval, computing, and learning: Recent progress and future challenges,” *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 3, pp. 729–748, 2022.
- [31] D. Asonov and J. C. Freytag, “Repudiative information retrieval,” in *2002 ACM Workshop on Privacy in the Electronic Society*, Washington, DC, USA, Nov. 2002, pp. 32–40.
- [32] R. R. Toledo, G. Danezis, and I. Goldberg, “Lower-cost ϵ -private information retrieval,” in *2016 Privacy Enhancing Technologies Symposium (PETS)*, Darmstadt, Germany, Jul. 2016, pp. 184–201.
- [33] I. Samy, R. Tandon, and L. Lazos, “On the capacity of leaky private information retrieval,” in *2019 IEEE International Symposium on Information Theory (ISIT)*, Paris, France, Jul. 2019, pp. 1262–1266.
- [34] Z. Jia, “On the capacity of weakly-private information retrieval,” Master’s thesis, University of California, Irvine, CA, 2019.

- [35] H.-Y. Lin, S. Kumar, E. Rosnes, A. Graell i Amat, and E. Yaakobi, “Weakly-private information retrieval,” in *2019 IEEE International Symposium on Information Theory (ISIT)*, Paris, France, Jun. 2019, pp. 1257–1261.
- [36] R. Zhou, T. Guo, and C. Tian, “Weakly private information retrieval under the maximal leakage metric,” in *2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 1089–1094.
- [37] H.-Y. Lin, S. Member, S. Kumar, E. Rosnes, A. Graell i Amat, and E. Yaakobi, “Multi-server weakly-private information retrieval,” *IEEE Transactions on Information Theory*, vol. 68, no. 2, pp. 1197–1219, 2022.
- [38] I. Samy, M. Attia, R. Tandon, and L. Lazos, “Asymmetric leaky private information retrieval,” *IEEE Transactions on Information Theory*, vol. 67, no. 8, pp. 5352–5369, Aug. 2021.
- [39] H.-Y. Lin, S. Kumar, E. Rosnes, A. Graell i Amat, and E. Yaakobi, “The capacity of single-server weakly-private information retrieval,” *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 415–427, 2021.
- [40] Y. Yakimenka, H.-Y. Lin, E. Rosnes, and J. Kliewer, “Optimal rate-distortion-leakage tradeoff for single-server information retrieval,” *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 3, pp. 832–846, 2022.
- [41] I. Issa, A. B. Wagner, and S. Kamath, “An operational approach to information leakage,” *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1625–1657, Mar. 2020.
- [42] C. Qian, R. Zhou, C. Tian, and T. Liu, “Improved weakly private information retrieval codes,” in *Proc. 2022 IEEE International Symposium on Information Theory (ISIT)*, Jul. 2022, pp. 2827–2832.
- [43] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed. Cambridge University Press, 2004.

A Proof of Proposition 2

Proof. The direction (P1) ≤ (P2): Given the explicit formulas given in Proposition 1, this direction is trivially true since (P2) can be viewed as (P1) under the additional constraints enforced through (19).

The direction (P1) ≥ (P2): Given an optimal solution in (P1), we can find the following assignment of $p_{\#}, p_0, \dots, p_{K-1}$:

$$p_j = \frac{1}{NKs_j} \sum_{k=1}^K \sum_{\pi \in \mathcal{P}} \sum_{f \in \mathcal{F}_j} p_{(f)}^{k,\pi}, \quad j \in [0 : K - 1], \quad (61)$$

$$p_{\#} = \frac{1}{NK} \sum_{n=1}^N \sum_{k=1}^K p_{(\#)}^{k,n}, \quad (62)$$

With the relation (61), we have $p_j \geq 0$ for any $j \in [0 : K - 1]$, and moreover,

$$\begin{aligned} & \sum_{j=0}^{K-1} Ns_j p_j + Np_{\#} \\ &= \frac{1}{K} \left[\sum_{k=1}^K \left(\sum_{\pi \in \mathcal{P}} \sum_{f \in \mathcal{F}} p_{(f)}^{k,\pi} + \sum_{n=1}^N p_{(\#)}^{k,n} \right) \right] = 1, \end{aligned} \quad (63)$$

$$\begin{aligned}
& \frac{1}{N} \sum_{n=1}^N 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} \\
&= \frac{1}{N} \sum_{n=1}^N \left[\sum_{k=1}^K p_{(\#)}^{k,n} + \max_k \left(\sum_{j \in [1:N]: j \neq n} p_{(\#)}^{k,j} + \sum_{\pi: \phi_n^*(k, (0, \pi))=0} p_{(0)}^{k,\pi} \right) + \sum_{\|q\| \neq 0} \max_k \left(\sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k,\pi} \right) \right] \tag{66}
\end{aligned}$$

$$\begin{aligned}
& \geq \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K p_{(\#)}^{k,n} + \max_k \left(\frac{1}{N} \sum_{n=1}^N \left(\sum_{j \in [1:N]: j \neq n} p_{(\#)}^{k,j} + \sum_{\pi: \phi_n^*(k, (0, \pi))=0} p_{(0)}^{k,\pi} \right) \right) \\
& \quad + \sum_{\|q\| \neq 0} \max_k \left(\frac{1}{N} \sum_{n=1}^N \left(\sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k,\pi} \right) \right) \tag{67}
\end{aligned}$$

$$\begin{aligned}
&= \underbrace{Kp_{\#} + \max_k \left(\frac{N-1}{N} \sum_{n=1}^N p_{(\#)}^{k,n} + \frac{1}{N} \sum_{n=1}^N \sum_{\pi: \phi_n^*(k, (0, \pi))=0} p_{(0)}^{k,\pi} \right)}_{T_1} \\
& \quad + \underbrace{\sum_{\|q\|=K} \max_k \left(\frac{1}{N} \sum_{n=1}^N \left(\sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k,\pi} \right) \right)}_{T_2} + \underbrace{\sum_{j=1}^{K-1} \sum_{\|q\|=j} \max_k \left(\frac{1}{N} \sum_{n=1}^N \left(\sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k,\pi} \right) \right)}_{\sum_{j=1}^{K-1} T_3(j)}. \tag{68}
\end{aligned}$$

and

$$\begin{aligned}
& \frac{N - (Np_{\#} + Np_0)}{N-1} \\
& \leq \frac{N - \frac{1}{K} \sum_{n=1}^N \sum_{k=1}^K p_{(\#)}^{k,n} - \frac{1}{K} \sum_{k=1}^K \sum_{\pi \in \mathcal{P}} p_{(0)}^{k,\pi}}{N-1} \tag{64}
\end{aligned}$$

$$\begin{aligned}
& \leq \frac{\frac{1}{K} \sum_{k=1}^K \left(N - \sum_{n=1}^N p_{(\#)}^{k,n} - \sum_{\pi} p_{(0)}^{k,\pi} \right)}{N-1} \leq D, \tag{65}
\end{aligned}$$

due to the last set of constraints in (P1).

Therefore, $\{p_{\#}, p_0, \dots, p_{K-1}\}$ indeed satisfies the constraints in problem P2. It remains to show that this assignment leads to a lower objective function value in (P2) than the optimal value of (P1). For this purpose, we write the inequalities (66-68).

Let us consider the last three terms in (68) individually. For the first term, observe that:

$$\begin{aligned}
T_1 & \geq \frac{1}{K} \sum_{k=1}^K \left(\frac{N-1}{N} \sum_{n=1}^N p_{(\#)}^{k,n} + \frac{1}{N} \sum_{n=1}^N \sum_{\pi: \phi_n^*(k, (0, \pi))=0} p_{(0)}^{k,\pi} \right) \\
&= (N-1)p_{\#} + \frac{1}{KN} \sum_{k=1}^K \sum_{n=1}^N \sum_{\pi: \phi_n^*(k, (0, \pi))=0} p_{(0)}^{k,\pi} \tag{69}
\end{aligned}$$

$$\begin{aligned}
&= (N-1)p_{\#} + \frac{1}{KN} \sum_{k=1}^K \sum_{\pi \in \mathcal{P}} p_{(0)}^{k,\pi} \tag{70}
\end{aligned}$$

$$\begin{aligned}
&= (N-1)p_{\#} + p_0, \tag{71}
\end{aligned}$$

where the inequality is due to the convexity of the max function, and (70) is by the fact that for each k , each permutation is counted exactly once in the summation $\sum_{n=1}^N \sum_{\pi: \phi_n^*(k, (0, \pi))=0}$. To see that latter, observe that each π must map $f = 0$ to a query $q = 0$ at one and only one of the servers. In a similar manner

$$\begin{aligned} T_2 &\geq \sum_{\|q\|=K} \frac{1}{K} \sum_{k=1}^K \left(\frac{1}{N} \sum_{n=1}^N \left(\sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k, \pi} \right) \right) \\ &= \frac{1}{KN} \sum_{k=1}^K \sum_{\|q\|=K} \sum_{n=1}^N \sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k, \pi} \end{aligned} \quad (72)$$

$$= \frac{N-1}{KN} \sum_{k=1}^K \sum_{\|f\|=K-1} \sum_{\pi} p_{(f)}^{k, \pi} \quad (73)$$

$$= t_K p_{K-1} = t_K \max(p_{K-1}, p_K), \quad (74)$$

where the inequality is again due to the convexity of the max function. To see (73), let us introduce the notation

$$q|k = (q_1, q_2, \dots, q_{k-1}, q_{k+1}, \dots, q_K), \quad (75)$$

i.e., the query vector with the k -th symbol removed. Then

$$\sum_{n=1}^N \sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k, \pi} = \sum_{\pi} p_{(q|k)}^{k, \pi}, \quad (76)$$

because for that fixed q , the corresponding f is fixed, and for each π , there is one and only one n such that $\phi_n^*(k, (f, \pi)) = q$ holds. Therefore,

$$\begin{aligned} &\sum_{\|q\|=K} \sum_{n=1}^N \sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k, \pi} \\ &= \sum_{\|q\|=K} \sum_{\pi} p_{(q|k)}^{k, \pi} = (N-1) \sum_{\|f\|=K-1} \sum_{\pi} p_{(f)}^{k, \pi}, \end{aligned} \quad (77)$$

because for each k , each f with $\|f\| = K-1$ corresponds to exactly $N-1$ queries with $\|q\| = K$.

For the last term, consider a fixed j , and then

$$\begin{aligned} T_3(j) &\geq \sum_{\|q\|=j} \max_k \left(\frac{1}{N} \sum_{n=1}^N \left(\sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k, \pi} \right) \right) \\ &= \frac{1}{N} \sum_{\|q\|=j} \max_k \sum_{\pi} p_{(q|k)}^{k, \pi} \end{aligned} \quad (78)$$

$$\begin{aligned} &\geq \frac{1}{N} \sum_{\|q\|=j} \max \left\{ \frac{1}{j} \sum_{k=1}^K \mathbb{1}(\|q|k\| = j-1) \sum_{\pi} p_{(q|k)}^{k, \pi}, \right. \\ &\quad \left. \frac{1}{K-j} \sum_{k=1}^K \mathbb{1}(\|q|k\| = j) \sum_{\pi} p_{(q|k)}^{k, \pi} \right\} \end{aligned} \quad (79)$$

$$\begin{aligned} &\geq \frac{1}{N} \max \left\{ \frac{1}{j} \sum_{k=1}^K \sum_{\|q\|=j} \mathbb{1}(\|q|k\| = j-1) \sum_{\pi} p_{(q|k)}^{k, \pi}, \right. \\ &\quad \left. \frac{1}{K-j} \sum_{k=1}^K \sum_{\|q\|=j} \mathbb{1}(\|q|k\| = j) \sum_{\pi} p_{(q|k)}^{k, \pi} \right\} \end{aligned} \quad (80)$$

$$\begin{aligned}
&= \frac{1}{N} \max \left\{ \frac{(N-1)}{j} \sum_{k=1}^K \sum_{\|f\|=j-1} \sum_{\pi} p_{(f)}^{k,\pi}, \right. \\
&\quad \left. \frac{1}{K-j} \sum_{k=1}^K \sum_{\|f\|=j} \sum_{\pi} p_{(f)}^{k,\pi} \right\} \tag{81}
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{N} \max \left\{ \frac{t_j}{K s_{j-1}} \sum_{k=1}^K \sum_{\|f\|=j-1} \sum_{\pi} p_{(f)}^{k,\pi}, \right. \\
&\quad \left. \frac{t_j}{K s_j} \sum_{k=1}^K \sum_{\|f\|=j} \sum_{\pi} p_{(f)}^{k,\pi} \right\} \tag{82}
\end{aligned}$$

$$= t_j \cdot \max \{p_{j-1}, p_j\}, \tag{83}$$

where (79) follows from $|\{f : f = q|k, \|f\| = j-1\}| = j$ and $|\{f : f = q|k, \|f\| = j\}| = K-j$ for a given q , and $\mathbf{1}(\cdot)$ is the indicator function, (80) follows from the convexity of the max function, (81) follows by counting the number of f for each q , (82) follows from $\frac{t_j}{s_{j-1}} = \frac{K(N-1)}{j}$ and $\frac{t_j}{s_j} = \frac{K}{K-j}$, and (83) follows by the assignment of p_j in (61). This proves the inequality $(P1) \geq (P2)$, and the proof is complete. \square

B Proof of Theorem 2

Proof. The proof follows a similar line as that in [36], however, with the additional escape # retrieval patterns, the construction of the dual variables becomes considerably more complex.

First define $\hat{p} = 1 - D + D/N$, where $\hat{p} \in [N^{-K}, N^{-1}]$. We can rewrite the problem (P2) as a linear program denoted as $P2'$

$$\begin{aligned}
&\underset{p_{\#}, p_0, \dots, p_{K-1}, m_1, \dots, m_K}{\text{minimize}} && \sum_{j=1}^K t_j m_j + p_0 + (N+K-1)p_{\#} \\
&\text{subject to} && p_{\#}, p_0, p_1, \dots, p_{K-1} \geq 0, \\
&&& Np_{\#} + \sum_{j=0}^{K-1} N s_j p_j = 1, \\
&&& p_{j-1} - m_j \leq 0, \quad \forall j \in [1 : K], \\
&&& p_j - m_j \leq 0, \quad \forall j \in [1 : K], \\
&&& p_0 + p_{\#} \geq \hat{p}.
\end{aligned} \tag{84}$$

The Lagrangian is

$$\begin{aligned}
\mathcal{L} &= p_0 + (N+K-1)p_{\#} + \sum_{j=1}^K t_j m_j - \sum_{j=0}^{K-1} \eta_j p_j \\
&\quad - \eta_{\#} p_{\#} + \mu \left(Np_{\#} + \sum_{j=0}^{K-1} N s_j p_j - 1 \right) \\
&\quad + \sum_{j=1}^K [\lambda_j (p_j - m_j) + \mu_j (p_{j-1} - m_j)] \\
&\quad + \lambda (\hat{p} - p_0 - p_{\#}).
\end{aligned} \tag{85}$$

Then we can write the KKT conditions as follows:

1. stationarity:

$$\begin{cases} (N - 1 + K) - \eta_{\#} + N\mu - \lambda = 0 & (86) \end{cases}$$

$$\begin{cases} 1 - \eta_0 + N\mu + \mu_1 - \lambda = 0 & (87) \end{cases}$$

$$\begin{cases} -\eta_j + N\mu s_j + \lambda_j + \mu_{j+1} = 0, j \in [1 : K - 1] & (88) \end{cases}$$

$$\begin{cases} t_j - \lambda_j - \mu_j = 0, j \in [1 : K], & (89) \end{cases}$$

2. primal feasibility:

$$\begin{cases} Np_{\#} + N \sum_{j=0}^{K-1} s_j p_j - 1 = 0 & (90) \end{cases}$$

$$\begin{cases} 0 \leq p_{\#}, 0 \leq p_{j-1}, p_j \leq m_j, j \in [1 : K] & (91) \end{cases}$$

$$\begin{cases} p_0 + p_{\#} \geq \hat{p}, & (92) \end{cases}$$

3. dual feasibility:

$$\begin{cases} \lambda \geq 0, \eta_{\#} \geq 0 & (93) \end{cases}$$

$$\begin{cases} \lambda_j \geq 0, \mu_j \geq 0, \eta_{j-1} \geq 0, j \in [1 : K], & (94) \end{cases}$$

4. complementary slackness:

$$\begin{cases} \eta_{\#} p_{\#} = 0 & (95) \end{cases}$$

$$\begin{cases} \eta_j p_j = 0, j \in [1 : K - 1] & (96) \end{cases}$$

$$\begin{cases} \lambda_j (p_j - m_j) = 0, j \in [1 : K] & (97) \end{cases}$$

$$\begin{cases} \mu_j (p_{j-1} - m_j) = 0, j \in [1 : K] & (98) \end{cases}$$

$$\begin{cases} \lambda(\hat{p} - p_0 - p_{\#}) = 0. & (99) \end{cases}$$

Since the problem is linear and feasible, any solution to the KKT conditions is optimal. Therefore, finding such a solution whose primal variables yield the values in Theorem 2 would conclude the proof. We claim that such a solution to the KKT conditions is as follows:

1) primal variables:

$$\begin{cases} p_{\#} = \frac{N^K \hat{p} - 1}{N^K - N} & (100) \end{cases}$$

$$\begin{cases} p_j = \frac{1 - Np_{\#}}{N^K}, j \in [0 : K - 1] & (101) \end{cases}$$

$$\begin{cases} m_j = p_{j-1}, j \in [1 : K], & (102) \end{cases}$$

2) dual variables:

$$\begin{cases} \eta_{\#} = 0 & (103) \end{cases}$$

$$\begin{cases} \eta_j = 0, j \in [0 : K - 1] & (104) \end{cases}$$

$$\begin{cases} \lambda = \frac{N^{K-1}(K-1)}{N^{K-1}-1} & (105) \end{cases}$$

$$\begin{cases} \mu = \frac{N^{K-2}(K-1)}{N^{K-1}-1} - \frac{N+K-1}{N} & (106) \end{cases}$$

$$\begin{cases} \lambda_j = \sum_{i=0}^j t_i - (N+K-1) \sum_{i=0}^{j-1} s_i + \lambda \sum_{i=1}^{j-1} s_i, & (107) \\ j \in [1 : K] \end{cases}$$

$$\begin{cases} \mu_j = -\sum_{i=0}^{j-1} t_i + (N+K-1) \sum_{i=0}^{j-1} s_i - \lambda \sum_{i=1}^{j-1} s_i, & (108) \\ j \in [1 : K] \end{cases}$$

It remains to show that the solution above indeed satisfies all the KKT conditions. First note that with the given assignment, $\lambda_K = 0$. With this observation, the conditions of stationarity, primal feasibility, and complementary slackness can be verified by simply plugging in the variable assignments. For dual feasibility, observe that $\lambda \geq 0$, and it remains to show that $\lambda_k \geq 0$ and $\mu_k \geq 0$ for $j = 1, 2, \dots, K$. This is established in Lemma 2 below. By Proposition 1, with homogeneous trustworthy $\gamma_1 = \dots = \gamma_n = \gamma$, it is straightforward to verify the primal variable assignment indeed leads to the surrogate leakage

$$\begin{aligned} \rho_{(\text{Max-L})} &= \sum_{n=1}^N \gamma \left(\sum_{j=1}^K t_j m_j + (p_0 + (N-1)p_{\#}) + K p_{\#} \right) \\ &= N\gamma \left(1 + \frac{(K-1) [N^{K-1}(N - (N-1)D) - 1]}{N^K - N} \right) \end{aligned} \quad (109)$$

Now it remains to show that the allocation in Theorem 1 provides us with the same optimal surrogate maximal leakage given above. By assigning $\hat{p}_{\#} = N p_{\#}$, we have

$$\rho_{(\text{Max-L})} = \sum_{n=1}^N \gamma 2^{\mathcal{L}(M \rightarrow Q_n^{[M]})} \quad (110)$$

$$\begin{aligned} &= \gamma \left(N^{K-1} \left(\frac{1 - \hat{p}_{\#}}{N^{K-1}} \right) + K \hat{p}_{\#} \right) \\ &\quad + (N-1)\gamma \left(N^{K-1} \left(\frac{1 - \hat{p}_{\#}}{N^{K-1}} \right) + \hat{p}_{\#} \right) \end{aligned} \quad (111)$$

$$= \gamma (1 + (K-1)\hat{p}_{\#}) + (N-1)\gamma \quad (112)$$

$$= N\gamma + \gamma(K-1)\hat{p}_{\#} \quad (113)$$

$$= N\gamma \left(1 + \frac{(K-1) [N^{K-1}(N - (N-1)D) - 1]}{N^K - N} \right) \quad (114)$$

This completes the proof. □

Lemma 2. *The solution given above satisfies*

$$\begin{aligned} &\frac{(N+K-1) \sum_{i=0}^{j-1} s_i - \lambda \sum_{i=1}^{j-1} s_i}{\sum_{i=0}^{j-1} t_i} \geq 1 \\ &\geq \frac{(N+K-1) \sum_{i=0}^{j-1} s_i - \lambda \sum_{i=1}^{j-1} s_i}{\sum_{i=0}^j t_i}, \quad j \in [1:K]. \end{aligned}$$

Proof. It is straightforward to verify that $(N+K-1-\lambda) \geq 0$ whenever $N \geq 2$ and $K \geq 1$. When $j = 1$, let $R_1 = (N+K-1)s_0$ and $\hat{R}_1 = t_0 + t_1$, the RHS function satisfies

$$\frac{R_1}{\hat{R}_1} = \frac{(N+K-1)}{1+K(N-1)} \leq 1,$$

when $N \geq 2$ and $K \geq 1$. Next, notice that the function below is monotonically increasing with respect to j for $j \in [2:K]$, because

$$\begin{aligned} \frac{R_j}{\hat{R}_j} &= \frac{(N+K-1-\lambda)s_{j-1}}{t_j} \\ &= \frac{(N+K-1-\lambda) \binom{K-1}{j-1} (N-1)^{j-1}}{\binom{K}{j} (N-1)^j} \\ &= \frac{(N+K-1-\lambda)j}{K(N-1)}, \quad j \in [2:K]. \end{aligned} \quad (115)$$

Observe that when $j = K$,

$$\frac{R_K}{\hat{R}_K} = \frac{(N + K - 1 - \lambda)K}{K(N - 1)} \geq 1. \quad (116)$$

Clearly there exists a $j^* \in [2 : K - 1]$ s.t.

$$\frac{R_2}{\hat{R}_2} \leq \dots \leq \frac{R_{j^*}}{\hat{R}_{j^*}} \leq \frac{R_1}{\hat{R}_1} \leq \frac{R_{j^*+1}}{\hat{R}_{j^*+1}} \leq \dots \leq \frac{R_K}{\hat{R}_K}. \quad (117)$$

For $j \leq j^*$, the RHS inequality holds because

$$RHS = \frac{R_1 + \dots + R_j}{\hat{R}_1 + \dots + \hat{R}_j} \leq \frac{R_1}{\hat{R}_1} \leq 1, \quad j \in [1 : j^*]. \quad (118)$$

On the other hand, for $j > j^*$, the right-hand function is monotonically increasing with respect to j since

$$\frac{R_1 + \dots + R_{j-1}}{\hat{R}_1 + \dots + \hat{R}_{j-1}} \leq \frac{R_1 + \dots + R_j}{\hat{R}_1 + \dots + \hat{R}_j} \leq \frac{R_j}{\hat{R}_j}, \quad j \in [j^* + 1 : K]. \quad (119)$$

It follows that the RHS inequalities hold also for $j > j^*$, since the RHS reaches its maximum when $j = K$ and

$$\begin{aligned} & \frac{(N + K - 1) \sum_{i=0}^{j-1} s_i - \lambda \sum_{i=1}^{j-1} s_i}{\sum_{i=0}^j t_i} \\ & \leq \frac{(N + K - 1) \sum_{i=0}^{K-1} s_i - \lambda \sum_{i=1}^{K-1} s_i}{\sum_{i=0}^K t_i} = 1, \quad j \in [1 : K]. \end{aligned} \quad (120)$$

For the LHS, the function below is monotonically decreasing with respect to $j \in [1 : K]$, since

$$\begin{aligned} \frac{L_j}{\hat{L}_j} &= \frac{(N + K - 1 - \lambda)s_{j-1}}{t_{j-1}} \\ &= \frac{(N + K - 1 - \lambda) \binom{K-1}{j-1} (N-1)^{j-1}}{\binom{K}{j-1} (N-1)^{j-1}} \\ &= \frac{(N + K - 1 - \lambda)(K - j + 1)}{K}, \quad j \in [2 : K]. \end{aligned} \quad (121)$$

and

$$\begin{aligned} \frac{L_1}{\hat{L}_1} &= \frac{(N + K - 1)s_0}{t_0} = (N + K - 1) \\ &\geq \frac{L_2}{\hat{L}_2} = \frac{(N + K - 1 - \lambda)(K - 1)}{K}. \end{aligned} \quad (122)$$

The left-hand function is decreasing in j because

$$\frac{L_1 + \dots + L_{j-1}}{\hat{L}_1 + \dots + \hat{L}_{j-1}} \geq \frac{L_1 + \dots + L_j}{\hat{L}_1 + \dots + \hat{L}_j} \geq \frac{L_j}{\hat{L}_j}, \quad j \in [2 : K]. \quad (123)$$

Therefore, the LHS inequalities hold because the function on the left-hand side reaches its minimum when $j = K$ and

$$\begin{aligned} & \frac{(N + K - 1) \sum_{i=0}^{j-1} s_i - \lambda \sum_{i=1}^{j-1} s_i}{\sum_{i=0}^{j-1} t_i} \\ & \geq \frac{(N + K - 1) \sum_{i=0}^{K-1} s_i - \lambda \sum_{i=1}^{K-1} s_i}{\sum_{i=0}^{K-1} t_i} \\ & = \frac{(N + K - 1)N^{K-1} - \lambda(N^{K-1} - 1)}{N^K - (N - 1)^K} \\ & = \frac{N^K}{N^K - (N - 1)^K} > 1, \quad \forall j \in [1 : K]. \end{aligned} \quad (124)$$

This completes the proof. □

C Proof of Proposition 4

Proof. The direction (P3)≤(P4): Proof of this direction is trivial since (P4) can be viewed as (P3) with additional constraints enforced through (19).

The direction (P3)≥(P4): Given an optimal solution in (P3), we can find the assignment of $p_{\#}, p_0, p_1, \dots, p_{K-1}$:

$$p_{\#} = \frac{1}{NK} \sum_{k=1}^K \sum_{n=1}^N p_{(\#)}^{k,n}, \quad (125)$$

$$p_j = \frac{1}{NKs_j} \sum_{k=1}^K \sum_{\pi \in \mathcal{P}} \sum_{f \in \mathcal{F}_j} p_{(f)}^{k,\pi}, j \in [0 : K-1]. \quad (126)$$

The constraints in problem (P4) can be easily verified using the same nature in the Max-L setting (Eq. 63-65). We only need to show that (P4) using this assignment gives a lower bound on the objective function in (P3). We firstly introduce the notation

$$p_n(0|k) \triangleq \sum_{j \in [1:N]: j \neq n} p_{(\#)}^{k,j} + \sum_{\pi: \phi_n^*(k, (0, \pi))=0} p_{(0)}^{k,\pi}, \quad (127)$$

$$p_n(q|k) \triangleq \sum_{(f, \pi): \phi_n^*(k, (f, \pi))=q} p_{(f)}^{k,\pi} \quad (128)$$

The homogeneous MI leakage can be written as:

$$\rho_{(\text{MI})} = \frac{1}{N} \sum_{n=1}^N \text{MI} \left(M \rightarrow Q_n^{[M]} \right) \quad (129)$$

$$= \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K \sum_{q=\# \& q \in \mathcal{Q}} \frac{p_n(q|k)}{K} \cdot \left\{ H(M) - H(M|Q_n^{[M]} = q) \right\} \quad (130)$$

$$= p_{\#} \log K + \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K \sum_{\|q\|=0} \frac{p_n(0|k)}{K} \cdot \left\{ H(M) - H(M|Q_n^{[M]} = 0) \right\} \\ + \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K \sum_{\|q\|>0} \frac{p_n(q|k)}{K} \cdot \left\{ H(M) - H(M|Q_n^{[M]} = q) \right\} \quad (131)$$

$$\geq p_{\#} \log K \\ + \underbrace{\frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K \sum_{\|q\|>0} \frac{p_n(q|k)}{K} \left\{ H(M) - H(M|Q_n^{[M]} = q) \right\}}_{\mathcal{T}}, \quad (132)$$

where the second equality is obtained by splitting the queries into those of the type # and otherwise, and the inequality is because the uniform distribution maximizes the entropy. On the other hand, for the last

term \mathcal{T} , we have

$$\mathcal{T} = \frac{1}{K} \sum_{j=1}^K \sum_{\|q\|=j} \left\{ \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K p_n(q|k) \log \frac{K p_n(q|k)}{\sum_{k'=1}^K p_n(q|k')} \right\} \quad (133)$$

$$\begin{aligned} &\geq \frac{1}{K} \sum_{j=1}^K \sum_{\|q\|=j} \left\{ \frac{1}{N} \sum_{k=1}^K \left(\sum_{n=1}^N p_n(q|k) \right) \right. \\ &\quad \left. \log \left(\frac{K \sum_{n=1}^N p_n(q|k)}{\sum_{n=1}^N \sum_{k'=1}^K p_n(q|k')} \right) \right\} \end{aligned} \quad (134)$$

$$\begin{aligned} &\geq \frac{1}{K} \sum_{j=1}^K \left\{ \frac{1}{N} \sum_{k=1}^K \sum_{\|q\|=j} \mathbf{1}(\|q|k\| = j-1) \right. \\ &\quad \left. \sum_{\pi} p_{(q|k)}^{k,\pi} \log \frac{K \sum_{\pi} p_{(q|k)}^{k,\pi}}{\sum_{k'=1}^K \sum_{\pi} p_{(q|k')}^{k,\pi}} \right\} \end{aligned} \quad (135)$$

$$\begin{aligned} &+ \frac{1}{K} \sum_{j=1}^K \left\{ \frac{1}{N} \sum_{k=1}^K \sum_{\|q\|=j} \mathbf{1}(\|q|k\| = j) \right. \\ &\quad \left. \sum_{\pi} p_{(q|k)}^{k,\pi} \log \frac{K \sum_{\pi} p_{(q|k)}^{k,\pi}}{\sum_{k'=1}^K \sum_{\pi} p_{(q|k')}^{k,\pi}} \right\} \end{aligned} \quad (136)$$

$$\begin{aligned} &= \frac{1}{NK} \sum_{j=1}^K \left\{ (N-1) \sum_{k=1}^K \sum_{\|f\|=j-1} \sum_{\pi} p_{(f)}^{k,\pi} \right. \\ &\quad \left. \log \frac{K \sum_{\pi} p_{(f)}^{k,\pi}}{\sum_{k'=1}^K \sum_{\pi} p_{(q|k')}^{k,\pi}} \right\} \end{aligned} \quad (137)$$

$$\begin{aligned} &+ \frac{1}{NK} \sum_{j=1}^K \left\{ \sum_{k=1}^K \sum_{\|f\|=j} \sum_{\pi} p_{(f)}^{k,\pi} \right. \\ &\quad \left. \log \frac{K \sum_{\pi} p_{(f)}^{k,\pi}}{\sum_{k'=1}^K \sum_{\pi} p_{(q|k')}^{k,\pi}} \right\} \end{aligned} \quad (138)$$

$$\begin{aligned} &\geq \frac{1}{K} \sum_{j=1}^K \left\{ \frac{t_j j}{NK s_{j-1}} \sum_{k=1}^K \sum_{\|f\|=j-1} \sum_{\pi} p_{(f)}^{k,\pi} \right. \\ &\quad \left. \log \frac{K \frac{1}{NK s_{j-1}} \sum_{k=1}^K \sum_{\pi} \sum_f p_{(f)}^{k,\pi}}{\sum_{k'=1}^K \sum_{\pi} p_{(q|k')}^{k,\pi}} \right\} \end{aligned} \quad (139)$$

$$\begin{aligned} &+ \frac{1}{K} \sum_{j=1}^K \left\{ \frac{t_j (K-j)}{NK s_j} \sum_{k=1}^K \sum_{\|f\|=j} \sum_{\pi} p_{(f)}^{k,\pi} \right. \\ &\quad \left. \log \frac{K \frac{1}{NK s_j} \sum_{k=1}^K \sum_{\pi} \sum_f p_{(f)}^{k,\pi}}{\sum_{k'=1}^K \sum_{\pi} p_{(q|k')}^{k,\pi}} \right\} \end{aligned} \quad (140)$$

$$\begin{aligned} &= \frac{1}{K} \sum_{j=1}^K t_j \left\{ j p_{j-1} \log \frac{K p_{j-1}}{j p_{j-1} + (K-j) p_j} \right. \\ &\quad \left. + (K-j) p_j \log \frac{K p_j}{j p_{j-1} + (K-j) p_j} \right\} \end{aligned} \quad (141)$$

$$\begin{aligned}
&= \frac{1}{K} \sum_{j=1}^K \binom{K}{j} (N-1)^j \\
&\quad \left\{ jp_{j-1} \log p_{j-1} + (K-j)p_j \log p_j \right. \\
&\quad \left. - [jp_{j-1} + (K-j)p_j] \log \frac{jp_{j-1} + (K-j)p_j}{K} \right\}, \tag{142}
\end{aligned}$$

where (134) follows from the log sum inequality shown in Lemma 3 below; (136) follows from $|\{f : f = q|k, \|f\| = j-1\}| = j$ and $|\{f : f = q|k, \|f\| = j\}| = K-j$ for a given q , and $\mathbb{1}(\cdot)$ is the indicator function; (140) follows from Lemma 4 and counting the number of f for each q . This proves the direction $(P3) \geq (P4)$ and completes the proof. \square

Lemma 3. (*Log sum inequality*) The term \mathcal{T} given above satisfies $(133) \geq (134)$.

Proof. Notice that to show $(133) \geq (134)$, we only need to show for each fixed k

$$\begin{aligned}
&\sum_{n=1}^N p_n(q|k) \log \frac{K p_n(q|k)}{\sum_{k'=1}^K p_n(q|k')} \geq \\
&\left(\sum_{n=1}^N p_n(q|k) \right) \log \left(\frac{K \sum_{n=1}^N p_n(q|k)}{\sum_{n=1}^N \sum_{k'=1}^K p_n(q|k')} \right). \tag{143}
\end{aligned}$$

That is to show

$$\begin{aligned}
&\sum_{n=1}^N p_n(q|k) \log \frac{p_n(q|k)}{\sum_{k'=1}^K p_n(q|k')} \geq \\
&\left(\sum_{n=1}^N p_n(q|k) \right) \log \left(\frac{\sum_{n=1}^N p_n(q|k)}{\sum_{n=1}^N \sum_{k'=1}^K p_n(q|k')} \right). \tag{144}
\end{aligned}$$

Let $f(t) = t \log t$. Notice that $f(t)$ is strictly convex since $f''(t) = \frac{1}{t} > 0$. Hence by Jensen's inequality, we have

$$\sum_{n=1}^N \alpha_n f(t_n) \geq f \left(\sum_{n=1}^N \alpha_n t_n \right), \tag{145}$$

for $\alpha_n \geq 0$, $\sum_n \alpha_n = 1$. Hence we can obtain the inequality we want by setting

$$\alpha_n = \frac{\sum_{k'=1}^K p_n(q|k')}{\sum_{j=1}^N \sum_{k'=1}^K p_j(q|k')}, \tag{146}$$

$$t_n = \frac{p_n(q|k)}{\sum_{k'=1}^K p_n(q|k')}. \tag{147}$$

The proof is thus completed. \square

Lemma 4.

$$\sum_{n=1}^N p_n \log \frac{p_n}{Z} \geq N p' \log \frac{p'}{Z},$$

where $p' = \sum_{n=1}^N p_n / N$ and Z is a positive constant.

Proof. The LHS is equivalent to

$$\begin{aligned} \text{LHS} &= \sum_{n=1}^N p_n \log \frac{p_n}{Z} = \sum_{n=1}^N p_n \log p_n - \sum_{n=1}^N p_n \log Z \\ &= \sum_{n=1}^N p_n \log p_n - Np' \log Z. \end{aligned} \quad (148)$$

Since uniform distribution maximizes the entropy, we have

$$\begin{aligned} \sum_{n=1}^N p_n \log p_n - Np' \log Z &\geq Np' \log p' - Np' \log Z \\ &= Np' \log \frac{p'}{Z} = \text{RHS} \end{aligned} \quad (149)$$

□

D Proof of Lemma 1

Proof. Supposing $\mathbf{p} = (p_{\#}, p_0, \dots, p_{K-1})$ is a valid solution, we first let $\hat{p}^* \triangleq p_0 + p_{\#}$, $\hat{p} \triangleq 1 - D + D/N \leq \hat{p}^*$, $\alpha = (1 - N\hat{p})/(1 - N\hat{p}^*)$. We explicitly construct the following new assignment $\mathbf{p}' = (p'_{\#}, p'_0, \dots, p'_{K-1})$:

$$p'_j = \alpha p_j, \quad j \in [0, K-1], \quad (150)$$

$$p'_{\#} = \hat{p} - p'_0, \quad (151)$$

The download cost constraint is obtained trivially since $p'_{\#} + p'_0 = \hat{p}$. The total probability constraint can be verified by

$$Np'_{\#} + \sum_{j=0}^{K-1} Ns_j p'_j = N(p'_{\#} + p'_0) + \sum_{j=1}^{K-1} Ns_j p'_j \quad (152)$$

$$= N\hat{p} + \frac{1 - N\hat{p}}{1 - N\hat{p}^*} \sum_{j=1}^{K-1} Ns_j p_j \quad (153)$$

$$\begin{aligned} &= N\hat{p} + \frac{1 - N\hat{p}}{1 - N\hat{p}^*} (1 - N\hat{p}^*) \\ &= 1. \end{aligned} \quad (154)$$

The MI leakage under this newly constructed assignment is given by

$$\begin{aligned} I(\mathbf{p}') &= p'_{\#} \log K + \frac{1}{K} \sum_{j=1}^K \binom{K}{j} (N-1)^j \\ &\quad \left\{ j\alpha p_{j-1} \log \alpha p_{j-1} + (K-j)\alpha p_j \log \alpha p_j \right. \\ &\quad \left. - [j\alpha p_{j-1} + (K-j)\alpha p_j] \log \frac{j\alpha p_{j-1} + (K-j)\alpha p_j}{K} \right\} \\ &= p'_{\#} \log K + \frac{\alpha}{K} \sum_{j=1}^K \binom{K}{j} (N-1)^j \left\{ jp_{j-1} \log \alpha p_{j-1} \right. \\ &\quad \left. + (K-j)p_j \log \alpha p_j - [jp_{j-1} + (K-j)p_j] \right. \\ &\quad \left. \left(\log \alpha + \log \frac{jp_{j-1} + (K-j)p_j}{K} \right) \right\} \end{aligned} \quad (155)$$

$$\begin{aligned}
&= p'_{\#} \log K + \frac{\alpha}{K} \sum_{j=1}^K \binom{K}{j} (N-1)^j \left\{ j p_{j-1} \log p_{j-1} \right. \\
&\quad \left. + (K-j) p_j \log p_j \right. \\
&\quad \left. - [j p_{j-1} + (K-j) p_j] \log \frac{j p_{j-1} + (K-j) p_j}{K} \right\}
\end{aligned} \tag{157}$$

$$= p'_{\#} \log K + \alpha (I(\mathbf{p}) - p_{\#} \log K) \tag{158}$$

$$= (p'_{\#} - \alpha p_{\#}) \log K + \alpha I(\mathbf{p}) \tag{159}$$

$$= (\hat{p} - \alpha \hat{p}^*) \log K + \alpha I(\mathbf{p}) \tag{160}$$

Therefore, we have

$$I(\mathbf{p}') - I(\mathbf{p}) = (\hat{p} - \alpha \hat{p}^*) \log K + (\alpha - 1) I(\mathbf{p}) \tag{161}$$

$$= \left(\hat{p} - \frac{1 - N \hat{p}}{1 - N \hat{p}^*} \hat{p}^* \right) \log K + \left(\frac{1 - N \hat{p}}{1 - N \hat{p}^*} - 1 \right) I(\mathbf{p}) \tag{162}$$

$$= \frac{\hat{p} - \hat{p}^*}{1 - N \hat{p}^*} \log K + \frac{N \hat{p}^* - N \hat{p}}{1 - N \hat{p}^*} I(\mathbf{p}) \tag{163}$$

$$= \frac{N(\hat{p}^* - \hat{p})}{1 - N \hat{p}^*} \left(I(\mathbf{p}) - \frac{\log K}{N} \right) \leq 0, \tag{164}$$

where the inequality follows from the fact that

$$\begin{aligned}
I(\mathbf{p}) &\leq p_{\#} \log K + \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K \sum_{\|q\|>0} \frac{p_n(q|k)}{K} \\
&\quad \left\{ H(M) - H(M|Q_n^{[M]} = q) \right\}
\end{aligned} \tag{165}$$

$$\leq p_{\#} \log K + \frac{1}{N} (1 - N p_{\#}) H(M) = \frac{\log K}{N}. \tag{166}$$

Therefore, $I(\mathbf{p}') \leq I(\mathbf{p})$, and this completes the proof. \square