Weakly Private Information Retrieval from Heterogeneously Trusted Servers

Yu-Shin Huang*, Wenyuan Zhao*, Ruida Zhou†, and Chao Tian*
*Department of Electrical and Computer Engineering, Texas A&M University
†Department of Electrical Engineering, University of California, Los Angeles
{yushin1002, wyzhao, chao.tian}@tamu.edu, ruida@g.ucla.edu

***Abstract*—We study the problem of weakly private information retrieval (PIR) when there is heterogeneity in servers' trustfulness under the maximal leakage (Max-L) 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. 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.**

I. Introduction

The study of *private information retrieval* (PIR) systems [1] was motivated by the need to protect user privacy during information retrieval. In the canonical PIR setting, a user retrieves a message from N non-colluding servers, each keeping a copy of all K messages. The user wishes to ensure that the servers can infer no information about the identity of the desired message. The message is usually quite large, and the dominant communication cost is the download from the servers. The highest possible information bits per downloaded bit is referred to as the PIR capacity, which was fully characterized by Sun and Jafar [2]. An alternative optimal code (referred to as the TSC code) was later proposed [3], which has the minimum possible message length and query set. Many variations and extensions of the canonical PIR problem has 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].

For some applications, it may not be necessary to maintain perfect privacy, i.e., the user may not mind if the server can infer the identity of the desired message with only relatively low confidence. This setting, where a weaker privacy constraint is placed, is referred to as weakly private information retrieval (W-PIR) [31]–[39]. In exchange for the loss of privacy, a higher retrieval rate can be attained. Several different metrics have been proposed to measure the privacy leakage in W-PIR. Differential privacy was used in [32], [33], conditional entropy was used in [34], mutual information in [35], and the maximal leakage metric (see [40]) was adopted in [36], [37], [41]. The maximal leakage metric has the advantage of a clear information-theoretic operational meaning, and more importantly, it is agnostic to the message retrieval probability distribution. The W-PIR code proposed in [36] for the maximal leakage metric was obtained by adjusting the code proposed in [3]; similar or identical code constructions were also analyzed in [37] and [38] under different metrics. An improved code construction was later proposed in [41].

In this work, we consider the setting when there is heterogeneity in servers' trustfulness, i.e., some of the servers may be more trustworthy than others. We adopt a general version of the improved W-PIR code [41], and refer it to as the W-PIR$^{\#}$ code. We optimize the probability allocation in this W-PIR$^{\#}$ code, and show that the optimal solution has a particular simple structure: it is essentially a probabilistic sharing between the original TSC code and a direct download from the most trustworthy server. The optimal solution is established through a sophisticated analysis of the underlying convex optimization problem with homogeneously trusted servers, and a critical reduction between the homogeneous setting and the heterogeneous setting that utilizes the property of the maximal leakage metric.

II. Preliminaries

In this section, we formally introduce the weakly private information retrieval (W-PIR) problem under the maximal leakage (Max-L) metric, with either homogeneously or heterogeneously trusted servers. Then we provide a review of the PIR code proposed in [3], and discuss one variant of this code that is suitable for constructing W-PIR codes.

A. Information Retrieval Systems

There are a total of N servers, and each server stores an independent copy of K mutually independent messages, denoted as $W_{1:K} := (W_1, W_2, \ldots, W_K)$, where $K \geq 2$ without loss of generality. Each message consists of L symbols, and each symbol is distributed uniformly in a finite set $\mathcal{X}$, which implies that

$$L := H(W_1) = H(W_2) = \cdots = H(W_K),$$

This work was supported in part by the National Science Foundation via Grant CCF-20-07067.

where the entropy is taken under the logarithm of base $|\mathcal{X}|$. The i-th symbol of the message W_k is denoted as $W_k[i]$, where $i \in [1:L]$ and $k \in [1:K]$. An information retrieval code consists of the following component functions. When a user wishes to retrieve a message W_k, $k \in [1:K]$, the (random) query $Q_n^{[k]}$ sent to server-n is generated according to an encoding function

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

by leveraging some private random key $F^* \in \mathcal{F}^*$. Let $\mathcal{Q}_n$ be the union of all possible queries $Q_n^{[k]}$ over all k. For each $n \in [1:N]$, upon receiving a query $q \in \mathcal{Q}_n$, server-n responds with an answer $A_n^{(q)}$ produced as

$$A_n^{(q)} := \varphi_n(q, W_{1:K}), \tag{2}$$

which is represented by $\ell_n^{(q)}$ symbols in certain coding alphabet $\mathcal{Y}$; to simplify the notation, we assume $\mathcal{X} = \mathcal{Y}$ in this work. We assume that $\ell_n^{(q)}$ may vary according to the query but not the messages, and as such the user knows how many symbols are expected in that answer.

For notation simplicity, we denote $A_n^{(Q_n^{[k]})}$ as $A_n^{[k]}$ and $\ell_n^{(Q_n^{[k]})}$ as $\ell_n^{[k]}$, both of which are random variables. With the answers from the servers, the user attempts to recover the message $\hat{W}_k$ using the decoding function

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

A valid information retrieval code must first satisfy $\hat{W}_k = W_k$, i.e., the desired message should be correctly recovered.

We measure the download cost by the normalized (worst-case) *average download cost*,

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

where $\ell_n^{[k]}$ is the length of the answer in the code and the expectation is taken with respect to the random key F^*.

B. Maximal Leakage

The index of the desired message, denoted as M, is viewed as a random variable following a certain distribution. The identity of the desired message W_M may be leaked to server-n due to the query $Q_n^{[M]}$ sent by the user. We use the maximal leakage metric in this work.

The maximal leakage metric $\mathcal{L}(M \to Q_n^{[M]})$: It was shown in [40] and [36] that the privacy leakage to server-n is given as

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

which in fact does not depend on the probability distribution of M. When $\mathcal{L}(M \to Q_n^{[M]})$ is large, $Q_n^{[M]}$ leaks more information about M in the sense that server-n can estimate M more accurately; on the other hand, when $\mathcal{L}(M \to Q_n^{[M]}) = 0$, the retrieval is private in the sense that the distribution of $Q_n^{[k]}$ and $Q_n^{[k']}$ is identical for any $k, k' \in [1:K]$.

We measure the overall privacy leakage by the weighted sum of the exponential leakage amounts to the individual servers

$$\rho = \sum_{n=1}^{N} \gamma_n 2^{\mathcal{L}(M \to Q_n^{[M]})},$$

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

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 $D \le d$. A leakage ρ is called achievable for the download cost constraint d, if there exists a valid code such that the leakage $\mathcal{L} \le \rho$ under the download constraint d. The closure of the collection of such (ρ, d) pairs is called the achievable (ρ, d) region, denoted by $\mathcal{G}_{\text{MaxL}}$.

C. The TSC Code and its Permuted Variant

The TSC code given in [3] will play an instrumental role in this work. In this code, the message length is $L = N - 1$. A dummy symbol $W_k[0] = 0$ is prepended at the beginning of all messages. To better facilitate the construction of the new code, particularly in a heterogeneous environment, we provide below a variation of the original construction, which can be viewed as probabilistic sharing between the permutations (over the N servers) of the PIR code in [3].

Let the random key F^* be the concatenation of a random length-$(K-1)$ vector in $[0:N-1]^{K-1}$, and a random bijective mapping $\pi : [1:N] \to [0:N-1]$ (i.e., a permutation on the set $[1:N]$ but downshifted by 1)

$$F^* := (F, \pi) = (F_1, F_2, \ldots, F_{K-1}, \pi), \tag{6}$$

where $F_1, \ldots, F_{K-1}, \pi$ are mutually independent random variables; each F_k is uniformly distributed over the set $[0 : N-1]$, and the distribution of π will be specified later. We shall use f to denote a specific realization of the random key 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 query $Q_n^{[k]}$ to server-n is generated by the function $\phi_n^*(k, F^*)$ defined as,

$$\begin{aligned}\phi_n^*(k, F^*) \triangleq (F_1, F_2, \ldots, F_{k-1}, (\pi(n) - \sum_{j=1}^{K-1} F_j)_N,\\ F_k, F_{k+1}, \ldots, F_{K-1}),\end{aligned} \tag{7}$$

where $(\cdot)_N$ represents the modulo N operation. Upon receiving the query, the server-n returns the answer $A_n^{[k]}$ generated

by the function $\varphi^*(q, W_{1:K})$,

$$\begin{aligned}\varphi^*(q, W_{1:K}) &\triangleq W_1[Q_{n,1}^{[k]}] \oplus W_2[Q_{n,2}^{[k]}] \oplus \cdots \oplus W_K[Q_{n,K}^{[k]}] \\ &= W_k[(\pi(n) - \sum_{j=1}^{K-1} F_j)_N] \oplus \mathscr{I}, \end{aligned} \tag{8}$$

where $\oplus$ denotes addition in the given finite field, $Q_{n,m}^{[k]}$ represents the m-th symbol of $Q_n^{[k]}$, and $\mathscr{I}$ is the interference signal defined as

$$\begin{aligned}\mathscr{I} = W_1[F_1] \oplus \cdots \oplus W_{k-1}[F_{k-1}] \\ \oplus W_{k+1}[F_k] \oplus \cdots \oplus W_K[F_{K-1}].\end{aligned} \tag{9}$$

Since there exists an $n^* \in [1 : N]$, such that $(\pi(n^*) - \sum_{j=1}^{K-1} F_j)_N = 0$, it follows that $A_{n^*}^{[k]} = \mathscr{I}$. Therefore, the user can retrieve the desired message W_k by subtracting $\mathscr{I}$ from $A_n^{[k]}$ for all $n \neq n^*$. Note that with probability $N^{-(K-1)}$ the interference signal $\mathscr{I}$ consists of only dummy symbols and need not be downloaded at all, in which case a direct download will be performed by retrieving the desired message from $N-1$ servers, one symbol per server. The download cost is therefore

$$D^* = \frac{N}{N-1}\left(1 - \frac{1}{N^{K-1}}\right) + \frac{1}{N^{K-1}} = \frac{1 - N^{-K}}{1 - N^{-1}}, \tag{10}$$

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, can be found in [42] (Table 1 (a) and (b), the bottom halves without the # parts); more details on the code can be found in [3].

D. 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 $F_1 = F_2 = \ldots = F_{K-1} = 0$, 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 more likely be downloaded directly from $N-1$ servers, resulting in privacy leakage but lower download cost; if the probabilities of these random keys are the same as 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 tradeoffs between the download cost and the privacy leakage. Almost all existing W-PIR code constructions are essentially utilizing such an approach [35]–[38].

III. W-PIR$^{\#}$: Generalized TSC Code with Escape Retrieval Symbols

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 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 $[1 : N] \to [0 : N-1]$. This probability distribution is denoted as

$$\mathbb{P}_k(F^*) = \begin{cases} p_{(\#)}^{k,F^*}, & F^* \in [1 : N] \\ p_{(f)}^{k,\pi}, & F^* = (f, \pi) \in [0 : N-1]^{K-1} \times \mathcal{P} \end{cases}, \tag{11}$$

which needs to satisfy

$$\sum_{n=1}^{N} p_{(\#)}^{k,n} + \sum_{f \in \mathcal{F}} \sum_{\pi \in \mathcal{P}} p_{(f)}^{k,\pi} = 1, \quad k = 1, 2, \ldots, K. \tag{12}$$

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

$$Q_n^{[k]} = \begin{cases} \#_k, & F^* = n \\ \underline{0_K}, & F^* \in [1 : N],\ F^* \neq n \\ \phi_n^*(k, F^*), & F^* \notin [1 : N] \end{cases}, \tag{13}$$

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

$$A_n^{[k]} = \begin{cases} W_k, & q = \#_k \\ \varphi^*(q, W_{1:K}), & q \notin \{\#_k : k \in [1 : K]\}. \end{cases} \tag{14}$$

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 the code, which does not allow all permutations, was first presented in [41].

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

$$p_d^k \triangleq \sum_{n=1}^{N} p_{(\#)}^{k,n} + \sum_{\pi \in \mathcal{P}} p_{(\underline{0_{K-1}})}^{k,\pi}, k \in [1 : K], \tag{15}$$

$$D = \max_k \left(p_d^k + \frac{N}{N-1}(1 - p_d^k)\right), \tag{16}$$

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 the next section.

IV. Main Result

We summarize the main result with heterogeneous server trustfulness under the Max-L metric in the following theorem.

Theorem 1. *An optimal probability assignment for W-PIR$^{\#}$ under the Max-L metric is given by*

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

where π^* is the mapping $\pi^*(n) = n+1$, and other $p_{(\#)}^{k,n}$ and $p_{(f)}^{k,\pi}$ are assigned value zero. As a consequence, with download cost $D \in [1, D^*]$, we have the optimal surrogate leakage for the W-PIR$^{\#}$ code as

$$\rho^*(D) = \sum_{n=1}^{N} \gamma_n + \gamma_1 \frac{(K-1)\left[N^{K-1}(N-(N-1)D)-1\right]}{N^{K-1}-1}. \tag{17}$$

This theorem implies that without the 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 tradeoff. Intuitively, this strategy makes perfect sense since the most trusted server will induce the least amount of leakage, and we might as well retrieve the whole message from it. Note that the probability assignment given in the theorem for the heterogeneous W-PIR$^{\#}$ code is also an optimal probability assignment for the homogeneous setting.

The proof of this theorem 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, which we refer to as 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 again 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 trustfulness setting.

A. 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 in establishing the optimal probability allocation for W-PIR$^{\#}$. In this reduced version, we set the probability as follows

$$\mathbb{P}_k(F^*) = \begin{cases} p_{\#}, & F^* \in [1:N] \\ p_j, & F^* = (F,\pi) \in [0:N-1]^{K-1} \times \mathcal{P} \\ & \quad : \pi \text{ is cyclic and } \|F\| = j \\ 0, & \text{otherwise} \end{cases}, \tag{18}$$

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. Note that this reduced W-PIR$^{\#}$ is symmetric even when it is 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

$$t_j = \binom{K}{j} (N-1)^j, \forall\ j \in [0:K]. \tag{19}$$

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

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

The download cost and maximal leakage of the reduced W-PIR$^{\#}$ code is given in the following proposition. The proof is relatively straightforward, and we omit it here for brevity.

Proposition 1. *The reduced generalized TSC scheme induces the download cost and maximal leakage pair (ρ, D) given as*

$$D = \frac{N-(Np_{\#}+Np_0)}{N-1}, \tag{21}$$

$$\rho = \sum_{n=1}^{N} \gamma_n 2^{\mathcal{L}(M\to Q_n^{[M]})} = \sum_{n=1}^{N} \gamma_n \Bigg(\sum_{j=1}^{K} t_j \max\{p_{j-1}, p_j\} + p_0 + (N+K-1)p_{\#} \Bigg), \tag{22}$$

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

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

Let us consider the homogeneous case where $\gamma_1 = \gamma_2 = \ldots = \gamma_N = 1/N$, which we shall refer to as problem $P1$:

$$\begin{aligned} \underset{p_{(\#)}^{k,n},\, p_{(f)}^{k,\pi}}{\text{minimize}} \quad & \frac{1}{N}\sum_{n=1}^{N} 2^{\mathcal{L}(M\to Q_n^{[M]})} \\ \text{subject to} \quad & p_{(\#)}^{k,n} \geq 0, \quad \forall k,n, \\ & p_{(f)}^{k,\pi} \geq 0, \quad \forall k,\pi,f, \\ & \sum_{n=1}^{N} p_{(\#)}^{k,n} + \sum_{f\in\mathcal{F}}\sum_{\pi\in\mathcal{P}} p_{(f)}^{k,\pi} = 1, \quad \forall k, \\ & \textstyle\sum_{n=1}^{N} p_{(\#)}^{k,n} + \sum_{\pi} p_{(0)}^{k,\pi} \\ & \textstyle + \frac{N}{N-1}\left(1 - \sum_{n=1}^{N} p_{(\#)}^{k,n} - \sum_{\pi} p_{(0)}^{k,\pi}\right) \leq D, \forall k \end{aligned} \tag{23}$$

Recall that $p_{(\#)}^{k,n}$ is the probability of requesting server-n only for the k^{th} message, and $p_{(f)}^{k,\pi}$ is the probability of query for the k^{th} message under the random key f and permutation π. We denote $p_{(0_{K-1})}^{k,\pi}$ as $p_{(0)}^{k,\pi}$ for simplicity. See Table 1 in [42] for an example.

We first show that the optimal value $(P1)$ of the optimization problem above, which is achieved under the optimal probably distribution in W-PIR$^{\#}$ code, is the same as the optimal value $(P2)$ of the optimization problem below, which is achieved by the optimal distribution allocation for the

reduced W-PIR$^{\#}$ code.

$$\begin{aligned} \underset{p_{\#},p_0,p_1,\ldots,p_{K-1}}{\text{minimize}} \quad & \textstyle\sum_{j=1}^{K} t_j \max\{p_{j-1},p_j\} \\ & +(p_0+(N-1)p_{\#})+Kp_{\#} \\ \text{subject to} \quad & p_{\#},p_0,p_1,\ldots,p_{K-1}\geq 0, \\ & Np_{\#}+\sum_{j=0}^{K-1} Ns_jp_j = 1, \\ & \frac{N-(Np_{\#}+Np_0)}{N-1} \leq D \end{aligned} \tag{24}$$

For notation simplicity, 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. $(P1) = (P2)$.

The proof of this proposition can be found in [42], which was obtained by carefully constructing a sequence of inequalities based mostly on the convexity of the maximum function.

C. Homogeneous Trustfulness: Optimal Reduced W-PIR$^{\#}$

We establish the optimality of the probabilistic sharing solution of the reduced W-PIR$^{\#}$ code in the homogeneous setting.

Theorem 2. *For the homogeneous setting with download cost $D \in [1, D^*]$, the optimal surrogate leakage loss is given as*

$$\begin{aligned} &\gamma \sum_{n=1}^{N} 2^{\mathcal{L}(M\to Q_n^{[M]})} \\ &\quad = N\gamma\left(1+\frac{(K-1)\left[N^{K-1}(N-(N-1)D)-1\right]}{N^K-N}\right), \end{aligned} \tag{25}$$

which is achieved using the allocation in Theorem 1.

The proof of this theorem can be found in [42], which was obtained by analyzing the KKT conditions [43] of the given convex optimization problem.

D. 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 setting is

$$\rho = \sum_{n=1}^{N} \gamma_n 2^{\mathcal{L}(M\to Q_n^{[M]})}. \tag{26}$$

We can alternatively consider an equivalent loss function ρ_o defined as

$$\rho_o = \sum_{n=1}^{N} \gamma_n \left(2^{\mathcal{L}(M\to Q_n^{[M]})}-1\right). \tag{27}$$

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

$$\rho_o^*(D) = \rho^*(D) - \sum_{n=1}^{N} \gamma_n. \tag{28}$$

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

$$\hat{\rho} = \gamma_1 \sum_{n=1}^{N} 2^{\mathcal{L}(M\to Q_n^{[M]})}, \tag{29}$$

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

$$\hat{\rho}_o = \gamma_1 \sum_{n=1}^{N} (2^{\mathcal{L}(M\to Q_n^{[M]})}-1). \tag{30}$$

It is clear that the optimal value of 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 $\gamma_1 \leq \gamma_2 \leq \ldots \leq \gamma_N$ and $2^{\mathcal{L}(M\to Q_n^{[M]})} \geq 1$ 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

$$\begin{aligned} \hat{\rho}_o^*(D) &= \hat{\rho}^*(D) - N\gamma_1 \\ &= N\gamma_1\left(\frac{(K-1)\left[N^{K-1}(N-(N-1)D)-1\right]}{N^K-N}\right), \end{aligned} \tag{31}$$

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

$$\begin{aligned} \rho^*(D) &= \rho_o^*(D) + \sum_{n=1}^{N}\gamma_n \geq \hat{\rho}_o^*(D) + \sum_{n=1}^{N}\gamma_n \\ &= N\gamma_1\left(\frac{(K-1)\left[N^{K-1}(N-(N-1)D)-1\right]}{N^K-N}\right) + \sum_{n=1}^{N}\gamma_n. \end{aligned} \tag{32}$$

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

$$\hat{p}_{\#} = \frac{N^K(1-D+D/N)-1}{N^{K-1}-1}. \tag{33}$$

The proof is thus complete. □

V. 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. The optimal probability allocation for the W-PIR$^{\#}$ code has a simple structure that can be interpreted as a probabilistic sharing between a capacity-achieving PIR code and a direct download from the most trusted server, and a specific optimal code for the homogeneous setting is in fact also optimal for the heterogeneous setting.

In the extended version of this work [42], we further study W-PIR under the mutual information leakage metric for both the homogeneous and the heterogeneous settings, where the optimal solutions for the two settings become rather different.

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*, in press.

[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. G. 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 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. G. 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] 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.

[41] 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.

[42] W. Zhao, Y. S. Huang, R. Zhou, and C. Tian, "Weakly private information retrieval from heterogeneously trusted servers," *arXiv preprint arXiv:2402.17940*, 2024.

[43] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed. Cambridge University Press, 2004.