On Single Server Private Information Retrieval With Private Coded Side Information

Yuxiang Lu, *Graduate Student Member, IEEE*, and Syed A. Jafar, *Fellow, IEEE*

***Abstract*— Motivated by an open problem and a conjecture, this work studies the problem of single server private information retrieval with private coded side information (PIR-PCSI) that was recently introduced by Heidarzadeh et al. The goal of PIR-PCSI is to allow a user to efficiently retrieve a desired message W_θ, which is one of K independent messages that are stored at a server, while utilizing private side information of a linear combination of a uniformly chosen size-M subset ($\mathcal{S} \subset [K]$) of messages. The settings PIR-PCSI-I and PIR-PCSI-II correspond to the constraints that θ is generated uniformly from $[K]\backslash\mathcal{S}$, and $\mathcal{S}$, respectively. In each case, $(\theta, \mathcal{S})$ must be kept private from the server. The capacity is defined as the supremum over message and field sizes, of achievable rates (number of bits of desired message retrieved per bit of download) and is characterized by Heidarzadeh et al. for PIR-PCSI-I in general, and for PIR-PCSI-II for $M > (K+1)/2$ as $(K-M+1)^{-1}$. For $2 \leq M \leq (K+1)/2$ the capacity of PIR-PCSI-II remains open, and it is conjectured that even in this case the capacity is $(K-M+1)^{-1}$. We show the capacity of PIR-PCSI-II is equal to $2/K$ for $2 \leq M \leq \frac{K+1}{2}$, which is strictly larger than the conjectured value, and does not depend on M within this parameter regime. Remarkably, half the side-information is found to be redundant. We also characterize the infimum capacity (infimum over fields instead of supremum), and the capacity with private coefficients. The results are generalized to PIR-PCSI-I ($\theta \in [K] \setminus \mathcal{S}$) and PIR-PCSI ($\theta \in [K]$) settings.**

***Index Terms*— Capacity, Private Information Retrieval (PIR), coded side information (CSI), interference alignment.**

I. Introduction

As CLOUD services and distributed data storage become increasingly prevalent, growing concerns about users' privacy have sparked much recent interest in the problem of Private Information Retrieval (PIR). Originally introduced in [1] and [2], the goal of PIR is to allow a user to efficiently retrieve a desired message from a server or a set of servers where multiple messages are stored, without revealing any information about which message is desired. In the information theoretic framework, which requires perfect privacy and assumes long messages, the capacity of PIR is the maximum number of bits of desired information that can be retrieved per bit of download from the server(s) [3]. Capacity characterizations have recently been obtained for various forms of PIR, especially for the multi-server setting [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22].

PIR in the basic single server setting would be most valuable if it could be made efficient. However, it was already shown in the earliest works on PIR [1], [2] that in the single server case there is no better alternative to the trivial solution of downloading everything, which is prohibitively expensive. Since the optimal solution turns out to be trivial, single server PIR generally received less attention from the information theoretic perspective, until recently. Interest in the capacity of single-server PIR was revived by the seminal contribution of Kadhe et al. in [23] which showed that the presence of *side information* at the user can significantly improve the efficiency of PIR, and that capacity characterizations under side information are far from trivial. This crucial observation inspired much work on understanding the role of side-information in PIR [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], which remains an active topic of research. Among the recent advances in this area is the study of single-server PIR with private coded side information (PIR-PCSI) that was initiated by Heidarzadeh, Kazemi and Sprintson in [33]. Heidarzadeh et al. obtain sharp capacity characterizations for PIR-PCSI in many cases, and also note an open problem, along with an intriguing conjecture that motivates our work in this paper.

In the PIR-PCSI problem, a single server stores K independent messages $\boldsymbol{W}_1, \cdots, \boldsymbol{W}_K$, each represented by L i.i.d. uniform symbols from a finite field $\mathbb{F}_q$. A user wishes to efficiently retrieve a desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$, while utilizing private side information $(\boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]})$ that is unknown to the server, comprised of a linear combination $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} = \sum_{m=1}^{M} \boldsymbol{\lambda}_m \boldsymbol{W}_{i_m}$ of a uniformly chosen size-M subset of messages, $\boldsymbol{\mathcal{S}} = \{\boldsymbol{i}_1, \boldsymbol{i}_2, \cdots, \boldsymbol{i}_M\} \subset [K], \boldsymbol{i}_1 < \boldsymbol{i}_2 < \cdots < \boldsymbol{i}_M$, with the coefficient vector $\boldsymbol{\Lambda} = (\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_M)$ whose elements are chosen i.i.d. uniform from $\mathbb{F}_q^{\times}$, i.e., the multiplicative subgroup of $\mathbb{F}_q$. Depending on whether $\boldsymbol{\theta}$ is drawn uniformly from $[K] \setminus \boldsymbol{\mathcal{S}}$ or uniformly from $\boldsymbol{\mathcal{S}}$, there are two settings, known as PIR-PCSI-I and PIR-PCSI-II, respectively. In each case, $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ must be kept private. Capacity of PIR is typically defined as the maximum number of bits of desired message that can be retrieved per bit of download from the server(s), and includes a supremum over message size L. Since the side-information formulation specifies a finite field $\mathbb{F}_q$, the capacity of PIR-PCSI can potentially depend on the field. A field-independent notion of capacity is introduced in [33] by allowing a supremum over all finite fields. For PIR-PCSI-I, where $\boldsymbol{\theta} \notin \boldsymbol{\mathcal{S}}$, Heidarzadeh et al. fully characterize the capacity as $(K-M)^{-1}$ for $1 \leq M \leq K-1$. For PIR-PCSI-II, the capacity is characterized as $(K-M+1)^{-1}$ for $\frac{K+1}{2} <$

Manuscript received 15 February 2022; revised 18 August 2022; accepted 23 February 2023. Date of publication 6 March 2023; date of current version 21 April 2023. This work was supported in part by NSF under Grant CCF-1907053 and Grant CCF-2221379, in part by the Office of Naval Research (ONR) under Grant N00014-21-1-2386, and in part by the Army Research Office (ARO) under Grant W911NF1910344. *(Corresponding author: Yuxiang Lu.)*

The authors are with the Center for Pervasive Communications and Computing (CPCC), University of California Irvine, Irvine, CA 92697 USA (e-mail: yuxiang.lu@uci.edu; syed@uci.edu).

Communicated by M. Bloch, Associate Editor for Security and Privacy.
Digital Object Identifier 10.1109/TIT.2023.3253078

$M \leq K$. Capacity characterization for the remaining case of $2 \leq M \leq \frac{K+1}{2}$ is noted as an open problem in [33], and it is conjectured that the capacity in this case is also $(K-M+1)^{-1}$.

The main motivation of our work is to settle this conjecture and obtain the capacity characterization for PIR-PCSI-II when $2 \leq M \leq \frac{K+1}{2}$. Given the importance of better understanding the role of side information for single-server PIR, additional motivation comes from the following questions: What is the infimum capacity (infimum over all finite fields instead of supremum)? What if the coefficient vector $\boldsymbol{\Lambda}$ (whose privacy is not required in [33]) is also required to be private? Can the side-information be reduced, e.g., to save storage, without reducing capacity?

The contributions of this work are summarized in Table I, along with prior results from [33]. As our main contribution we show that the capacity of PIR-PCSI-II for $2 \leq M \leq \frac{K+1}{2}$ is equal to $2/K$, which is strictly higher than the conjectured value in this parameter regime. The result reveals two surprising aspects of this parameter regime. First, whereas previously known capacity characterizations of PIR-PCSI-II (and PIR-PCSI-I) in [33] are all strictly increasing with M (the size of the support set of side information), here the capacity does not depend on M. Second, in this parameter regime (and also when $M = \lfloor (K+1)/2 \rfloor + 1$), half of the side information turns out to be redundant, i.e., the supremum capacity remains the same even if the user discards half of the side information. We also show that if more than half of the side information is discarded, then the supremum capacity is strictly smaller. By contrast, in other regimes no redundancy exists in the side information, i.e., any reduction in side information would lead to a loss in supremum capacity. The results regarding the redundancy in the side information when the supremum capacity is achieved are summarized in Table II in Section III as the definition of redundancy will be clear then.

The optimal rate $2/K$ is shown to be achievable for any finite field $\mathbb{F}_q$ where q is an *even* power of a prime. The achievable scheme requires downloads that are ostensibly non-linear in $\mathbb{F}_q$, but in its essence the scheme is linear, as can be seen by interpreting $\mathbb{F}_q$ as a 2 dimensional vector space over the base field $\mathbb{F}_{\sqrt{q}}$, over which the downloads are indeed linear. Intuitively, the scheme may be understood as follows. A rate of $2/K$ means a download of $K/2$, which is achieved by downloading *half* of every message (one of the two dimensions in the 2 dimensional vector space over $\mathbb{F}_{\sqrt{q}}$). The key idea is *interference alignment* – for the undesired messages that appear in the side information, the halves that are downloaded are perfectly *aligned* with each other, whereas for the desired message, the half that is downloaded is not aligned with the downloaded halves of the undesired messages. For messages that are not included in the side information, any random half can be downloaded to preserve privacy.

With a bit of oversimplification for the sake of intuition, suppose there are $K = 4$ messages, that can be represented as 2-dimensional vectors $\boldsymbol{A} = [\boldsymbol{a}_1 \;\; \boldsymbol{a}_2], \boldsymbol{B} = [\boldsymbol{b}_1 \;\; \boldsymbol{b}_2], \boldsymbol{C} = [\boldsymbol{c}_2 \;\; \boldsymbol{c}_2], \boldsymbol{D} = [\boldsymbol{d}_1 \;\; \boldsymbol{d}_2]$, the side information is comprised of $M = 3$ messages, say at first $\boldsymbol{A} + \boldsymbol{B} + \boldsymbol{C} = [\boldsymbol{a}_1 + \boldsymbol{b}_1 + \boldsymbol{c}_1 \;\; \boldsymbol{a}_2 + \boldsymbol{b}_2 + \boldsymbol{c}_2]$, and the desired message is $\boldsymbol{A}$. Then the user could recover $\boldsymbol{A}$ by downloading $\boldsymbol{a}_1, \boldsymbol{b}_2, \boldsymbol{c}_2$ and either $\boldsymbol{d}_1$ or $\boldsymbol{d}_2$, i.e., half of each message for a total download of $K/2 = 2$ (normalized by message size). We may also note that half of the side information is redundant, i.e., the user only needs $\boldsymbol{a}_2 + \boldsymbol{b}_2 + \boldsymbol{c}_2$, and can discard the rest. But there is a problem with this oversimplification – this toy example seemingly loses privacy because the matching indices reveal that $\boldsymbol{b}_2$ aligns with $\boldsymbol{c}_2$ but not $\boldsymbol{a}_1$. This issue is resolved by noting that the side information is in fact $\boldsymbol{\lambda}_1\boldsymbol{A} + \boldsymbol{\lambda}_2\boldsymbol{B} + \boldsymbol{\lambda}_3\boldsymbol{C} = \boldsymbol{A}' + \boldsymbol{B}' + \boldsymbol{C}'$. Suppose $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \boldsymbol{\lambda}_3$ are random (unknown to the server) independent linear transformations (*matrices*) that independently '*rotate*' $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ vectors into $\boldsymbol{A}', \boldsymbol{B}', \boldsymbol{C}'$ vectors, respectively, such that the projections (combining coefficients) of each along any particular dimension become independent of each other. In other words, $\boldsymbol{a}'_i, \boldsymbol{b}'_i, \boldsymbol{c}'_i$ are independent projections of $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$, and downloading, say $(\boldsymbol{a}'_1, \boldsymbol{b}'_2, \boldsymbol{c}'_2, \boldsymbol{d}'_2)$ reveals to the server no information about their relative alignments in the side information. From the server's perspective, each downloaded symbol is simply an independent random linear combination of the two components of each message. Intuitively, since the random rotation is needed to maintain privacy, it is important that $\boldsymbol{\lambda}_i$ are matrices, not scalars (because scalars only scale, they do not rotate vectors). This is not directly the case in $\mathbb{F}_q$ because $\boldsymbol{\lambda}_i$ are scalars in $\mathbb{F}_q$. However, viewed as a 2 dimensional vector space over $\mathbb{F}_{\sqrt{q}}$, the $\boldsymbol{\lambda}_i$ indeed act as invertible 2×2 matrices that act on the vectors $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$, rotating each vector randomly and independently, thus ensuring privacy.

In order for $\mathbb{F}_{\sqrt{q}}$ to be a valid finite field we need q to be an *even* power of a prime. This suffices to characterize the capacity because the capacity definition in [33] allows a supremum over all fields. However, the question remains about whether the rate $2/K$ is achievable over every finite field. To understand this better, we explore an alternative definition of capacity (called infimum capacity in this work) which considers the infimum (instead of supremum) over all $\mathbb{F}_q$. We find that the infimum capacity of PIR-PCSI-II is always equal to $M/((M-1)K)$. Evidently, for $M = 2$ the capacity is field independent because the infimum and supremum over fields produce the same capacity result. In general however, the infimum capacity can be strictly smaller, thus confirming field-dependence. The worst case corresponds to the binary field $\mathbb{F}_2$. Intuitively, the reason that the infimum capacity corresponds to the binary field is that over $\mathbb{F}_2$ the non-zero coefficients $\boldsymbol{\lambda}_m$ must all be equal to one, and thus the coefficients are essentially known to the server. On the other hand, we also present an example with $q = 3$ (and $M = 3, K = 4$) where $2/K$ is achievable (and optimal), to show that the achievability of $2/K$ for $M > 2$ is not limited to just field sizes that are even powers of a prime number. We also show that for PIR-PCSI-II, the the infimum capacity with private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ is the same as the (supremum or infimum) capacity with private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$, i.e., when the coefficients $\boldsymbol{\Lambda}$ must also be kept private from the server.

Next we consider PIR-PCSI-I where $\boldsymbol{\theta}$ is drawn from $[K] \setminus \boldsymbol{\mathcal{S}}$. The supremum capacity of PIR-PCSI-I is fully characterized in [33]. In this case, we show that there is no redundancy in the CSI. As in PIR-PCSI-II, we find that the infimum capacity of PIR-PCSI-I is strictly smaller than the

TABLE I
CAPACITY RESULTS FOR PIR-PCSI-I, PIR-PCSI-II AND PIR-PCSI

PIR-PCSI-I ($1 \le M \le K-1$)	PIR-PCSI-II ($2 \le M \le K$)	PIR-PCSI ($1 \le M \le K$)
$C^{\sup}_{\text{PCSI-I}} = \frac{1}{K-M}$, [33]	$C^{\sup}_{\text{PCSI-II}} = \begin{cases} \frac{2}{K}, & 2 \le M \le \frac{K+1}{2} \\ \frac{1}{K-M+1}, & \frac{K+1}{2} < M \le K, \end{cases}$ Thm. 1 [33]	$C^{\sup}_{\text{PCSI}} = \begin{cases} \frac{1}{K-1}, & M = 1, \\ \frac{1}{K-M+1}, & 2 \le M \le K, \end{cases}$ Thm. 10
$C^{\inf}_{\text{PCSI-I}} = \begin{cases} \frac{1}{K-1}, & 1 \le M \le \frac{K}{2}, \\ (K - \frac{M}{K-M})^{-1}, & \frac{K}{2} < M \le K-1, \end{cases}$ Thm. 8	$C^{\inf}_{\text{PCSI-II}} = \frac{M}{(M-1)K}$, Thm. 3	$C^{\inf}_{\text{PCSI}} = \frac{1}{K-1}$, Thm. 12
$C^{\inf}_{\text{PCSI-I}} \le C_{\text{PCSI-I}}(q) \le C^{\sup}_{\text{PCSI-I}}$ When $M = K-1$, $C_{\text{PCSI-I}}(q) = 1$, Rmk. 2	$C^{\inf}_{\text{PCSI-II}} \le C_{\text{PCSI-II}}(q) \le C^{\sup}_{\text{PCSI-II}}$ When $M = K$, $C_{\text{PCSI-II}}(q) = \begin{cases} 1/(K-1), & q = 2, \\ 1, & q \ne 2, \end{cases}$ Thm. 4 When $M = 3, K = 4$, $C_{\text{PCSI-II}}(q) = \begin{cases} 3/8, & q = 2, \\ 1/2, & q \ne 2, \end{cases}$ Thm. 5	$C^{\inf}_{\text{PCSI}} \le C_{\text{PCSI}}(q) \le C^{\sup}_{\text{PCSI}}$
$C^{\text{pri,sup}}_{\text{PCSI-I}} = C^{\inf}_{\text{PCSI-I}}$ $\frac{1}{K-1} \le C^{\text{pri,inf}}_{\text{PCSI-I}} \le \min\left(C^{\inf}_{\text{PCSI-I}}, \frac{1}{K-2}\right)$, Thm. 9	$C^{\text{pri}}_{\text{PCSI-II}}(q) = C^{\inf}_{\text{PCSI-II}}$, Thm. 6	$C^{\text{pri}}_{\text{PCSI}}(q) = C^{\inf}_{\text{PCSI}}$, Thm. 13

Notation summary: C stands for capacity, q in the parentheses denotes the problem lies in $\mathbb{F}_q$, the subscript denotes the type of problem (PIR-PCSI-I, PIR-PCSI-II, or PIR-PCSI). In the superscript, 'inf' (resp. 'sup') denotes that the infimum (resp. supremum) of the capacity over all valid q is considered. The term 'pri' as a superscript indicates that it is the capacity when coefficients must also be kept private. Thm. (resp. Rmk.) points out the theorem (resp. remark), where the result appears.

supremum capacity in general, and the binary field $\mathbb{F}_2$ yields the worst case. Unlike PIR-PCSI-II, however, the infimum capacity of PIR-PCSI-I with private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ does not always match the infimum capacity with private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$. For example, if $M = K-1$, then both the supremum and infimum capacities of PIR-PCSI-I are equal to 1 for private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$, but if the coefficient vector $\boldsymbol{\Lambda}$ must also be kept private then the infimum capacity is no more than $1/(K-2)$. Thus, the loss in capacity from requiring privacy of coefficients can be quite significant.

To complete the picture, we finally consider the capacity of PIR-PCSI where $\boldsymbol{\theta}$ is drawn uniformly from $[K]$. In PIR-PCSI the server is not allowed to learn anything about whether or not $\boldsymbol{\theta} \in \boldsymbol{\mathcal{S}}$. The supremum capacity of PIR-PCSI is found to be $(K-M+1)^{-1}$ for $2 \le M \le K$. Remarkably, this is not just the smaller of the two capacities of PIR-PCSI-I and PIR-PCSI-II, so there is an additional cost to be paid for hiding from the server whether $\boldsymbol{\theta} \in \boldsymbol{\mathcal{S}}$ or $\boldsymbol{\theta} \notin \boldsymbol{\mathcal{S}}$. Depending on the relative values of M and K, in this case we find that the redundancy in CSI can be as high as $1/2$ or as low as 0. The infimum capacity of PIR-PCSI is smaller than the supremum capacity, the binary field $\mathbb{F}_2$ yields the worst case, and as in PIR-PCSI-II, the infimum capacity with private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ is the same as the (supremum or infimum) capacity with private $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$.

This paper is organized as follows: Section II states PIR-PCSI, PIR-PCSI-I, PIR-PCSI-II problems in [33]. Section III states our capacity and redundancy (in the CSI) results for PIR-PCSI-II, PIR-PCSI-I, PIR-PCSI with fourteen theorems which are proved in Section IV to Section XVI. Section XVII concludes this paper and gives possible future directions.

Notation: For a positive integer a, let $[a]$ denote the set $\{1, 2, \cdots, a\}$. For two integers a, b where $a < b$, $[a : b]$ denotes the set $\{a, a+1, \cdots, b\}$. For a set $\mathcal{S} = \{i_1, i_2, \cdots, i_n\}$, $|\mathcal{S}|$ denotes the cardinality of $\mathcal{S}$. $\mathbf{I}_M$ denotes the $M \times M$ identity matrix, and $\mathbf{0}_M$ denotes the $M \times M$ all-zero matrix. For a matrix $\mathbf{A}$, let $\mathbf{A}(i,:)$ be the i^{th} row of $\mathbf{A}$. For a set $\mathcal{A}$ whose elements are integers, let $\mathcal{A}(i)$ denote the i^{th} element of $\mathcal{A}$ in ascending order. Let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_q^{\times}$ contain all the non-zero elements of $\mathbb{F}_q$. The notation $\mathbb{F}_q^{a \times b}$ represents the set of all $a \times b$ matrices with elements in $\mathbb{F}_q$. The notation $\mathbb{F}_q^{a \times 1}$ may be shortened to $\mathbb{F}_q^{a}$. Let $\mathfrak{S}$ be the set of all the subsets with cardinality M of $[K]$, i.e., $|\mathfrak{S}| = \binom{K}{M}$, and let $\mathfrak{C}$ be the set of all length M sequences with elements in $\mathbb{F}_q^{\times}$, i.e., $|\mathfrak{C}| = (q-1)^M$. For an index set $S \subset [K]$, define the subscript notation $X_S = \{X_s \mid s \in S\}$. All entropies are in q-ary units. For a random variable $\boldsymbol{A}$, $\mathbb{E}[\boldsymbol{A}]$ is the expectation of $\boldsymbol{A}$, $\Pr(\boldsymbol{A} = A)$ denotes the probability of $\boldsymbol{A}$ being A.

II. PROBLEM STATEMENT

A. Capacity of PIR-PCSI-I, PIR-PCSI-II, PIR-PCSI

A single server stores K independent messages $\boldsymbol{W}_1, \boldsymbol{W}_2, \cdots, \boldsymbol{W}_K \in \mathbb{F}_q^L$, each comprised of L i.i.d. uniform symbols from $\mathbb{F}_q$, i.e., $\boldsymbol{W}_k = (\boldsymbol{W}_k(1), \boldsymbol{W}_k(2), \cdots, \boldsymbol{W}_k(L))^T$, and each $\boldsymbol{W}_k(\ell)$, which denotes the ℓ^{th} instance of the k^{th} message, is drawn i.i.d. uniform from $\mathbb{F}_q$. The number of instances L may be chosen freely by the coding scheme. We refer to $\mathbb{F}_q$ as the *base field*. In terms of entropies,

$$H(\boldsymbol{W}_1) = H(\boldsymbol{W}_2) = \cdots = H(\boldsymbol{W}_K) = L, \tag{1}$$

$$H(\boldsymbol{W}_{[K]}) = \sum_{k \in [K]} H(\boldsymbol{W}_k) = KL. \tag{2}$$

A user wishes to retrieve a message $\boldsymbol{W}_{\boldsymbol{\theta}}$ for a privately generated index $\boldsymbol{\theta}$. The user has a linear combination of M messages available as coded side information (CSI). M is globally known. The CSI is comprised of $(\boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{Y}^{[\boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}]})$, defined as follows. The *support index set* $\boldsymbol{\mathcal{S}}$, drawn uniformly from $\mathfrak{S}$, is a subset of $[K]$, of cardinality M. The vector of coefficients $\boldsymbol{\Lambda} = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \cdots, \boldsymbol{\lambda}_M)$ is drawn uniformly from $\mathfrak{C}$, and applied across all L instances, i.e., the same linear combining coefficients appear in each of the L instances of the CSI. The linear combination available to the user is

$$\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}]} \triangleq \boldsymbol{\lambda}_1 \boldsymbol{W}_{\boldsymbol{\mathcal{S}}(1)} + \boldsymbol{\lambda}_2 \boldsymbol{W}_{\boldsymbol{\mathcal{S}}(2)} + \cdots + \boldsymbol{\lambda}_M \boldsymbol{W}_{\boldsymbol{\mathcal{S}}(M)}, \tag{3}$$

where we recall the notation that $\boldsymbol{\mathcal{S}}(m)$ denotes the m^{th} element of $\boldsymbol{\mathcal{S}}$, in ascending order, i.e., $\boldsymbol{\mathcal{S}}(1) < \boldsymbol{\mathcal{S}}(2) < \cdots < \boldsymbol{\mathcal{S}}(M)$. We assume that $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$, $\boldsymbol{\Lambda}$, $\boldsymbol{W}_{[K]}$ are independent.

$$H(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{W}_{[K]}) = H(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}) + H(\boldsymbol{\Lambda}) + H(\boldsymbol{W}_{[K]}). \tag{4}$$

There are three formulations of the problem depending on how $\boldsymbol{\theta}$ is chosen by the user.

1) **PIR-PCSI-I**: $\boldsymbol{\theta}$ is chosen uniformly from $[K] \setminus \boldsymbol{\mathcal{S}}$.
2) **PIR-PCSI-II**: $\boldsymbol{\theta}$ is chosen uniformly from $\boldsymbol{\mathcal{S}}$.
3) **PIR-PCSI**: $\boldsymbol{\theta}$ is chosen uniformly from $[K]$.

When referring to all three formulations, we will refer to the problem as **PIR-PCSI*** for brevity. In such statements, PCSI* can be replaced with PCSI-I, PCSI-II, or PCSI to obtain corresponding statements for each of the three formulations.

The server knows the distributions but not the realizations of $\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}$. It is required that $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ be kept jointly private from the server. Note that the privacy of $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}$ or the coefficient vector $\boldsymbol{\Lambda}$ is not required. While the server initially knows nothing about the realization of $\boldsymbol{\Lambda}$, a PIR-PCSI* scheme may reveal some information about the coefficients, especially if it allows for efficient retrieval without leaking any information about $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$. Leaking information about $\boldsymbol{\Lambda}$ has implications for reusability of side-information, an issue that is explored recently in [34].

In order to retrieve $\boldsymbol{W}_{\boldsymbol{\theta}}$, we assume as in [33] that the user generates a random query $\boldsymbol{Q}$ that is independent of the messages. Specifically,

$$I(\boldsymbol{W}_{[K]}; \boldsymbol{Q}, \boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}) = 0. \tag{5}$$

Let $\mathcal{Q}$ denote the alphabet of $\boldsymbol{Q}$.

Because the messages are i.i.d. uniform, and the coefficients are non-zero, according to the construction of $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}$, it follows that

$$\begin{aligned} L &= H(\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}), && (6)\\ &= H(\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} \mid \boldsymbol{Q}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{W}_{[K]\setminus\{\boldsymbol{\mathcal{S}}(m)\}}), \forall m \in [M]. && (7)\end{aligned}$$

The user uploads $\boldsymbol{Q}$ to the server. Mathematically, the privacy constraint is expressed as,

$$[(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}) \text{ Privacy}] \qquad I\left(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}; \boldsymbol{Q}, \boldsymbol{W}_{[K]}\right) = 0. \tag{8}$$

The server returns an answer $\boldsymbol{\Delta}$ as a function of $\boldsymbol{Q}$ and the messages, i.e.,

$$H\left(\boldsymbol{\Delta} \mid \boldsymbol{Q}, \boldsymbol{W}_{[K]}\right) = 0. \tag{9}$$

The answer $\boldsymbol{\Delta}$ takes values in an alphabet set $\mathcal{A}_{\boldsymbol{Q}}$ that depends on the query $\boldsymbol{Q}$. The download cost, measured in q-ary symbols is $\log_q |\mathcal{A}_{\boldsymbol{Q}}|$. Since $\mathcal{A}_{\boldsymbol{Q}}$ is a function of $\boldsymbol{Q}$, note that different queries may result in different download costs.

Upon receiving the answer, the user must be able to decode the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$.

$$[\text{Correctness}] \quad H(\boldsymbol{W}_{\boldsymbol{\theta}} \mid \boldsymbol{\Delta}, \boldsymbol{Q}, \boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{\theta}) = 0. \tag{10}$$

We are interested in the *average* download cost, D, across all queries, which is defined and bounded as follows.

$$\begin{aligned} D &\triangleq \mathbb{E}_{\boldsymbol{Q}}\left[\log_q |\mathcal{A}_{\boldsymbol{Q}}|\right] && (11)\\ &= \sum_{Q \in \mathcal{Q}} \Pr(\boldsymbol{Q} = Q) \log_q |\mathcal{A}_Q| && (12)\\ &\geq \sum_{Q \in \mathcal{Q}} \Pr(\boldsymbol{Q} = Q) H(\boldsymbol{\Delta} \mid \boldsymbol{Q} = Q) && (13)\\ &= H(\boldsymbol{\Delta} \mid \boldsymbol{Q}). && (14)\end{aligned}$$

In (13) we used the fact that the entropy of a random variable is no more than the logarithm of the cardinality of its alphabet, corresponding to the fact that the uniform distribution maximizes entropy. This bound will be useful for converse proofs.

The rate achieved by a PIR scheme is defined as,

$$R \triangleq \frac{L}{D} \tag{15}$$

The capacity is the supremum of achievable rates over all message sizes L,

$$C_{\text{PCSI*}}(q) = \sup_{L, \text{achievable } R} R. \tag{16}$$

The capacity can depend on the field $\mathbb{F}_q$ which affects the nature of side information. Field-independent measures of capacity may be obtained by taking a supremum (as in [33]) or infimum over all finite fields. These are called supremum and infimum capacity, respectively.

$$C^{\sup}_{\text{PCSI*}} = \sup_q C_{\text{PCSI*}}(q), \tag{17}$$

$$C^{\inf}_{\text{PCSI*}} = \inf_q C_{\text{PCSI*}}(q). \tag{18}$$

Remark 1: Throughout this paper, we will use the notation $\mathbb{F}_q$ (and accordingly the symbol q) only to represent the field in which the message symbols, and in particular the linear combinations that constitute the CSI lie. The encoding operations may occasionally take place in a different field, typically a sub-field (e.g., $\mathbb{F}_{\sqrt{q}}$ if it exists) or an extension field (e.g., $\mathbb{F}_{q^l}$) of $\mathbb{F}_q$, which will be identified as such.

B. Capacity of PIR-PCSI* With Private Coefficients

Recall that in the formulation of PIR-PCSI* as presented above, while $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ must be kept private, the privacy of the coefficient vector $\boldsymbol{\Lambda}$ is not required. As an important benchmark, we consider the setting where the privacy of coefficients must also be preserved. In this setting, the privacy constraint is modified so that instead of (8) we require the following.

$$[(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}) \text{ Privacy}] \qquad I\left(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}; \boldsymbol{Q}, \boldsymbol{W}_{[K]}\right) = 0. \tag{19}$$

The capacity under this privacy constraint is referred to as the capacity with private coefficients and is denoted as $C^{\text{pri}}_{\text{PCSI*}}(q)$, which is potentially a function of the field size q. The supremum and infimum (over q) of $C^{\text{pri}}_{\text{PCSI*}}(q)$ are denoted as $C^{\text{pri,sup}}_{\text{PCSI*}}, C^{\text{pri,inf}}_{\text{PCSI*}}$, respectively.

C. Redundancy of CSI

In addition to the capacity of PIR-PCSI*, we also wish to determine how much (if any) of the side information is redundant, i.e., can be discarded without any loss in the *supremum capacity*.

For all $\mathcal{S} \in \mathfrak{S}, \Lambda \in \mathfrak{C}$, let $f_{\mathcal{S},\Lambda} : \mathbb{F}_q^L \to \overline{\mathcal{Y}}$ be arbitrary functions that take the CSI $\boldsymbol{Y}^{[\mathcal{S},\Lambda]}$ as input and output some $\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]} \in \overline{\mathcal{Y}}$. These functions could be used to discard some

TABLE II
REDUNDANCY RESULTS FOR PIR-PCSI-I, PIR-PCSI-II AND PIR-PCSI

PIR-PCSI-I ($1 \le M \le K-1$)	PIR-PCSI-II ($2 \le M \le K$)	PIR-PCSI ($1 \le M \le K$)
$\rho_{\text{PCSI-I}} = 0$, Thm. 7	$\rho_{\text{PCSI-II}} = \begin{cases} 1/2, & 1 < M \le (K+2)/2, \\ 0, & (K+2)/2 < M \le K, \end{cases}$, Thm. 2	$\rho_{\text{PCSI}} = \frac{1}{2}, M = 2,$ $\rho_{\text{PCSI}} \le \frac{1}{M}, 3 \le M \le \frac{K+2}{2}$, , Thm. 11 $\rho_{\text{PCSI}} = 0$, otherwise,

parts of the side-information, and retain other parts, e.g., to reduce storage cost.

$$\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]} = f_{\mathcal{S},\Lambda}(\boldsymbol{Y}^{[\mathcal{S},\Lambda]}). \tag{20}$$

Let us refer to all these functions collectively as $\mathcal{F} = (f_{\mathcal{S},\Lambda})_{\mathcal{S}\in\mathfrak{S},\Lambda\in\mathfrak{L}}$. Define, $\overline{C}_{\text{PCSI*}}(q,\mathcal{F})$ as the capacity (supremum of achievable rates) if the decoding must be based on $\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}$ instead of $\boldsymbol{Y}^{[\mathcal{S},\Lambda]}$, i.e., the correctness condition is modified to

$$H(\boldsymbol{W}_{\boldsymbol{\theta}} \mid \boldsymbol{\Delta}, \boldsymbol{Q}, \overline{\boldsymbol{Y}}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}, \boldsymbol{\theta}) = 0. \tag{21}$$

We say that $\mathcal{F}$ uses α-CSI, where

$$\alpha = \max_{\mathcal{S}\in\mathfrak{S},\Lambda\in\mathfrak{L}} H(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]})/L \tag{22}$$

Whereas storing $\boldsymbol{Y}^{[\mathcal{S},\Lambda]}$ requires L q-ary symbols, note that storing $\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}$ requires only αL storage, i.e., storage is reduced by a factor α. Define the α-CSI constrained capacity as

$$\overline{C}_{\text{PCSI*}}(q,\alpha) = \sup_{\mathcal{F}\text{: uses no more than } \alpha\text{-CSI}} \overline{C}_{\text{PCSI*}}(q,\mathcal{F}) \tag{23}$$

In other words, $\overline{C}_{\text{PCSI*}}(q,\alpha)$ is the capacity when the user is allowed to retain no more than a fraction α of the CSI $\boldsymbol{Y}^{[\mathcal{S},\Lambda]}$. The notion of α-CSI constrained capacity is of broader interest on its own. However, in this work we will explore only the redundancy of CSI with regard to the supremum capacity. We say that 'α-CSI is sufficient' if

$$\sup_q \overline{C}_{\text{PCSI*}}(q,\alpha) = C^{\text{sup}}_{\text{PCSI*}} \tag{24}$$

Define α^* as the smallest value of α such that α-CSI is sufficient. The redundancy of PCSI is defined as $\rho_{\text{PCSI*}} = 1 - \alpha^*$. Note that the opposite extremes of $\rho_{\text{PCSI*}} = 1$ and $\rho_{\text{PCSI*}} = 0$ correspond to situations where all of the side information is redundant, and where none of the side information is redundant, respectively.

For later use, it is worthwhile to note that for any scheme that uses no more than α-CSI, because $\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}$ is a function of $\boldsymbol{Y}^{[\mathcal{S},\Lambda]}$, it follows from (7) that for all[1] feasible $(Q,\mathcal{S},\Lambda)$,

$$H\left(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]} \mid (\boldsymbol{Q},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}) = (Q,\mathcal{S},\Lambda)\right) = H(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}) \le \alpha L. \tag{25}$$

This is because of the property that if A is independent of B, then any function of A is also independent of B. In this case, (7) tells us that $\boldsymbol{Y}^{[\mathcal{S},\Lambda]}$ is independent of $\mathbf{Q}$, therefore so is $\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}$.

[1]We say $(Q,\mathcal{S},\Lambda)$ is feasible if $\Pr((\boldsymbol{Q},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}) = (Q,\mathcal{S},\Lambda)) > 0$.

III. MAIN RESULTS

Our main results are presented as theorems in this section, and summarized in Table I and Table II for quick reference. We start with PIR-PCSI-II (where $\boldsymbol{\theta} \in \boldsymbol{\mathcal{S}}$), which is the main motivation for this work. Note that the case $M = 1$ is trivial, because in that case the user already has the desired message. Therefore, for PIR-PCSI-II we will always assume that $M > 1$.

A. PIR-PCSI-II (Where $\boldsymbol{\theta}$ Is Drawn Uniformly From $\boldsymbol{\mathcal{S}}$)

Theorem 1: The supremum capacity of PIR-PCSI-II is

$$C^{\text{sup}}_{\text{PCSI-II}} = \max\left(\frac{2}{K}, \frac{1}{K-M+1}\right) \tag{26}$$

$$= \begin{cases} \frac{2}{K}, & 1 < M \le \frac{K+1}{2}, \\ \frac{1}{K-M+1}, & \frac{K+1}{2} < M \le K, \text{ [33]} \end{cases} \tag{27}$$

The case $(K+1)/2 < M \le K$ was already settled by Heidarzadeh et al. [33], and is included in Theorem 1 primarily for the sake of completeness. Our contribution to Theorem 1 is for the case $1 < M \le (K+1)/2$ which was noted as an open problem in [33] along with a conjecture that the supremum capacity for this case may also be equal to $1/(K-M+1)$. Theorem 1 settles this open problem and resolves the conjecture by establishing that the supremum capacity in this case is $2/K$. The proof of Theorem 1 for the case $2 \le M \le (K+1)/2$ appears in Section IV.

Note that when $2 \le M \le (K+1)/2$, the supremum capacity value $2/K$ is strictly higher than the conjectured value $1/(K-M+1)$, and does not depend on the support size M of the coded side information. Achievability of $2/K$ is shown in Section IV for any field $\mathbb{F}_q$ where q is an even power of a prime, by viewing $\mathbb{F}_q$ as a 2 dimensional vector space over $\mathbb{F}_{\sqrt{q}}$. Note that q needs to be an even power of a prime, in order for $\mathbb{F}_{\sqrt{q}}$ to be a valid finite field. Specifically, we choose $L = 1$, so each message is comprised of 1 symbol from $\mathbb{F}_q$, equivalently 2 symbols from $\mathbb{F}_{\sqrt{q}}$, which can be represented as a 2×1 vector over $\mathbb{F}_{\sqrt{q}}$, while the coefficients $\boldsymbol{\lambda}_m \in \mathbb{F}_q, m \in [M]$ take the role of 2×2 matrices in $\mathbb{F}_{\sqrt{q}}$ that *rotate* the vectors corresponding to the messages $\boldsymbol{W}_{\boldsymbol{\mathcal{S}}_m}$ involved in the CSI, thus randomizing their relative alignments.[2] Half of the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$ is recovered by downloading the corresponding halves of undesired messages that align (interfere) with that half of $\boldsymbol{W}_{\boldsymbol{\theta}}$ (so that the interference can be subtracted), while the other half of $\boldsymbol{W}_{\boldsymbol{\theta}}$ is downloaded directly. The private rotations due to $\boldsymbol{\Lambda}$ in the CSI hide the alignments

[2]As an alternative, suppose instead we consider each message as comprised of $L = 2$ symbols from $\mathbb{F}_q$, which also allows us to work with a 2 dimensional vector space (over $\mathbb{F}_q$). However, since the coefficients are scalars in $\mathbb{F}_q$ and constant across $\ell \in [L]$, in this 2 dimensional vector space the coefficients translate to only scaled versions of 2×2 identity matrices, which does not yield the *rotations* that are essential for privacy.

from the server. For the messages that are not involved in the CSI any random half can be downloaded. Since a random half of every message is downloaded, no information is leaked about $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ and the scheme is private.

Intuitively, since one half of the desired message is directly downloaded, it stands to reason that the corresponding half of the CSI may be redundant and could be discarded by the user, thus saving storage cost. Indeed, this intuition turns out to be correct, as encapsulated in the next theorem which characterizes precisely how much of the side information in each parameter regime is redundant, i.e., can be discarded without any loss in the supremum capacity specified in Theorem 1.

Theorem 2: For the supremum capacity of PIR-PCSI-II, the redundancy in coded side information is characterized as,

$$\rho_{\text{PCSI-II}} = \begin{cases} 1/2, & 1 < M \leq (K+2)/2, \\ 0, & (K+2)/2 < M \leq K. \end{cases} \tag{28}$$

In particular, $\rho_{\text{PCSI-II}} = 1/2$ implies that exactly half of the side information is redundant, and $\rho_{\text{PCSI-II}} = 0$ implies that there is no redundancy in the side information. The proof of Theorem 2 appears in Section V. Thus, for all (M, K) parameters where the supremum capacity is equal to $2/K$, half of the coded side information is redundant. Note that in the boundary case where $M = (K+2)/2$, we have $2/K = 1/(K-M+1)$, i.e., this boundary case could be included in either of the two cases in Theorem 1. Remarkably, these are the only cases where we have any redundancy in coded side information. According to Theorem 2, there is no redundancy when $(K+2)/2 < M \leq K$.

As our next result for PIR-PCSI-II, we characterize the infimum capacity $C^{\inf}_{\text{PCSI-II}}$ in the following theorem.

Theorem 3: The infimum capacity of PIR-PCSI-II,

$$C^{\inf}_{\text{PCSI-II}} = C_{\text{PCSI-II}}(q=2) = \frac{M}{(M-1)K}. \tag{29}$$

The proof of Theorem 3 appears in Section VI. Evidently, the infimum capacity of PIR-PCSI-II matches its capacity over the binary field. Intuitively, one might expect that the binary field would represent the worst case because over $\mathbb{F}_2$, the coefficients $\boldsymbol{\lambda}_m$, which must be non-zero, can only take the value 1. Thus, the coefficients are known to the server. It is also worth noting that constant $\boldsymbol{\Lambda}$ trivially satisfy $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$ privacy whenever $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ privacy is satisfied.

Note that for $M = 2$, the infimum capacity of PIR-PCSI-II matches the supremum capacity, therefore for any field $\mathbb{F}_q$, we have the exact capacity characterization, $C_{\text{PCSI-II}}(q) = C^{\inf}_{\text{PCSI-II}} = C^{\sup}_{\text{PCSI-II}}$. However, in general the infimum capacity is strictly smaller. The gap can be significant, for example when $M = K$ the supremum capacity is 1 while the infimum capacity is $1/(K-1)$. In general the capacity for arbitrary fields, arbitrary support size M and arbitrary number of messages K remains open. Intuitively, we expect that the capacity for most fields should be either equal to or close to the supremum capacity, whereas fields where the capacity is closer to the infimum capacity should be relatively rare. For certain M, K values, however, we are able to characterize the capacity of PIR-PCSI-II for arbitrary fields. These results are presented in the next two theorems. Notably, for these specific M, K, while the binary field $\mathbb{F}_2$ yields the infimum capacity, for all other fields ($\mathbb{F}_q$, $q > 2$), the capacity matches the supremum capacity, i.e., $C_{\text{PCSI-II}}(q) = C^{\sup}_{\text{PCSI-II}}$.

Theorem 4: For PIR-PCSI-II with $M = K$,

$$C_{\text{PCSI-II}}(q) = \begin{cases} 1/(K-1) = C^{\inf}_{\text{PCSI-II}}, & q = 2, \\ 1 = C^{\sup}_{\text{PCSI-II}}, & q \neq 2. \end{cases} \tag{30}$$

The proof of Theorem 4 appears in Section VII.

Theorem 5: For PIR-PCSI-II with $M = 3, K = 4$,

$$C_{\text{PCSI-II}}(q) = \begin{cases} 3/8 = C^{\inf}_{\text{PCSI-II}}, & q = 2, \\ 1/2 = C^{\sup}_{\text{PCSI-II}}, & q \neq 2. \end{cases} \tag{31}$$

Note that $M = 3, K = 4$ is a boundary case for which $1/(K-M+1) = 2/K$, therefore the supremum capacity is achievable by both the Modified Specialized GRS Codes scheme presented in [33] and by the interference alignment scheme that appears in the proof of Theorem 1. However, the former requires field size $q \geq K = 4$, and the latter requires q to be an even power of a prime. Aside from $q = 2$ which corresponds to the infimum capacity, this leaves only $q = 3$, which is neither greater than or equal to 4 nor an even power of a prime, as the only new result in Theorem 5. The proof for $q = 3$ appears in Section VIII.

Building on the observation that the infimum capacity corresponds to the binary field where the coefficients are essentially constants such that the $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$ privacy is automatically satisfied, we next explore the capacity of PIR-PCSI-II for the case of private coefficients. The result appears as the next theorem.

Theorem 6: The capacity of PIR-PCSI-II, for the setting with private coefficients, is given by

$$C^{\text{pri}}_{\text{PCSI-II}}(q) = C^{\text{pri,inf}}_{\text{PCSI-II}} = C^{\text{pri,sup}}_{\text{PCSI-II}} = C^{\inf}_{\text{PCSI-II}}. \tag{32}$$

The proof of Theorem 6 appears in Section IX. Note that the capacity with private coefficients does not depend on the field (infimum and supremum are the same). Compared with the case where the coefficients are not required to be kept private, i.e., the case where only $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$ privacy is required, there is a loss of the supremum capacity, which represents the cost of also keeping the coefficients private.

B. PIR-PCSI-I (Where $\boldsymbol{\theta}$ Is Drawn Uniformly From $[K] \setminus \boldsymbol{\mathcal{S}}$)

In this section we consider the setting of PIR-PCSI-I (where $\boldsymbol{\theta} \in [K] \setminus \boldsymbol{\mathcal{S}}$). Note that the case $M = K$ is not valid, because in that case the desired message is also contained in the support set. Therefore, for PIR-PCSI-I we will always restrict $1 \leq M \leq K-1$.

The supremum capacity of PIR-PCSI-I is already found in [33] as $C^{\sup}_{\text{PCSI}} = (K-M)^{-1}$ and is achievable by Specialized GRS Codes. We start by characterizing the redundancy in the side information in the following theorem, whose proof appears in Section X.

Theorem 7: For the supremum capacity of PIR-PCSI-I, there is no redundancy in coded side information i.e., $\rho_{\text{PCSI-I}} = 0$.

Next we characterize the infimum capacity of PIR-PCSI-I.

Theorem 8: The infimum capacity of PIR-PCSI-I,

$$\begin{aligned} C^{\inf}_{\text{PCSI-I}} &= C_{\text{PCSI-I}}(q=2) \\ &= \max\left(\frac{1}{K-1}, \left(K-\frac{M}{K-M}\right)^{-1}\right) \\ &= \begin{cases} \frac{1}{K-1}, & 1 \le M \le \frac{K}{2}, \\ \left(K-\frac{M}{K-M}\right)^{-1}, & \frac{K}{2} < M \le K-1. \end{cases} \end{aligned} \tag{33}$$

The proof of Theorem 8 appears in Section XI. The infimum capacity of PIR-PCSI-I also matches its capacity over binary field. The intuition why $\mathbb{F}_2$ represents the worst case, is similar to the PIR-PCSI-II setting.

Remark 2: Note that for $M = K-1$, the infimum capacity of PIR-PCSI-I matches the supremum capacity, therefore for any field $\mathbb{F}_q$, we have the exact capacity characterization, $C_{\text{PCSI-I}}(q) = C^{\inf}_{\text{PCSI-I}} = C^{\sup}_{\text{PCSI-I}} = 1$. However, in general the infimum capacity is strictly smaller and the gap can be significant. For example, when $M = K/2$ the supremum capacity is $2/K$ while the infimum capacity is $1/(K-1)$, i.e., for large K, the infimum capacity is nearly half of the supremum capacity.

We next explore the capacity of PIR-PCSI-I for the case of private coefficients.

Theorem 9: The supremum capacity of PIR-PCSI-I, for the setting with private coefficients, is given by

$$C^{\text{pri},\sup}_{\text{PCSI-I}} = C^{\inf}_{\text{PCSI-I}}, \tag{34}$$

while the infimum capacity of the private coefficients setting can be bounded as

$$\frac{1}{K-1} \le C^{\text{pri},\inf}_{\text{PCSI-I}} \le \min\left(C^{\inf}_{\text{PCSI-I}}, \frac{1}{K-2}\right). \tag{35}$$

The proof of Theorem 9 appears in Section XII. Unlike PIR-PCSI-II, for PIR-PCSI-I the capacity with private coefficients may depend on the field, and may be strictly smaller than the infimum capacity. For example, if $M = K-1$, then the infimum capacity is 1, but the infimum capacity with private coefficients is no more than $1/(K-2)$. Remarkably, infimum capacity with private coefficients does not correspond to the binary field $\mathbb{F}_2$, i.e., there exist other fields that yield strictly lower capacities than $\mathbb{F}_2$ for PIR-PCSI-I when the coefficients are fully private.

C. PIR-PCSI (Where $\boldsymbol{\theta}$ Is Drawn Uniformly From $[K]$)

To complete the picture, in this section we characterize the capacity of PIR-PCSI which was not studied in [33]. Since $\boldsymbol{\theta} \in [K]$, any $1 \le M \le K$ is valid. We start with the supremum capacity.

Theorem 10: The supremum capacity of PIR-PCSI is

$$\begin{aligned} C^{\sup}_{\text{PCSI}} &= \max\left(\frac{1}{K-1}, \frac{1}{K-M+1}\right) \\ &= \begin{cases} \frac{1}{K-1}, & M=1, \\ \frac{1}{K-M+1}, & 2 \le M \le K, \end{cases} \end{aligned} \tag{36}$$

The proof of Theorem 10 appears in Section XIII. For $M = 1$, this problem is dominated by the PIR-PCSI-I setting, and the capacity is $(K-1)^{-1}$.

The redundancy of CSI to achieve the supremum capacity of PIR-PCSI is bounded in the following theorem.

Theorem 11: The redundancy of the CSI to achieve the supremum capacity of PIR-PCSI is bounded as

$$\begin{aligned} &\rho_{\text{PCSI}} = \frac{1}{2}, && M = 2 \\ &\rho_{\text{PCSI}} \le \frac{1}{M}, && 3 \le M \le \frac{K+2}{2}, \\ &\rho_{\text{PCSI}} = 0, && \text{otherwise.} \end{aligned} \tag{37}$$

The proof of Theorem 11 appears in Section XIV. Evidently, for different values of M the redundancy can be as high as $1/2$ and as low as 0.

The infimum capacity of PIR-PCSI is found next.

Theorem 12: The infimum capacity of PIR-PCSI corresponds to $q = 2$, and,

$$C^{\inf}_{\text{PCSI}} = C_{\text{PCSI}}(q=2) = \frac{1}{K-1}. \tag{38}$$

The proof of Theorem 12 appears in Section XV.

Note that for $M = 1$, the infimum capacity of PIR-PCSI matches the supremum capacity, therefore for any field $\mathbb{F}_q$, we have the exact capacity characterization, $C_{\text{PCSI}}(q) = C^{\inf}_{\text{PCSI}} = C^{\sup}_{\text{PCSI}}$. However, in general the infimum capacity is strictly smaller and the gap can be significant. For example, when $M = K$ the supremum capacity is 1 while the infimum capacity is $1/(K-1)$.

Finally, the capacity of PIR-PCSI for the case of private coefficients is characterized.

Theorem 13: The capacity of PIR-PCSI, for the setting with private coefficients, is given by

$$C^{\text{pri}}_{\text{PCSI}}(q) = C^{\inf}_{\text{PCSI}}. \tag{39}$$

The proof of Theorem 13 appears in Section XVI. Similar to PIR-PCSI-II, and unlike PIR-PCSI-I, for PIR-PCSI the capacity with private coefficients does not depend on the field, and is always equal to the infimum capacity.

Let us conclude this section with Table III which summarizes the solved and open cases of various PIR-PCSI* problems considered in this work.

IV. Proof of Theorem 1

A. Converse

The following lemma, which is essentially Lemma 1 of [33], states that for PIR-PCSI*, for every feasible $(Q, \mathcal{S}, \theta)$, there must exist at least one coefficient vector that allows successful decoding.

Lemma 1:

PIR-PCSI: $\forall (Q, \mathcal{S}, \theta) \in \mathcal{Q} \times \mathfrak{S} \times [K], \quad \exists \Lambda \in \mathfrak{C}, \text{ s. t.}$

$$H(\boldsymbol{W}_\theta \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},\Lambda]}, \boldsymbol{Q} = Q) = 0. \tag{40}$$

PIR-PCSI-I: $\forall (Q, \mathcal{S}, \theta) \in \mathcal{Q} \times \mathfrak{S} \times ([K] \setminus \mathcal{S}), \quad \exists \Lambda \in \mathfrak{C}, \text{ s. t.}$

$$H(\boldsymbol{W}_\theta \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},\Lambda]}, \boldsymbol{Q} = Q) = 0. \tag{41}$$

PIR-PCSI-II: $\forall (Q, \mathcal{S}, \theta) \in \mathcal{Q} \times \mathfrak{S} \times \mathcal{S}, \quad \exists \Lambda \in \mathfrak{C}, \text{ s. t.}$

$$H(\boldsymbol{W}_\theta \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},\Lambda]}, \boldsymbol{Q} = Q) = 0. \tag{42}$$

TABLE III
A SUMMARY OF SOLVED AND OPEN PROBLEMS FOR PIR-PCSI*

	PIR-PCSI-I	PIR-PCSI-II	PIR-PCSI
Supremum Capacity	Solved	Solved	Solved
Infimum Capacity	Solved	Solved	Solved
Field-dependent Capacity	Only solved for $M = K - 1$	Only solved for $M = K$ and $M = 3, K = 4$	Open
Capacity with private coeff.	Open for infimum capacity and arbitrary q	Solved	Solved
Redundancy in CSI	Solved	Solved	Open for $3 \leq M \leq \frac{K+2}{2}$

Proof: Since the server knows $\boldsymbol{\Delta}, \boldsymbol{Q}$ and can test all possible realizations of $\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}$ for decodability, if no coefficient vector exists for a particular $(\boldsymbol{\theta} = \theta, \boldsymbol{\mathcal{S}} = \mathcal{S})$ then that $(\theta, \mathcal{S})$ can be ruled out by the server. This contradicts the privacy constraint. □

Let us prove the converse for $2 \leq M \leq \frac{K+1}{2}$.

Consider any particular realization $Q \in \mathcal{Q}$ of $\boldsymbol{Q}$. For all $i \in [M-1]$, consider $\mathcal{S}_i = [i : i + M - 1]$ and $\theta = i$, and let Λ_i be a coefficient vector that satisfies (42) according to Lemma 1, so that

$$H(\boldsymbol{W}_i \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S}_i, \Lambda_i]}, \boldsymbol{Q} = Q) = 0. \tag{43}$$

Writing $\boldsymbol{Y}^{[\mathcal{S}_i, \Lambda_i]}$ as $\boldsymbol{Y}_i$ for compact notation, we have

$$\begin{aligned}
&H(\boldsymbol{W}_{[M-1]}, \boldsymbol{Y}_{[M-1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (44)\\
&\leq \sum_{i \in [M-1]} H(\boldsymbol{W}_i, \boldsymbol{Y}_i \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (45)\\
&= \sum_{i \in [M-1]} H(\boldsymbol{Y}_i \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q)\\
&\quad + \sum_{i \in [M-1]} H(\boldsymbol{W}_i \mid \boldsymbol{\Delta}, \boldsymbol{Y}_i, \boldsymbol{Q} = Q) && (46)\\
&= \sum_{i \in [M-1]} H(\boldsymbol{Y}_i \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (47)\\
&\leq (M-1)L && (48)
\end{aligned}$$

where (45) results from chain rule and the property that conditioning reduces entropy. Step (46) is simply the chain rule of entropy. (47) is implied by (43), and (48) is true since $\forall i \in [M-1], \boldsymbol{Y}_i \in \mathbb{F}_q$.

Next we note[3] that $\boldsymbol{W}_{[2M-2]}$ can be obtained from $(\boldsymbol{W}_{[M-1]}, \boldsymbol{Y}_{[M-1]})$, as follows: $\boldsymbol{W}_M$ is obtained by subtracting $\boldsymbol{W}_{[M-1]}$ terms from $\boldsymbol{Y}_1$ which is a linear combination of $\boldsymbol{W}_{[M]}$; $\boldsymbol{W}_{M+1}$ by subtracting $\boldsymbol{W}_{[2:M]}$ terms from $\boldsymbol{Y}_2$ which is a linear combination of $\boldsymbol{W}_{[2:M+1]}$; $\cdots$; and finally $\boldsymbol{W}_{2M-2}$ by subtracting $\boldsymbol{W}_{[M-1:2M-3]}$ terms from $\boldsymbol{Y}_{M-1}$ which is a linear combination of $\boldsymbol{W}_{[M-1:2M-2]}$. Thus,

$$\begin{aligned}
&H(\boldsymbol{W}_{[2M-2]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (49)\\
&\leq H(\boldsymbol{W}_{[M-1]}, \boldsymbol{Y}_{[M-1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (50)\\
&\overset{(48)}{\leq} (M-1)L, \qquad \forall Q \in \mathcal{Q}. && (51)
\end{aligned}$$

Averaging over $\boldsymbol{Q}$, we have

$$H(\boldsymbol{W}_{[2M-2]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \leq (M-1)L. \tag{52}$$

We can follow the same argument for any $2M-2$ out of the K messages, thus (52) must be true for any $2M-2$ of K messages. Thus, by submodularity,

$$\begin{aligned}
H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) &\leq \frac{K(M-1)}{2M-2} L\\
&= \frac{K}{2} L. && (53)
\end{aligned}$$

Next we have,

$$\begin{aligned}
&H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q})\\
&= H(\boldsymbol{W}_{[K]}, \boldsymbol{\Delta} \mid \boldsymbol{Q}) - H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) && (54)\\
&= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) + H(\boldsymbol{\Delta} \mid \boldsymbol{W}_{[K]}, \boldsymbol{Q}) - H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) && (55)\\
&= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) - H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) && (56)\\
&= H(\boldsymbol{W}_{[K]}) - H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) && (57)\\
&= KL - H(\boldsymbol{\Delta} \mid \boldsymbol{Q}), && (58)
\end{aligned}$$

where the first two steps apply the chain rule of entropy, (56) results from the fact that $\boldsymbol{\Delta}$ is a function of the messages and query, and (57) follows from the independence of messages and queries as specified in (5). Thus, we have

$$\begin{aligned}
D &\geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q})\\
&\overset{(58)}{=} KL - H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) && (59)\\
&\overset{(53)}{\geq} \frac{K}{2} L. && (60)
\end{aligned}$$

Thus, the rate achieved must be bounded as $R = L/D \leq 2/K$. Since this is true for every achievable scheme, $C_{\text{PCSI-II}}(q) \leq 2/K$ for $2 \leq M \leq \frac{K+1}{2}$. The remaining case, $C_{\text{PCSI-II}}(q) \leq (K-M+1)^{-1}$ for $\frac{K+1}{2} < M \leq K$ is already shown in [33].

B. Achievability

We present an interference alignment based scheme that works for arbitrary $2 \leq M \leq K$ and is capacity achieving for $2 \leq M \leq \frac{K+1}{2}$. The capacity-achieving scheme for the remaining case is already shown in [33]. The scheme requires that q should be an even power of a prime number, so that $\mathbb{F}_{\sqrt{q}}$ is also a finite field. Recall that according to polynomial representations of finite fields, $\mathbb{F}_q = \mathbb{F}_{\sqrt{q}}[x]/g(x)$ for some degree 2 irreducible polynomial $g(x) = x^2 + a_1 x + a_0 \in \mathbb{F}_{\sqrt{q}}[x]$, and $\mathbb{F}_q$ can be repesented as $\mathbb{F}_q = \{\mu x + \gamma \mid \forall \mu, \gamma \in \mathbb{F}_{\sqrt{q}}\}$. Alternatively, $\mathbb{F}_q$ can be seen as a 2 dimensional vector space over $\mathbb{F}_{\sqrt{q}}$. Any element $c = \mu_c x + \gamma_c \in \mathbb{F}_q$, where $\mu_c, \gamma_c \in \mathbb{F}_{\sqrt{q}}$, has a corresponding 2×1 vector representation $V_c \in \mathbb{F}_{\sqrt{q}}^{2\times 1}$ and a 2×2 matrix representation $M_c \in \mathbb{F}_{\sqrt{q}}^{2\times 2}$ as follows (see p. 65 of [35]).

$$V_c = \begin{bmatrix} \gamma_c \\ \mu_c \end{bmatrix}, \qquad M_c = \begin{bmatrix} \gamma_c & -\mu_c a_0 \\ \mu_c & \gamma_c - \mu_c a_1 \end{bmatrix} \tag{61}$$

such that for any $a, b, c \in \mathbb{F}_q$ we have $a = bc$, if and only if

$$V_a = M_b V_c. \tag{62}$$

[3] $2M - 2 \leq K$ since we consider the case where $2 \leq M \leq \frac{K+1}{2}$.

Let us start with the following lemma.

Lemma 2: If $\boldsymbol{c}$ is chosen uniformly randomly over $\mathbb{F}_q^\times$, then each row of $M_{\boldsymbol{c}}$ is uniformly distributed over $\mathbb{F}_{\sqrt{q}}^{1\times 2}\setminus\{[0,0]\}$.

Proof: Since a_0, a_1 are given constants, the second row, $M_{\boldsymbol{c}}(2,:)=[\mu_{\boldsymbol{c}}, \gamma_{\boldsymbol{c}}-\mu_{\boldsymbol{c}}a_1]$ is an invertible function of $V_{\boldsymbol{c}}$. Next, note that $a_0\neq 0$ because otherwise $g(x)=x(x+a_1)$ would not be irreducible. Therefore, the first row, $M_{\boldsymbol{c}}(1,:)=[\gamma_{\boldsymbol{c}}, -\mu_{\boldsymbol{c}}a_0]$ is also an invertible function of $V_{\boldsymbol{c}}$. Finally, since $\boldsymbol{c}$ is uniform over $\mathbb{F}_q^\times$, it follows that $V_{\boldsymbol{c}}$ is uniform over $\mathbb{F}_{\sqrt{q}}^{1\times 2}\setminus\{[0,0]\}$, and as an invertible function of $V_{\boldsymbol{c}}$ that maps non-zero vectors to non-zero vectors, so is each row of $M_{\boldsymbol{c}}$. □

The scheme proposed in this section needs only $L=1$, so let us say $L=1$. Recall that the coded side information (CSI) $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} \triangleq \boldsymbol{\lambda}_1\boldsymbol{W}_{\boldsymbol{i}_1}+\cdots+\boldsymbol{\lambda}_M\boldsymbol{W}_{\boldsymbol{i}_M}$ where $\boldsymbol{\mathcal{S}}=\{\boldsymbol{i}_1,\cdots,\boldsymbol{i}_M\}$ and $\boldsymbol{i}_1<\boldsymbol{i}_2<\cdots<\boldsymbol{i}_M$.

Since $L=1$, each message is a symbol in $\mathbb{F}_q$. Thus each message $\boldsymbol{W}_k, k\in[K]$ has vector representation $V_{\boldsymbol{W}_k}\in\mathbb{F}_{\sqrt{q}}^{2\times 1}$. The first and second entry of $V_{\boldsymbol{W}_k}$, namely $V_{\boldsymbol{W}_k}(1)$ and $V_{\boldsymbol{W}_k}(2)$ respectively, are both elements in $\mathbb{F}_{\sqrt{q}}$ and $\boldsymbol{W}_k=V_{\boldsymbol{W}_k}(2)x+V_{\boldsymbol{W}_k}(1)$.

Each coefficient $\boldsymbol{\lambda}_m, m\in[M]$ is drawn from $\mathbb{F}_q^\times$, and can be represented as $M_{\boldsymbol{\lambda}_m}\in\mathbb{F}_{\sqrt{q}}^{2\times 2}$ such that $M_{\boldsymbol{\lambda}_m}V_{\boldsymbol{W}_{\boldsymbol{i}_m}}\in\mathbb{F}_{\sqrt{q}}^{2\times 1}$ is the vector representation of $\boldsymbol{\lambda}_m\boldsymbol{W}_{\boldsymbol{i}_m}\in\mathbb{F}_q$.

Thus,

$$V_{\boldsymbol{Y}}=M_{\boldsymbol{\lambda}_1}V_{\boldsymbol{W}_{\boldsymbol{i}_1}}+\cdots+M_{\boldsymbol{\lambda}_M}V_{\boldsymbol{W}_{\boldsymbol{i}_M}}\in\mathbb{F}_{\sqrt{q}}^{2\times 1}, \tag{63}$$

is the vector representation of $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}\in\mathbb{F}_q$.

Let $M_{\boldsymbol{\lambda}_m}(1,:), M_{\boldsymbol{\lambda}_m}(2,:)$ denote the first and second row of $M_{\boldsymbol{\lambda}_m}$ respectively, and $M_{\boldsymbol{\lambda}_m}(r,:)V_{\boldsymbol{W}_{\boldsymbol{i}_m}}$ the dot product of the r^{th} row of $M_{\boldsymbol{\lambda}_m}$ with $V_{\boldsymbol{W}_{\boldsymbol{i}_m}}$. Then the first and second entry of $V_{\boldsymbol{Y}}$ are

$$V_{\boldsymbol{Y}}(1)=M_{\boldsymbol{\lambda}_1}(1,:)V_{\boldsymbol{W}_{\boldsymbol{i}_1}}+\cdots+M_{\boldsymbol{\lambda}_M}(1,:)V_{\boldsymbol{W}_{\boldsymbol{i}_M}}, \tag{64}$$

$$V_{\boldsymbol{Y}}(2)=M_{\boldsymbol{\lambda}_1}(2,:)V_{\boldsymbol{W}_{\boldsymbol{i}_1}}+\cdots+M_{\boldsymbol{\lambda}_M}(2,:)V_{\boldsymbol{W}_{\boldsymbol{i}_M}}, \tag{65}$$

respectively.

To privately retrieve $\boldsymbol{W}_{\boldsymbol{\theta}}$ for some $\boldsymbol{\theta}\in\boldsymbol{\mathcal{S}}$, the user's download $\boldsymbol{\Delta}$ is

$$\boldsymbol{\Delta}=(\mathbf{L}_kV_{\boldsymbol{W}_k})_{k\in[K]}, \tag{66}$$

where $\mathbf{L}_{\boldsymbol{i}_m}=M_{\boldsymbol{\lambda}_m}(1,:)$ for $\boldsymbol{i}_m\in\boldsymbol{\mathcal{S}}\setminus\{\boldsymbol{\theta}\}$, and $\mathbf{L}_{\boldsymbol{i}_m}=M_{\boldsymbol{\lambda}_m}(2,:)$ for $\boldsymbol{i}_m=\boldsymbol{\theta}$. For $k\in[K]\setminus\boldsymbol{\mathcal{S}}$, $\mathbf{L}_k$ is uniformly drawn from $\mathbb{F}_{\sqrt{q}}^{1\times 2}\setminus\{[0\ \ 0]\}$.

Upon receiving $\boldsymbol{\Delta}$, by subtracting the $\{M_{\boldsymbol{\lambda}_m}(1,:)V_{\boldsymbol{W}_{\boldsymbol{i}_m}}\}_{\boldsymbol{i}_m\in\boldsymbol{\mathcal{S}}\setminus\{\boldsymbol{\theta}\}}$ terms from $V_{\boldsymbol{Y}}(1)$, the user is able to obtain $M_{\boldsymbol{\lambda}_t}(1,:)V_{\boldsymbol{W}_{\boldsymbol{\theta}}}$, where $\boldsymbol{i}_t=\boldsymbol{\theta}$. Together with $M_{\boldsymbol{\lambda}_t}(2,:)V_{\boldsymbol{W}_{\boldsymbol{\theta}}}$, which is directly downloaded, the user is able to recover $M_{\boldsymbol{\lambda}_t}V_{\boldsymbol{W}_{\boldsymbol{\theta}}}$, i.e., $\boldsymbol{\lambda}_t\boldsymbol{W}_{\boldsymbol{\theta}}$, and since $\boldsymbol{\lambda}_t$ is a non-zero value in $\mathbb{F}_q$ that is known to the user, the user is able to retrieve the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$.

Since $\boldsymbol{\lambda}_{[M]}$ are i.i.d. uniform over $\mathbb{F}_q^\times$, it follows from Lemma 2 that all $\mathbf{L}_k, k\in[K]$ are i.i.d. uniform over $\mathbb{F}_{\sqrt{q}}^{1\times 2}\setminus\{[0\ \ 0]\}$. Thus, the queries are independent of $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}})$, and the privacy constraint is satisfied.

Remark 3: The scheme is also capacity achieving for the boundary case $\frac{K+1}{2}<M\leq\frac{K+2}{2}$ (i.e., $2M=K+2$) because in this case, $2/K=(K-M+1)^{-1}$.

Remark 4: The scheme only uses $V_{\boldsymbol{Y}}(1)$ specified in (63), i.e., $V_{\boldsymbol{Y}}(2)$ is never used so it can be discarded by the user. Thus, at least half of the side-information is redundant.

Let us consider an example for illustration.

Example 1: Suppose $q=4$, $L=1$. There are $K=3$ messages $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in\mathbb{F}_4$. We have $M=2$. Say the CSI is the linear combination $\boldsymbol{Y}=\boldsymbol{\lambda}_1\boldsymbol{A}+\boldsymbol{\lambda}_2\boldsymbol{B}$, with $\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2$ i.i.d. uniform in $\mathbb{F}_4^\times$, and the desired message is $\boldsymbol{A}$.

We note that $\mathbb{F}_4=\mathbb{F}_2[x]/(x^2+x+1)$ has the 4 elements: $0,1,x,1+x$, which have matrix representations:

$$M_0=\begin{bmatrix}0&0\\0&0\end{bmatrix}, M_1=\begin{bmatrix}1&0\\0&1\end{bmatrix}, M_x=\begin{bmatrix}0&1\\1&1\end{bmatrix}, M_{1+x}=\begin{bmatrix}1&1\\1&0\end{bmatrix}.$$

Note that if $\mathbf{c}$ is uniform over $\mathbb{F}_4^\times=\{1,x,1+x\}$ then the first row of M_c, i.e., $M_{\boldsymbol{c}}(1,:)$ is uniform over $\{[1\ \ 0],[0\ \ 1],[1\ \ 1]\}=\mathbb{F}_2^{1\times 2}\setminus\{[0\ \ 0]\}$, and so is the second row, $M_{\boldsymbol{c}}(2,:)$, as claimed by Lemma 2. Define $\boldsymbol{A}=\boldsymbol{A}_1+\boldsymbol{A}_2x$, where $\boldsymbol{A}_1,\boldsymbol{A}_2\in\mathbb{F}_2$, so that $V_{\boldsymbol{A}}=[\boldsymbol{A}_1\ \ \boldsymbol{A}_2]^T$, and use similar definitions for $\boldsymbol{B},\boldsymbol{C}$ as well.

Let $\boldsymbol{\lambda}_1\boldsymbol{A}=\boldsymbol{A}'=\boldsymbol{A}'_1+\boldsymbol{A}'_2x$. The vector representation of it can thus be written as $V_{\boldsymbol{A}'}=M_{\boldsymbol{\lambda}_1}V_{\boldsymbol{A}}=[\boldsymbol{A}'_1\ \ \boldsymbol{A}'_2]^{\mathrm{T}}$. Note that $\boldsymbol{A}'_1=M_{\boldsymbol{\lambda}_1}(1,:)[\boldsymbol{A}_1\ \ \boldsymbol{A}_2]^{\mathrm{T}}$ and $M_{\boldsymbol{\lambda}_1}(1,:)$ is uniform over $\{[1\ \ 0],[0\ \ 1],[1\ \ 1]\}$, thus $\boldsymbol{A}'_1$ is uniform over $\{\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_1+\boldsymbol{A}_2\}$. $\boldsymbol{A}'_2$ is uniform over the same set because $M_{\boldsymbol{\lambda}_1}(1,:)$ and $M_{\boldsymbol{\lambda}_1}(2,:)$ have the same distribution. Similarly, let $\boldsymbol{\lambda}_2\boldsymbol{B}=\boldsymbol{B}'_1+\boldsymbol{B}'_2x$, and note that $\boldsymbol{B}'_1,\boldsymbol{B}'_2$ are individually uniform over $\{\boldsymbol{B}_1,\boldsymbol{B}_2,\boldsymbol{B}_1+\boldsymbol{B}_2\}$. Then the side information can be denoted as $\boldsymbol{Y}=(\boldsymbol{A}'_1+\boldsymbol{B}'_1)+(\boldsymbol{A}'_2+\boldsymbol{B}'_2)x$. According to our scheme, $\boldsymbol{B}'_1=M_{\boldsymbol{\lambda}_2}(1,:)V_{\boldsymbol{B}}$ is downloaded which enables the user to retrieve $\boldsymbol{A}'_1$ by subtracting it from the first dimension of $\boldsymbol{Y}$. The $\boldsymbol{A}'_2=M_{\boldsymbol{\lambda}_1}(2,:)V_{\boldsymbol{A}}$ is also downloaded. $\boldsymbol{A}'_1,\boldsymbol{A}'_2$ together enable the user to get $\boldsymbol{A}'$ and thus $\boldsymbol{A}$. Note that in our scheme, a non-zero random linear combination of $\boldsymbol{C}_1,\boldsymbol{C}_2$ is also downloaded. Thus, the download, made up of $\boldsymbol{A}'_2,\boldsymbol{B}'_1$ and a linear combination of $\boldsymbol{C}_1,\boldsymbol{C}_2$ is uniform over $\{\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_1+\boldsymbol{A}_2\}\times\{\boldsymbol{B}_1,\boldsymbol{B}_2,\boldsymbol{B}_1+\boldsymbol{B}_2\}\times\{\boldsymbol{C}_1,\boldsymbol{C}_2,\boldsymbol{C}_1+\boldsymbol{C}_2\}$. For any other realization of $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}})$, a similar argument applies. Thus, the download is always uniform over the same set, regardless of the realization of $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}})$, which guarantees privacy.

For example, let us say $\boldsymbol{\lambda}_1=1+x, \boldsymbol{\lambda}_2=x$, then $V_{\boldsymbol{Y}}(1)=\boldsymbol{A}_1+\boldsymbol{A}_2+\boldsymbol{B}_2$. The user downloads, say $\boldsymbol{\Delta}=(\boldsymbol{A}_1,\boldsymbol{B}_2,\boldsymbol{C}_1+\boldsymbol{C}_2)$ which allows $\boldsymbol{A}$ to be retrieved with the help of the side information $V_{\boldsymbol{Y}}(1)$. However, from the server's perspective, the following possibilities are equally likely, as the download $\boldsymbol{\Delta}=(\boldsymbol{A}_1,\boldsymbol{B}_2,\boldsymbol{C}_1+\boldsymbol{C}_2)$ enables the user to decode the desired message under all conditions.

Support Set	CSI	Desired
$\{\boldsymbol{A},\boldsymbol{B}\}$	$(1+x)\boldsymbol{A}+x\boldsymbol{B}$	$\boldsymbol{A}$
$\{\boldsymbol{A},\boldsymbol{B}\}$	$\boldsymbol{A}+\boldsymbol{B}$	$\boldsymbol{B}$
$\{\boldsymbol{B},\boldsymbol{C}\}$	$\boldsymbol{B}+(1+x)\boldsymbol{C}$	$\boldsymbol{B}$
$\{\boldsymbol{B},\boldsymbol{C}\}$	$x\boldsymbol{B}+x\boldsymbol{C}$	$\boldsymbol{C}$
$\{\boldsymbol{A},\boldsymbol{C}\}$	$(1+x)\boldsymbol{A}+(1+x)\boldsymbol{C}$	$\boldsymbol{A}$
$\{\boldsymbol{A},\boldsymbol{C}\}$	$\boldsymbol{A}+x\boldsymbol{C}$	$\boldsymbol{C}$

(67)

V. Proof of Theorem 2

We need Lemma 3 and 4 to bound the redundancy $\rho_{\text{PCSI-II}}$ from above, (equivalently, lower-bound α^*) for $2 \le M \le \frac{K+2}{2}$ and $\frac{K+2}{2} < M \le K$, respectively.

Lemma 3: For $2 \le M \le \frac{K+2}{2}$, the redundancy $\rho_{\text{PCSI-II}} \le 1/2$.

Intuitively, the entropy of the download is $H(\boldsymbol{\Delta}) = \frac{K}{2}L$. On average, at most $L/2$ symbols of each message are contained in the download. In order to fully recover the desired message, the user must have at least another $L/2$ q-ary symbols as the side information.

Proof: Recall that the capacity for this case is $2/K$, i.e., the optimal average download cost is $D/L = K/2$. Since this is the infimum across all achievable schemes, there must exist achievable schemes that achieve $D/L \le K/2 + \epsilon$ for any $\epsilon > 0$. So consider an achievable scheme such that α-CSI is sufficient and the average download cost $D/L \le K/2 + \epsilon$ for some L. Since $D/L \le K/2 + \epsilon$, we have

$$
\begin{aligned}
&LK/2 + \epsilon L \\
&\ge D && (68)\\
&\ge H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) && (69)\\
&\ge I(\boldsymbol{\Delta}; \boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) && (70)\\
&= \sum_{k\in[K]} I(\boldsymbol{\Delta}; \boldsymbol{W}_k \mid \boldsymbol{Q}, \boldsymbol{W}_{[k-1]}) && (71)\\
&= \sum_{k\in[K]} \Big(H(\boldsymbol{W}_k \mid \boldsymbol{Q}, \boldsymbol{W}_{[k-1]}) - H(\boldsymbol{W}_k \mid \boldsymbol{\Delta}, \boldsymbol{Q}, \boldsymbol{W}_{[k-1]}) \Big) && (72)\\
&= \sum_{k\in[K]} \Big(H(\boldsymbol{W}_k) - H(\boldsymbol{W}_k \mid \boldsymbol{\Delta}, \boldsymbol{Q}, \boldsymbol{W}_{[k-1]}) \Big) && (73)\\
&\ge \sum_{k\in[K]} \Big(H(\boldsymbol{W}_k) - H(\boldsymbol{W}_k \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \Big) && (74)\\
&= \sum_{k\in[K]} I(\boldsymbol{W}_k; \boldsymbol{\Delta}, \boldsymbol{Q}), && (75)\\
&\ge K I(\boldsymbol{W}_{k^*}; \boldsymbol{\Delta}, \boldsymbol{Q}) && (76)
\end{aligned}
$$

where (70) follows from the non-negativity of entropy, (71) follows from the chain rule of mutual information, (73) holds since all the messages and the query are mutually independent, (74) results from conditioning reduces entropy and (76) is true by setting

$$k^* = \arg\min_{k\in[K]} I(\boldsymbol{W}_k; \boldsymbol{\Delta}, \boldsymbol{Q}) \tag{77}$$

From (76) we have,

$$
\begin{aligned}
&H(\boldsymbol{W}_{k^*} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) && (78)\\
&= H(\boldsymbol{W}_{k^*}) - I(\boldsymbol{W}_{k^*}; \boldsymbol{\Delta}, \boldsymbol{Q}) && (79)\\
&\ge L - (L/2 + \epsilon L/K) && (80)\\
&= L/2 - \epsilon L/K. && (81)
\end{aligned}
$$

Thus, there must exist a feasible query Q such that

$$H(\boldsymbol{W}_{k^*} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) \ge L/2 - \epsilon L/K. \tag{82}$$

Let $\mathcal{S} = \{i_1, \cdots, i_{M-1}, k^*\} \subset [K]$, such that $|\mathcal{S}| = M$. Then according to Lemma 1 and (25), there must exist $\Lambda \in \mathfrak{C}$ such that

$$
\begin{aligned}
&H(\boldsymbol{W}_{k^*} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}, \boldsymbol{Q} = Q) = 0, && (83)\\
&H(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]} \mid \boldsymbol{Q} = Q) = H(\overline{\boldsymbol{Y}}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}) \le \alpha L. && (84)
\end{aligned}
$$

Combining (82) and (83), we have

$$I(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}; \boldsymbol{W}_{k^*} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) \ge L/2 - \epsilon L/K. \tag{85}$$

Thus

$$
\begin{aligned}
\alpha L &\ge H(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]} \mid \boldsymbol{Q} = Q)\\
&\ge I(\overline{\boldsymbol{Y}}^{[\mathcal{S},\Lambda]}; \boldsymbol{W}_{k^*} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) \ge \frac{L}{2} - \epsilon L/K && (86)
\end{aligned}
$$

which implies that $\alpha \ge 1/2 - \epsilon/K$. In order to approach capacity, we must have $\epsilon \to 0$, therefore we need $\alpha \ge 1/2$. Since this is true for any α such that α-CSI is sufficient, it is also true for α^*, and therefore the redundancy is $\rho_{\text{PCSI-II}} \le 1/2$.

Lemma 4: For $\frac{K+2}{2} < M \le K$, the redundancy $\rho_{\text{PCSI-II}} \le 0$.

Proof: Recall that the capacity for this case is $(K - M + 1)^{-1}$, i.e., the optimal average download cost is $D/L = K - M + 1$. Consider an achievable scheme such that α-CSI is sufficient and the average download cost $D/L \le K - M + 1 + \epsilon$ for some L. Since $D/L \le K - M + 1 + \epsilon$, we have $L(K - M + 1) + \epsilon L \ge D \ge H(\boldsymbol{\Delta} \mid \boldsymbol{Q})$. Thus, there exists a feasible Q such that

$$H(\boldsymbol{\Delta} \mid \boldsymbol{Q} = Q) \le (K - M + 1)L + \epsilon L. \tag{87}$$

For all $i \in [K - M + 1]$, let $\mathcal{S}_i = [i : i + M - 1]$. Also, let $\mathcal{S}_{K-M+2} = \{1\} \cup [K - M + 2 : K]$. For all $i \in [K - M + 2]$, let $\Lambda_i \in \mathfrak{C}$ satisfy

$$H(\boldsymbol{W}_i \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}^{[\mathcal{S}_i,\Lambda_i]}, \boldsymbol{Q} = Q) = 0. \tag{88}$$

Such Λ_i's must exist according to Lemma 1.

Writing $\overline{\boldsymbol{Y}}^{[\mathcal{S}_i,\Lambda_i]}$ as $\overline{\boldsymbol{Y}}_i$ for compact notation, we have

$$H(\boldsymbol{W}_{[K-M+2]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[K-M+2]}, \boldsymbol{Q} = Q) = 0. \tag{89}$$

According to (25),

$$H(\overline{\boldsymbol{Y}}_i \mid \boldsymbol{Q} = Q) \le \alpha L. \tag{90}$$

so we have

$$
\begin{aligned}
&(K - M + 1)L + \epsilon L + H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{Q} = Q) + \alpha L\\
&\ge H(\boldsymbol{\Delta} \mid \boldsymbol{Q} = Q) + H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{Q} = Q)\\
&\quad + H(\overline{\boldsymbol{Y}}_{K-M+2} \mid \boldsymbol{Q} = Q) && (91)\\
&\ge H(\boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[K-M+2]} \mid \boldsymbol{Q} = Q) && (92)\\
&\ge I(\boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[K-M+2]}; \boldsymbol{W}_{[K-M+2]}, \overline{\boldsymbol{Y}}_{[K-M+2]} \mid \boldsymbol{Q} = Q) && (93)\\
&= H(\boldsymbol{W}_{[K-M+2]}, \overline{\boldsymbol{Y}}_{[K-M+2]} \mid \boldsymbol{Q} = Q) && (94)\\
&\ge H(\boldsymbol{W}_{[K-M+2]}, \overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{Q} = Q) && (95)\\
&= H(\boldsymbol{W}_{[K-M+2]} \mid \boldsymbol{Q} = Q)\\
&\quad + H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{W}_{[K-M+2]}, \boldsymbol{Q} = Q) && (96)\\
&\ge (K - M + 2)L\\
&\quad + H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{W}_{[M-1]}, \boldsymbol{Q} = Q), && (97)
\end{aligned}
$$

where (91) follows from (87) and (90). (93) results from the non-negativity of entropy. (94) follows from (89). (96) is true according to the chain rule. Step (97) uses the independence of messages and queries according to (5), and the fact that $M-1 \geq K-M+2$, because we require $M > (K+2)/2$. We further bound

$$\begin{aligned} &H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{W}_{[M-1]}, \boldsymbol{Q}=Q) \\ &= H(\overline{\boldsymbol{Y}}_1 \mid \boldsymbol{W}_{[M-1]}, \boldsymbol{Q}=Q) + \cdots \\ &\quad + H(\overline{\boldsymbol{Y}}_{K-M+1} \mid \boldsymbol{W}_{[M-1]}, \overline{\boldsymbol{Y}}_{[K-M]}, \boldsymbol{Q}=Q) \quad (98) \\ &\geq \sum_{i=1}^{K-M+1} H(\overline{\boldsymbol{Y}}_i \mid \boldsymbol{W}_{[i+M-2]}, \boldsymbol{Q}=Q) \quad (99) \\ &= \sum_{i=1}^{K-M+1} H(\overline{\boldsymbol{Y}}_i \mid \boldsymbol{Q}=Q) \quad (100) \\ &\geq H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{Q}=Q) \quad (101) \end{aligned}$$

(98) follows from the chain rule. (99) holds because $\overline{\boldsymbol{Y}}_{[i-1]}$ is a function of $\boldsymbol{W}_{[i+M-2]}$ for all $i \in [2 : K-M+1]$. Step (100) follows from (25). Substituting from (101) into (97), and subtracting $H(\overline{\boldsymbol{Y}}_{[K-M+1]} \mid \boldsymbol{Q}=Q)$ from both sides, we have

$$(K-M+1)L + \epsilon L + \alpha L \geq (K-M+2)L, \quad (102)$$

which gives $\alpha \geq 1-\epsilon$. In order to approach capacity, we must have $\epsilon \to 0$, so we need $\alpha \geq 1$, and since this is true for any α such that α-CSI is sufficient, it is also true for α^*. Thus, the redundancy is bounded as $\rho_{\text{PCSI-II}} \leq 0$. □

According to Remark 3 and 4, $\alpha = 1/2$ is sufficient for $2 \leq M \leq \frac{K+2}{2}$ and by the construction of CSI (a linear combination of messages), $\alpha \leq 1$. Theorem 2 is thus proved.

VI. Proof of Theorem 3

We prove Theorem 3 by first showing that $C_{\text{PCSI-II}}(q=2) \leq M/((M-1)K)$ and then presenting a PIR-PCSI-II scheme with rate $M/((M-1)K)$ that works for any $\mathbb{F}_q$.

A. Converse for $C_{\text{PCSI-II}}(q=2)$

Note that Lemma 1 is true for arbitrary $\mathbb{F}_q$. In $\mathbb{F}_2$, we can only have $\boldsymbol{\Lambda} = (1,1,\cdots,1) = 1_M$, i.e., the length M vector whose elements are all equal to 1. As a direct result of Lemma 1, for PIR-PCSI-II in $\mathbb{F}_2$,

$$H(\boldsymbol{W}_{\mathcal{S}} \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},1_M]}, \boldsymbol{Q}=Q) = 0, \ \forall (Q,\mathcal{S}) \in \mathcal{Q} \times \mathfrak{S}. \quad (103)$$

Thus, $\forall (Q,\mathcal{S}) \in \mathcal{Q} \times \mathfrak{S}$,

$$\begin{aligned} &H(\boldsymbol{W}_{\mathcal{S}} \mid \boldsymbol{\Delta}, \boldsymbol{Q}=Q) \\ &= H(\boldsymbol{W}_{\mathcal{S}}, \boldsymbol{Y}^{[\mathcal{S},1_M]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}=Q) \quad (104) \\ &= H(\boldsymbol{Y}^{[\mathcal{S},1_M]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}=Q) \\ &\quad + H(\boldsymbol{W}_{\mathcal{S}} \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},1_M]}, \boldsymbol{Q}=Q) \quad (105) \\ &\leq L. \quad (106) \end{aligned}$$

(104) holds because $\boldsymbol{Y}^{[\mathcal{S},1_M]}$ is simply the summation of $\boldsymbol{W}_{\mathcal{S}}$. (106) follows from (103). Averaging over $\boldsymbol{Q}$, we have $H(\boldsymbol{W}_{\mathcal{S}} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \leq L, \forall \mathcal{S} \in \mathfrak{S}$. By submodularity,

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \leq KL/M. \quad (107)$$

The download cost can now be lower bounded as,

$$D \geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) \geq KL - H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q})) \geq \frac{(M-1)KL}{M}. \quad (108)$$

Thus, we have shown that $C_{\text{PCSI-II}}(q=2) \leq \frac{M}{(M-1)K}$.

B. A PIR-PCSI-II Scheme for Arbitrary q

In this section, we prove $C_{\text{PCSI-II}}(q) \geq \frac{M}{(M-1)K}$ for all q by proposing a scheme, namely *Generic Linear Combination Based Scheme*, that can achieve the rate $\frac{M}{(M-1)K}$ for any $\mathbb{F}_q$.

Let us choose $L = Ml$ where M is the size of the support index set and l is a positive integer which can be arbitrarily large. Thus, any message $\boldsymbol{W}_k, k \in [K]$ can be represented as a length-M column vector $V_{\boldsymbol{W}_k} \in \mathbb{F}_{q^l}^{M \times 1}$. Let

$$V_{\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}} = \begin{bmatrix} V_{\boldsymbol{W}_{\boldsymbol{i}_1}}^{\mathrm{T}} & \cdots & V_{\boldsymbol{W}_{\boldsymbol{i}_M}}^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}} \in \mathbb{F}_{q^l}^{M^2 \times 1} \quad (109)$$

where $\boldsymbol{\mathcal{S}} = \{\boldsymbol{i}_1, \cdots, \boldsymbol{i}_M\}$ is the support index set. The CSI $\boldsymbol{Y}$ can be represented as $V_{\boldsymbol{Y}} \in \mathbb{F}_{q^l}^{M \times 1}$ such that,

$$V_{\boldsymbol{Y}} = \underbrace{\begin{bmatrix} \boldsymbol{\lambda}_1 \mathbf{I}_M & \boldsymbol{\lambda}_2 \mathbf{I}_M & \cdots & \boldsymbol{\lambda}_M \mathbf{I}_M \end{bmatrix}}_{M} V_{\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}}, \quad (110)$$

where $\mathbf{I}_M \in \mathbb{F}_{q^l}^{M \times M}$ is the $M \times M$ identity matrix.

The download is specified as,

$$\begin{aligned} \boldsymbol{\Delta} = \{&\mathbf{L}_1^{(1)} V_{\boldsymbol{W}_1}, \cdots, \mathbf{L}_1^{(M-1)} V_{\boldsymbol{W}_1}, \\ &\cdots, \mathbf{L}_K^{(1)} V_{\boldsymbol{W}_K}, \cdots, \mathbf{L}_K^{(M-1)} V_{\boldsymbol{W}_K}\}, \end{aligned} \quad (111)$$

where $\forall k \in [K], m \in [M-1], \mathbf{L}_k^{(m)} \in \mathbb{F}_{q^l}^{1 \times M}$ is a length-M row vector, i.e., for any message vector $V_{\boldsymbol{W}_k} \in \mathbb{F}_{q^l}^{M \times 1}$, $\boldsymbol{\Delta}$ contains $M-1$ linear combinations of that message vector.

Suppose the vectors $\mathbf{L}_k^{(m)}$ are chosen such that $\forall \mathcal{S} = \{j_1, \cdots, j_M\} \in \mathfrak{S}$ the following $M^2 \times M^2$ square matrix has full rank.

$$\mathbf{G}_{\mathcal{S}} = \begin{bmatrix} \lambda_1 \mathbf{I}_M & \cdots & \lambda_M \mathbf{I}_M \\ & \mathbf{e}_1 \otimes \mathbf{L}_{j_1}^{(1)} & \\ & \cdots & \\ & \mathbf{e}_1 \otimes \mathbf{L}_{j_1}^{(M-1)} & \\ & \cdots & \\ & \mathbf{e}_M \otimes \mathbf{L}_{j_M}^{(1)} & \\ & \cdots & \\ & \mathbf{e}_M \otimes \mathbf{L}_{j_M}^{(M-1)} & \end{bmatrix}, \quad (112)$$

$\mathcal{S} = \{j_1, \cdots, j_M\} \in \mathfrak{S}$. Note that $(\lambda_1, \cdots, \lambda_M) \in \mathfrak{C}$ is the realization of $\boldsymbol{\Lambda}$, $\mathbf{e}_m, m \in [M]$ is the m^{th} row of the $M \times M$ identity matrix and "$\otimes$" is the Kronecker product.

The correctness constraint is satisfied because the side-information and the downloads allow the user to obtain $\mathbf{G}_{\boldsymbol{\mathcal{S}}} V_{\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}}$, which can then be multiplied by the inverse of $\mathbf{G}_{\boldsymbol{\mathcal{S}}}$ to obtain $V_{\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}}$, i.e., $\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}$ which contains $\boldsymbol{W}_{\boldsymbol{\theta}}$. Specifically the side-information corresponds to the first M rows of $\mathbf{G}_{\boldsymbol{\mathcal{S}}} V_{\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}}$, the downloads $\mathbf{L}_{j_1}^{(1)} V_{\boldsymbol{W}_{j_1}}, \cdots, \mathbf{L}_{j_1}^{(M-1)} V_{\boldsymbol{W}_{j_1}}$ correspond to the next $M-1$ rows of $\mathbf{G}_{\boldsymbol{\mathcal{S}}} V_{\boldsymbol{W}_{\boldsymbol{\mathcal{S}}}}$, and so on.

On the other hand, the privacy constraint is satisfied because the construction is such that for every feasible $\mathcal{S}$, the user is able to decode all M messages $\boldsymbol{W}_{\mathcal{S}}$.

Finally let us evaluate the rate achieved by this scheme. Since the user downloads $\frac{M-1}{M}$ portion of every message, the download cost is $D = LK(M-1)/M$, and the rate achieved is $M/((M-1)K))$. Since this rate is achieved for any $\mathbb{F}_q$, we have the lower bound $C_{\text{PCSI-II}}(q) \geq M/((M-1)K))$.

It remains to show the existence of such $\mathbf{L}_k^{(m)}$, for which we need the following lemma.

Lemma 5: There exist $\{\mathbf{L}_k^{(m)}\}_{k\in[K],m\in[M-1]}$ such that for every $\mathcal{S} = \{j_1, \cdots, j_M\} \in \mathfrak{S}$, the matrix $\mathbf{G}_{\mathcal{S}}$ in (112) has full rank, provided

$$q^l > \tbinom{K}{M} M(M-1). \tag{113}$$

Proof: The proof is in Appendix A. □

With the help of Lemma 5, Theorem 3 is proved. Let us illustrate the scheme with an example.

Example 2: Consider $M = 2, K = 4, L = 2l, q = 2$. The 4 messages are $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$ each of which has $L = 2l$ symbols in $\mathbb{F}_2$. Let $l \geq 3$.

$\boldsymbol{A}$ can be represented as a 2×1 vector $V_{\boldsymbol{A}} = [V_{\boldsymbol{A}}(1) \quad V_{\boldsymbol{A}}(2)]^{\mathrm{T}}$ where $V_{\boldsymbol{A}}(1), V_{\boldsymbol{A}}(2) \in \mathbb{F}_{2^l}$. Similarly, $\boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$ can be represented as $V_{\boldsymbol{B}}$, $V_{\boldsymbol{C}}$, $V_{\boldsymbol{D}}$, respectively. Choose $\alpha_1, \cdots, \alpha_4$ as any elements of $\mathbb{F}_{2^l}$ such that $\alpha_1, \alpha_2, \alpha_3, \alpha_4, 1, 0$ are all distinct. This is feasible if $l \geq 3$ because $\mathbb{F}_{2^l}$ has $2^l \geq 8$ distinct elements that include $1, 0$ (the elements of $\mathbb{F}_2$). For all possible realizations of $(\boldsymbol{\mathcal{S}}, \boldsymbol{\theta})$, the download $\boldsymbol{\Delta}$ remains the same as follows.

$$\boldsymbol{\Delta} = \begin{bmatrix} \boldsymbol{\Delta}_A \\ \boldsymbol{\Delta}_B \\ \boldsymbol{\Delta}_C \\ \boldsymbol{\Delta}_D \end{bmatrix} = \begin{bmatrix} V_{\boldsymbol{A}}(1) + \alpha_1 V_{\boldsymbol{A}}(2) \\ V_{\boldsymbol{B}}(1) + \alpha_2 V_{\boldsymbol{B}}(2) \\ V_{\boldsymbol{C}}(1) + \alpha_3 V_{\boldsymbol{C}}(2) \\ V_{\boldsymbol{D}}(1) + \alpha_4 V_{\boldsymbol{D}}(2) \end{bmatrix}, \tag{114}$$

As the download is the same regardless of the realizations of $\boldsymbol{\mathcal{S}}$ and $\boldsymbol{\theta}$, the query is actually a constant which is trivially independent of $\boldsymbol{\mathcal{S}}, \boldsymbol{\theta}$ and thus the privacy is guaranteed.

What remains to be proved is the correctness of this scheme, i.e., this specific download enables the user to decode the desired message under all realizations of $\boldsymbol{\mathcal{S}}, \boldsymbol{\theta}$.

Let us consider the case where the support set is $\{\boldsymbol{A}, \boldsymbol{B}\}$, i.e., the side information is $\boldsymbol{A} + \boldsymbol{B}$, and the desired message is $\boldsymbol{A}$. The side information can be represented as $V_{\boldsymbol{Y}} \in \mathbb{F}_{2^l}^{2\times 1}$ where

$$V_{\boldsymbol{Y}} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} V_{\boldsymbol{A}}(1) \\ V_{\boldsymbol{A}}(2) \\ V_{\boldsymbol{B}}(1) \\ V_{\boldsymbol{B}}(2) \end{bmatrix} = \begin{bmatrix} V_{\boldsymbol{A}}(1) + V_{\boldsymbol{B}}(1) \\ V_{\boldsymbol{A}}(2) + V_{\boldsymbol{B}}(2) \end{bmatrix}. \tag{115}$$

$V_{\boldsymbol{Y}}$, together with $\boldsymbol{\Delta}_A, \boldsymbol{\Delta}_B$, can be written as follows

$$\begin{bmatrix} V_{\boldsymbol{Y}} \\ \boldsymbol{\Delta}_A \\ \boldsymbol{\Delta}_B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & \alpha_1 & 0 & 0 \\ 0 & 0 & 1 & \alpha_2 \end{bmatrix} \begin{bmatrix} V_{\boldsymbol{A}}(1) \\ V_{\boldsymbol{A}}(2) \\ V_{\boldsymbol{B}}(1) \\ V_{\boldsymbol{B}}(2) \end{bmatrix}, \tag{116}$$

where the invertibility of the matrix is guaranteed by the condition that $\alpha_1, \alpha_2, \alpha_3, \alpha_4, 1, 0$ are distinct. The user is thus able to recover both $\boldsymbol{A}, \boldsymbol{B}$ by inverting the matrix. Evidently, the scheme is also correct even if the support set is $\{\boldsymbol{A}, \boldsymbol{B}\}$ and the desired message is $\boldsymbol{B}$.

Suppose the user has $\boldsymbol{A}+\boldsymbol{C}$ as the side information. Let the vector representation of the side information in this case be $V_{\boldsymbol{Y}'} \in \mathbb{F}_{2^l}^{2\times 1}$. With the same download as specified in (114), the user has

$$\begin{bmatrix} V_{\boldsymbol{Y}'} \\ \boldsymbol{\Delta}_A \\ \boldsymbol{\Delta}_C \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & \alpha_1 & 0 & 0 \\ 0 & 0 & 1 & \alpha_3 \end{bmatrix} \begin{bmatrix} V_{\boldsymbol{A}}(1) \\ V_{\boldsymbol{A}}(2) \\ V_{\boldsymbol{C}}(1) \\ V_{\boldsymbol{C}}(2) \end{bmatrix}, \tag{117}$$

which again guarantees the decodability of both $\boldsymbol{A}, \boldsymbol{C}$ as the matrix is invertible. Thus the scheme is also correct when $\boldsymbol{\mathcal{S}} = \{\boldsymbol{A}, \boldsymbol{C}\}$ and the desired message is $\boldsymbol{A}$ or $\boldsymbol{C}$.

Similarly, for all other 4 possible realizations of the support set ($\{\boldsymbol{A}, \boldsymbol{D}\}$, $\{\boldsymbol{B}, \boldsymbol{C}\}$, $\{\boldsymbol{B}, \boldsymbol{D}\}$, $\{\boldsymbol{C}, \boldsymbol{D}\}$) and any valid realization of $\boldsymbol{\theta} \in \mathcal{S}$, the same $\boldsymbol{\Delta}$ enables the user to decode both messages in the support set. Thus, the scheme is also correct.

VII. Proof of Theorem 4

For the case $q = 2$, it suffices to download any $K-1$ messages out of the K messages to achieve the capacity $\frac{1}{K-1}$, since the desired message is either directly downloaded or can be recovered by subtracting the $K-1$ downloaded messages from the CSI.

For $q \neq 2$, to achieve the capacity 1, it suffices to download a linear combination of all K messages with non-zero coefficients. Specifically,

$$\boldsymbol{\Delta} = \boldsymbol{Y} + \boldsymbol{\lambda}' \boldsymbol{W}_{\boldsymbol{\theta}}, \tag{118}$$

where $\boldsymbol{Y}$ is the CSI and $\boldsymbol{\lambda}' \in \mathbb{F}_q^{\times}$ is a non-zero element in $\mathbb{F}_q$ such that $\boldsymbol{\lambda_t} + \boldsymbol{\lambda}' \neq 0$ (let $\boldsymbol{\lambda_t}$ denote the coefficient in front of $\boldsymbol{W}_{\boldsymbol{\theta}}$ in the CSI $\boldsymbol{Y}$). Such $\boldsymbol{\lambda}'$ always exists for $q \neq 2$. From the server's perspective, the user is downloading a random linear combination of K messages so the privacy constraint is satisfied. The user is able to decode $\boldsymbol{W}_{\boldsymbol{\theta}}$ by subtracting $\boldsymbol{Y}$ from $\boldsymbol{\Delta}$ so the correctness constraint is satisfied.

VIII. Proof of Theorem 5

Let us denote the $K = 4$ messages as $\boldsymbol{W}_1 = \boldsymbol{A}, \boldsymbol{W}_2 = \boldsymbol{B}, \boldsymbol{W}_3 = \boldsymbol{C}, \boldsymbol{W}_4 = \boldsymbol{D}$ for simpler notation. We have $M = 3$, the base field is $\mathbb{F}_3$ and the length of each message is $L = 1$. Our goal is to prove the achievability of rate $1/2$, i.e., download cost $D = 2$ for $L = 1$. The user downloads,

$$\begin{aligned} \boldsymbol{\Delta} = \{&\boldsymbol{\Delta}_1 = \boldsymbol{A} + \boldsymbol{\eta}_b \boldsymbol{B} + \boldsymbol{\eta}_c \boldsymbol{C}, \\ &\boldsymbol{\Delta}_2 = 2\boldsymbol{\eta}_b \boldsymbol{B} + \boldsymbol{\eta}_c \boldsymbol{C} + \boldsymbol{\eta}_d \boldsymbol{D}\}. \end{aligned} \tag{119}$$

From $\boldsymbol{\Delta}$, the user is able to also compute

$$\boldsymbol{L}_1 = \boldsymbol{\Delta}_1 + \boldsymbol{\Delta}_2 = \boldsymbol{A} + 2\boldsymbol{\eta}_c \boldsymbol{C} + \boldsymbol{\eta}_d \boldsymbol{D}, \tag{120}$$

$$\boldsymbol{L}_2 = \boldsymbol{\Delta}_1 + 2\boldsymbol{\Delta}_2 = \boldsymbol{A} + 2\boldsymbol{\eta}_b \boldsymbol{B} + 2\boldsymbol{\eta}_d \boldsymbol{D}. \tag{121}$$

Let $\boldsymbol{W}_{\boldsymbol{\theta}}$ denote the desired message. Let us normalize $\boldsymbol{\lambda_1} = 1$ without loss of generality. The $\boldsymbol{\eta}_b, \boldsymbol{\eta}_c, \boldsymbol{\eta}_d$ values are specified as follows.

1) When $\boldsymbol{\mathcal{S}} = \{1, 2, 3\}$ and $\boldsymbol{Y} = \boldsymbol{A} + \boldsymbol{\lambda}_2 \boldsymbol{B} + \boldsymbol{\lambda}_3 \boldsymbol{C}$, then $\boldsymbol{\eta}_d$ is randomly chosen from $\mathbb{F}_3^{\times} = \{1, 2\}$ and $\boldsymbol{\eta}_b, \boldsymbol{\eta}_c$ are chosen so that the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$ can be recovered from $\boldsymbol{Y}$ and $\boldsymbol{\Delta}_1$ as follows.

$$\begin{aligned} &\boldsymbol{W}_{\boldsymbol{\theta}} = \boldsymbol{A} : (\boldsymbol{\eta}_b, \boldsymbol{\eta}_c) = (2\boldsymbol{\lambda}_2, 2\boldsymbol{\lambda}_3), 2\boldsymbol{A} = \boldsymbol{Y} + \boldsymbol{\Delta}_1 \\ &\boldsymbol{W}_{\boldsymbol{\theta}} = \boldsymbol{B} : (\boldsymbol{\eta}_b, \boldsymbol{\eta}_c) = (2\boldsymbol{\lambda}_2, \boldsymbol{\lambda}_3), \boldsymbol{\lambda}_2 \boldsymbol{B} = 2\boldsymbol{Y} + \boldsymbol{\Delta}_1 \\ &\boldsymbol{W}_{\boldsymbol{\theta}} = \boldsymbol{C} : (\boldsymbol{\eta}_b, \boldsymbol{\eta}_c) = (\boldsymbol{\lambda}_2, 2\boldsymbol{\lambda}_3), \boldsymbol{\lambda}_3 \boldsymbol{C} = 2\boldsymbol{Y} + \boldsymbol{\Delta}_1 \end{aligned}$$

2) When $\boldsymbol{\mathcal{S}}=\{2,3,4\}$ and $\boldsymbol{Y}=\boldsymbol{B}+\boldsymbol{\lambda}_2\boldsymbol{C}+\boldsymbol{\lambda}_3\boldsymbol{D}$, then $\boldsymbol{\eta}_b$ is randomly chosen from $\mathbb{F}_q^{\times}=\{1,2\}$ and $\boldsymbol{\eta}_c,\boldsymbol{\eta}_d$ are chosen so that the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$ can be recovered from $\boldsymbol{Y}$ and $\boldsymbol{\Delta}_2$ as follows.

$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{B}:(\boldsymbol{\eta}_c,\boldsymbol{\eta}_d)=(\boldsymbol{\eta}_b\boldsymbol{\lambda}_2,\boldsymbol{\eta}_b\boldsymbol{\lambda}_3),\boldsymbol{B}=2\boldsymbol{Y}+\boldsymbol{\Delta}_2/\boldsymbol{\eta}_b$$
$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{C}:(\boldsymbol{\eta}_c,\boldsymbol{\eta}_d)=(\boldsymbol{\eta}_b\boldsymbol{\lambda}_2,2\boldsymbol{\eta}_b\boldsymbol{\lambda}_3),2\boldsymbol{\lambda}_2\boldsymbol{C}=\boldsymbol{Y}+\boldsymbol{\Delta}_2/\boldsymbol{\eta}_b$$
$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{D}:(\boldsymbol{\eta}_c,\boldsymbol{\eta}_d)=(2\boldsymbol{\eta}_b\boldsymbol{\lambda}_2,\boldsymbol{\eta}_b\boldsymbol{\lambda}_3),2\boldsymbol{\lambda}_3\boldsymbol{D}=\boldsymbol{Y}+\boldsymbol{\Delta}_2/\boldsymbol{\eta}_b$$

3) When $\boldsymbol{\mathcal{S}}=\{1,3,4\}$ and $\boldsymbol{Y}=\boldsymbol{A}+\boldsymbol{\lambda}_2\boldsymbol{C}+\boldsymbol{\lambda}_3\boldsymbol{D}$, then $\boldsymbol{\eta}_b$ is randomly chosen from $\mathbb{F}_q^{\times}$ and $\boldsymbol{\eta}_c,\boldsymbol{\eta}_d$ are chosen so that the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$ can be recovered from $\boldsymbol{Y}$ and $\boldsymbol{L}_1$ as follows.

$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{A}:(\boldsymbol{\eta}_c,\boldsymbol{\eta}_d)=(\boldsymbol{\lambda}_2,2\boldsymbol{\lambda}_3),2\boldsymbol{A}=\boldsymbol{Y}+\boldsymbol{L}_1$$
$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{C}:(\boldsymbol{\eta}_c,\boldsymbol{\eta}_d)=(\boldsymbol{\lambda}_2,\boldsymbol{\lambda}_3),\boldsymbol{\lambda}_2\boldsymbol{C}=2\boldsymbol{Y}+\boldsymbol{L}_1$$
$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{D}:(\boldsymbol{\eta}_c,\boldsymbol{\eta}_d)=(2\boldsymbol{\lambda}_2,2\boldsymbol{\lambda}_3),\boldsymbol{\lambda}_3\boldsymbol{D}=2\boldsymbol{Y}+\boldsymbol{L}_1$$

4) When $\boldsymbol{\mathcal{S}}=\{1,2,4\}$ and $\boldsymbol{Y}=\boldsymbol{A}+\boldsymbol{\lambda}_2\boldsymbol{B}+\boldsymbol{\lambda}_3\boldsymbol{D}$, then $\boldsymbol{\eta}_c$ is randomly chosen from $\mathbb{F}_q^{\times}$ and $\boldsymbol{\eta}_b,\boldsymbol{\eta}_d$ are chosen so that the desired message $\boldsymbol{W}_{\boldsymbol{\theta}}$ can be recovered from $\boldsymbol{Y}$ and $\boldsymbol{L}_2$ as follows.

$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{A}:(\boldsymbol{\eta}_b,\boldsymbol{\eta}_d)=(\boldsymbol{\lambda}_2,\boldsymbol{\lambda}_3),2\boldsymbol{A}=\boldsymbol{Y}+\boldsymbol{L}_2$$
$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{B}:(\boldsymbol{\eta}_b,\boldsymbol{\eta}_d)=(\boldsymbol{\lambda}_2,2\boldsymbol{\lambda}_3),\boldsymbol{\lambda}_2\boldsymbol{B}=2\boldsymbol{Y}+\boldsymbol{L}_2$$
$$\boldsymbol{W}_{\boldsymbol{\theta}}=\boldsymbol{D}:(\boldsymbol{\eta}_b,\boldsymbol{\eta}_d)=(2\boldsymbol{\lambda}_2,\boldsymbol{\lambda}_3),\boldsymbol{\lambda}_3\boldsymbol{D}=2\boldsymbol{Y}+\boldsymbol{L}_2$$

Correctness is already shown. For privacy, note that the form of the query is fixed as in (119) so the user only needs to specify $\boldsymbol{\eta}_b,\boldsymbol{\eta}_c,\boldsymbol{\eta}_d$, and those are i.i.d. uniform over $\mathbb{F}_3^{\times}=\{1,2\}$, regardless of $(\boldsymbol{\mathcal{S}},\boldsymbol{\theta})$. Thus, the scheme is private, and the rate achieved is $1/2$, which completes the proof of Theorem 5.

IX. Proof of Theorem 6

A. Converse

Here we prove that

$$C^{\text{pri}}_{\text{PCSI-II}}(q)\le C_{\text{PCSI-II}}(q=2)=C^{\inf}_{\text{PCSI-II}}. \tag{122}$$

The following lemma states that for PIR-PCSI*, for every feasible Q and $(\theta,\mathcal{S})$ value, all possible coefficient vectors must allow successful decoding.

Lemma 6: Under the constraint of $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda})$ privacy,

PIR-PCSI: $\forall(Q,\mathcal{S},\theta,\Lambda)\in\mathcal{Q}\times\mathfrak{S}\times[K]\times\mathfrak{C}$,
$$H(\boldsymbol{W}_\theta\mid\boldsymbol{\Delta},\boldsymbol{Y}^{[\mathcal{S},\Lambda]},\boldsymbol{Q}=Q)=0. \tag{123}$$
PIR-PCSI-I: $\forall(Q,\mathcal{S},\theta,\Lambda)\in\mathcal{Q}\times\mathfrak{S}\times([K]\setminus\mathcal{S})\times\mathfrak{C}$,
$$H(\boldsymbol{W}_\theta\mid\boldsymbol{\Delta},\boldsymbol{Y}^{[\mathcal{S},\Lambda]},\boldsymbol{Q}=Q)=0. \tag{124}$$
PIR-PCSI-II: $\forall(Q,\mathcal{S},\theta,\Lambda)\in\mathcal{Q}\times\mathfrak{S}\times\mathcal{S}\times\mathfrak{C}$,
$$H(\boldsymbol{W}_\theta\mid\boldsymbol{\Delta},\boldsymbol{Y}^{[\mathcal{S},\Lambda]},\boldsymbol{Q}=Q)=0. \tag{125}$$

Proof: Since the server knows $\boldsymbol{\Delta},\boldsymbol{Q}$ and can test all possible realizations of $\boldsymbol{\theta},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}$ for decodability. If there exists $(\theta,\mathcal{S},\Lambda)$ such that $\boldsymbol{W}_\theta$ cannot be decoded, then that $(\theta,\mathcal{S},\Lambda)$ can be ruled out by the server. This contradicts the joint $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda})$ privacy constraint. □

As a direct result of (125), for any PIR-PCSI-II scheme that preserves joint $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda})$ privacy,

$$H(\boldsymbol{W}_{\mathcal{S}}\mid\boldsymbol{\Delta},\boldsymbol{Y}^{[\mathcal{S},\Lambda]},\boldsymbol{Q}=Q)=0,\quad\forall(\mathcal{S},\Lambda,Q)\in\mathfrak{S}\times\mathfrak{C}\times\mathcal{Q}. \tag{126}$$

Note that (126) is a *stronger* version of (103) which is sufficient to bound $C_{\text{PCSI-II}}(q=2)$. Thus, we have $C^{\text{pri}}_{\text{PCSI-II}}(q)\le C_{\text{PCSI-II}}(q=2)=C^{\inf}_{\text{PCSI-II}}$.

B. Achievability

The *Generic Linear Combination Based Scheme* in Section VI-B where $M-1$ linear combinations of each messages (represented in the extended field $\mathbb{F}_{q^l}$ where $L=Ml$) are downloaded, also works under $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda})$ privacy, but with a slight modification. The only difference between the modified scheme and the infimum capacity achieving scheme of PIR-PCSI-II in Section VI-B is that, instead of the matrix in (112), the following matrix

$$\mathbf{G}_{\mathcal{S}}^{(\gamma_1,\gamma_2,\cdots,\gamma_M)}=\begin{bmatrix}\gamma_1\mathbf{I}_M & \cdots & \gamma_M\mathbf{I}_M\\ \mathbf{e}_1\otimes\mathbf{L}_{j_1}^{(1)}\\ \cdots\\ \mathbf{e}_1\otimes\mathbf{L}_{j_1}^{(M-1)}\\ \cdots\\ \mathbf{e}_M\otimes\mathbf{L}_{j_M}^{(1)}\\ \cdots\\ \mathbf{e}_M\otimes\mathbf{L}_{j_M}^{(M-1)}\end{bmatrix}, \tag{127}$$

must have full rank for every $\mathcal{S}=\{j_1,\cdots,j_M\}\in\mathfrak{S}$ and every realization of $(\gamma_1,\gamma_2,\cdots,\gamma_M)\in\mathfrak{C}$. Let us prove that the scheme is correct, jointly private and such $\mathbf{L}^{(\cdot)}$ vectors exist when l is large enough that,

$$q^l>(q-1)^M\tbinom{K}{M}M(M-1). \tag{128}$$

Proof: For a particular realization of $(\gamma_1,\gamma_2,\cdots,\gamma_M)$, e.g., $(\gamma_1,\gamma_2,\cdots,\gamma_M)=(1,1,\cdots,1)$, (127) yields a set of $\tbinom{K}{M}$ matrices

$$\mathcal{G}^{(1,1,\cdots,1)}=\{\mathbf{G}_{\mathcal{S}_1}^{(1,1,\cdots,1)},\mathbf{G}_{\mathcal{S}_2}^{(1,1,\cdots,1)},\cdots,\mathbf{G}_{\mathcal{S}_{\binom{K}{M}}}^{(1,1,\cdots,1)}\}$$

corresponding to all possible $\{j_1,j_2,\cdots,j_M\}\in\mathfrak{S}$. If all the $\tbinom{K}{M}$ matrices in $\mathcal{G}^{(1,1,\cdots,1)}$ are invertible, this scheme preserves the joint privacy of $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}})$ and enables the user to decode all the M messages in the support set, when all the coefficients in CSI are 1, according to Appendix A.

Going over all the possible realizations of $(\gamma_1,\cdots,\gamma_M)\in\mathfrak{C}$ and $\{j_1,j_2,\cdots,j_M\}\in\mathfrak{S}$, (127) yields $(q-1)^M$ sets of matrices

$$\mathcal{G}^{(1,\cdots,1)},\mathcal{G}^{(1,\cdots,1,2)},\cdots,\mathcal{G}^{(q-1,\cdots,q-1)}, \tag{129}$$

each of which contains $\tbinom{K}{M}$ matrices, i.e., there are in total $(q-1)^M\tbinom{K}{M}$ matrices. If all the $(q-1)^M\tbinom{K}{M}$ matrices are invertible, then for arbitrary realization of $(\gamma_1,\gamma_2,\cdots,\gamma_M)$, i.e., arbitrary M coefficients in the CSI, this scheme enables the user to decode all the M messages in the support set and preserves the joint $(\boldsymbol{\theta},\boldsymbol{\mathcal{S}})$ privacy. Since this scheme works for arbitrary coefficients, from the server's perspective, all the realizations of M coefficients are equally likely. Thus, the joint privacy of coefficients $\boldsymbol{\Lambda}$, index $\boldsymbol{\theta}$, and support set $\boldsymbol{\mathcal{S}}$, is preserved.

To prove the existence of such linear combinations, note that the determinant of each one of the $(q-1)^M\tbinom{K}{M}$ matrices

yields a degree $M(M-1)$ multi-variate polynomial as proved in Appendix A. Thus, the product of the determinants of all the matrices F is a multi-variate polynomial of degree $(q-1)^M\binom{K}{M}M(M-1)$. Again, as in Appendix A, according to the Schwartz-Zippel Lemma, when $q^l > (q-1)^M\binom{K}{M}$, there exists elements in $\mathbb{F}_{q^l}$ such that the polynomial F does not evaluate to 0, i.e., all the $(q-1)^M\binom{K}{M}M(M-1)$ matrices are invertible.

Let us give an example.

Example 3: Consider $M=2, K=4, L=2l, q=3$. The 4 messages are $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}$ each of which has $L=2l$ symbols in $\mathbb{F}_3$. Let $l \geq 2$.

$\boldsymbol{A}$ can be represented as a 2×1 vector $V_{\boldsymbol{A}} = [V_{\boldsymbol{A}}(1) \;\; V_{\boldsymbol{A}}(2)]^{\mathrm{T}}$ where $V_{\boldsymbol{A}}(1), V_{\boldsymbol{A}}(2) \in \mathbb{F}_{3^l}$. Similarly, $\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}$ can be represented as $V_{\boldsymbol{B}}$, $V_{\boldsymbol{C}}$, $V_{\boldsymbol{D}}$, respectively. Choose $\alpha_1,\cdots,\alpha_4$ as elements of $\mathbb{F}_{3^l}$ such that $\alpha_1,\alpha_2,\alpha_3,\alpha_4,0,1,2$ are all distinct elements of $\mathbb{F}_{3^l}$. Note that $0,1,2$, are the elements of $\mathbb{F}_3$, which are also elements of $\mathbb{F}_{3^l}$ because $\mathbb{F}_3$ is a sub-field of $\mathbb{F}_{3^l}$. Furthermore, since $\mathbb{F}_{3^l}$ has $3^l \geq 9$ distinct elements, such α_i are guaranteed to exist. For all possible realizations of $(\boldsymbol{\mathcal{S}},\boldsymbol{\theta})$, the download $\boldsymbol{\Delta}$ remains the same as follows,

$$\boldsymbol{\Delta} = \begin{bmatrix}\boldsymbol{\Delta}_A\\ \boldsymbol{\Delta}_B\\ \boldsymbol{\Delta}_C\\ \boldsymbol{\Delta}_D\end{bmatrix} = \begin{bmatrix}V_{\boldsymbol{A}}(1)+\alpha_1 V_{\boldsymbol{A}}(2)\\ V_{\boldsymbol{B}}(1)+\alpha_2 V_{\boldsymbol{B}}(2)\\ V_{\boldsymbol{C}}(1)+\alpha_3 V_{\boldsymbol{C}}(2)\\ V_{\boldsymbol{D}}(1)+\alpha_4 V_{\boldsymbol{D}}(2)\end{bmatrix}, \tag{130}$$

The query is a constant as the $\boldsymbol{\Delta}$ remains unchanged for any realizations of $\boldsymbol{\mathcal{S}},\boldsymbol{\theta},\boldsymbol{\Lambda}$. Thus, the privacy is guaranteed. We then prove the correctness, i.e., this specific download enables the user to decode the desired message under all realizations of $\boldsymbol{\mathcal{S}},\boldsymbol{\theta},\boldsymbol{\Lambda}$.

Let us consider the case where the support set is $\{\boldsymbol{A},\boldsymbol{B}\}$ and the side information is $\boldsymbol{A}+2\boldsymbol{B}$ (i.e., $\Lambda=[1 \;\; 2]$), and the desired message is $\boldsymbol{A}$. The side information can be represented as $V_{\boldsymbol{Y}} \in \mathbb{F}_{3^l}^{2\times 1}$ where

$$V_{\boldsymbol{Y}} = \begin{bmatrix}1&0&2&0\\0&1&0&2\end{bmatrix}\begin{bmatrix}V_{\boldsymbol{A}}(1)\\V_{\boldsymbol{A}}(2)\\V_{\boldsymbol{B}}(1)\\V_{\boldsymbol{B}}(2)\end{bmatrix} = \begin{bmatrix}V_{\boldsymbol{A}}(1)+2V_{\boldsymbol{B}}(1)\\V_{\boldsymbol{A}}(2)+2V_{\boldsymbol{B}}(2)\end{bmatrix}. \tag{131}$$

$V_{\boldsymbol{Y}}$, together with $\boldsymbol{\Delta}_A,\boldsymbol{\Delta}_B$, can be written as follows

$$\begin{bmatrix}V_{\boldsymbol{Y}}\\ \boldsymbol{\Delta}_A\\ \boldsymbol{\Delta}_B\end{bmatrix} = \begin{bmatrix}1&0&2&0\\0&1&0&2\\1&\alpha_1&0&0\\0&0&1&\alpha_2\end{bmatrix}\begin{bmatrix}V_{\boldsymbol{A}}(1)\\V_{\boldsymbol{A}}(2)\\V_{\boldsymbol{B}}(1)\\V_{\boldsymbol{B}}(2)\end{bmatrix}, \tag{132}$$

where the matrix is invertible because $\alpha_1,\cdots,\alpha_4,0,1,2$ are distinct by design. The user is thus able to recover both $\boldsymbol{A},\boldsymbol{B}$ by inverting the matrix.

Similarly, suppose the side information is instead $\boldsymbol{A}+\boldsymbol{B}$ (i.e., $\boldsymbol{\Lambda}=[1 \;\; 1]$), the vector representation of the side information is $V_{\boldsymbol{Y}'} \in \mathbb{F}_{3^l}^{2\times 1}$.

$V'_{\boldsymbol{Y}}$, together with $\boldsymbol{\Delta}_A,\boldsymbol{\Delta}_B$, can be written as follows

$$\begin{bmatrix}V_{\boldsymbol{Y}'}\\ \boldsymbol{\Delta}_A\\ \boldsymbol{\Delta}_B\end{bmatrix} = \begin{bmatrix}1&0&1&0\\0&1&0&1\\1&\alpha_1&0&0\\0&0&1&\alpha_2\end{bmatrix}\begin{bmatrix}V_{\boldsymbol{A}}(1)\\V_{\boldsymbol{A}}(2)\\V_{\boldsymbol{B}}(1)\\V_{\boldsymbol{B}}(2)\end{bmatrix}. \tag{133}$$

Since the matrix is invertible by design, the user is able to recover both $\boldsymbol{A},\boldsymbol{B}$.

Note that the recoverability of both $\boldsymbol{A},\boldsymbol{B}$ when the support set is $\{\boldsymbol{A},\boldsymbol{B}\}$ and $\boldsymbol{\Lambda}=[2 \;\; 1]$ or $\boldsymbol{\Lambda}=[2 \;\; 2]$ is automatically proved as $[2 \;\; 1]=2[1 \;\; 2]$ and $[2 \;\; 2]=2[1 \;\; 1]$ in $\mathbb{F}_3$.

Thus when the support set is $\{\boldsymbol{A},\boldsymbol{B}\}$, this scheme is correct for arbitrary realizations of $\boldsymbol{\theta},\boldsymbol{\Lambda}$.

Similarly, the scheme is also correct for arbitrary realizations of $\boldsymbol{\theta},\boldsymbol{\Lambda}$ when $\boldsymbol{\mathcal{S}} = \{\boldsymbol{A},\boldsymbol{C}\}$, $\{\boldsymbol{A},\boldsymbol{D}\}$, $\{\boldsymbol{B},\boldsymbol{C}\}$, $\{\boldsymbol{B},\boldsymbol{D}\}$, $\{\boldsymbol{C},\boldsymbol{D}\}$. Thus, this scheme is correct for arbitrary realizations of $\boldsymbol{\mathcal{S}},\boldsymbol{\theta},\boldsymbol{\Lambda}$.

X. Proof of Theorem 7

Here we bound the redundancy $\rho_{\text{PCSI-I}}$ from above (equivalently, lower-bound α^*) for $1 \leq M \leq K-1$.

Recall that the supremum capacity for PIR-PCSI-I is $(K-M)^{-1}$, i.e., the optimal average download cost is $D/L = K-M$. Consider an achievable scheme such that α-CSI is sufficient and the average download cost $D/L \leq K-M+\epsilon$ for some L. Since $D/L \leq K-M+\epsilon$, we have $L(K-M)+\epsilon L \geq D \geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q})$. Thus, there exists a feasible Q such that

$$H(\boldsymbol{\Delta} \mid \boldsymbol{Q}=Q) \leq (K-M)L + \epsilon L. \tag{134}$$

For all $i \in [M]$, let $\mathcal{S}_i = [M+1] \setminus \{i\}$. ALso, for all $i \in [M+1:K]$, let $\mathcal{S}_i = [M]$. For all $i \in [K]$, let $\Lambda_i \in \mathfrak{C}$ satisfy

$$H(\boldsymbol{W}_i \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}^{[\mathcal{S}_i,\Lambda_i]}, \boldsymbol{Q}=Q) = 0. \tag{135}$$

Such Λ_i's must exist according to (41) in Lemma 1.

Writing $\overline{\boldsymbol{Y}}^{[\mathcal{S}_i,\Lambda_i]}$ as $\overline{\boldsymbol{Y}}_i$ for compact notation, we have

$$\begin{aligned}
&H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]}, \boldsymbol{Q}=Q) && (136)\\
&= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]}, \boldsymbol{W}_{[M]}, \boldsymbol{Q}=Q) && (137)\\
&= H(\boldsymbol{W}_{[M+1:K]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[K]}, \boldsymbol{W}_{[M]}, \boldsymbol{Q}=Q) && (138)\\
&= 0, && (139)
\end{aligned}$$

where (137) follows from (135). (138) is correct since $\overline{\boldsymbol{Y}}_{[M+1:K]}$ are functions of $\boldsymbol{W}_{[M]}$. (139) follows from (135). Since we are considering the case where the supremum capacity is achieved, we have

$$\begin{aligned}
&(K-M)L + \epsilon L + M\alpha L\\
&\geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q}=Q) + H(\overline{\boldsymbol{Y}}_{[M]} \mid \boldsymbol{Q}=Q) && (140)\\
&\geq H(\boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]} \mid \boldsymbol{Q}=Q) && (141)\\
&\geq I(\boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]}; \boldsymbol{W}_{[K]} \mid \boldsymbol{Q}=Q)\\
&= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{Q}=Q) = KL. && (142)
\end{aligned}$$

(140) follows from (134) and (25). Step (142) follows from (139) and the fact that the query and the messages are mutually independent according to (5). Thus we have $\alpha \geq 1-\frac{\epsilon}{M}$. In order to approach capacity, we must have $\epsilon \to 0$, so we need $\alpha \geq 1$, and since this is true for any α such that α-CSI is sufficient, it is also true for α^*. Thus, the redundancy is bounded as $\rho_{\text{PCSI-I}} \leq 0$.

XI. Proof of Theorem 8

A. Converse for $C_{\text{PCSI-I}}(q=2)$

Again, (41) is true for arbitrary $\mathbb{F}_q$. The only thing different in $\mathbb{F}_2$ is that $\mathbf{\Lambda}$ must be the vector of all ones. As a direct result of (41), for PIR-PCSI-I in $\mathbb{F}_2$,

$$H(\boldsymbol{W}_{[K]\setminus\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Y}^{[\mathcal{S},1_M]}, \boldsymbol{Q}=Q)=0, \forall (Q,\mathcal{S}) \in \mathcal{Q}\times\mathfrak{S} \tag{143}$$

and thus

$$\begin{aligned} & H(\boldsymbol{W}_{[K]\setminus\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q) && (144)\\ & \overset{(143)}{=} I(\boldsymbol{W}_{[K]\setminus\mathcal{S}}; \boldsymbol{Y}^{[\mathcal{S},1_M]} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q) && (145)\\ & \le H(\boldsymbol{Y}^{[\mathcal{S},1_M]} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q) && (146)\\ & \overset{(3)}{\le} L, \quad \forall (Q,\mathcal{S}) \in \mathcal{Q}\times\mathfrak{S}. && (147)\end{aligned}$$

Averaging over $\boldsymbol{Q}$ gives

$$H(\boldsymbol{W}_{[K]\setminus\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Q}) \le L, \forall \mathcal{S}\in\mathfrak{S}. \tag{148}$$

Also, for all $\mathcal{S}\in\mathfrak{S}$ and $Q\in\mathcal{Q}$,

$$\begin{aligned} & H(\boldsymbol{W}_{[K]} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q) && (149)\\ & = H(\boldsymbol{W}_{\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q) \\ & \quad + H(\boldsymbol{W}_{[K]\setminus\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{W}_{\mathcal{S}}, \boldsymbol{Q}=Q) && (150)\\ & = H(\boldsymbol{W}_{\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q) \\ & \quad + H(\boldsymbol{W}_{[K]\setminus\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{W}_{\mathcal{S}}, \boldsymbol{Y}^{[\mathcal{S},1_M]}, \boldsymbol{Q}=Q) && (151)\\ & = H(\boldsymbol{W}_{\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Q}=Q), && (152)\end{aligned}$$

where (151) results from the fact that $\overline{\boldsymbol{Y}}^{[\mathcal{S},1_M]}=\sum_{s\in\mathcal{S}}\boldsymbol{W}_s$, and the last step follows from (143). Averaging over $\boldsymbol{Q}$, it follows that

$$H(\boldsymbol{W}_{[K]} \mid \mathbf{\Delta}, \boldsymbol{Q}) = H(\boldsymbol{W}_{\mathcal{S}} \mid \mathbf{\Delta}, \boldsymbol{Q}), \quad \forall \mathcal{S}\in\mathfrak{S}. \tag{153}$$

Let us first prove $C_{\text{PCSI-I}}(q=2)\le (K-1)^{-1}$ in the regime where $1\le M\le \frac{K}{2}$.

$$\begin{aligned} & H(\boldsymbol{W}_{[K]} \mid \mathbf{\Delta}, \boldsymbol{Q}) \\ & = H(\boldsymbol{W}_{[M]} \mid \mathbf{\Delta}, \boldsymbol{Q}) && (154)\\ & \le H(\boldsymbol{W}_{[K-M]} \mid \mathbf{\Delta}, \boldsymbol{Q}) && (155)\\ & \le L, && (156)\end{aligned}$$

where (154) is true according to (153), (155) follows from $(K-M\ge M)$ and (143), and (156) follows from (148). Thus

$$\begin{aligned} H(\mathbf{\Delta} \mid \boldsymbol{Q}) & \ge I(\mathbf{\Delta}; \boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) && (157)\\ & = H(\boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) - H(\boldsymbol{W}_{[K]} \mid \mathbf{\Delta}, \boldsymbol{Q}) && (158)\\ & \ge KL - L. && (159)\end{aligned}$$

Thus $D\ge H(\mathbf{\Delta}\mid\boldsymbol{Q})\ge KL-L$ and since the rate $L/D\le (K-1)^{-1}$ for every achievable scheme, we have shown that $C_{\text{PCSI-I}}(q=2)\le (K-1)^{-1}$ when $K-M\ge M\ge 1$, i.e., $1\le M\le K/2$.

Next let us prove that $C_{\text{PCSI-I}}(q=2)\le \left(K-\frac{M}{K-M}\right)^{-1}$ for the regime $\frac{K}{2}<M\le K-1$. It suffices to prove $H(\mathbf{\Delta}\mid\boldsymbol{Q})\ge KL-\frac{ML}{K-M}$. Define,

$$H_m^K = \frac{1}{\binom{K}{m}} \sum_{\mathcal{M}:\mathcal{M}\subset[K],|\mathcal{M}|=m} \frac{H(\boldsymbol{W}_{\mathcal{M}} \mid \mathbf{\Delta}, \boldsymbol{Q})}{m}, \tag{160}$$

we have

$$\begin{aligned} H_{K-M}^K & \ge H_M^K && (161)\\ & = \frac{H(\boldsymbol{W}_{[K]} \mid \mathbf{\Delta}, \boldsymbol{Q})}{M}, && (162)\end{aligned}$$

where (161) follows from Han's inequality [36], and (162) follows from (153). Note that according to (148),

$$\frac{L}{K-M} \ge H_{K-M}^K, \tag{163}$$

and therefore,

$$H(\boldsymbol{W}_{[K]} \mid \mathbf{\Delta}, \boldsymbol{Q}) \le \frac{ML}{K-M}. \tag{164}$$

Thus, $H(\mathbf{\Delta}\mid\boldsymbol{Q})\ge KL-\frac{ML}{K-M}$, which completes the converse proof for Theorem 8. We next prove achievability.

B. Two PIR-PCSI-I Schemes for Arbitrary q

1) Achieving Rate $\frac{1}{K-1}$ When $1\le M\le \frac{K}{2}$: The goal here is to download $K-1$ generic linear combinations so that along with the one linear combination already available as side-information, the user has enough information to retrieve all K messages. Let L be large enough that $q^L>\binom{K}{M}(K-1)$. For all $k\in[K]$, message $\boldsymbol{W}_k\in\mathbb{F}_q^{L\times 1}$ can be represented as a scalar $\boldsymbol{w}_k\in\mathbb{F}_{q^L}$. Let

$$\boldsymbol{w}_{[K]} = \begin{bmatrix}\boldsymbol{w}_1 & \boldsymbol{w}_2 & \cdots & \boldsymbol{w}_K\end{bmatrix}^{\mathrm{T}} \in \mathbb{F}_{q^L}^{K\times 1}, \tag{165}$$

be the length K column vector whose entries are the messages represented in $\mathbb{F}_{q^L}$. Let $\Psi\in\mathbb{F}_{q^L}^{K\times(K-1)}$ be a $K\times(K-1)$ matrix whose elements are the variables ψ_{ij}. The user downloads

$$\mathbf{\Delta} = \Psi^T \boldsymbol{w}_{[K]} \in \mathbb{F}_{q^L}^{(K-1)\times 1}. \tag{166}$$

Suppose the realization of the coefficient vector is $\mathbf{\Lambda}=\Lambda$. The linear combination available to the user can be expressed as $\boldsymbol{Y}^{[\Lambda,\boldsymbol{\mathcal{S}}]}=U_{\Lambda,\boldsymbol{\mathcal{S}}}^T\boldsymbol{w}_{[K]}$ for some $K\times 1$ vector $U_{\Lambda,\boldsymbol{\mathcal{S}}}$ that depends on $(\Lambda,\boldsymbol{\mathcal{S}})$. Combined with the download, the user has

$$[U_{\Lambda,\boldsymbol{\mathcal{S}}}, \Psi]^T \boldsymbol{w}_{[K]}, \tag{167}$$

so if the $K\times K$ matrix $G_{\Lambda,\boldsymbol{\mathcal{S}}}=[U_{\Lambda,\boldsymbol{\mathcal{S}}},\Psi]$ is invertible (full rank) then the user can decode all K messages. For all $\mathcal{S}\in\mathfrak{S}$, let $f_{\Lambda,\mathcal{S}}(\cdot)$ be the multi-variate polynomial of degree $K-1$ in variables ψ_{ij}, representing the determinant of $G_{\Lambda,\mathcal{S}}$. This is not the zero polynomial because the $K-1$ columns of Ψ can always be chosen to be linearly independent of the vector $U_{\Lambda,\mathcal{S}}$ in a K dimensional vector space. The product of all such polynomials, $f_\Lambda=\prod_{\mathcal{S}\in\mathfrak{S}} f_{\Lambda,\mathcal{S}}$ is itself a multi-variate non-zero polynomial of degree $(K-1)\binom{K}{M}$ in the variables ψ_{ij}. By Schwartz-Zippel Lemma, if the ψ_{ij} are chosen randomly from $\mathbb{F}_{q^L}$ then the probability that the corresponding

evaluation of f_Λ is zero, is no more than $(K-1)\binom{K}{M}/q^L < 1$, so there exists a choice of ψ_{ij} for which all $f_{\Lambda,\mathcal{S}}$ evaluate to non-zero values, i.e., $G_{\Lambda,\mathcal{S}}$ is invertible for every $\mathcal{S} \in \mathfrak{S}$. Thus, with this choice of Ψ, we have a scheme with rate $1/(K-1)$ that is correct and private and allows the user to retrieve all K messages. To verify privacy, note that the user constructs the query based on the realization of $\boldsymbol{\Lambda}$ alone, and does not need to know $(\boldsymbol{\mathcal{S}}, \boldsymbol{\theta})$ before it sends the query, so the query is independent of $(\boldsymbol{\mathcal{S}}, \boldsymbol{\theta})$.

Remark 5: Since the scheme allows the user to decode all messages, the scheme also works if $\boldsymbol{\theta}$ is uniformly drawn from $[K]$, i.e., in the PIR-PCSI setting.

2) Achieving Rate $(K-\frac{M}{K-M})^{-1}$ When $K/2 < M \leq K-1$: Now let us present a scheme with rate $(K-\frac{M}{K-M})^{-1}$ which is optimal for the regime $\frac{K}{2} < M \leq K-1$. The scheme is comprised of two steps.

Step 1: The user converts the (M, K) PIR-PCSI-I problem to $(K-M, K)$ PIR-PCSI-II problem as follows.

The user first downloads

$$\boldsymbol{\Delta}_1 = \sum_{k\in[K]} \boldsymbol{a}_k \boldsymbol{W}_k, \tag{168}$$

where $\boldsymbol{a}_{\boldsymbol{i}_m} = \boldsymbol{\lambda}_m$ for $\boldsymbol{i}_m \in \boldsymbol{\mathcal{S}}$ while for $k \notin \boldsymbol{\mathcal{S}}$, $\boldsymbol{a}_k$'s are independently and uniformly drawn from $\mathbb{F}_q^\times$. The user then computes

$$\boldsymbol{Y}' = \boldsymbol{\Delta}_1 - \boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} = \sum_{k\in[K]\setminus\boldsymbol{\mathcal{S}}} \boldsymbol{a}_k \boldsymbol{W}_k. \tag{169}$$

In this step, from the server's perspective, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_K$ are i.i.d. uniform over $\mathbb{F}_q^\times$, thus there is no loss of privacy. The download cost of this step is $H(\boldsymbol{\Delta}_1) = L$.

Step 2: The user has $\boldsymbol{Y}'$ as coded side information and applies the fully private PIR-PCSI-II scheme described in Section IX that protects the privacy of all the coefficients.

The reason to apply the PIR-PCSI-II scheme that maintains the privacy of coefficients is that in *Step 1*, server knows $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_K$. If in the second step, the Query is not independent of $\boldsymbol{a}_i, i \in [K] \setminus \boldsymbol{\mathcal{S}}$, then the server may be able to rule out some realizations of $\boldsymbol{\mathcal{S}}$. The download cost of this step is $\frac{K(K-M-1)L}{K-M}$. Thus, the total download cost of this scheme is $KL - \frac{ML}{K-M}$ and the rate is $\left(K-\frac{M}{K-M}\right)^{-1}$.

XII. Proof of Theorem 9

A. Proof of $C_{PCSI\text{-}I}^{pri,\sup} = C_{PCSI\text{-}I}^{\inf}$

First let us prove the converse. As a direct result of (124) in Lemma 6, for any PIR-PCSI-I scheme that preserves joint $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$ privacy,

$$H(\boldsymbol{W}_{[K]\setminus\mathcal{S}} \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},\Lambda]}, \boldsymbol{Q} = Q) = 0, \quad \forall (\mathcal{S}, \Lambda, Q) \in \mathfrak{S} \times \mathfrak{C} \times \mathcal{Q}. \tag{170}$$

Note that (170) is a stronger version of (143) which is sufficient to bound $C_{\text{PCSI-I}}(q=2)$. Thus, we have $C_{\text{PCSI-I}}^{\text{pri}}(q) \leq C_{\text{PCSI-I}}(q=2) = C_{\text{PCSI-I}}^{\inf}$, which completes the proof of converse.

For achievability, let us note that $C_{\text{PCSI-I}}^{\text{pri},\sup} \geq C_{\text{PCSI-I}}^{\text{pri}}(q=2) = C_{\text{PCSI-I}}(q=2) = C_{\text{PCSI-I}}^{\inf}$, because over $\mathbb{F}_2$, the $\boldsymbol{\Lambda}$ vector is constant (all ones) and therefore trivially private.

B. Proof of the Bound: $C_{PCSI\text{-}I}^{pri,\inf} \leq \min(C_{PCSI\text{-}I}^{\inf}, \frac{1}{K-2})$

Since privacy of $\boldsymbol{\Lambda}$ only further constrains PIR-PCSI, it is trivial that $C_{\text{PCSI-I}}^{\text{pri},\inf} \leq C_{\text{PCSI-I}}^{\inf}$. For the remaining bound, $C_{\text{PCSI-I}}^{\text{pri},\inf} \leq \frac{1}{K-2}$, it suffices to show that $C_{\text{PCSI-I}}^{\text{pri}}(q \geq M) \leq \frac{1}{K-2}$, because $C_{\text{PCSI-I}}^{\text{pri},\inf} \leq C_{\text{PCSI-I}}^{\text{pri}}(q \geq M)$. Note that by $C_{\text{PCSI-I}}^{\text{pri}}(q \geq M)$ we mean $C_{\text{PCSI-I}}^{\text{pri}}(q)$ for all $q \geq M$.

Let

$$\boldsymbol{Y}_1 = \boldsymbol{W}_2 + \alpha_3 \boldsymbol{W}_3 + \cdots \alpha_{M+1} \boldsymbol{W}_{M+1}, \tag{171}$$

$$\boldsymbol{Y}_2 = \boldsymbol{W}_1 + \boldsymbol{W}_3 + \boldsymbol{W}_4 + \cdots \boldsymbol{W}_{M+1}, \tag{172}$$

where $\alpha_3, \alpha_4, \cdots, \alpha_{M+1}$ are $M-1$ distinct elements in $\mathbb{F}_q^\times$.

Let $\beta_3, \beta_4, \ldots \beta_{M+1}$ be $M-1$ distinct elements in $\mathbb{F}_q^\times$ such that $\forall m \in [3 : M+1], \beta_m \alpha_m + 1 = 0$ in $\mathbb{F}_q$.

Note that such α's and β's exist since $q \geq M$.

Then let

$$\begin{aligned}\boldsymbol{Y}_m &= \beta_m \boldsymbol{Y}_1 + \boldsymbol{Y}_2 \\ &= \boldsymbol{W}_1 + \beta_m \boldsymbol{W}_2 + (\beta_m\alpha_3 + 1)\boldsymbol{W}_3 + \cdots \\ &\quad + (\beta_m\alpha_i + 1)\boldsymbol{W}_i + \cdots + (\beta_m\alpha_{M+1} + 1)\boldsymbol{W}_{M+1}, \\ &\forall m \in [3 : M+1],\end{aligned} \tag{173}$$

be $M-1$ linear combinations of the first $M+1$ messages $\boldsymbol{W}_{[M+1]}$. Note that for any $m \in [3 : M+1]$, the coefficient for $\boldsymbol{W}_m$ in $\boldsymbol{Y}_m$ (i.e., $\beta_m\alpha_m + 1$) is 0 while the coefficient for any $\boldsymbol{W}_i, i \in [M+1], i \neq m$ (i.e., $\beta_m\alpha_i + 1$) is non-zero.[4] For example,

$$\begin{aligned}\boldsymbol{Y}_3 = \boldsymbol{W}_1 + \beta_3 \boldsymbol{W}_2 + 0\boldsymbol{W}_3 + (\beta_3\alpha_4 + 1)\boldsymbol{W}_4 \\ + \cdots + (\beta_3\alpha_{M+1} + 1)\boldsymbol{W}_{M+1}.\end{aligned} \tag{174}$$

Thus, for any $m \in [M+1]$, $\boldsymbol{Y}_m$ is a linear combination of M messages $\boldsymbol{W}_{[M+1]\setminus\{m\}}$ with non-zero coefficients. For $\mathcal{S}_m = [M+1]/\{m\}$ and Λ_m as the vector of coefficients that appear in $\boldsymbol{Y}_m$, we $\boldsymbol{Y}^{[\mathcal{S}_m,\Lambda_m]} = \boldsymbol{Y}_m$.

According to (170),

$$H(\boldsymbol{W}_m, \boldsymbol{W}_{[M+2:K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}_m, \boldsymbol{Q} = Q) = 0, \quad \forall m \in [M+1], Q \in \mathcal{Q}. \tag{175}$$

Thus, for all $Q \in \mathcal{Q}$,

$$\begin{aligned}&H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) \\ &\leq H(\boldsymbol{W}_{[K]}, \boldsymbol{Y}_{[M+1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (176)\\ &= H(\boldsymbol{Y}_{[M+1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) + H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}_{[M+1]}, \boldsymbol{Q} = Q) && (177)\\ &= H(\boldsymbol{Y}_1, \boldsymbol{Y}_2 \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (178)\\ &\leq 2L, && (179)\end{aligned}$$

where (178) follows from (175) and the fact that $\boldsymbol{Y}_{[3:M+1]}$ are functions of $\boldsymbol{Y}_1, \boldsymbol{Y}_2$. Averaging over $\boldsymbol{Q}$ we have

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \leq 2L. \tag{180}$$

Therefore, the average download cost is bounded as,

$$\begin{aligned}D &\geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) \geq H(\boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) - H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) && (181)\\ &\geq (K-2)L. && (182)\end{aligned}$$

Thus, for $q \geq M$, we have $C_{\text{PCSI-I}}^{\text{pri}}(q) \leq \frac{1}{K-2}$.

[4] Since $\beta_m\alpha_m + 1 = 0$, $\beta_m\alpha_i + 1 \neq 0$ for $i \neq m$.

C. Proof of $C^{pri,\inf}_{PCSI\text{-}I} \geq \frac{1}{K-1}$

We need to show that $C^{\text{pri}}_{\text{PCSI-I}}(q) \geq \frac{1}{K-1}$ for all $\mathbb{F}_q$. The scheme is identical to the scheme with rate $(K-1)^{-1}$ in Section XI-B1 with a slight modification. Instead of fixing a realization $\boldsymbol{\Lambda} = \Lambda$, we will consider all possible realizations $\Lambda \in \mathfrak{C}$, and consider the product polynomial $f = \prod_{\Lambda \in \mathfrak{C}} f_\Lambda$ which is a multi-variate polynomial of degree $(K-1)\binom{K}{M}(q-1)^M$ in variables ψ_{ij}. Following the same argument based on the Schwartz-Zippel Lemma, we find that there exists a Ψ for which all $G_{\Lambda,\mathcal{S}}$ are invertible matrices, provided that L is large enough that $q^L > (q-1)^M(K-1)\binom{K}{M}$. Thus, with this choice of Ψ we have a scheme that is allows the user to retrieve all K messages. The scheme is also $(\boldsymbol{\mathcal{S}}, \boldsymbol{\theta}, \boldsymbol{\Lambda})$ private because we note that the user does not need to know the realization of $(\boldsymbol{\mathcal{S}}, \boldsymbol{\theta}, \boldsymbol{\Lambda})$ before it sends the query, so the query is independent of $(\boldsymbol{\mathcal{S}}, \boldsymbol{\theta}, \boldsymbol{\Lambda})$.

Remark 6: Since the scheme allows the user to decode all messages, and the query does not depend on $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$, the scheme also works if $\boldsymbol{\theta}$ is uniformly drawn from $[K]$, i.e., in the PIR-PCSI setting.

XIII. Proof of Theorem 10

A. Converse

The converse is divided into two regimes.

Regime 1: $2 \leq M \leq K$. The proof relies on (40) in Lemma 1. Consider any particular realization $Q \in \mathcal{Q}$ of $\boldsymbol{Q}$. For all $i \in [K]$, consider $\mathcal{S} = [M], \theta = i$, and let Λ_i be a coefficient vector that satisfies (40) according to Lemma 1, so that

$$H(\boldsymbol{W}_i \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[[M],\Lambda_i]}, \boldsymbol{Q} = Q) = 0. \tag{183}$$

Writing $\boldsymbol{Y}^{[[M],\Lambda_i]}$ as $\boldsymbol{Y}_i$ for compact notation, we have

$$\begin{aligned}
&H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}_{[M-1]}, \boldsymbol{Q} = Q) \\
&= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}_{[M-1]}, \boldsymbol{W}_{[M-1]}, \boldsymbol{Q} = Q) && (184)\\
&= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{W}_{[M]}, \boldsymbol{Q} = Q) && (185)\\
&= H(\boldsymbol{W}_{[M+1:K]} \mid \boldsymbol{\Delta}, \boldsymbol{W}_{[M]}, \boldsymbol{Y}_{[M+1:K]}, \boldsymbol{Q} = Q) && (186)\\
&= 0, && (187)
\end{aligned}$$

where (184) holds according to (183), and (185) follows from the fact that $\boldsymbol{W}_M$ is decodable by subtracting $\boldsymbol{W}_{[M-1]}$ terms from $\boldsymbol{Y}_1$. Then, (186) uses the fact that $\boldsymbol{Y}_{[M+1:K]}$ are functions of $\boldsymbol{W}_{[M]}$. Finally, (187) follows from (183).

Averaging over $\boldsymbol{Q}$,

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}_{[M-1]}, \boldsymbol{Q}) = 0. \tag{188}$$

Then we have

$$\begin{aligned}
&H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) && (189)\\
&= H(\boldsymbol{W}_{[K]}, \boldsymbol{Y}_{[M-1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) && (190)\\
&= H(\boldsymbol{Y}_{[M-1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) + H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}, \boldsymbol{Y}_{[M-1]}) && (191)\\
&\leq H(\boldsymbol{Y}_{[M-1]}) && (192)\\
&\leq (M-1)L, && (193)
\end{aligned}$$

where (190) follows from the fact that $\boldsymbol{Y}_{[M-1]}$ are linear combinations of $\boldsymbol{W}_{[M]}$. Step (192) holds because of (188), and because conditioning reduces entropy.

Thus $D \geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) \geq H(\boldsymbol{W}_{[K]}) - H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \geq (K-M+1)L$, which implies that $C^{\text{sup}}_{\text{PCSI}} \leq (K-M+1)^{-1}$ for $2 \leq M \leq K$.

Regime 2: $M = 1$.

Consider any particular realization $Q \in \mathcal{Q}$ of $\boldsymbol{Q}$. Since $M = 1$, $\boldsymbol{\Lambda}$ is irrelevant, e.g., we may assume $\boldsymbol{\Lambda} = \Lambda = 1$ without loss of generality. For all $j \in [2:K]$, consider $\mathcal{S} = \{1\}, \theta = j$, and apply (40) according to Lemma 1 so that

$$\begin{aligned}
&H(\boldsymbol{W}_j \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\{1\},1]}, \boldsymbol{Q} = Q) = 0 && (194)\\
\implies &H(\boldsymbol{W}_{[2:K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\{1\},1]}, \boldsymbol{Q} = Q) = 0 && (195)\\
&H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (196)\\
&\leq H(\boldsymbol{W}_1, \boldsymbol{W}_{[2:K]}, \boldsymbol{Y}^{[\{1\}]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (197)\\
&= H(\boldsymbol{W}_1, \boldsymbol{Y}^{[\{1\},1]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (198)\\
&= H(\boldsymbol{W}_1 \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (199)\\
&\leq L, && (200)
\end{aligned}$$

where (198) holds since (195) holds, and (199) is true as $\boldsymbol{Y}^{[\{1\},1]}$ is simply $\boldsymbol{W}_1$. Averaging over $\boldsymbol{Q}$, $H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \leq L$. Thus $D \geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) \geq H(\boldsymbol{W}_{[K]}) - H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \geq KL - L$, which implies that $C_{\text{PCSI}}(q) \leq (K-1)^{-1}$ for $M = 1$.

B. Achievability

For $2 \leq M \leq K$, the achievable scheme will be a combination of *Specialized GRS Codes* and *Modified Specialized GRS Codes* which are schemes in [33] for PIR-PCSI-I and PIR-PCSI-II setting, respectively.

The rate $(K-M)^{-1}$ is achievable by *Specialized GRS Codes* for PIR-PCSI-I setting and the rate $(K-M+1)^{-1}$ is achievable by *Modified Specialized GRS Codes* for the PIR-PCSI-II setting. Both schemes work for $L = 1$, so let us say $L = 1$ here. Intuitively, these two achievable schemes have the same structures as explained below.

For the PIR-PCSI-I setting, the desired message is not contained in the support set. The download will be $K-M$ linear equations of K unknowns (K messages). These $K-M$ linear equations are independent by design, so they allow the user to eliminate any $K-M-1$ unknowns and get an equation in the remaining $K-(K-M-1) = M+1$ unknowns (messages). Let these $M+1$ unknowns be the M messages in the support set and the desired message. With careful design, the equation will be equal to $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} + \boldsymbol{\lambda}'\boldsymbol{W}_{\boldsymbol{\theta}}$ for some non-zero $\boldsymbol{\lambda}'$. Thus by subtracting CSI from the equation the user is able to recover $\boldsymbol{W}_{\boldsymbol{\theta}}$.

For the PIR-PCSI-II setting the desired message is contained in the support set. The download will be $K-M+1$ linear equations in K unknowns (messages). These $K-M+1$ linear equations are independent by design, so they allow the user to eliminate any $K-M$ unknowns and get an equation in the remaining $K-(K-M) = M$ unknowns (messages). Let these M unknowns be the M messages in the support set. With careful design, the equation will be equal to $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} + \boldsymbol{\lambda}'\boldsymbol{W}_{\boldsymbol{\theta}}$

for some $\boldsymbol{\lambda}' \neq 0$. Thus by subtracting CSI from the equation the user is able to recover $\boldsymbol{W}_{\boldsymbol{\theta}}$.

Consider a scheme where the user applies *Specialized GRS Codes* when $\boldsymbol{\theta} \notin \boldsymbol{\mathcal{S}}$ and applies *Modified Specialized GRS Codes* when $\boldsymbol{\theta} \in \boldsymbol{\mathcal{S}}$. This scheme is obviously correct but not private because the server can tell if $\boldsymbol{\theta} \in \boldsymbol{\mathcal{S}}$ or not from the download cost since the download cost of the two schemes are different. However, if the user always downloads one more redundant equation when applying *Specialized GRS Codes*, then there is no difference in the download cost. This is essentially the idea for the achievable scheme.

Let us first present the *Specialized GRS Codes* in [33] here for ease of understanding. There are K distinct evaluation points in $\mathbb{F}_q$, namely $\omega_1, \cdots, \omega_K$. A polynomial $\boldsymbol{p}(x)$ is constructed as

$$\boldsymbol{p}(x) \triangleq \prod_{k \in [K] \setminus (\boldsymbol{\mathcal{S}} \cup \{\boldsymbol{\theta}\})} (x - \omega_k) \tag{201}$$

$$= \sum_{i=1}^{K-M} \boldsymbol{p}_i x^{i-1}. \tag{202}$$

The query $\boldsymbol{Q}$ is comprised of $K-M$ row vectors, each $1 \times K$, namely $\boldsymbol{Q}_1, \cdots, \boldsymbol{Q}_{K-M}$ such that

$$\boldsymbol{Q}_i = [\boldsymbol{v}_1 \omega_1^{i-1} \quad \cdots \quad \boldsymbol{v}_K \omega_K^{i-1}], \forall i \in [K-M], \tag{203}$$

where for $\boldsymbol{i}_m \in \boldsymbol{\mathcal{S}}, m \in [M]$, $\boldsymbol{v}_{\boldsymbol{i}_m} = \frac{\boldsymbol{\lambda}_m}{p(\omega_{\boldsymbol{i}_m})}$ ($\boldsymbol{\lambda}_m$ is the m^{th} coefficient in the CSI), while for $k \notin \boldsymbol{\mathcal{S}}$, $\boldsymbol{v}_k$ is randomly drawn from $\mathbb{F}_q^{\times}$. Upon receiving $\boldsymbol{Q}$, the server sends

$$\boldsymbol{\Delta} = \begin{bmatrix} \boldsymbol{\Delta}_1 \\ \vdots \\ \boldsymbol{\Delta}_{K-M} \end{bmatrix} = \begin{bmatrix} \boldsymbol{Q}_1 \\ \vdots \\ \boldsymbol{Q}_{K-M} \end{bmatrix} \begin{bmatrix} \boldsymbol{W}_1 \\ \boldsymbol{W}_2 \\ \vdots \\ \boldsymbol{W}_K \end{bmatrix} \tag{204}$$

to the user. Let us call $[\boldsymbol{Q}_1^{\mathrm{T}} \ \cdots \ \boldsymbol{Q}_{K-M}^{\mathrm{T}}]^{\mathrm{T}}$ the *Specialized GRS Matrix* and $[\boldsymbol{\Delta}_1 \ \cdots \ \boldsymbol{\Delta}_{K-M}]^{\mathrm{T}}$ *Specialized GRS Codes* of $\boldsymbol{W}_{[K]}$ for ease of reference. Note that the *Specialized GRS Matrix* is uniquely defined by $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_K$ as ω's are constants.

The user gets $\boldsymbol{W}_{\boldsymbol{\theta}}$ by subtracting $\boldsymbol{Y}^{[\boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}]}$ from

$$\sum_{i=1}^{K-M} \boldsymbol{p}_i \boldsymbol{\Delta}_i = \boldsymbol{Y}^{[\boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda}]} + \boldsymbol{v}_{\boldsymbol{\theta}} \boldsymbol{p}(\omega_{\boldsymbol{\theta}}) \boldsymbol{W}_{\boldsymbol{\theta}}. \tag{205}$$

Our PIR-PCSI scheme is as follows. For any realization $(\theta, \mathcal{S})$ of $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$, *1)* When $\theta \in [K] \setminus \mathcal{S}$, first apply the Specialized GRS Codes in [33]. Besides $Q_1, Q_2, \cdots, Q_{K-M}$ as specified in the *Specialized GRS Codes* of [33], the user also has

$$Q_{K-M+1} = [v_1 \omega_1^{K-M}, \cdots, v_K \omega_K^{K-M}] \tag{206}$$

as part of the query. And the answer $\boldsymbol{\Delta}_{K-M+1} = \sum_{j=1}^{K} v_j \omega_j^{K-M} \boldsymbol{W}_j$ will be generated for Q_{K-M+1} and downloaded by the user as a redundant equation. Note that the matrix $[Q_1^{\mathrm{T}}, Q_2^{\mathrm{T}}, \cdots, Q_{K-M+1}^{\mathrm{T}}]^{\mathrm{T}}$ is the generator matrix of a $(K, K-M+1)$ GRS code [37].

2) When $\theta \in \mathcal{S}$, the user will directly apply *Modified Specialized GRS Codes* where the queries also form a generator matrix of a $(K, K-M+1)$ GRS code as specified in [33].

Such a scheme is private since the queries in both cases form a generator matrix of a $(K, K-M+1)$ GRS code, and the $v_1, \cdots, v_K$ in both cases are identically uniform over $\mathbb{F}_q^{\times}$ for any realization of $\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}$.

For the corner case $M = 1$, it suffices to download $K-1$ generic linear combinations of all the K messages such that from the $K-1$ downloaded linear combinations and the CSI, all the K messages are decodable as noted in Remark 5.

XIV. Proof of Theorem 11

Here we bound the redundancy ρ_{PCSI} from above (equivalently, lower-bound α^*) for $1 \leq M \leq K$. For $\frac{K+2}{2} < M \leq K$, the proof for $\rho_{\text{PCSI}} = 0$ is the same as in Section V show that so it will not be repeated.

Consider an achievable scheme such that α-CSI is sufficient and the average download cost, $D \leq \frac{1}{C_{\text{PCSI}}^{\sup}} L + \epsilon L$ for some L. Note that $D \geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q})$, therefore,

$$H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) \leq \frac{1}{C_{\text{PCSI}}^{\sup}} L + \epsilon L \tag{207}$$

It follows from (207) that there exists a feasible $Q \in \mathcal{Q}$ such that

$$H(\boldsymbol{\Delta} \mid \boldsymbol{Q} = Q) \leq \frac{1}{C_{\text{PCSI}}^{\sup}} L + \epsilon L. \tag{208}$$

For all $i \in [K]$, let $\Lambda_i \in \mathfrak{C}$ satisfy

$$H(\boldsymbol{W}_i \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}^{[[M], \Lambda_i]}, \boldsymbol{Q} = Q) = 0. \tag{209}$$

The argument that such Λ_i's must exist is identical to the proof of Lemma 1. Writing $\overline{\boldsymbol{Y}}^{[[M], \Lambda_i]}$ as $\overline{\boldsymbol{Y}}_i$ for compact notation,

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]}, \boldsymbol{Q} = Q) \tag{210}$$

$$= H(\boldsymbol{W}_{[M]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_M, \boldsymbol{Q} = Q) + H(\boldsymbol{W}_{[M+1:K]} \mid \boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]}, \boldsymbol{W}_{[M]}, \boldsymbol{Q} = Q) \tag{211}$$

$$= 0 + H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{W}_{[M]}, \overline{\boldsymbol{Y}}_{[K]}, \boldsymbol{Q} = Q) \tag{212}$$

$$= 0. \tag{213}$$

where (212) follows from (209) and the fact that $\overline{\boldsymbol{Y}}_{[K]}$ are functions of $\boldsymbol{W}_{[M]}$. The last step also follows from (209). Thus,

$$\frac{1}{C_{\text{PCSI}}^{\sup}} L + \epsilon L + M \alpha L$$

$$\geq H(\boldsymbol{\Delta} \mid \boldsymbol{Q} = Q) + H(\overline{\boldsymbol{Y}}_{[M]} \mid \boldsymbol{Q} = Q) \tag{214}$$

$$\geq H(\boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]} \mid \boldsymbol{Q} = Q) \tag{215}$$

$$\geq I(\boldsymbol{\Delta}, \overline{\boldsymbol{Y}}_{[M]}; \boldsymbol{W}_{[K]} \mid \boldsymbol{Q} = Q) \tag{216}$$

$$= H(\boldsymbol{W}_{[K]} \mid \boldsymbol{Q} = Q) = KL. \tag{217}$$

(214) is true because (208), (25) hold. Step (217) follows from (209) and the fact that the query and messages are mutually independent according to (5). Thus, $\alpha \geq (K - \frac{1}{C_{\text{PCSI}}^{\sup}})/M - \epsilon/M$. In order to achieve capacity, we must have $\epsilon \to 0$, so we must have $\alpha \geq (K - \frac{1}{C_{\text{PCSI}}^{\sup}})/M$, for all $1 \leq M \leq K$.

Now note that for $M = 1$, since $C_{\text{PCSI}}^{\sup} = (K-1)^{-1}$, we have shown that $\alpha \geq 1$, which implies $\rho_{\text{PCSI}} = 0$ in this case.

For $2 \leq M \leq \frac{K+2}{2}$, since $C_{\text{PCSI}}^{\sup} = (K-M+1)^{-1}$, we have shown that $\alpha \geq \frac{M-1}{M}$, which implies $\rho_{\text{PCSI}} \leq \frac{1}{M}$ in this case.

It only remains to show that for $M = 2$, $\rho_{\text{PCSI}} = \frac{1}{2}$ is achievable, or equivalently, $\alpha^* = \frac{1}{2}$. For this case, let us present a PIR-PCSI scheme that achieves the rate $(K - M/2)^{-1}$ for arbitrary $1 \leq M \leq K$. Note that $K - M/2 = K - M + 1$ when $M = 2$, which is the only case where the supremum capacity is achieved by this scheme. The rate of this scheme is strictly smaller than $C_{\text{PCSI}}^{\text{sup}}$ for other $M \neq 2$.

Let the size of the base field q be an even power of a prime number such that $\sqrt{q}$ is a prime power and $\sqrt{q} \geq K$. For arbitrary realization $(\theta, \mathcal{S}) \in [K] \times \mathfrak{S}$ of $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$, if $\theta \in \mathcal{S}$, the user can apply the *Interference Alignment* based PIR-PCSI-II scheme where half of each message is downloaded. If $\theta \in [K] \backslash \mathcal{S}$, then user can apply the *Specialized GRS Codes* based scheme for the halves of the messages corresponding to the CSI dimension that is retained (while the other half of the CSI dimensions is discarded as redundant) and download the other half dimension of all the messages directly. Note that in both cases, a half-dimension of each of the K messages is directly downloaded. The other halves are involved in the download corresponding to the *Specialized GRS Codes* which is not needed for decodability/correctness if $\theta \in \mathcal{S}$, but is still included for privacy, i.e., to hide whether or not $\boldsymbol{\theta} \in \boldsymbol{\mathcal{S}}$. The download cost required is $K\left(\frac{L}{2}\right)$ for the direct downloads of half of every message, plus $(K - M)\frac{L}{2}$ for the *Specialized GRS Codes* based scheme that usually requires $K - M$ downloads per message symbol, but is applied here to only half the symbols from each message, for a total download cost of $(K - M/2)L$ which achieves the supremum capacity of PIR-PCSI for $M = 2$. The details of the scheme are presented next.

For all $k \in [K]$, let $V_{\boldsymbol{W}_k} \in \mathbb{F}_{\sqrt{q}}^{2\times 1}$ be the length 2 vector representation of $\boldsymbol{W}_k \in \mathbb{F}_q$. For all $m \in [M]$, let $M_{\boldsymbol{\lambda}_m} \in \mathbb{F}_{\sqrt{q}}^{2\times 2}$ be the matrix representation of $\boldsymbol{\lambda}_m \in \mathbb{F}_q^{\times}$ where $\boldsymbol{\lambda}_m$ is the m^{th} entry of the coefficient vector $\boldsymbol{\Lambda}$. Let

$$\overline{\boldsymbol{Y}}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]} = M_{\boldsymbol{\lambda}_1}(1,:)V_{\boldsymbol{W}_{i_1}} + \cdots + M_{\boldsymbol{\lambda}_M}(1,:)V_{\boldsymbol{W}_{i_M}}, \quad (218)$$

where $\boldsymbol{\mathcal{S}} = \{\boldsymbol{i}_1, \boldsymbol{i}_2, \cdots, \boldsymbol{i}_M\}$ is the support index set, be the processed CSI where $H(\overline{\boldsymbol{Y}}^{[\boldsymbol{\mathcal{S}},\boldsymbol{\Lambda}]}) = \frac{1}{2}H(\boldsymbol{W}_k)$. Note that $\forall m \in [M], M_{\boldsymbol{\lambda}_m}(1,:)$ is uniform over $\mathbb{F}_{\sqrt{q}}^{1\times 2} \setminus \{[0 \quad 0]\}$ according to Lemma 2.

The query $\boldsymbol{Q} = \{\boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{Q}_3\}$,

$$\boldsymbol{Q}_1 = \{\mathbf{L}_1, \mathbf{L}_2, \cdots, \mathbf{L}_K\}, \quad (219)$$

$$\boldsymbol{Q}_2 = \{\mathbf{L}'_1, \mathbf{L}'_2, \cdots, \mathbf{L}'_K\}, \quad (220)$$

$$\boldsymbol{Q}_3 = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_K\}. \quad (221)$$

where $\mathbf{L}_k, \mathbf{L}'_k \in \mathbb{F}_{\sqrt{q}}^{1\times 2} \setminus \{[0 \quad 0]\}$. $\mathbf{L}_k, \mathbf{L}'_k$ serve as two linearly independent projections that ask the server to split $\boldsymbol{W}_k$ into two halves

$$\boldsymbol{w}_k(1) = \mathbf{L}_k V_{\boldsymbol{W}_k} \in \mathbb{F}_{\sqrt{q}}, \quad (222)$$

$$\boldsymbol{w}_k(2) = \mathbf{L}'_k V_{\boldsymbol{W}_k} \in \mathbb{F}_{\sqrt{q}}. \quad (223)$$

$\boldsymbol{Q}_3$ uniquely defines a *Specialized GRS Matrix* whose elements are in $\mathbb{F}_{\sqrt{q}}$.

The user will download the first halves of all the K messages after projection, i.e., $\boldsymbol{w}_{[K]}(1)$ and apply the *Specialized GRS Matrix* to download a *Specialized GRS Codes* of the second halves of all the K messages after projection, i.e., $\boldsymbol{w}_{[K]}(2)$.

Let us specify $\mathbf{L}_k, \mathbf{L}'_k, \boldsymbol{v}_k$. Consider any realization $(\theta, \mathcal{S}) \in [K] \times \mathfrak{S}$ of $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$. Let us say $\mathcal{S} = \{i_1, i_2, \cdots, i_M\}$. For the messages not involved in the CSI, they are randomly projected to two linearly independent directions, i.e., for any $k \in [K] \backslash \mathcal{S}$, $\mathbf{L}_k, \mathbf{L}'_k$ are linearly independent and are randomly drawn from $\mathbb{F}_{\sqrt{q}}^{1\times 2} \setminus \{[0 \quad 0]\}$. Also, for any $k \in [K] \setminus \mathcal{S}$, $\boldsymbol{v}_k$ is uniformly distributed in $\mathbb{F}_{\sqrt{q}}^{\times}$.

For messages involved in the CSI, the construction of projections and $\boldsymbol{v}$'s depends on whether θ is in $\mathcal{S}$ or not.

1) When $\theta \in \mathcal{S}$, for any $m \in [M]$,

$$\mathbf{L}_{i_m} = \begin{cases} M_{\boldsymbol{\lambda}_m}(2,:), i_m = \theta, \\ M_{\boldsymbol{\lambda}_m}(1,:), i_m \neq \theta. \end{cases} \quad (224)$$

$\mathbf{L}'_{i_m}$ is then chosen randomly from $\mathbb{F}_{\sqrt{q}}^{1\times 2} \setminus \{[0 \quad 0]\}$ such that it is linearly independent with $\mathbf{L}_{i_m}$. Meanwhile, $\boldsymbol{v}_{i_m}$ is randomly drawn from $\mathbb{F}_{\sqrt{q}}^{\times}$. Under this case, the user has

$$\overline{\boldsymbol{Y}}^{[\mathcal{S},\boldsymbol{\Lambda}]} = \sum_{i_m \in \mathcal{S}\backslash\{\theta\}} \boldsymbol{w}_{i_m}(1) + \boldsymbol{w}_\theta(2) \quad (225)$$

according to the construction of $\mathbf{L}_{i_m}$. $\boldsymbol{w}_\theta(1)$ is directly downloaded and $\boldsymbol{w}_\theta(2)$ can be recovered by subtracting $\{\boldsymbol{w}_{i_m}(1)\}_{i_m \neq \theta}$ from $\overline{\boldsymbol{Y}}^{[\mathcal{S},\boldsymbol{\Lambda}]}$. The user is then able to recover $\boldsymbol{W}_\theta$ as the two projections are linearly independent. $\boldsymbol{Q}_3$ uniquely defines a *Specialized GRS Matrix* and applying $\boldsymbol{Q}_3$ to download a *Specialized GRS Codes* of $\boldsymbol{w}_{[K]}(2)$ is just for privacy.

2) When $\theta \in [K] \setminus \mathcal{S}$, for any $m \in [M]$,

$$\mathbf{L}'_{i_m} = \frac{1}{\boldsymbol{a}_m} M_{\boldsymbol{\lambda}_m}(1,:), \quad (226)$$

where $\boldsymbol{a}_m$ is randomly drawn from $\mathbb{F}_{\sqrt{q}}^{\times}$. $\mathbf{L}_{i_m}$ is then chosen randomly from $\mathbb{F}_{\sqrt{q}}^{1\times 2} \setminus \{[0 \quad 0]\}$ such that they are linearly independent with $\mathbf{L}'_{i_m}$. Under this case, the user has

$$\sum_{m\in[M]} \boldsymbol{a}_m \boldsymbol{w}_{i_m}(2) = \overline{\boldsymbol{Y}}^{[\mathcal{S},\boldsymbol{\Lambda}]}, \quad (227)$$

and sets

$$\boldsymbol{v}_{i_m} = \frac{\boldsymbol{a}_m}{p(\omega_{i_m})}, \forall m \in [M], \quad (228)$$

where $p(\omega_{i_m})$ is the evaluation of the polynomial specified in (202) (when $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}) = (\theta, \mathcal{S})$) at ω_{i_m}, which is a non-zero constant given $(\theta, \mathcal{S})$. Thus, given $(\theta, \mathcal{S})$, $\boldsymbol{v}_{i_m}$ is still uniform over $\mathbb{F}_{\sqrt{q}}^{\times}$. $\boldsymbol{Q}_3$ uniquely defines a *Specialized GRS Matrix*. Applying $\boldsymbol{Q}_3$ to download a *Specialized GRS Codes* of $\boldsymbol{w}_{[K]}(2)$, together with $\sum_{m\in[M]} \boldsymbol{a}_m \boldsymbol{w}_{i_m}(2)$ as the side information, enable the user to recover $\boldsymbol{w}_\theta(2)$. Since the first halves of all the projected messages are also downloaded, the user also has $\boldsymbol{w}_\theta(1)$, thus, is able to decode $\boldsymbol{W}_\theta$.

Note that for arbitrary realization $(\theta, \mathcal{S})$ of $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$, no matter $\theta \in \mathcal{S}$ or not, $\mathbf{L}_1, \cdots, \mathbf{L}_K$, $\mathbf{L}'_1, \cdots, \mathbf{L}'_K$, $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_K$ are independent, and for any $k \in [K]$, the matrix whose first row is

$\mathbf{L}_k$ and second row is $\mathbf{L}'_k$ is uniform over the set that contains all the full-rank matrix in $\mathbb{F}_{\sqrt{q}}^{2\times 2}$, $\boldsymbol{v}_k$ is uniform over $\mathbb{F}_{\sqrt{q}}^{\times}$. Thus, the scheme is private.

XV. Proof of Theorem 12

The rate $\frac{1}{K-1}$ PIR-PCSI-I scheme in Section XI-B is also the infimum capacity achieving PIR-PCSI scheme as noted in Remark 5, so we just prove the converse here.

As a result of (40) and the fact that in $\mathbb{F}_2$, we can only have $\boldsymbol{\Lambda} = 1_M$, i.e., the length-$M$ vector all of whose elements are equal to 1, we have

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},1_M]}, \boldsymbol{Q} = Q) = 0, \quad \forall (Q, \mathcal{S}) \in \mathcal{Q} \times \mathfrak{S}. \tag{229}$$

Writing $\boldsymbol{Y}^{[[M],1_M]}$ as $\boldsymbol{Y}$ for compact notation, for any $Q \in \mathcal{Q}$, we have

$$\begin{aligned} &H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) \\ &= H(\boldsymbol{W}_{[K]}, \boldsymbol{Y} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) && (230)\\ &= H(\boldsymbol{Y} \mid \boldsymbol{\Delta}, \boldsymbol{Q} = Q) + H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}, \boldsymbol{Q} = Q) && (231)\\ &\le H(\boldsymbol{Y}) = L. && (232) \end{aligned}$$

(230) is true since $\boldsymbol{Y}$ is a summation of the first M messages, and (231) follows from (229). Averaging over $\boldsymbol{Q}$ we have,

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \le L. \tag{233}$$

Thus, $D \ge H(\boldsymbol{\Delta} \mid \boldsymbol{Q}) \ge I(\boldsymbol{\Delta}; \boldsymbol{W}_{[K]} \mid \boldsymbol{Q}) = H(\boldsymbol{W}_{[K]}) - H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Q}) \ge KL - L$ which implies that $C^{\inf}_{\text{PCSI}}(q = 2) \le (K-1)^{-1}$.

XVI. Proof of Theorem 13

The rate $\frac{1}{K-1}$ PIR-PCSI-I scheme which preserves $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}}, \boldsymbol{\Lambda})$ in Section XII-C is also the capacity achieving PIR-PCSI scheme with private coefficients as noted in Remark 6, so we just prove the converse here. Specifically, we prove that $C^{\text{pri}}_{\text{PCSI}}(q) \le C_{\text{PCSI}}(q = 2) = C^{\inf}_{\text{PCSI}}$.

According to (123) in Lemma 6, for a fully private PIR-PCSI scheme,

$$H(\boldsymbol{W}_{[K]} \mid \boldsymbol{\Delta}, \boldsymbol{Y}^{[\mathcal{S},\Lambda]}, \boldsymbol{Q} = Q) = 0, \quad \forall (Q, \mathcal{S}, \Lambda) \in \mathcal{Q} \times \mathfrak{S} \times \mathfrak{C}. \tag{234}$$

Note that (234) is a *stronger* version of (229) which is sufficient to bound $C_{\text{PCSI}}(q = 2) = C^{\inf}_{\text{PCSI}}$. Thus, $C^{\text{pri}}_{\text{PCSI}}(q) \le C^{\inf}_{\text{PCSI}}$.

XVII. Conclusion

Side-information is a highly valuable resource for PIR in general, and for single-server PIR in particular. Building on the foundation laid by Heidarzadeh et al. [33], this work presents a more complete picture, as encapsulated in Table I, revealing new insights that are described in the introduction. The redundancy of side-information is particularly noteworthy, because it allows the user to save storage cost, which may be used to store additional non-redundant side-information, e.g., multiple linear combinations instead of just one, as assumed in this work and in [33]. An interesting direction for future work is to understand the trade-off between the size of side information and the efficiency of single-server PIR, e.g., by characterizing the α-CSI constrained capacity of PIR-PCSI-I, PIR-PCSI-II, PIR-PCSI. Other questions that remain open include issues that are field-specific. For example, is the supremum capacity of PIR-PCSI-II for $M > 2$ achievable for all fields except $\mathbb{F}_2$? Are there other fields besides $\mathbb{F}_2$ over which the capacity is equal to the infimum capacity? Can the capacity over certain fields take values other than the supremum and infimum capacities? Progress on these issues may require field-dependent constructions of interference alignment schemes for achievability, and combinatorial arguments for converse bounds, both of which may be of broader interest.

Appendix

A. Proof of Lemma 5

For all $k \in [K], m \in [M-1]$, let us say

$$\mathbf{L}_k^{(m)} = \begin{bmatrix} x_{k,1}^{(m)} & x_{k,2}^{(m)} & \cdots & x_{k,M}^{(m)} \end{bmatrix}, \tag{235}$$

where $x_{\cdot,\cdot}^{(\cdot)} \in \mathbb{F}_{q^l}$. Let

$$\mathbf{H}_k = \begin{bmatrix} \mathbf{L}_k^{(1)^{\mathrm{T}}} & \mathbf{L}_k^{(2)^{\mathrm{T}}} & \cdots & \mathbf{L}_k^{(M-1)^{\mathrm{T}}} \end{bmatrix}^{\mathrm{T}}. \tag{236}$$

Let us denote by $\mathcal{S}_1, \mathcal{S}_2, \cdots \mathcal{S}_{\binom{K}{M}}$, the $\binom{K}{M}$ distinct elements of $\mathfrak{S}$. Let $\mathcal{S}_1 = [M]$. Then $\mathbf{G}_{\mathcal{S}_1}$ can be written as

$$\mathbf{G}_{\mathcal{S}_1} = \begin{bmatrix} \lambda_1 \mathbf{I}_M & \lambda_2 \mathbf{I}_M & \cdots & \lambda_M \mathbf{I}_M \\ \mathbf{H}_1 & \mathbf{0}_{(M-1)\times M} & \cdots & \mathbf{0}_{(M-1)\times M} \\ \mathbf{0}_{(M-1)\times M} & \mathbf{H}_2 & \cdots & \mathbf{0}_{(M-1)\times M} \\ \vdots & & \ddots & \\ \mathbf{0}_{(M-1)\times M} & \mathbf{0}_{(M-1)\times M} & \cdots & \mathbf{H}_M \end{bmatrix} \tag{237}$$

which is an $M^2 \times M^2$ matrix. Note that

$$\det(\mathbf{G}_{\mathcal{S}_1}) = f_1(x_{1,1}^{(1)}, \cdots, x_{M,M}^{(M-1)}), \tag{238}$$

where $f_1(\cdot)$ is an $M^2(M-1)$-variate polynomial with degree $\deg(f_1) = M(M-1)$. To verify that $f_1(\cdot)$ is not the zero polynomial, note that if each $\mathbf{H}_m, m \in [M]$ is chosen as the $(M-1)\times M$ matrix obtained by inserting the all-zero column into the $(M-1)\times(M-1)$ identity matrix after its first $m-1$ columns, then $\det(\mathbf{G}_{\mathcal{S}_1}) = \lambda_1\lambda_2\cdots\lambda_M \neq 0$.

Similarly, $\forall j \in [2 : \binom{K}{M}]$,

$$\det(\mathbf{G}_{\mathcal{S}_j}) = f_j\Big((x_{k,1}^{(m)}, \cdots x_{k,M}^{(m)})_{k\in\mathcal{S}_j, m\in[M-1]}\Big), \tag{239}$$

where $f_j(\cdot)$ is an $M^2(M-1)$-variate polynomial with degree $\deg(f_j) = M(M-1)$.

Now, to satisfy the correctness and privacy constraints, we must choose all $\mathbf{L}_k^{(m)}$ to simultaneously have all the polynomials $f_j(\cdot)$ evaluate to non-zero values. Equivalently, the polynomial f that is the product of all $f_j(\cdot)$ should evaluate to a non-zero value.

$$\prod_{j\in[\binom{K}{M}]} \det(\mathbf{G}_{\mathcal{S}_j}) = \prod_{j\in[\binom{K}{M}]} f_j = f \neq 0, \tag{240}$$

where f is a $KM(M-1)$-variate polynomial with degree

$$\deg(f) = \prod_{j\in[\binom{K}{M}]} \deg(f_j) = \tbinom{K}{M}M(M-1). \tag{241}$$

Now, since it is a product of non-zero polynomials, f is also a non-zero polynomial. Therefore, by Schwartz-Zippel Lemma, if the values of the $KM(M-1)$ variables are randomly chosen from $\mathbb{F}_{q^l}$, then the probability of the polynomial f evaluating to 0 is bounded as,

$$\Pr(f=0) \leq \frac{\deg(f)}{q^l} = \frac{\binom{K}{M}M(M-1)}{q^l}. \tag{242}$$

Therefore, if $q^l > \binom{K}{M}M(M-1)$, then $\Pr(f=0) < 1$, which implies that there exists a choice of the $KM(M-1)$ variables such that $f \neq 0$. That choice satisfies the condition of Lemma 5, thus completing the proof of Lemma 5.

For ease of understanding, consider the following example.

Example 4: Consider $M = 3$, $K = 4$ messages: $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$, each of which consists $Ml = 3l$ symbols in $\mathbb{F}_3$. Message $\boldsymbol{A}$ can be represented as a length $M = 3$ column vector with all the 3 entries in $\mathbb{F}_{3^l}$, i.e., $V_{\boldsymbol{A}} \in \mathbb{F}_{3^l}^{3\times 1}$. $V_{\boldsymbol{B}}, V_{\boldsymbol{C}}, V_{\boldsymbol{D}}$ are similarly defined.

Let us say $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ are in the support set and $\boldsymbol{Y} = 2\boldsymbol{A} + \boldsymbol{B} + \boldsymbol{C}$. $\boldsymbol{Y}$ can also be represented by $V_{\boldsymbol{Y}} \in \mathbb{F}_{3^l}^{3\times 1}$ where

$$V_{\boldsymbol{Y}} = 2\mathbf{I}_3 V_{\boldsymbol{A}} + \mathbf{I}_3 V_{\boldsymbol{B}} + \mathbf{I}_3 V_{\boldsymbol{C}}. \tag{243}$$

For each one of $V_{\boldsymbol{A}}, V_{\boldsymbol{B}}, V_{\boldsymbol{C}}, V_{\boldsymbol{D}}$, the user will download $M-1=2$ linear combinations. For example, the download corresponding to $V_{\boldsymbol{A}}$ is,

$$\boldsymbol{\Delta}_{\boldsymbol{A}} = \begin{bmatrix} \mathbf{L}_1^{(1)} \\ \mathbf{L}_1^{(2)} \end{bmatrix} V_{\boldsymbol{A}} = \mathbf{H}_1 V_{\boldsymbol{A}}, \tag{244}$$

where $\mathbf{L}_1^{(1)}, \mathbf{L}_1^{(2)} \in \mathbb{F}_{3^l}^{1\times 3}$, and $\boldsymbol{\Delta}_{\boldsymbol{A}} \in \mathbb{F}_{3^l}^{2\times 1}$. Similarly, the user downloads

$$\boldsymbol{\Delta}_{\boldsymbol{B}} = \mathbf{H}_2 V_{\boldsymbol{B}}, \boldsymbol{\Delta}_{\boldsymbol{C}} = \mathbf{H}_3 V_{\boldsymbol{C}}, \boldsymbol{\Delta}_{\boldsymbol{D}} = \mathbf{H}_4 V_{\boldsymbol{D}} \tag{245}$$

Regarding messages $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$, the user has

$$\begin{bmatrix} V_{\boldsymbol{Y}} \\ \boldsymbol{\Delta}_{\boldsymbol{A}} \\ \boldsymbol{\Delta}_{\boldsymbol{B}} \\ \boldsymbol{\Delta}_{\boldsymbol{C}} \end{bmatrix} = \underbrace{\begin{bmatrix} 2\mathbf{I}_3 & \mathbf{I}_3 & \mathbf{I}_3 \\ \mathbf{H}_1 & \mathbf{0}_{2\times 3} & \mathbf{0}_{2\times 3} \\ \mathbf{0}_{2\times 3} & \mathbf{H}_2 & \mathbf{0}_{2\times 3} \\ \mathbf{0}_{2\times 3} & \mathbf{0}_{2\times 3} & \mathbf{H}_3 \end{bmatrix}}_{\mathbf{G}_{\{1,2,3\}}} \begin{bmatrix} V_{\boldsymbol{A}} \\ V_{\boldsymbol{B}} \\ V_{\boldsymbol{C}} \end{bmatrix} \tag{246}$$

To recover $V_{\boldsymbol{A}}, V_{\boldsymbol{B}}, V_{\boldsymbol{C}}$ and thus recover $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$, $\mathbf{G}_{\{1,2,3\}} \in \mathbb{F}_{3^l}^{9\times 9}$ must have full rank. Let us explicitly write down $\mathbf{G}_{\{1,2,3\}}$ as

$$\begin{bmatrix} 2 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 1 \\ x_{1,1}^{(1)} & x_{1,2}^{(1)} & x_{1,3}^{(1)} & 0 & 0 & 0 & 0 & 0 & 0 \\ x_{1,1}^{(2)} & x_{1,2}^{(2)} & x_{1,3}^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_{2,1}^{(1)} & x_{2,2}^{(1)} & x_{2,3}^{(1)} & 0 & 0 & 0 \\ 0 & 0 & 0 & x_{2,1}^{(2)} & x_{2,2}^{(2)} & x_{2,3}^{(2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{3,1}^{(1)} & x_{3,2}^{(1)} & x_{3,3}^{(1)} \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{3,1}^{(2)} & x_{3,2}^{(2)} & x_{3,3}^{(2)} \end{bmatrix}.$$

Now note that $\det(\mathbf{G}_{\{1,2,3\}}) = f_1$ is an $M^2(M-1) = 18$-variate non-zero polynomial of degree 6. The polynomial is non-zero because e.g., setting the variables shown in red color as 1 and the rest of the variables to 0, yields the evaluation $f_1 = \lambda_1\lambda_2\lambda_3 = 2$.

To ensure the joint privacy of $(\boldsymbol{\theta}, \boldsymbol{\mathcal{S}})$, the matrix

$$\mathbf{G}_{\{1,2,4\}} = \begin{bmatrix} 2\mathbf{I}_3 & \mathbf{I}_3 & \mathbf{I}_3 \\ \mathbf{H}_1 & \mathbf{0}_{2\times 3} & \mathbf{0}_{2\times 3} \\ \mathbf{0}_{2\times 3} & \mathbf{H}_2 & \mathbf{0}_{2\times 3} \\ \mathbf{0}_{2\times 3} & \mathbf{0}_{2\times 3} & \mathbf{H}_4 \end{bmatrix} \tag{247}$$

should also be invertible, which enables the user to recover $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{D}$ if the CSI is $2\boldsymbol{A} + \boldsymbol{B} + \boldsymbol{D}$. Similarly, $\mathbf{G}_{\{1,3,4\}}, \mathbf{G}_{\{2,3,4\}}$ should also be invertible. Let

$$f_2 = \det(\mathbf{G}_{\{1,2,4\}}), f_3 = \det(\mathbf{G}_{\{1,3,4\}}), f_4 = \det(\mathbf{G}_{\{2,3,4\}}).$$

Similarly, f_2, f_3, f_4 are 18-variate polynomials of degree 6. Thus $f = f_1 f_2 f_3 f_4$ is a $KM(M-1) = 24$-variate non-zero polynomial of degree $\binom{K}{M}M(M-1) = 24$. According to Schwartz-Zippel Lemma, if the 24 variables are randomly chosen from $\mathbb{F}_{3^l}$,

$$\Pr(f=0) \leq \frac{\deg(f)}{3^l} = \frac{24}{3^l}. \tag{248}$$

When $l \geq 3$ we have $\Pr(f=0) < 1$ which implies that there exists a choice of the 24 variable such that $f \neq 0$ and $\mathbf{G}_{\{1,2,3\}}, \mathbf{G}_{\{1,2,4\}}, \mathbf{G}_{\{1,3,4\}}, \mathbf{G}_{\{2,3,4\}}$ are all invertible.

REFERENCES

[1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proc. 36th Annu. Symp. Found. Comput. Sci.*, 1995, pp. 41–50.

[2] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[3] H. Sun and S. A. Jafar, "The capacity of private information retrieval," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4075–4088, Jul. 2017.

[4] N. B. Shah, K. V. Rashmi, and K. Ramchandran, "One extra bit of download ensures perfectly private information retrieval," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 856–860.

[5] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, and C. Hollanti, "Private information retrieval from coded storage systems with colluding, Byzantine, and unresponsive servers," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3898–3906, Jun. 2019.

[6] H. Sun and S. A. Jafar, "The capacity of robust private information retrieval with colluding databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2361–2370, Apr. 2018.

[7] H. Sun and S. A. Jafar, "The capacity of symmetric private information retrieval," *IEEE Trans. Inf. Theory*, vol. 65, no. 1, pp. 322–329, Jan. 2018.

[8] K. Banawan and S. Ulukus, "The capacity of private information retrieval from Byzantine and colluding databases," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 1206–1219, Feb. 2019.

[9] Q. Wang and M. Skoglund, "On PIR and symmetric PIR from colluding databases with adversaries and eavesdroppers," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 3183–3197, May 2018.

[10] Q. Wang and M. Skoglund, "Linear symmetric private information retrieval for MDS coded distributed storage with colluding servers," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2017, pp. 71–75.

[11] R. Freij-Hollanti, O. Gnilke, C. Hollanti, and D. Karpuk, "Private information retrieval from coded databases with colluding servers," *SIAM J. Appl. Algebra Geometry*, vol. 1, no. 1, pp. 647–664, 2017.

[12] H. Sun and S. A. Jafar, "Private information retrieval from MDS coded data with colluding servers: Settling a conjecture by Freij-Hollanti," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 1000–1022, Feb. 2018.

[13] Q. Wang and M. Skoglund, "Symmetric private information retrieval from MDS coded distributed storage with non-colluding and colluding servers," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5160–5175, Aug. 2019.

[14] Z. Jia, H. Sun, and S. A. Jafar, "Cross subspace alignment and the asymptotic capacity of X-secure T-private information retrieval," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5783–5798, Sep. 2019.

[15] Z. Jia and S. A. Jafar, "X-secure T-private information retrieval from MDS coded storage with byzantine and unresponsive servers," *IEEE Trans. Inf. Theory*, vol. 66, no. 12, pp. 7427–7438, Dec. 2020.

[16] H. Yang, W. Shin, and J. Lee, "Private information retrieval for secure distributed storage systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 12, pp. 2953–2964, Dec. 2018.

[17] Z. Jia and S. A. Jafar, "On the asymptotic capacity of X-secure T-private information retrieval with graph-based replicated storage," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6280–6296, Oct. 2020.

[18] R. Tandon, "The capacity of cache aided private information retrieval," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2017, pp. 1078–1082.

[19] Y. Wei, K. Banawan, and S. Ulukus, "Fundamental limits of cache-aided private information retrieval with unknown and uncoded prefetching," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 3215–3232, May 2019.

[20] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, C. Hollanti, and S. E. Rouayheb, "Private information retrieval schemes for coded data with arbitrary collusion patterns," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1908–1912.

[21] X. Yao, N. Liu, and W. Kang, "The capacity of private information retrieval under arbitrary collusion patterns for replicated databases," *IEEE Trans. Inf. Theory*, vol. 67, no. 10, pp. 6841–6855, Oct. 2021.

[22] 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 J. Sel. Areas Commun.*, vol. 40, no. 3, pp. 729–748, Mar. 2022.

[23] S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb, and A. Sprintson, "Private information retrieval with side information," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2032–2043, Apr. 2020.

[24] Z. Chen, Z. Wang, and S. Jafar, "The capacity of T-private information retrieval with private side information," *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 4761–4773, Aug. 2020.

[25] A. Heidarzadeh, B. Garcia, S. Kadhe, S. E. Rouayheb, and A. Sprintson, "On the capacity of single-server multi-message private information retrieval with side information," in *Proc. 56th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2018, pp. 180–187.

[26] S. Li and M. Gastpar, "Single-server multi-user private information retrieval with side information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 1954–1958.

[27] S. Li and M. Gastpar, "Single-server multi-message private information retrieval with side information: The general cases," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 1083–1088.

[28] F. Kazemi, E. Karimi, A. Heidarzadeh, and A. Sprintson, "Single-server single-message online private information retrieval with side information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 350–354.

[29] A. Heidarzadeh, S. Kadhe, S. E. Rouayheb, and A. Sprintson, "Single-server multi-message individually-private information retrieval with side information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1042–1046.

[30] A. Heidarzadeh, F. Kazemi, and A. Sprintson, "Capacity of single-server single-message private information retrieval with coded side information," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.

[31] A. Heidarzadeh, F. Kazemi, and A. Sprintson, "Capacity of single-server single-message private information retrieval with private coded side information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1662–1666.

[32] Y.-P. Wei, K. Banawan, and S. Ulukus, "The capacity of private information retrieval with partially known private side information," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8222–8231, Dec. 2019.

[33] A. Heidarzadeh, F. Kazemi, and A. Sprintson, "The role of coded side information in single-server private information retrieval," *IEEE Trans. Inf. Theory*, vol. 67, no. 1, pp. 25–44, Jan. 2021.

[34] A. Heidarzadeh and A. Sprintson, "The role of reusable and single-use side information in private information retrieval," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2022, pp. 414–419.

[35] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, U.K.: Cambridge Univ. Press, 1994.

[36] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

[37] R. M. Roth, "Introduction to coding theory," *IET Commun.*, vol. 47, nos. 18–19, p. 4, 2006.

Yuxiang Lu (Graduate Student Member, IEEE) received the B.E. degree in information engineering from the Southeast University, Nanjing, Jiangsu, China, in 2019, and the M.S. degree in electrical and computer engineering from the University of California Irvine, Irvine, CA, USA, in 2021, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His research interests include information theory and its application to distributed computation, privacy, and security.

Syed A. Jafar (Fellow, IEEE) received the B.Tech. degree in electrical engineering from IIT Delhi, India, in 1997, the M.S. degree in electrical engineering from Caltech, USA, in 1999, and the Ph.D. degree in electrical engineering from Stanford, USA, in 2003.

His industry experience includes positions with the Lucent Bell Laboratories and Qualcomm. He is currently a Chancellor's Professor of electrical engineering and computer science with the University of California Irvine, Irvine, CA, USA. His research interests include multiuser information theory, wireless communications, and network coding. He was an University of Canterbury Erskine Fellow, an IEEE Communications Society Distinguished Lecturer, an IEEE Information Theory Society Distinguished Lecturer, and a Thomson Reuters/Clarivate Analytics Highly Cited Researcher. He was a recipient of the New York Academy of Sciences Blavatnik National Laureate in physical sciences and engineering, the NSF CAREER Award, the ONR Young Investigator Award, the UCI Academic Senate Distinguished Mid-Career Faculty Award for Research, the School of Engineering Mid-Career Excellence in Research Award, and the School of Engineering Maseeh Outstanding Research Award. His coauthored papers received the IEEE Information Theory Society Paper Award, the IEEE Communication Society and Information Theory Society Joint Paper Award, the IEEE Communications Society Best Tutorial Paper Award, the IEEE Communications Society Heinrich Hertz Award, the IEEE Signal Processing Society Young Author Best Paper Award, the IEEE Information Theory Society Jack Wolf ISIT Best Student Paper Award, and three IEEE GLOBECOM Best Paper Awards. He received the UC Irvine EECS Professor of the Year award six times from the Engineering Students Council, the School of Engineering Teaching Excellence Award in 2012, and the Senior Career Innovation in Teaching Award in 2018. He served as an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS from 2004 to 2009, IEEE COMMUNICATIONS LETTERS from 2008 to 2009, and IEEE TRANSACTIONS ON INFORMATION THEORY from 2009 to 2012.