Capacity of Single-Server Single-Message Private Information Retrieval with Private Coded Side Information

Anoosheh Heidarzadeh, Fatemeh Kazemi, and Alex Sprintson

***Abstract*— We study the problem of single-server single-message Private Information Retrieval with Private Coded Side Information (PIR-PCSI). In this problem, there is a server that stores a database, and a user who knows a random linear combination of a random subset of messages in the database. The number of messages contributing to the user's side information is known to the server a priori, whereas the indices and the coefficients of these messages are unknown to the server a priori. The user wants to retrieve a message from the server, while protecting the identities of both the demand message and the side information messages.**

Depending on whether the demand is part of the coded side information or not, we consider two different models for the problem. For the model in which the demand does not contribute to the side information, we prove a lower bound on the minimum download cost for all (linear and non-linear) PIR schemes; and for the model wherein the demand is one of the messages contributing to the side information, we prove a lower bound for all scalar-linear PIR protocols. In addition, we propose novel PIR protocols that achieve these lower bounds.

I. INTRODUCTION

In the information-theoretic Private Information Retrieval (PIR) problem (see, e.g., [1], [2]), there is a user that wishes to download a single or multiple messages belonging to a database stored on a single or multiple (non-colluding or colluding) servers. The goal of the user is to minimize the download cost (i.e., the amount of information downloaded from the server(s)), while hiding the identity of its demanded message(s) from the server(s). This setup was recently extended in [3]–[12] to the settings wherein the user has some side information about the messages in the database, and the side information is unknown to the server(s).

For the single-server setting of the PIR problem in the presence of some side information, we studied the cases in which the side information is a random subset of messages (a.k.a. PIR with Side Information (PIR-SI)) and a random linear combination of a random subset of messages (a.k.a. PIR with Coded Side Information (PIR-CSI)) in [3], [11] and [9], respectively. The multi-server setting of the PIR-SI problem was also studied in [7], [8], [10]. For the PIR-SI problem, two different types of privacy, known as W*-privacy* (i.e., only the identities of the demand messages must be protected) and (W, S)*-privacy* (i.e., the identities of both the demand and side information messages must be protected jointly) have been considered, whereas the problem of PIR-CSI has only been studied when W-privacy is required.

In this work, we study the single-server single-message PIR-CSI problem where (W, S)-privacy is required. In this problem, referred to as *PIR with Private Coded Side Information (PIR-PCSI)*, there is a single server storing a database of K messages, and there is a user who knows a random linear combination of a random subset of M messages in the database. The user is interested in downloading a single message from the server while preserving the privacy of both the demand message and the messages contributing to the side information. This problem setting can be motivated by several practical scenarios. For instance, the user may have obtained their side information via overhearing in a wireless network; or from a trusted server with limited knowledge about the database; or from the information locally stored in the user's cache of limited size.

A. Main Contributions

We define the (scalar-linear) capacity of the PIR-PCSI problem as the supremum of all achievable rates (i.e., the ratio of the entropy of a message to the entropy of the download cost) over all (scalar-linear) PIR-PCSI protocols. Depending on whether the user's demanded message itself contributes to the user's coded side information or not, we consider two different models of the problem.

For the model in which the demanded message is not part of the side information, we characterize the capacity and the scalar-linear capacity. In particular, we show that for this model the capacity and the scalar-linear capacity are both equal to $(K-M)^{-1}$ for any $0 \leq M \leq K-1$. This is interesting because, as shown in [3, Theorem 2], even when the user knows M randomly chosen (uncoded) messages as their side information, in order to guarantee (W, S)-privacy, the capacity is equal to $(K-M)^{-1}$.

For the model wherein the user's demanded message contributes to their side information, we show that the scalar-linear capacity is equal to $(K-M+1)^{-1}$ for any $2 \leq M \leq K$. Interestingly, this result shows that when the user knows $M-1$ randomly chosen messages (different from the demand), achieving (W, S)-privacy is as costly as that when the user knows only *one* random linear combination of their demanded message and $M-1$ other random messages.

The converse proofs are based on new information-theoretic arguments, and the proofs of achievability rely on novel PIR protocols based on the Generalized Reed-Solomon (GRS) codes that contain a specific codeword which depends

The authors are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (E-mail: {anoosheh, fatemeh.kazemi, spalex}@tamu.edu).

This material is based upon work supported by the National Science Foundation under Grants No. 1718658 and 1642983.

on the coefficients and the indices of messages in the side information and the index of the demanded message.

II. Problem Formulation

Throughout, we denote random variables and their realizations by bold-face letters and regular letters, respectively.

Let $\mathbb{F}_q$ be a finite field for some prime q, and let $\mathbb{F}_{q^l}$ be an extension field of $\mathbb{F}_q$ for some integer $l \geq 1$, and let $L \triangleq l \log_2 q$. For an integer $i \geq 1$, let $[i] \triangleq \{1, \ldots, i\}$. Let $K \geq 1$ and $0 \leq M \leq K$ be two integers. We denote by $\mathcal{S}$ the set of all M-subsets of $[K]$, and denote by $\mathcal{C}$ the set of all length-M sequences with elements from $\mathbb{F}_q^{\times} \triangleq \mathbb{F}_q \setminus \{0\}$.

Assume that there is a server that stores a set of K messages, denoted by $X \triangleq \{X_1, \ldots, X_K\}$, where each message X_i is independently and uniformly distributed over $\mathbb{F}_{q^l}$, i.e., $H(\mathbf{X}_i) = L$ for $i \in [K]$ and $H(\mathbf{X}) = KL$, where $\mathbf{X} \triangleq \{\mathbf{X}_1, \ldots, \mathbf{X}_K\}$. Also assume that there is a user that wishes to retrieve a message X_W from the server for some $W \in [K]$, and knows a linear combination $Y^{[S,C]} \triangleq \sum_{i \in S} c_i X_i$ for some $S \triangleq \{i_1, \ldots, i_M\} \in \mathcal{S}$ and $C \triangleq \{c_{i_1}, \ldots, c_{i_M}\} \in \mathcal{C}$. We refer to W as the *demand index*, X_W as the *demand*, S as the *side information index set*, $Y^{[S,C]}$ as the *side information*, and M as the *side information size*.

We assume that $\mathbf{S}$ is uniformly distributed over $\mathcal{S}$, and $\mathbf{C}$ is uniformly distributed over $\mathcal{C}$. Also, we consider two different models as follows for the conditional distribution of $\mathbf{W}$ given $\mathbf{S} = S$:

Model I: $\mathbf{W}$ is uniformly distributed over $[K] \setminus S$;

Model II: $\mathbf{W}$ is uniformly distributed over S.

To avoid the degenerate cases, we assume $0 \leq M \leq K-1$ and $2 \leq M \leq K$ for the models I and II, respectively. Note that $\Pr(\mathbf{W} = W, \mathbf{S} = S | \mathbf{W} \notin \mathbf{S})$ is equal to $((K-M)\binom{K}{M})^{-1}$ for all $W \in [K], S \in \mathcal{S}$ such that $W \notin S$, and it is zero otherwise; and $\Pr(\mathbf{W} = W, \mathbf{S} = S | \mathbf{W} \in \mathbf{S})$ is equal to $(M\binom{K}{M})^{-1}$ for all $W \in [K], S \in \mathcal{S}$ such that $W \in S$, and it is zero otherwise.

We assume that *a priori* the server knows the underlying problem model (i.e., $\mathbf{W} \notin \mathbf{S}$ or $\mathbf{W} \in \mathbf{S}$), the side information size (M), the distributions of $\mathbf{S}$ and $\mathbf{C}$, and the conditional distribution of $\mathbf{W}$ given $\mathbf{S}$; whereas the realizations S, C, and W are unknown to the server *a priori*.

For any S, C, W, in order to retrieve X_W, the user sends to the server a query $Q^{[W,S,C]}$, which is a (potentially stochastic) function of W, S, C. We denote $\mathbf{Q}^{[\mathbf{W},\mathbf{S},\mathbf{C}]}$ by $\mathbf{Q}$. The query must protect the privacy of both the user's demand index and side information index set from the server. That is, for any $\theta \in \{0, 1\}$, it must hold that

$$\begin{aligned}&\Pr(\mathbf{W} = W, \mathbf{S} = S | \mathbf{Q} = Q, \mathbb{1}_{\{\mathbf{W} \in \mathbf{S}\}} = \theta, \mathbf{X} = X)\\ &\quad = \Pr(\mathbf{W} = W, \mathbf{S} = S | \mathbb{1}_{\{\mathbf{W} \in \mathbf{S}\}} = \theta)\end{aligned}$$

for all $W \in [K], S \in \mathcal{S}$. We refer to this condition as the (W, S)-*privacy condition*. Note that (W, S)-privacy is a stronger condition than W-privacy considered in [9], where the query must protect only the privacy of the user's demand index from the server.

Upon receiving $Q^{[W,S,C]}$, the server sends to the user an answer $A^{[W,S,C]}$, which is a (deterministic) function of the query $Q^{[W,S,C]}$, the indicator variable $\mathbb{1}_{\{W \in S\}}$, and the messages in X. We denote $\mathbf{A}^{[\mathbf{W},\mathbf{S},\mathbf{C}]}$ by $\mathbf{A}$. Note that $(\mathbf{W}, \mathbf{S}) \to (\mathbf{Q}, \mathbb{1}_{\{\mathbf{W} \in \mathbf{S}\}}, \mathbf{X}) \to \mathbf{A}$ forms a Markov chain, and $H(\mathbf{A} | \mathbf{Q}, \mathbb{1}_{\{\mathbf{W} \in \mathbf{S}\}}, \mathbf{X}) = 0$. The answer $A^{[W,S,C]}$ along with $Q^{[W,S,C]}, \mathbb{1}_{\{W \in S\}}, Y^{[S,C]}$, and W, S, C must enable the user to retrieve the demand X_W. That is, it must hold that

$$H(\mathbf{X}_{\mathbf{W}} | \mathbf{A}, \mathbf{Q}, \mathbb{1}_{\{\mathbf{W} \in \mathbf{S}\}}, \mathbf{Y}^{[\mathbf{S},\mathbf{C}]}, \mathbf{W}, \mathbf{S}, \mathbf{C}) = 0.$$

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

The following lemma, which follows from a simple contradiction and hence appears without proof, gives a necessary condition for (W, S)-privacy and recoverability.

Lemma 1. *For any $\theta \in \{0, 1\}$, for any $W \in [K]$, $S \in \mathcal{S}$ such that $\mathbb{1}_{\{W \in S\}} = \theta$, there must exist $C \in \mathcal{C}$ such that*

$$H(\mathbf{X}_W | \mathbf{A}, \mathbf{Q}, \mathbb{1}_{\{\mathbf{W} \in \mathbf{S}\}} = \theta, \mathbf{Y}^{[S,C]}) = 0.$$

For each model (I or II), the problem is to design a protocol for generating a query $Q^{[W,S,C]}$ (and the corresponding answer $A^{[W,S,C]}$, given $Q^{[W,S,C]}$, $\mathbb{1}_{\{W \in S\}}$, and X) for any given W, S, C, such that both the privacy and recoverability conditions are satisfied. We refer to this problem as *single-server Private Information Retrieval (PIR) with Private Coded Side Information (PCSI)*, or *PIR-PCSI* for short. The PIR-PCSI problem under the model I or model II is referred to as *PIR-PCSI–I* or *PIR-PCSI–II*, respectively.

The *rate* of a PIR-PCSI–I (or PIR-PCSI–II) protocol is defined as the ratio of the entropy of a message, i.e., L, to the conditional entropy of the answer $\mathbf{A}^{[\mathbf{W},\mathbf{S},\mathbf{C}]}$ given that $\mathbf{W} \notin \mathbf{S}$ (or $\mathbf{W} \in \mathbf{S}$). The *capacity* of PIR-PCSI–I (or PIR-PCSI–II) problem is defined as the supremum of rates over all PIR-PCSI–I (or PIR-PCSI–II) protocols. The supremum of rates over all scalar-linear PIR-PCSI–I (or PIR-PCSI–II) protocols, i.e., where the answer contains only scalar-linear combinations of the messages in X, is defined as the *scalar-linear capacity* of PIR-PCSI–I (or PIR-PCSI–II) problem.

In this work, our goal is to characterize the capacity and the scalar-linear capacity of the PIR-PCSI–I and PIR-PCSI–II problems, and to design PIR-PCSI–I and PIR-PCSI–II protocols that are capacity-achieving.

III. Main Results

We present our main results in this section. The capacity and the scalar-linear capacity of PIR-CSI–I problem are characterized in Theorem 1, and the scalar-linear capacity of PIR-CSI–II problem is characterized in Theorem 2. The proofs are given in Sections IV and V.

Theorem 1. *The capacity and the scalar-linear capacity of PIR-PCSI–I problem with K messages and side information size $0 \leq M \leq K-1$ are given by $(K-M)^{-1}$.*

The converse follows directly from the result of [3, Theorem 2], which was proven using an index coding argument, for single-server single-message PIR with (uncoded) side information when (W, S)-privacy is required. In this work, we provide an alternative proof by upper bounding the rate of any PIR-PCSI–I protocol using information-theoretic

arguments (see Section IV-A). The key component of the proof is the necessary condition presented in Lemma 1.

The achievability proof relies on a new PIR-PCSI–I protocol, termed the *Specialized GRS Code protocol*, which achieves the rate $(K-M)^{-1}$ (see Section IV-B). This protocol is based on the Generalized Reed-Solomon (GRS) codes that contain a specific codeword depending on W, S, C.

Remark 1. As shown in [3], when there is a single server storing K independent and identically distributed messages, and there is a user that knows M randomly chosen (uncoded) messages as their side information and demands a single message not in their side information, in order to guarantee (W,S)-privacy, the minimum download cost is $(K-M)L$, where L is the entropy of a message. Surprisingly, this result matches the result of Theorem 1. This shows that, when compared to having M random messages separately as side information, for achieving (W,S)-privacy there will be no additional loss in capacity even if only *one* random linear combination of M random messages is known to the user.

Remark 2. When W-privacy is required, the result of [9, Theorem 1] shows that the capacity of single-server single-message PIR with a coded side information that does not include the demand (known as the PIR-CSI–I problem in [9]) is equal to $\lceil \frac{K}{M+1} \rceil^{-1}$. Since $\lceil \frac{K}{M+1} \rceil < K-M$ for all $1 \leq M \leq K-2$, the capacity of PIR-PCSI–I is strictly smaller than that of PIR-CSI–I. This is expected because W-privacy is a weaker notion of privacy when compared to (W,S)-privacy. However, for the two extremal cases of $M=0$ and $M=K-1$, it follows that (W,S)-privacy comes at no extra cost than W-privacy.

Theorem 2. *The scalar-linear capacity of PIR-PCSI–II problem with K messages and side information size $2 \leq M \leq K$ is given by $(K-M+1)^{-1}$.*

The converse proof is based on a mix of algebraic and information-theoretic arguments (see Section V-A), and the proof of achievability is based on a modified version of the Specialized GRS Code protocol which achieves the rate $(K-M+1)^{-1}$ (see Section V-B).

Remark 3. Interestingly, comparing the results of [3, Theorem 2] and Theorem 2, one can see that when the side information is composed of $M-1$ randomly chosen messages (different from the demand message), (W,S)-privacy cannot be achieved more efficiently than the case in which the side information is only *one* random linear combination of M random messages including the demand.

Remark 4. As shown in [9, Theorem 2], when W-privacy is required, the capacity of single-server single-message PIR with a coded side information to which the demand message contributes (known as the PIR-CSI–II problem in [9]) is equal to 1 for $M=2$ and $M=K$, and is equal to $\frac{1}{2}$ for all $3 \leq M \leq K-1$. The result of Theorem 2 matches this result for the cases of $M=K$ and $M=K-1$, and thereby, (W,S)-privacy and W-privacy are attainable at the same cost. For other cases of M, as expected, achieving (W,S)-privacy is more costly than achieving W-privacy.

IV. The PIR-PCSI–I Problem

A. Converse for Theorem 1

As shown in [3] using an index-coding argument, when (W,S)-privacy is required, the capacity of PIR with M uncoded messages as side information is given by $(K-M)^{-1}$. Obviously, the capacity of PIR-PCSI–I is upper bounded by this quantity. This proves the converse for Theorem 1. We present an alternative information-theoretic proof here.

Lemma 2. *For any $0 \leq M \leq K-1$, the capacity of PIR-PCSI–I is upper bounded by $(K-M)^{-1}$.*

Proof: Fix W, S, and C (and $\mathbf{Y} \triangleq \mathbf{Y}^{[S,C]}$) such that $W \notin S$. Let $\mathbf{E}$ denote the event that $\mathbf{W} \notin \mathbf{S}$. We need to show that $H(\mathbf{A}|\mathbf{E}) \geq (K-M)L$. Similar to the proof of [9, Theorem 1], it can be shown that

$$H(\mathbf{A}|\mathbf{E}) \geq H(\mathbf{X}_W) + H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W). \tag{1}$$

If $W \cup S = [K]$ (i.e., $M = K-1$), then $H(\mathbf{A}|\mathbf{E}) \geq H(\mathbf{X}_W) = L$, as was to be shown. If $W \cup S \neq [K]$, for any $i \in [K] \setminus (W \cup S)$ there exists $C_i \in \mathcal{C}$ (and $\mathbf{Y}_i \triangleq \mathbf{Y}^{[S,C_i]}$) such that $H(\mathbf{X}_i|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y}_i) = 0$ (by Lemma 1). Let I be a maximal subset of $[K] \setminus (W \cup S)$ such that $\mathbf{Y}$ and $\mathbf{Y}_I \triangleq \{\mathbf{Y}_i\}_{i \in I}$ are linearly independent. (Note that $|I| \leq |S| - 1 = M-1$.) Let $\mathbf{X}_I \triangleq \{\mathbf{X}_i\}_{i \in I}$. Then,

$$\begin{aligned} H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W) &\geq H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I) \\ &\quad + H(\mathbf{X}_I|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I) \quad (2) \\ &= H(\mathbf{X}_I|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I) \\ &\quad + H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I) \\ &= H(\mathbf{X}_I) \\ &\quad + H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I) \quad (3) \end{aligned}$$

where (2) holds because $H(\mathbf{X}_i|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y}_i) = 0$ for all $j \in I$ (by assumption); and (3) holds since $\mathbf{X}_I$ is independent of $(\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I)$ (noting that I and $W \cup S$ are disjoint). Note also that, by the maximality of I, for any $j \in J \triangleq [K] \setminus (W \cup S \cup I)$, there exists $C_j \in C$ (and $\mathbf{Y}_j \triangleq \mathbf{Y}^{[S,C_j]}$, which is linearly dependent on $\{\mathbf{Y},\mathbf{Y}_I\}$) such that $H(\mathbf{X}_j|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y}_j) = 0$, and subsequently, $H(\mathbf{X}_j|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y}_I) = 0$. (Note that $|J| = K-M-1-|I|$.) Let $\mathbf{X}_J \triangleq \{X_j\}_{j \in J}$. Thus, we can write

$$\begin{aligned} &H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I) \\ &\quad = H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I) \\ &\qquad + H(\mathbf{X}_J|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I) \quad (4) \\ &\quad = H(\mathbf{X}_J|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I) \\ &\qquad + H(\mathbf{A}|\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I,\mathbf{X}_J) \\ &\quad \geq H(\mathbf{X}_J) \quad (5) \end{aligned}$$

where (4) holds since $H(\mathbf{X}_j|\mathbf{A},\mathbf{Q},\mathbf{E},\mathbf{Y}_I) = 0$ for all $j \in J$ (by assumption); and (5) holds because $\mathbf{X}_J$ and $(\mathbf{Q},\mathbf{E},\mathbf{Y},\mathbf{X}_W,\mathbf{Y}_I,\mathbf{X}_I)$ are independent (noting that J and $W \cup S \cup I$ are disjoint). Putting (1), (3), and (5) together, it follows that $H(\mathbf{A}|\mathbf{E}) \geq H(\mathbf{X}_W) + H(\mathbf{X}_I) + H(\mathbf{X}_J) = (K-M)L$, as was to be shown. □

B. Achievability for Theorem 1

In this section, we propose a PIR-PCSI–I protocol that achieves the rate $(K-M)^{-1}$. Throughout, we assume that $q \geq K$. It is noteworthy that for $q < K$ the achievability of the rate $(K-M)^{-1}$ is not necessarily feasible, and it is conditional upon the existence of a $(K, K-M)$ maximum-distance-seperable (MDS) code over $\mathbb{F}_q$ that includes a codeword such that the ith codeword symbol is zero for any $i \notin W \cup S$, it is equal to c_i for any $i \in S$ (where c_i is the coefficient of X_i in $Y^{[S,C]}$), and is non-zero for $i = W$.

Specialized GRS Code Protocol: This protocol consists of four steps as follows:

Step 1: First, the user arbitrarily chooses K distinct elements $\omega_1, \ldots, \omega_K$ from $\mathbb{F}_q$, and constructs a polynomial $p(x) = \sum_{i=0}^{K-M-1} p_i x^i \triangleq \prod_{i \notin W \cup S}(x - \omega_i)$. Then, the user constructs $K-M$ sequences $Q_1, \ldots, Q_{K-M}$, each of length K, defined as $Q_i = \{v_1 \omega_1^{i-1}, \ldots, v_K \omega_K^{i-1}\}$ for $i \in [K-M]$, where the choice of v_i's is specified as follows. For any $i \in S$, $v_i = \frac{c_i}{p(\omega_i)}$ where c_i is the coefficient of X_i in $Y^{[S,C]}$; and for any $i \notin S$, v_i is chosen at random from $\mathbb{F}_q^{\times}$.

For any $i \in [K-M]$ and any $j \in [K]$, the jth element in the sequence Q_i can be thought of as the entry (i,j) of a $(K-M) \times K$ matrix $G \triangleq [g_1^{\mathsf{T}}, \ldots, g_{K-M}^{\mathsf{T}}]^{\mathsf{T}}$, which is the generator matrix of a $(K, K-M)$ GRS code with distinct parameters $\omega_1, \ldots, \omega_K$ and non-zero multipliers $v_1, \ldots, v_K$ [13]. The above construction ensures that such a GRS code has a specific codeword with support $S \cup W$, namely $\sum_{i=1}^{K-M} p_{i-1} g_i$, where the ith codeword symbol is equal to c_i for $i \in S$, and is non-zero for $i = W$.

Step 2: The user sends the query $Q^{[W,S,C]} = \{Q_1, \ldots, Q_{K-M}\}$ to the server.

Step 3: By using Q_i, the server computes $A_i = \sum_{j=1}^{K} v_j \omega_j^{i-1} X_j$ for all $i \in [K-M]$, and it sends the answer $A^{[W,S,C]} = \{A_1, \ldots, A_{K-M}\}$ to the user.

Note that A_i's are the parity check equations of a (K, M) GRS code which is the dual code of the GRS code generated by the matrix G defined earlier.

Step 4: Upon receiving the answer, the user retrieves X_W by subtracting off the contribution of their side information $Y^{[S,C]}$ from $\sum_{i=1}^{K-M} p_{i-1} A_i = c_W X_W + \sum_{i \in S} c_i X_i$.

Example 1. Consider a scenario where the server has $K = 4$ messages $X_1, \ldots, X_4 \in \mathbb{F}_5$, and the user demands the message X_1 and has a coded side information of size $M = 2$, say $Y = X_2 + X_3$. For this example, $W = 1$, $S = \{2,3\}$, and $C = \{c_2, c_3\} = \{1,1\}$.

First, the user chooses $K = 4$ distinct elements $\omega_1, \ldots, \omega_4$ from $\mathbb{F}_5$, say $(\omega_1, \omega_2, \omega_3, \omega_4) = (0,1,2,3)$. Then, the user constructs the polynomial $p(x) = \prod_{i \notin W \cup S}(x - \omega_i) = x - \omega_4 = x + 2$. Note that $p(x) = p_0 + p_1 x = 2 + x$. The user then computes v_j for $j \in S$, i.e., v_2 and v_3, by setting $v_2 = \frac{c_2}{p(\omega_2)} = 2$ and $v_3 = \frac{c_3}{p(\omega_3)} = 4$, and chooses v_j for $j \notin S$, i.e., v_1 and v_4, at random (from $\mathbb{F}_5^{\times}$). Suppose that the user chooses $v_1 = 1$ and $v_4 = 2$. Then, the user constructs $K - M = 2$ sequences $Q_1 = \{v_1, \ldots, v_4\} = \{1,2,4,2\}$ and $Q_2 = \{v_1\omega_1, \ldots, v_4\omega_4\} = \{0,2,3,1\}$. The user then sends the query $Q = \{Q_1, Q_2\}$ to the server. The server computes $A_1 = \sum_{j=1}^{4} v_j X_j = X_1 + 2X_2 + 4X_3 + 2X_4$ and $A_2 = \sum_{j=1}^{4} v_j \omega_j X_j = 2X_2 + 3X_3 + X_4$, and sends the answer $A = \{A_1, A_2\}$ back to the user. Then, the user computes $\sum_{i=1}^{2} p_{i-1} A_i = 2A_1 + A_2 = 2X_1 + X_2 + X_3$, and recovers X_1 by subtracting off the side information $X_2 + X_3$. For this example, the rate of the proposed protocol is $1/2$.

Lemma 3. *The Specialized GRS Code protocol is a PIR-PCSI–I protocol, and achieves the rate* $(K-M)^{-1}$.

Proof: Since the matrix G, defined in Step 1 of the protocol, generates a $(K, K-M)$ GRS code which is an MDS code, the rows of G are linearly independent, and accordingly, $A_1, \ldots, A_{K-M}$ are linearly independent combinations of $X_1, \ldots, X_K$, which are themselves independently and uniformly distributed over $\mathbb{F}_{q^l}$. Thus, $A_1, \ldots, A_{K-M}$ are independently and uniformly distributed over $\mathbb{F}_{q^l}$. Since $H(\mathbf{X}_i) = L$ for all i, then $H(\mathbf{A}_i) = L$ for all i, and $H(\mathbf{A}^{[W,S,C]}) = H(\mathbf{A}_1, \ldots, \mathbf{A}_{K-M}) = \sum_{i=1}^{K-M} H(\mathbf{A}_i) = (K-M)L$ for any $W \in [K], S \in \mathcal{S}$ such that $W \notin S$, and $C \in \mathcal{C}$. Since $\mathbf{W}$ and $\mathbf{S}$ are jointly distributed uniformly (given that $\mathbf{W} \notin \mathbf{S}$) and $\mathbf{C}$ is uniformly distributed, then $H(\mathbf{A}^{[\boldsymbol{W},\boldsymbol{S},\boldsymbol{C}]} | \mathbf{W} \notin \mathbf{S}) = H(\mathbf{A}^{[W,S,C]}) = (K-M)L$. Thus, the rate is equal to $L/((K-M)L) = (K-M)^{-1}$.

From the construction, it should be obvious that the recoverability condition is satisfied. The (W,S)-privacy condition is also satisfied because: (i) the $(K, K-M)$ GRS code, generated by the matrix G, is an MDS code, and thereby, the minimum (Hamming) weight of a codeword is $K - (K-M) + 1 = M + 1$; and (ii) there exist the same number of minimum-weight codewords for any support of size $M+1$ [13]. Thus, for any $W \in [K]$, $S \in \mathcal{S}$ such that $W \notin S$, the dual code, defined by the parity check matrix G, contains the same number of parity check equations (with support $W \cup S$) from each of which the candidate demand message X_W can be recovered, given a potential side information $Y^{[S,C]}$ for some $C \in \mathcal{C}$. □

V. The PIR-PCSI–II Problem

A. Converse for Theorem 2

In this section, we give an information-theoretic proof of converse for Theorem 2.

Lemma 4. *For any* $2 \leq M \leq K$*, the scalar-linear capacity of PIR-PCSI–II is upper bounded by* $(K - M + 1)^{-1}$.

Proof: Fix W, S, and C (and $\mathbf{Y} \triangleq \mathbf{Y}^{[S,C]}$) such that $W \in S$. Let $\overline{\mathbf{E}}$ denote the event that $\mathbf{W} \in \mathbf{S}$. We need to show that $H(\mathbf{A}|\overline{\mathbf{E}}) \geq (K - M + 1)L$. Let I be the set of all $i \in [K]$ such that $H(\mathbf{X}_i | \mathbf{A}, \mathbf{Q}) = 0$, i.e., X_i is recoverable from A (given Q) directly. Let $\mathbf{X}_I \triangleq \{\mathbf{X}_i\}_{i \in I}$. There are two cases: (i) $I \neq \emptyset$, and (ii) $I = \emptyset$.

Case (i): Since $\mathbf{X}_I$ and $(\mathbf{Q}, \overline{\mathbf{E}})$ are independent, and $H(\mathbf{X}_I | \mathbf{A}, \mathbf{Q}, \overline{\mathbf{E}}) = 0$ (by assumption), then

$$\begin{aligned} H(\mathbf{A}|\overline{\mathbf{E}}) &\geq H(\mathbf{A}|\mathbf{Q}, \overline{\mathbf{E}}) + H(\mathbf{X}_I|\mathbf{A}, \mathbf{Q}, \overline{\mathbf{E}}) \\ &= H(\mathbf{X}_I|\mathbf{Q}, \overline{\mathbf{E}}) + H(\mathbf{A}|\mathbf{Q}, \overline{\mathbf{E}}, \mathbf{X}_I) \\ &= H(\mathbf{X}_I) + H(\mathbf{A}|\mathbf{Q}, \overline{\mathbf{E}}, \mathbf{X}_I). \end{aligned} \tag{6}$$

If $|I| \geq K-M+1$, then $H(\mathbf{X}_I) \geq (K-M+1)L$, and subsequently, $H(\mathbf{A}|\overline{\mathbf{E}}) \geq (K-M+1)L$, as was to be shown. If $|I| \leq K-M$, $H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I)$ can be further lower bounded as follows. Let $N \triangleq |I|$. Assume, w.l.o.g., that $I = [N]$. Let $J \triangleq [K-M-N+1]$, and $S_j \triangleq \{N+1, N+j+1, \ldots, N+j+M-1\}$ for $j \in J$. By Lemma 1, for any $j \in J$, there exists $C_j \in \mathcal{C}$ (and $\mathbf{Y}_j \triangleq \mathbf{Y}^{[S_j,C_j]}$) such that $H(\mathbf{X}_{N+1}|\mathbf{A},\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y}_j) = 0$. Let $\mathbf{Z}_j \triangleq \mathbf{Y}_j - c_j\mathbf{X}_{N+1}$ where c_j is the coefficient of $\mathbf{X}_{N+1}$ in $\mathbf{Y}_j$. For any scalar-linear protocol (i.e., the answer $\mathbf{A}$ consists only of scalar-linear combinations of messages in $\mathbf{X}$), it is easy to see that either $H(\mathbf{Z}_j|\mathbf{A},\mathbf{Q}) = 0$ or $H(\mathbf{Z}_j + c\mathbf{X}_{N+1}|\mathbf{A},\mathbf{Q}) = 0$ for some $c \in \mathbb{F}_q^\times \setminus \{c_j\}$. (Otherwise, the server learns that W and S cannot be $N+1$ and S_j, respectively. This obviously violates the (W,S)-privacy condition.) Thus, $H(\mathbf{Z}_j|\mathbf{A},\mathbf{Q},\mathbf{X}_{N+1}) = 0$. Let $\mathbf{Z}_J \triangleq \{\mathbf{Z}_j\}_{j\in J}$. Then, we have

$$\begin{aligned} H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I) &\geq H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I,\mathbf{X}_{N+1}) \\ &\quad + H(\mathbf{Z}_J|\mathbf{A},\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I,\mathbf{X}_{N+1}) \qquad (7) \\ &= H(\mathbf{Z}_J|\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I,\mathbf{X}_{N+1}) \\ &\quad + H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I,\mathbf{X}_{N+1},\mathbf{Z}_J) \\ &\geq H(\mathbf{Z}_J) \qquad (8) \end{aligned}$$

where (7) holds since $H(\mathbf{Z}_j|\mathbf{A},\mathbf{Q},\mathbf{X}_{N+1}) = 0$ for all $j \in J$ (by assumption); and (8) follows because $\mathbf{Z}_J$ is independent of $(\mathbf{Q},\overline{\mathbf{E}},\mathbf{X}_I,\mathbf{X}_{N+1})$, noting that $\mathbf{Z}_J$, $\mathbf{X}_I$, and $\mathbf{X}_{N+1}$ are linearly independent (by construction). By the linear independence of $\mathbf{Z}_j$'s for all $j \in J$, it follows that $H(\mathbf{Z}_J) = (K-M-N+1)L$. By (6) and (8), we get $H(\mathbf{A}|\overline{\mathbf{E}}) \geq NL + (K-M-N+1)L = (K-M+1)L$.

Case (ii): Assume, w.l.o.g., that $W = 1$ and $S = [M]$. Let $J \triangleq [K-M]$, and $S_j \triangleq \{1, j+2, \ldots, j+M\}$ for $j \in J$. Similarly as in the case (i), we define $\mathbf{Y}_j$ (and $\mathbf{Z}_j$) for all $j \in J$, where $\mathbf{X}_{N+1}$ is replaced by $\mathbf{X}_1$ everywhere.

For any scalar-linear protocol, by a similar argument as before, it can be shown that $H(\mathbf{Z}_j|\mathbf{A},\mathbf{Q},\mathbf{X}_1) = 0$ for all $j \in J$. Let $\mathbf{Z}_J \triangleq \{\mathbf{Z}_j\}_{j\in J}$. Then, we can write

$$\begin{aligned} H(\mathbf{A}|\overline{\mathbf{E}}) &\geq H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y}) + H(\mathbf{X}_1|\mathbf{A},\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y}) \qquad (9) \\ &= H(\mathbf{X}_1|\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y}) + H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1) \\ &= H(\mathbf{X}_1) + H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1) \\ &\quad + H(\mathbf{Z}_J|\mathbf{A},\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1) \qquad (10) \\ &= H(\mathbf{X}_1) + H(\mathbf{Z}_J|\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1) \\ &\quad + H(\mathbf{A}|\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1,\mathbf{Z}_J) \\ &\geq H(\mathbf{X}_1) + H(\mathbf{Z}_J) \qquad (11) \end{aligned}$$

where (9) follows because $H(\mathbf{X}_1|\mathbf{A},\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y}) = 0$ (by the recoverability condition); (10) holds since $H(\mathbf{Z}_j|\mathbf{A},\mathbf{Q},\mathbf{X}_1) = 0$, and subsequently, $H(\mathbf{Z}_j|\mathbf{A},\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1) = 0$, for all $j \in J$; and (11) follows because $\mathbf{Z}_J$ is independent of $(\mathbf{Q},\overline{\mathbf{E}},\mathbf{Y},\mathbf{X}_1)$ (due to the linear independence of $\mathbf{Z}_J$, $\mathbf{Y}$, and $\mathbf{X}_1$). Since $|J| = K-M$, we have $H(\mathbf{Z}_J) = (K-M)L$ (noting that $\mathbf{Z}_j$'s are linearly independent), and thereby, $H(\mathbf{A}|\overline{\mathbf{E}}) \geq L + (K-M)L = (K-M+1)L$. □

B. Achievability for Theorem 2

In this section, we propose a PIR-PCSI–II protocol, which is a slightly modified version of the Specialized GRS Code protocol, that achieves the rate $(K-M+1)^{-1}$.

Modified Specialized GRS Code Protocol: This protocol consists of four steps, where the steps 2-4 are the same as Steps 2-4 in the Specialized GRS Code protocol (Section IV-B), except that M is replaced with $M-1$ everywhere. The step 1 of the proposed protocol is as follows:

Step 1: The user first constructs a polynomial $p(x) = \sum_{i=0}^{K-M} p_i x^i \triangleq \prod_{i\notin S}(x-\omega_i)$, and then constructs $K-M+1$ sequences $Q_1, \ldots, Q_{K-M+1}$, each of length K, defined as $Q_i = \{v_1\omega_1^{i-1}, \ldots, v_K\omega_K^{i-1}\}$ for $i \in [K-M]$, where v_i's are chosen as follows. For any $i \in S \setminus W$, $v_i = \frac{c_i}{p(\omega_i)}$ where c_i is the coefficient of X_i in $Y^{[S,C]}$; $v_W = \frac{c}{p(\omega_W)}$ for a randomly chosen element c from $\mathbb{F}_q^\times \setminus \{c_W\}$ where c_W is the coefficient of X_W in $Y^{[S,C]}$; and for any $i \notin S$, v_i is chosen at random from $\mathbb{F}_q^\times$.

Lemma 5. *The Modified Specialized GRS Code protocol is a PIR-PCSI–II protocol, and achieves the rate* $(K-M+1)^{-1}$.

Proof: The proof, omitted to avoid repetition, follows from the same lines as in the proof of Lemma 3 where M is replaced by $M-1$, and $W \notin S$ is replaced by $W \in S$. □

REFERENCES

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

[2] ——, "The capacity of robust private information retrieval with colluding databases," *IEEE Trans. on Info. Theory*, vol. 64, no. 4, pp. 2361–2370, April 2018.

[3] S. Kadhe, B. Garcia, A. Heidarzadeh, S. E. Rouayheb, and A. Sprintson, "Private information retrieval with side information: The single server case," in *2017 55th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2017, pp. 1099–1106.

[4] R. Tandon, "The capacity of cache aided private information retrieval," in *55th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2017, pp. 1078–1082.

[5] Y. Wei, K. Banawan, and S. Ulukus, "Cache-aided private information retrieval with partially known uncoded prefetching: Fundamental limits," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 6, pp. 1126–1139, June 2018.

[6] ——, "Fundamental limits of cache-aided private information retrieval with unknown and uncoded prefetching," *IEEE Trans. on Info. Theory*, pp. 1–1, 2018.

[7] S. Kadhe, B. Garcia, A. Heidarzadeh, S. E. Rouayheb, and A. Sprintson, "Private information retrieval with side information," *CoRR*, vol. abs/1709.00112, 2017. [Online]. Available: http://arxiv.org/abs/1709.00112

[8] Z. Chen, Z. Wang, and S. Jafar, "The capacity of private information retrieval with private side information," *CoRR*, vol. abs/1709.03022, 2017. [Online]. Available: http://arxiv.org/abs/1709.03022

[9] A. Heidarzadeh, F. Kazemi, and A. Sprintson, "Capacity of single-server single-message private information retrieval with coded side information," June 2018. [Online]. Available: arXiv:1806.00661

[10] S. P. Shariatpanahi, M. J. Siavoshani, and M. A. Maddah-Ali, "Multi-message private information retrieval with private side information," May 2018. [Online]. Available: arXiv:1805.11892

[11] A. Heidarzadeh, S. Kadhe, B. Garcia, S. E. Rouayheb, and A. Sprintson, "On the capacity of single-server multi-message private information retrieval with side information," in *2018 56th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2018.

[12] S. Li and M. Gastpar, "Single-server multi-message private information retrieval with side information," in *2018 56th Annual Allerton Conf. on Commun., Control, and Computing*, Oct 2018.

[13] R. Roth, *Introduction to Coding Theory*. New York, NY, USA: Cambridge University Press, 2006.