Private Computation with Side Information: The Single-Server Case

Anoosheh Heidarzadeh and Alex Sprintson

***Abstract*— This paper considers the problem of single-server Private Computation wit Side Information (PC-SI). In this problem, there is a user that initially has a subset of M messages from a database stored on a single server, where the identities of the side information messages are initially unknown to the server. The user wishes to compute a linear combination of a subset of D messages (disjoint from the set of side information messages) while protecting the identities of the messages in the demanded linear combination. The objective of the user is to minimize the download cost, which is defined as the total amount of information that the user downloads from the server.**

We establish a lower bound on the capacity of the PC-SI problem, where the capacity is defined as the supremum of all achievable download rates. The proof relies on a novel achievability scheme which combines together the ideas of the interference alignment and the Partition and Code scheme previously introduced for private information retrieval with side information. In addition, for the case of $M = 1$ and $D = 2$, we prove the tightness of the rate achievable by the proposed scheme, when we restrict ourselves to the scalar-linear PC-SI schemes. The proof of converse is based on a combination of new algebraic and information-theoretic arguments.

I. INTRODUCTION

This work introduces the problem of Private Computation in the presence of Side Information (PC-SI) with information-theoretic privacy guarantees. In this problem, there is a user who knows a subset of messages from a database stored on a single (or multiple) remote server(s), and wishes to privately compute a linear combination of a subset of messages, disjoint from the set of side information messages. The identities of the side information messages are initially unknown to the server(s). The goal of the user is to minimize the download cost (which is defined as the total amount of information being downloaded from the server(s)), while hiding the identities of the messages in the demanded linear combination from the server(s).

The PC-SI problem is closely related to the problem of Private Information Retrieval with Side Information (PIR-SI), which was lately introduced by Kadhe *et al.* in [1], and the information-theoretic Private Computation (PC) problem introduced recently by Sun and Jafar in [2]. In particular, in the PIR-SI problem, the user has some side information about the messages at the server(s), and wants to retrieve a set of uncoded messages from the server(s) while protecting either the privacy of both the demand and the side information messages or the privacy of the demand messages only. In the PC problem, the user has no side information, and wishes to download a linear combination of the messages at the server(s), while hiding both the identities of the messages and their coefficients in the demanded linear combination.

The PIR-SI problem has been studied in several different scenarios. In particular, the single-server single-message setting of the PIR-SI problem with uncoded side information was studied in [1], and the scenario with coded side information was considered in [3]. The single-server multi-message setting of this problem was later studied in [4], [5]. The multi-server single-message and multi-message PIR-SI were considered in [6], [7] and [8], respectively. None of these works consider the scenario in which the user's demand consists of a linear combination of multiple messages. Several variants of the PC problem have also been studied in [9]–[12]. These works focus on the multi-server setting, and do not consider any side information at the user.

A. Main Contributions

In this work, we focus on the single-server setting of the PC-SI problem. In particular, we assume that there is a single server storing K messages over a field $\mathbb{F}_{q^l}$ (for some prime q and integer $l \geq 1$), and a user who has a subset of M messages as side information, and wants to download a linear combination (with non-zero coefficients from $\mathbb{F}_q$) of a subset of D other messages. We establish a lower bound on the capacity of the PC-SI problem (as a function of K, M, D, for sufficiently large q), where the capacity is defined as the supremum of all achievable download rates. The proof relies on a novel achievability scheme. This scheme, termed *Partition and Code with Interference Alignment (PC-IA)*, is based on a probabilistic partitioning, and allows the parts of the partition to overlap and have multiple aligned blocks of interference. In addition, for the case of $M = 1$ and $D = 2$, we prove the tightness of the rate achievable by the PC-IA scheme, when we restrict ourselves to the scalar-linear PC-SI schemes. The converse proof is based on a combination of new algebraic and information-theoretic arguments.

Surprisingly, our results indicate that the larger is D the less costly would be the private computation of a linear combination of D messages. Moreover, a simple comparison of our results with the results of [4] on the single-server multi-message PIR-SI problem shows that a linear combination of multiple messages can be computed privately much more efficiently than privately retrieving multiple messages first, and then computing the desired linear combination.

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

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

II. Problem Formulation

Throughout, random variables and their realizations are denoted by bold-face letters and regular letters, respectively.

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

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

We assume that $\mathbf{S}$ and $\mathbf{C}$ are distributed uniformly over $\mathcal{S}$ and $\mathcal{C}$, respectively, and $\mathbf{W}$, conditional on $\mathbf{S} = S$, is uniformly distributed over all $W \in \mathcal{W}$ such that $W \cap S = \emptyset$. By these assumptions, $\mathbf{W}$ is distributed uniformly over $\mathcal{W}$.

The server initially knows the side information size M and the demand size D along with the distributions of $\mathbf{S}, \mathbf{C}$, and the conditional distribution of $\mathbf{W}$ given $\mathbf{S}$; whereas the realizations S, C, and W are not initially known to the server.

For any S, C, W, the user sends to the server a query $Q^{[W,C,S]}$ in order to retrieve $Y^{[W,C]}$. The query, which is a (potentially stochastic) function of W, C, S, and X_S, must protect the privacy of the user's demand index set from the server, i.e., for all $W \in \mathcal{W}$,

$$\Pr(\mathbf{W} = W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q, \mathbf{X} = X) = \Pr(\mathbf{W} = W).$$

This condition, which we refer to as the *privacy condition*, is also known as the *W-privacy condition* in the private information retrieval with side information (PIR-SI) literature (see [1], [4]). Note that, unlike the problem model in [2], here the query does not need to protect the privacy of the coefficients of the messages in the demand (i.e., C).

Upon receiving $Q^{[W,C,S]}$, the server sends to the user an answer $A^{[W,C,S]}$, which is a (deterministic) function of the query $Q^{[W,C,S]}$ and the messages in X. In particular, $(\mathbf{W}, \mathbf{S})$ and $\mathbf{A}^{[\mathbf{W},\mathbf{C},\mathbf{S}]}$ are conditionally independent given $(\mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]}, \mathbf{X})$, and $H(\mathbf{A}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]}, \mathbf{X}) = 0$.

The collection of $A^{[W,C,S]}, Q^{[W,C,S]}, X_S, W, S, C$ must enable the user to retrieve the demand $Y^{[W,C]}$. That is,

$$H(\mathbf{Y}^{[\mathbf{W},\mathbf{C}]} | \mathbf{A}^{[\mathbf{W},\mathbf{C},\mathbf{S}]}, \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]}, \mathbf{X_S}, \mathbf{W}, \mathbf{C}, \mathbf{S}) = 0.$$

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

We are interested in designing a protocol to generate a pair $(Q^{[W,C,S]}, A^{[W,C,S]})$, for any given W, C, S, that satisfy both the privacy and recoverability conditions. We refer to this problem as *single-server Private Computation (PC) with Side Information (SI)*, or *PC-SI* for short.

We define the *rate* of a PC-SI protocol as the ratio of the entropy of a message, i.e., L, to the total entropy of the answer, i.e., $H(\mathbf{A}^{[\mathbf{W},\mathbf{C},\mathbf{S}]})$. The *capacity* of the PC-SI problem is defined as the supremum of rates over all PC-SI protocols; and the *scalar-linear capacity* of the PC-SI problem is defined similarly, except when the protocols are restricted to be scalar-linear, i.e., the answer can only contain scalar-linear combinations of the messages in X.

Our goal in this work is to characterize the capacity and the scalar-linear capacity of the PC-SI problem, and to design a PC-SI protocol that is capacity-achieving.

III. Main Results

In this section, we present our main results. For sufficiently large q (i.e., the order of the base field $\mathbb{F}_q$), Theorem 1 gives a lower bound on the capacity of the PC-SI problem for $M \geq 1$ and $D \geq 2$, and Theorem 2 characterizes the scalar-linear capacity for $M = 1$ and $D = 2$. The proofs of Theorems 1 and 2 are given in Sections IV and V, respectively.

Theorem 1. *The capacity of the PC-SI problem with K messages over $\mathbb{F}_{q^l}$ for $q > \lfloor \frac{K}{\lfloor M/D \rfloor + 1} \rfloor$, side information size $M \geq 1$, and demand size $D \geq 2$ is lower bounded by*

$$\left(\left\lceil \frac{K - M - D}{\lfloor \frac{M}{D} \rfloor + 1} \right\rceil + 1 \right)^{-1}.$$

The proof is based on a PC-SI protocol, which is a non-trivial extension of the Partition and Code protocol of [1] for single-server single-message PIR-SI with W-privacy, that achieves the rate lower bound. The proposed protocol, termed *Partition and Code with Interference Alignment (PC-IA)*, relies on a probabilistic construction of the partition, and allows the parts to overlap and have multiple aligned blocks of interference (for details, see Section IV).

Theorem 2. *The scalar-linear capacity of PC-SI with K messages over $\mathbb{F}_{q^l}$ for $q > \lfloor \frac{K}{\lfloor M/D \rfloor + 1} \rfloor$, side information size $M = 1$, and demand size $D = 2$ is given by $(K-2)^{-1}$.*

The proof of tightness of the lower bound given in Theorem 1 for $M = 1$ and $D = 2$ (when we restrict ourselves to the scalar-linear protocols) is based on a combination of new algebraic and information-theoretic arguments. These arguments rely on a necessary condition due to the privacy and recoverability conditions (see Lemma 2).

Remark 1. The result of Theorem 1 shows that the (minimum) normalized download cost (i.e., download cost normalized by the entropy of a message, L) of PC-SI for $D > M$ is upper bounded by $K - M - D + 1$. As shown in Theorem 2, this bound is also tight, when focusing on scalar-linear PC-SI protocols, for $D = 2$ and $M = 1$. This is while the result of [1, Theorem 2] shows that, when W-privacy is required, the normalized download cost of (single-server multi-message) PIR-SI for $D > M$ is equal to $K - M$. This result is interesting because it shows

that for any given M the larger is the demand size D ($> M$) the less costly would be the private computation of the demand. For $D \leq M$, under a few assumptions for divisibility, the normalized download cost of PIR-SI with W-privacy was shown to be upper bounded by $(\frac{D^2}{D^2+M})K$ [4, Theorem 1]. This is while the result of Theorem 1 shows that for $D \leq M$ the normalized download cost of PC-SI is upper bounded by $(\frac{D}{D+M})K - D + 1$. These results imply that the private computation of one linear combination of multiple messages can be performed much more efficiently than privately retrieving multiple messages first, and then computing the desired linear combination.

Remark 2. When the user wants to retrieve one single message from the server (i.e., $D = 1$), the PC-SI problem reduces to the problem of single-server single-message PIR-SI when W-privacy is required [1]. The capacity of this problem was previously shown to be equal to $\lceil K/(M+1)\rceil^{-1}$ (see [1, Theorem 1]). This confirms the tightness of the result of Theorem 1 for $D = 1$. Also, when the user has no side information (i.e., $M = 0$), a simple information-theoretic argument yields that the capacity of PC-SI is given by $(K-D+1)^{-1}$. This shows that the result of Theorem 1 is tight for $M = 0$. Comparing this result with that of [2] shows that relaxing the privacy condition to hide only the indices of messages (instead of both their indices and coefficients) in the demand can significantly increase the capacity.

Remark 3. Although not presented here, we have also proved that the scalar-linear capacity of the PC-SI problem for $M = 1$ and $D = 2$ when $q = 2$ is given by $(K - \lceil \log_2 K \rceil)^{-1}$. The tightness of the lower bound of Theorem 1 for $M \geq 2$ and $D \geq 2$ (and any q) remains open in general (for both linear and non-linear protocols).

IV. Proof of Theorem 1

In this section, we propose a PC-SI protocol, termed *Partition and Code with Interference Alignment (PC-IA)*, which achieves the rate lower bound of Theorem 1 for large enough q. Note that for $D > M$ a slightly modified version of the MDS Code protocol in [1] or the GRS Code protocol in [4] achieves the same rate, yet for $D \leq M$ such protocols, when compared to the PC-IA protocol, achieve lower rates.

Define $s \triangleq \lfloor \frac{M}{D} \rfloor + 1$, $n \triangleq \lceil \frac{K-M-D}{s} \rceil + 1$, $m \triangleq \lfloor \frac{K}{s} \rfloor$, $r \triangleq K - ms$, and $t \triangleq \max\{0, m-n\}$.

Assume that $q > m$, and let $x_1, \ldots, x_n, y_0, y_1, \ldots, y_{m-n}$ be distinct elements from $\mathbb{F}_q$.

PC-IA Protocol: This protocol consists of four steps:

Step 1: First, the user constructs $m+1$ disjoint sequences (ordered sets) $B_0, B_1, \ldots, B_m$ from the indices in $[K]$, where B_0 has length r, and B_j for $j \in [m]$ has length s, and then constructs n sequences $Q_1, \ldots, Q_n$, where $Q_i = \{B_0, B_1, \ldots, B_t, B_{t+i}\}$ for $i \in [n]$. Note that $B_0, B_1 \ldots, B_t$ are the blocks of interference between $Q_1, \ldots, Q_n$, whereas B_{t+i} belongs to Q_i only. The procedure for constructing $B_0, B_1, \ldots, B_m$ is as follows.

The user randomly places all elements (demand indices) of W into $B_0, B_1, \ldots, B_m$. The user then selects a minimal subset I of $[n]$ such that Q_i's for all $i \in I$ collectively contain all elements in W. If $B_0, B_1, \ldots, B_t$ do not contain all elements from W, then I is uniquely determined; otherwise, the user selects $I = \{1\}$. Let d_j be the number of elements from W in B_j, and let J be the set of all block indices j such that $d_j \neq 0$ and B_j belongs to Q_i for some $i \in I$. Then the user randomly selects $s - d_j$ for $j \neq 0$, $j \in J$ (or $r - d_0$ for $j = 0$, $j \in J$) elements (side information indices) from S that were not previously placed, and places them one at a time into B_j, where each element is placed in the least-indexed position which is not filled yet.

Starting from the least block index and moving upwards, for any block index $j \notin J$ the user places (one by one) randomly chosen elements from S, which were not placed yet, into B_j (with the same placement procedure as before), until all elements in S were placed. (By this construction, given the elements in W, all elements in S can be uniquely determined from $B_0, B_1, \ldots, B_m$.) Then, the user randomly places (one at a time, following the same procedure as above) the rest of the indices in $[K] \setminus (W \cup S)$, that are yet to be placed, into the remaining positions in $B_0, B_1, \ldots, B_m$.

Next, the user creates n sequences $Q'_1, \ldots, Q'_n$, where $Q'_i = \{C_{i,0}, C_{i,1}, \ldots, C_{i,t}, C_{i,t+i}\}$ for $i \in [n]$, such that $C_{i,0} = \{\alpha_{0,1}\omega_{i,0}, \ldots, \alpha_{0,r}\omega_{i,0}\}$, $C_{i,j} = \{\alpha_{j,1}\omega_{i,j}, \ldots, \alpha_{j,s}\omega_{i,j}\}$ for $j \in [t]$, and $C_{i,t+i} = \{\alpha_{t+i,1}, \ldots, \alpha_{t+i,s}\}$, where $\omega_{i,j} \triangleq 1/(x_i - y_j)$ is an element in $\mathbb{F}_q^\times$ (noting that x_i's and y_j's are all distinct), and the elements $\alpha_{i,j}$'s, which are determined by the coefficients of the messages that contribute to the demand, are properly chosen from $\mathbb{F}_q^\times$ as follows.

Let H be the set of $|I|-1$ largest indices in $[t] \cup \{0\} \setminus J$, and let T be a $|I| \times (|I|-1)$ matrix defined as $T \triangleq (\omega_{i,j})_{i \in I, j \in H}$. It can be easily shown that there exists a row-vector $v \triangleq (v_i)_{i \in I}$, $v_i \in \mathbb{F}_q^\times$ of length $|I|$ such that vT is an all-zero vector. (One can show that, other than the all-zero vector, no vector v such that vT is an all-zero vector has any zero element.) For any given $v_i \in \mathbb{F}_q^\times$, where i is an arbitrary index in I, it is easy to verify that such a vector v (with elements from $\mathbb{F}_q^\times$) is unique. The user then selects such a vector v such that $v_{i_*} = 1$ where i_* is the least index in I.

For any $j \neq 0$, $j \in J$ (or $j = 0$, $j \in J$) and any $k \in [s]$ (or any $k \in [r]$) such that the kth element of B_j, say w, belongs to W, the user selects $\alpha_{j,k} = c_w / \sum_{i \in I} v_i \omega_{i,j}$ for $j \in [t] \cup \{0\}$, and selects $\alpha_{j,k} = c_w / v_i$ for $j = t + i$, where c_w is the coefficient of X_w in the demand. (Since T is a Cauchy matrix and vT is an all-zero vector, it is easy to show that $\sum_{i \in I} v_i \omega_{i,j} \neq 0$ for $j \in J$.) For any other j and k, the user randomly chooses $\alpha_{j,k}$ from $\mathbb{F}_q^\times$.

Step 2: The user then sends to the server the query $Q^{[W,C,S]} = \{Q_1^*, \ldots, Q_n^*\}$, where $Q_i^* = (Q_i, Q'_i)$ for $i \in [n]$.

Step 3: By using $Q_i^* = (Q_i, Q'_i)$ for $i \in [n]$, the server computes $A_i = \sum_{k=1}^{r} c_{i,0,k} X_{b_{0,k}} + \sum_{j=1}^{t} \sum_{k=1}^{s} c_{i,j,k} X_{b_{j,k}} + \sum_{k=1}^{s} c_{i,t+i,k} X_{b_{t+i,k}}$ where $c_{i,j,k}$ and $b_{j,k}$ are the kth element of $C_{i,j}$ and B_j, respectively. The server then sends back to the user the answer $A^{[W,C,S]} = \{A_1, \ldots, A_n\}$.

Step 4: Upon receiving the answer from the server, the user

computes $\sum_{j\in W} c_j X_j$ by subtracting off the contribution of the side information messages from $\sum_{i\in I} v_i A_i$. Note that the set I, defined as in the construction of the sequences $B_0, B_1, \ldots, B_m$, is the index set of those equations A_i's (collected from the server) that the user combines linearly so as to compute the demand (where the coefficients of the linear combination are the elements of the vector v).

Example 1. *Consider a scenario with $K = 12$, $M = 4$, and $D = 3$, where the server has the messages $X_1, \ldots, X_{12} \in \mathbb{F}_7$, and the user knows $X_4, \ldots, X_7$, and wants to compute $X_1 + 2X_2 + X_3$. Thus, $W = \{1, 2, 3\}$, $\{c_1, c_2, c_3\} = \{1, 2, 1\}$, and $S = \{4, \ldots, 7\}$.*

The parameters of the PC-IA protocol for this example are listed as follows: $s = 2$, $n = 4$, $m = 6$, $r = 0$, $t = 2$, and $\{x_1, x_2, x_3, x_4, y_0, y_1, y_2\} = \{0, 1, \ldots, 6\}$.

First, the user creates $m = 6$ sequences $B_1, \ldots, B_6$, where $B_j = \{-, -\}$ for all j, i.e., each B_j has two slots to be filled. The user then randomly places the demand indices $1, 2, 3$ into three slots. Suppose that after this placement, we have $B_1 = \{-, -\}$, $B_2 = \{2, -\}$, $B_3 = \{-, 1\}$, $B_4 = \{3, -\}$, $B_5 = \{-, -\}$, and $B_6 = \{-, -\}$. Then the user fills B_2, B_3, and B_4, each with a randomly chosen side information index; e.g., $B_2 = \{2, 5\}$, $B_3 = \{7, 1\}$, and $B_4 = \{3, 4\}$. Next, the user places the remaining side information index, i.e., 6 in this example, into B_1, and randomly places the remaining indices $8, \ldots, 12$ into the remaining slots of B_1, B_5, and B_6; e.g., $B_1 = \{6, 11\}$, $B_5 = \{10, 12\}$, and $B_6 = \{8, 9\}$.

The user then constructs $n = 4$ sequences $Q_1, \ldots, Q_4$, where $Q_i = \{B_1, B_2, B_{2+i}\}$ for all i. That is, $Q_1 = \{6, 11, 2, 5, 7, 1\}$, $Q_2 = \{6, 11, 2, 5, 3, 4\}$, $Q_3 = \{6, 11, 2, 5, 10, 12\}$, and $Q_4 = \{6, 11, 2, 5, 8, 9\}$.

Next, the user finds the set J of indices j such that B_j contains some demand indices, and the minimal set I of (least) indices of Q_i's that collectively include all demand indices; for this example, $J = \{2, 3, 4\}$, and $I = \{1, 2\}$. The user then finds the set H of $|I|-1$ largest indices in $[t] \setminus J = \{1\}$; for this example, $H = \{1\}$.

Then the user forms the matrix $T = (\omega_{i,j})_{i\in I, j\in H} = [\omega_{1,1}, \omega_{2,1}]^{\mathsf{T}}$. The user then chooses $v_1 = 1$ and $v_2 = -\omega_{1,1}/\omega_{2,1} = 2$ such that $[v_1, v_2] \cdot T = 0$. Then the user selects $\alpha_{2,1}$, $\alpha_{3,2}$, and $\alpha_{4,1}$ (noting that the first element in B_2, the second element in B_3, and the first element in B_4 are the demand indices 2, 1, and 3, respectively) as follows: $\alpha_{2,1} = c_2/(v_1\omega_{1,2} + v_2\omega_{2,2}) = 1$, $\alpha_{3,2} = c_1/v_1 = 1$, and $\alpha_{4,1} = c_3/v_2 = 4$. The user then randomly selects $\alpha_{1,1} = 1$, $\alpha_{1,2} = 3$, $\alpha_{2,2} = 1$, $\alpha_{3,1} = 2$, $\alpha_{4,2} = 3$, $\alpha_{5,1} = 4$, $\alpha_{5,2} = 5$, $\alpha_{6,1} = 2$, and $\alpha_{6,2} = 1$.

Next, the user forms the sequences $C_{1,1} = \{4, 5\}$, $C_{1,2} = \{1, 1\}$, and $C_{1,3} = \{2, 1\}$; $C_{2,1} = \{5, 1\}$, $C_{2,2} = \{4, 4\}$, and $C_{2,4} = \{4, 3\}$; $C_{3,1} = \{2, 6\}$, $C_{3,2} = \{5, 5\}$, and $C_{3,5} = \{4, 5\}$; and $C_{4,1} = \{3, 2\}$, $C_{4,2} = \{2, 2\}$, and $C_{4,6} = \{2, 1\}$. The user then constructs $n = 4$ sequences $Q'_1, \ldots, Q'_4$, where $Q'_i = \{C_{i,1}, C_{i,2}, C_{i,i+2}\}$ for all i. For this example, $Q'_1 = \{4, 5, 1, 1, 2, 1\}$, $Q'_2 = \{5, 1, 4, 4, 4, 3\}$, $Q'_3 = \{2, 6, 5, 5, 4, 5\}$, and $Q'_4 = \{3, 2, 2, 2, 2, 1\}$.

The user then sends to the server

$$(Q_1, Q'_1) = (\{6, 11, 2, 5, 7, 1\}, \{4, 5, 1, 1, 2, 1\}),$$
$$(Q_2, Q'_2) = (\{6, 11, 2, 5, 3, 4\}, \{5, 1, 4, 4, 4, 3\}),$$
$$(Q_3, Q'_3) = (\{6, 11, 2, 5, 10, 12\}, \{2, 6, 5, 5, 4, 5\}),$$
$$(Q_3, Q'_4) = (\{6, 11, 2, 5, 8, 9\}, \{3, 2, 2, 2, 2, 1\}),$$

and the server sends the user back

$$A_1 = 4X_6 + 5X_{11} + X_2 + X_5 + 2X_7 + X_1,$$
$$A_2 = 5X_6 + X_{11} + 4X_2 + 4X_5 + 4X_3 + 3X_4,$$
$$A_3 = 2X_6 + 6X_{11} + 5X_2 + 5X_5 + 4X_{10} + 5X_{12},$$
$$A_4 = 3X_6 + 2X_{11} + 2X_2 + 2X_5 + 2X_8 + X_9.$$

The user then computes $v_1A_1 + v_2A_2 = X_1 + 2X_2 + X_3 + 6X_4 + 2X_5 + 2X_7$; and subtracting off the contribution of X_4, X_5, and X_7, then the user recovers $X_1 + 2X_2 + X_3$.

The rate of the PC-IA protocol for this example is $1/4$, whereas an MDS Code-based protocol, similar to those in [1] and [4], achieves a lower rate $1/(K - M - D) = 1/5$.

Lemma 1. *The PC-IA protocol is a PC-SI protocol, and achieves the rate*

$$\left(\left\lceil \frac{K - M - D}{\lfloor \frac{M}{D} \rfloor + 1} \right\rceil + 1\right)^{-1}.$$

Proof: It is easy to see that $A_1, \ldots, A_n$ are independently and uniformly distributed over $\mathbb{F}_{q^l}$. Thus, for any $W \in \mathcal{W}, C \in \mathcal{C}, S \in \mathcal{S}$ such that $W \cap S = \emptyset$, $H(\mathbf{A}^{[W,C,S]}) = H(\mathbf{A}_1, \ldots, \mathbf{A}_n) = nL$. Then, the rate of the protocol, i.e., $L/H(\mathbf{A}^{[\mathbf{W},\mathbf{C},\mathbf{S}]})$, is equal to $1/n = (\lceil (K - M - D)/s \rceil + 1)^{-1}$ where $s = \lfloor M/D \rfloor + 1$.

The proof of recoverability should be obvious from the construction of the protocol. To prove that the protocol satisfies the privacy condition, we need to show that for any query Q constructed by the protocol, $\Pr(\mathbf{W} = W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q) = \Pr(\mathbf{W} = W)$ for all $W \in \mathcal{W}$, or alternatively, $\Pr(\mathbf{W} = W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q)$ is the same for all $W \in \mathcal{W}$. (It should be noted that by the construction, Q is independent of the messages in X.)

By the structure of the protocol, for any $W \in \mathcal{W}$, there exist a unique $S_W \in \mathcal{S}$ and a unique $C_W \in \mathcal{C}$ such that (W, C_W, S_W) complies with Q, i.e., given that $Y^{[W,C]}$ and X_S are the user's demand and side information, respectively, the protocol could potentially construct Q. Thus,

$$\Pr(\mathbf{W} = W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q)$$
$$= \Pr(\mathbf{W} = W, \mathbf{C} = C_W, \mathbf{S} = S_W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q),$$

Since the distribution of $(\mathbf{W}, \mathbf{S}, \mathbf{C})$ is uniform, by applying the Bayes' rule one can easily verify that for all $W \in \mathcal{W}$, $\Pr(\mathbf{W} = W, \mathbf{C} = C_W, \mathbf{S} = S_W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q)$ is the same so long as $\Pr(\mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q | \mathbf{W} = W, \mathbf{C} = C_W, \mathbf{S} = S_W)$ is the same for all $W \in \mathcal{W}$. By the design of the protocol, it is easy to see that for all $W \in \mathcal{W}$, the latter probability is equal to $\frac{1}{K!}\binom{K-D}{M}(q-1)^{D-K}$, and hence independent of W. This implies that $\Pr(\mathbf{W} = W | \mathbf{Q}^{[\mathbf{W},\mathbf{C},\mathbf{S}]} = Q)$ is the same for all $W \in \mathcal{W}$, as was to be shown. □

V. Proof of Theorem 2

In this section, we prove the tightness of the capacity lower bound given in Theorem 1, when restricting ourselves to the scalar-linear PC-SI protocols, for $M = 1$ and $D = 2$.

The following lemma, which appears without proof and follows from a simple contradiction, shows a necessary condition imposed by the privacy and recoverability conditions.

Lemma 2. *For any $W \in \mathcal{W}$, there must exist $C \in \mathcal{C}$ and $S \in \mathcal{S}$ where $W \cap S = \emptyset$ such that*

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

Lemma 3. *The scalar-linear capacity of PC-SI with K messages over $\mathbb{F}_{q^l}$ for $q > 2$, side information size $M = 1$, and demand size $D = 2$, is upper bounded by $(K-2)^{-1}$.*

Proof: Fix arbitrary $W \in \mathcal{W}$, $C \in \mathcal{C}$, and $S \in \mathcal{S}$ (and $\mathbf{Y} \triangleq \mathbf{Y}^{[W,C]}$) such that $W \cap S = \emptyset$. (Note that $|W| = D = 2$ and $|S| = M = 1$.) Consider the query $\mathbf{Q} \triangleq \mathbf{Q}^{[W,C,S]}$ and the answer $\mathbf{A} \triangleq \mathbf{A}^{[W,C,S]}$ associated with an arbitrary scalar-linear PC-SI protocol. Note that $\mathbf{A}$ contains only scalar-linear combinations of messages in $\mathbf{X}$. We need to show that $H(\mathbf{A}) \geq (K-2)L$. Suppose that $H(\mathbf{A}) < (K-2)L$. We will show a contradiction.

Let $\mathrm{span}(\mathbf{A})$ be the set of all $\mathbb{F}_q$-linear combinations of the linear functions (i.e., the scalar-linear combinations of messages in $\mathbf{X}$) in $\mathbf{A}$. It is easy to show that since $H(\mathbf{A}) < (K-2)L$, there must exist $I \subset [K]$, $|I| = 2$ such that no $\mathbb{F}_q$-linear combination of $\mathbf{X}_I \triangleq \{\mathbf{X}_j\}_{j\in I}$ belongs to $\mathrm{span}(\mathbf{A})$. Assume, w.l.o.g., that $I = \{1, 2\}$. Let R be the set of all $j \in [K] \setminus I$ such that $H(\mathbf{X}_j|\mathbf{A}, \mathbf{Q}, \mathbf{X}_I) = 0$, i.e., X_j is recoverable from A, Q, X_I. Again, w.l.o.g., assume that $R = \{3, \ldots, l\}$. It is easy to see that $H(\mathbf{A}) \geq H(\mathbf{X}_R) = |R|L$. Since $H(\mathbf{A}) < (K-2)L$, then $|R| < K-2$ (i.e., $l < K$). Let $J \triangleq [K] \setminus (I \cup R) = \{l+1, \ldots, K\}$. Note that X_j for $j \in J$ is not recoverable from A, Q, X_I (otherwise, $j \in R$).

We denote by $\mathbf{Y}^1_{i,j}$ (or $\mathbf{Y}^2_{i,j}$) an $\mathbb{F}_q^\times$-linear combination of $\mathbf{X}_1$ (or $\mathbf{X}_2$), $\mathbf{X}_i$, and $\mathbf{X}_j$, and denote by $\tilde{\mathbf{Y}}^1_{i,j}$ (or $\tilde{\mathbf{Y}}^2_{i,j}$) the same linear combination excluding $\mathbf{X}_1$ (or $\mathbf{X}_2$).

First, consider the messages $\mathbf{X}_1$ and $\mathbf{X}_{l+1}$. Note that no $\mathbb{F}_q^\times$-linear combination of X_1 and X_{l+1} is recoverable from A, Q, and X_j for any $j \in [l] \setminus \{1\}$. By Lemma 2, there exists $j \in J \setminus \{l+1\}$, say $l+2$, such that $\mathbf{Y}^1_{l+1,l+2} \in \mathrm{span}(\mathbf{A})$ (otherwise, no $\mathbb{F}_q^\times$-linear combination of X_1 and X_{l+1} is recoverable from A, Q, and X_j for any $j \notin \{1, l+1\}$, and this violates the privacy condition). Now, consider the messages X_2 and X_{l+2}. Similarly as above, it can be shown that there exists $j \in J \setminus \{l+2\}$ such that $\mathbf{Y}^2_{l+2,j} \in \mathrm{span}(\mathbf{A})$.

Now, we will show that $j \neq l+1$. Suppose, for the sake of contradiction, that $j = l+1$. Note that $\tilde{\mathbf{Y}}^1_{l+1,l+2}$ and $\tilde{\mathbf{Y}}^2_{l+2,l+1}$ must be linearly independent (otherwise, there exists an $\mathbb{F}_q$-linear combination of $\mathbf{X}_1$ and $\mathbf{X}_2$ in $\mathrm{span}(\mathbf{A})$, which yields a contradiction). Thus, X_{l+1} and X_{l+2} must be recoverable from A, Q, X_I. This is however a contradiction because $l+1$ and $l+2$ do not belong to R. Thus, $j \neq l+1$. Assume, w.l.o.g., that $j = l+3$. Then, $\mathbf{Y}^2_{l+2,l+3} \in \mathrm{span}(\mathbf{A})$. Note that $\mathbf{Y}^1_{l+1,l+2}$ and $\mathbf{Y}^2_{l+2,l+3}$ are linearly independent.

Next, consider the messages $\mathbf{X}_1$ and $\mathbf{X}_{l+3}$. By a similar argument as above, it follows that there exists $\mathbf{Y}^1_{l+3,j} \in \mathrm{span}(\mathbf{A})$ for some $j \in J \setminus [l+3]$. We will show that $j \notin \{l+1, l+2\}$. Suppose, for the sake of contradiction, that $\mathbf{Y}^1_{l+3,l+1} \in \mathrm{span}(\mathbf{A})$ (or $\mathbf{Y}^1_{l+3,l+2} \in \mathrm{span}(\mathbf{A})$). If $\tilde{\mathbf{Y}}^1_{l+3,l+1}$ (or $\tilde{\mathbf{Y}}^1_{l+3,l+2}$) is not linearly dependent on $\tilde{\mathbf{Y}}^1_{l+1,l+2}$ and $\tilde{\mathbf{Y}}^2_{l+2,l+3}$, then $X_{l+1}, X_{l+2}, X_{l+3}$ are recoverable from A, Q, X_I. This is a contradiction. Otherwise, if linearly dependent, there must exist an $\mathbb{F}_q$-linear combination of $\mathbf{X}_1$ and $\mathbf{X}_2$ in $\mathrm{span}(\mathbf{A})$. This is again a contradiction. Thus, $j \notin \{l+1, l+2\}$. Assume, w.l.o.g., that $j = l+4$. Then, $\mathbf{Y}^1_{l+1,l+4} \in \mathrm{span}(\mathbf{A})$. Again, note that $\mathbf{Y}^1_{l+1,l+2}$, $\mathbf{Y}^2_{l+2,l+3}$, and $\mathbf{Y}^1_{l+1,l+4}$ are linearly independent.

By repeating the above arguments and reordering the indices of the messages (if needed), it can be shown that $\mathrm{span}(\mathbf{A})$ contains $K-l$ linearly independent $\mathbb{F}_q^\times$-linear combinations $\mathbf{Y}^1_{l+1,l+2}, \mathbf{Y}^2_{l+2,l+3}, \mathbf{Y}^1_{l+3,l+4}, \ldots,$ and $\mathbf{Y}^1_{K-1,K}$ (or $\mathbf{Y}^2_{K-1,K}$) if $K-l$ is odd (or even). Assume, w.l.o.g., that $K-l$ is odd. Consider the messages $\mathbf{X}_1$ and $\mathbf{X}_K$. Similarly as before, it follows that there exists no $\mathbb{F}_q^\times$-linear combination $\mathbf{Y}^1_{K,j} \notin \mathrm{span}(\mathbf{A})$ for any $j \in J \setminus \{K\}$. Thus, there exists $\mathbf{Y}^1_{K,j} \in \mathrm{span}(\mathbf{A})$ for some $j \in [l] \setminus \{1\}$ (otherwise, no $\mathbb{F}_q^\times$-linear combination of X_1 and X_K can be recovered from A, Q, and X_j for any $j \notin \{1, K\}$, violating the privacy condition). Thus, X_K must be recoverable from A, Q, X_I. This is however a contradiction because $K \notin R$. Then, it follows that the assumption that $H(\mathbf{A}) < (K-2)L$ does not hold, and hence, $H(\mathbf{A}) \geq (K-2)L$, as was to be shown. □

References

[1] 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.

[2] H. Sun and S. A. Jafar, "The capacity of private computation," Oct 2017. [Online]. Available: arXiv:1710.11098

[3] 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

[4] 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.

[5] 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.

[6] S. Kadhe, B. Garcia, A. Heidarzadeh, S. E. Rouayheb, and A. Sprintson, "Private information retrieval with side information," Sept 2017. [Online]. Available: arXiv:1709.00112

[7] Z. Chen, Z. Wang, and S. Jafar, "The capacity of private information retrieval with private side information."

[8] 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

[9] S. A. Obead and J. Kliewer, "Achievable rate of private function retrieval from MDS coded databases," Feb 2018. [Online]. Available: arXiv:1802.08223

[10] S. A. Obead, H.-Y. Lin, E. Rosnes, and J. Kliewer, "Capacity of private linear computation for coded databases," Oct 2018. [Online]. Available: arXiv:1810.04230

[11] M. Mirmohseni and M. A. Maddah-Ali, "Private function retrieval," in *2018 Iran Workshop on Communication and Information Theory (IWCIT)*, April 2018, pp. 1–6.

[12] Z. Chen, Z. Wang, and S. A. Jafar, "The asymptotic capacity of private search," Jan 2018. [Online]. Available: arXiv:1801.05768