The Capacity of Private Information Retrieval With Private Side Information Under Storage Constraints

Yi-Peng Wei, *Student Member, IEEE*, and Sennur Ulukus, *Fellow, IEEE*

***Abstract*— We consider the problem of private information retrieval (PIR) of a single message out of K messages from N replicated and non-colluding databases where a cache-enabled user (retriever) of cache-size S possesses side information in the form of uncoded portions of the messages where the message identities are unknown to the databases. The identities of these side information messages need to be kept private from the databases, i.e., we consider PIR with private side information (PSI). We characterize the optimal normalized download cost for this PIR-PSI problem under the storage constraint S as $D^* = 1+\frac{1}{N}+\frac{1}{N^2}+\cdots+\frac{1}{N^{K-1-M}}+\frac{1-r_M}{N^{K-M}}+\frac{1-r_{M-1}}{N^{K-M+1}}+\cdots+\frac{1-r_1}{N^{K-1}}$, where M is the number of side information messages and r_i is the portion of the ith side information message that is cached with $\sum_{i=1}^{M} r_i = S$. Based on this capacity result, we prove two facts: First, for a fixed memory size S and a fixed number of accessible messages M, uniform caching achieves the lowest normalized download cost, i.e., $r_i = \frac{S}{M}$, for $i = 1, \ldots, M$, is optimum. Second, for a fixed memory size S, among all possible $K - \lceil S \rceil + 1$ uniform caching schemes, the uniform caching scheme which caches $M = K$ messages achieves the lowest normalized download cost.**

***Index Terms*— Private information retrieval, private side information, uncoded caching, storage constraints.**

I. Introduction

WE CONSIDER the private information retrieval (PIR) problem with private side information (PSI) for a cache-enabled user (retriever) under a cache storage size constraint. PIR refers to the problem where a user wishes to download a desired message from distributed replicated databases while keeping the identity of the desired message private against the databases. PSI refers to the setting where the user (retriever) possesses cached messages in its local storage, which it wants to utilize to decrease the download cost during PIR, but at the same time, keep their identities private against the databases. The goal of the PIR-PSI problem is to devise the most efficient retrieval scheme under the joint desired message and side information privacy constraints. The efficiency of a PIR-PSI scheme is measured by the normalized download cost which is the ratio of the number of total downloaded bits to the number of desired bits. In this work, we consider the PIR-PSI problem under a storage size constraint at the user, and investigate how best the fixed-size user cache can be utilized.

We introduce the PIR-PSI problem under a storage constraint using the example shown in Fig. 1. Consider a user wanting to download a message from $N = 3$ non-communicating databases, each storing the same set of $K = 5$ messages. Assume that the user is already in possession of $M = 3$ messages through some unspecified means; the user may have obtained these from another user, or it may have prefetched them from another database. The databases do not know the identities of these messages, but they know that the user has access to $M = 3$ messages. (For this example, say these messages are W_2, W_4 and W_5.) However, the user has limited local storage with size $S = 1$ message. What should the user keep in order to minimize the download cost of the desired message during the PIR phase while keeping the identities of both desired and cached messages private? Should the user keep 1 full message in its cache and discard the other 2 messages, shown as caching option 1 in Fig. 1? Should the user choose 2 messages, store half of each chosen message and discard the remaining 1 message, shown as caching option 2 in Fig. 1? Or, should the user keep all 3 messages and store a portion of each? In that case, what portions of messages should the user store? E.g., should it store 25% of W_2, 25% of W_4 and 50% of W_5, shown as caching option 3, or should it store $\frac{1}{3}$ of all 3 messages, shown as caching option 4 in Fig. 1?

Different caching schemes result in different download costs for the PIR-PSI problem. Intuition may say that if portions of many messages are kept in the cache, then the user will need to protect many identities from the databases due to the PSI requirement, which may seem disadvantageous. On the other hand, intuition may also say that keeping portions of many messages may improve the diversity of side information for the PIR phase, which may seem advantageous. What is the optimum way to utilize the user's limited cache memory?

Manuscript received June 1, 2018; revised April 28, 2019; accepted November 5, 2019. Date of publication November 18, 2019; date of current version March 17, 2020. This work was supported by NSF under Grant CNS 13-14733, Grant CCF 14-22111, Grant CNS 15-26608, and Grant CCF 17-13977. This work was presented in part at the 2018 IEEE Information Theory Workshop.

Y.-P. Wei was with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA. He is now with Google Inc., Mountain View, CA 94043 USA (e-mail: yipengwei@google.com).

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Communicated by M. Bloch, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2953883

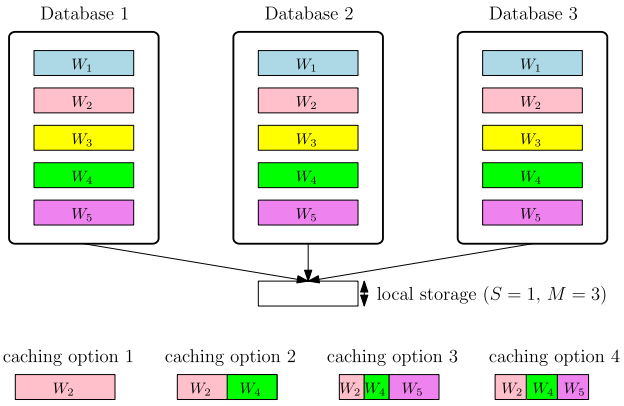

Fig. 1. PIR-PSI under a storage constraint. Here $N = 3$, $K = 5$, $S = 1$, and $M = 3$.

In this work, we characterize the optimal normalized download cost for any given caching strategy, and determine the optimal caching strategy under a given storage constraint.

Related Work: The PIR problem has originated in the computer science community [1]–[5] and has drawn attention in the information theory society [6]–[11] in recent years. In the classical setting of PIR, there are N non-communicating databases, each storing the same set of K messages. The user wishes to download one of these K messages without letting the databases know the identity of the desired message. Sun and Jafar [12] have characterized the optimal normalized download cost for the classical PIR problem to be $\frac{D}{L} = \left(1 + \frac{1}{N} + \cdots + \frac{1}{N^{K-1}}\right)$, where L is the message size and D is the total number of downloaded bits from the N databases. After [12], many interesting variants of the classical PIR problem have been investigated in [13]–[45]. The most closely related branch of PIR to our setting in this paper is cache-aided PIR in [26], [30]–[33], [36], [39].

Cache-aided PIR is first considered in [26], where the user has a local cache of storage S messages (SL bits) which can store any function of the K messages, and the cache content of the user is perfectly known to all the N databases. The optimal normalized download cost for this case is $D^*(S) = (1 - \frac{S}{K})\left(1 + \frac{1}{N} + \cdots + \frac{1}{N^{K-1}}\right)$, which indicates that the user should download the uncached part of the content via the optimum PIR scheme in [12]. The result is somewhat pessimistic since the user cannot further reduce the download cost by using the cache content. This has motivated subsequent works which have considered the case where the databases are completely unaware or partially unaware of the cache content [30]–[33], [36], [39]. Within this sub-branch of literature, references [30], [32], [33] have considered PIR with PSI.

In [30], the authors considered the case where the user randomly chooses M full messages out of K messages to cache, and none of the databases is aware of the identities of the M chosen messages. The user wishes to keep the identities of the M chosen messages and the desired message private, which is coined as PIR with PSI. For the case of a single database, the optimal normalized download cost is settled in [30]. For general number of databases, the optimal normalized download cost is characterized in [32] as $D^*(M) = \left(1 + \frac{1}{N} + \cdots + \frac{1}{N^{K-1-M}}\right)$. In [33], a more practical scenario is considered where each database is aware of the identities of the messages cached from that database only and unaware of the remaining identities of messages cached from other databases, which is coined as PIR with partially known PSI. Interestingly, the optimal normalized download cost for PIR with partially known PSI is the same as the optimal normalized download cost for PIR with PSI.

Coming back to our paper, in this work, we consider PIR-PSI under a storage constraint. In the prefetching phase, the user can access M messages, and has a local cache storage of S messages (SL symbols), where $S \leq M$. For each of these M messages, the user caches the first Lr_i symbols out of the total L symbols for $i = 1, \ldots, M$. The caching scheme is subject to a memory size constraint, i.e., $\sum_{i=1}^{M} r_i = S$, and is known to all the databases. Note that in [31], [36], [39], for each message, the user randomly chooses Lr symbols out of the total L symbols to cache, and the cached Lr symbols' indices are partially/totally unknown to all the databases, while in this work, the cached Lr_i symbols' indices are totally known to all the databases. In [31], [36], [39], to reliably reconstruct the desired message, the user should record the indices of the cached symbols within each message. In contrast, here, we consider the case where the user caches the first Lr_i symbols of each message instead of random Lr_i symbols; this saves the user extra storage overhead. The databases are aware of the caching scheme, but do not know the identities of the cached messages, i.e., the databases know M and r_i for $i = 1, \ldots, M$, but do not know the identities of the cached messages. In the retrieval phase, the user wishes to jointly keep the identities of the cached messages and the desired message private. We call this model as PIR-PSI under a storage constraint.

For any given caching scheme, i.e., for given M and $(r_1, r_2, \ldots, r_M)$, we characterize the optimal normalized download cost to be $D^* = 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}} + \frac{1-r_M}{N^{K-M}} + \frac{1-r_{M-1}}{N^{K-M+1}} + \cdots + \frac{1-r_1}{N^{K-1}}$, where without loss of generality $r_1 \geq r_2 \geq \cdots \geq r_M$. Based on this capacity result, we prove two important facts: First, for a fixed memory size S and fixed number of accessible messages M, uniform caching achieves the lowest normalized download cost, where uniform caching means $r_i = \frac{S}{M}$, for $i = 1, \ldots, M$. Second, for a fixed memory size S, among all the $K - \lceil S \rceil + 1$ uniform caching schemes, the uniform caching scheme which caches K messages achieves the lowest normalized download cost. That is, in order to optimally utilize the limited user cache memory, if the user has access to M files, it should keep SL/M bits (equal amounts) from each message in its cache memory; and second, if possible, the user should aim to have access to all K messages, i.e., $M = K$ yields the lowest download cost.

II. System Model

We consider a system consisting of N non-communicating databases and a user (retriever). Each database stores the same set of K independent messages $W_1, \ldots, W_K$, and each

message is of size L symbols, i.e.,

$$H(W_1) = \cdots = H(W_K) = L, \tag{1}$$

$$H(W_1, \ldots, W_K) = H(W_1) + \cdots + H(W_K). \tag{2}$$

The user has a local cache memory which is of size SL symbols, where $S \in [0, K]$. There are two phases in the system: the prefetching phase and the retrieval phase.

In the prefetching phase, the user can randomly access M messages out of total K messages, where $M \geq S$. For each of the M accessed messages, the user caches the first Lr_i symbols out of the total L symbols for $i = 1, \ldots, M$. The caching scheme is subject to a memory size constraint of S, i.e.,

$$\sum_{i=1}^{M} r_i = S. \tag{3}$$

We denote the indices (identities) of the cached M messages as $\mathbb{H}$, and denote $\mathcal{W}_{\mathbb{H}}$ as the cached messages. Therefore, $|\mathbb{H}| = M$, and $H(\mathcal{W}_{\mathbb{H}}) = SL$.

Note that M and $(r_1, \ldots, r_M)$ specify a caching scheme. If $r_1 = \cdots = r_M$, we call this a uniform caching scheme. For fixed S, there are $K - \lceil S \rceil + 1$ uniform caching schemes depending on the number of accessible messages since $M \geq S$. For instance, if there are $K = 3$ messages in the databases and $S = 1.5$, then since $M \geq S$, M can take one of two possible values: either 2 or 3. Thus, there are two uniform caching schemes depending on the value of M. Note, $K - \lceil S \rceil + 1 = 3 - \lceil 1.5 \rceil + 1 = 2$.

We assume that all the databases are aware of the caching scheme but are unaware of which messages are cached. For example, if $S = 2$, $M = 3$, and we say that the user has applied a uniform caching scheme, the databases know that the user has chosen 3 messages out of the total K messages to cache, and for each chosen message, the user has cached the first $\frac{2}{3}L$ symbols out of the total L symbols. However, the databases do not know which messages are cached by the user.

In the retrieval phase, the user privately generates an index $\theta \in [K] = \{1, \ldots, K\}$, and wishes to retrieve message W_θ such that it is impossible for any individual database to identify θ. At the same time, the user also wishes to keep the indices of the M cached messages private, i.e., in the retrieval phase the databases cannot learn which messages are cached. For random variables θ, $\mathbb{H}$, and $W_1, \ldots, W_K$, we have

$$\begin{aligned} &H(\theta, \mathbb{H}, W_1, \ldots, W_K) \\ &\quad = H(\theta) + H(\mathbb{H}) + H(W_1) + \cdots + H(W_K). \end{aligned} \tag{4}$$

In order to retrieve message W_θ, the user sends N queries $Q_1^{[\theta,\mathbb{H}]}, \ldots, Q_N^{[\theta,\mathbb{H}]}$ to the N databases, where $Q_n^{[\theta,\mathbb{H}]}$ is the query sent to the nth database for message W_θ. Note that the queries are generated according to $\mathbb{H}$, which are independent of the realization of the K messages. Therefore,

$$I(W_1, \ldots, W_K; Q_1^{[\theta,\mathbb{H}]}, \ldots, Q_N^{[\theta,\mathbb{H}]}) = 0. \tag{5}$$

Upon receiving the query $Q_n^{[\theta,\mathbb{H}]}$, the nth database replies with an answering string $A_n^{[\theta,\mathbb{H}]}$, which is a function of $Q_n^{[\theta,\mathbb{H}]}$ and all the K messages. Therefore, $\forall \theta \in [K], \forall n \in [N]$,

$$H(A_n^{[\theta,\mathbb{H}]} | Q_n^{[\theta,\mathbb{H}]}, W_1, \ldots, W_K) = 0. \tag{6}$$

After receiving the answering strings $A_1^{[\theta,\mathbb{H}]}, \ldots, A_N^{[\theta,\mathbb{H}]}$ from all the N databases, the user needs to decode the desired message W_θ reliably. By using Fano's inequality, we have the following reliability constraint

$$\begin{aligned} &H\left(W_\theta | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_1^{[\theta,\mathbb{H}]}, \ldots, Q_N^{[\theta,\mathbb{H}]}, A_1^{[\theta,\mathbb{H}]}, \ldots, A_N^{[\theta,\mathbb{H}]}\right) \\ &\quad = o(L), \end{aligned} \tag{7}$$

where $o(L)$ denotes a function such that $\frac{o(L)}{L} \to 0$ as $L \to \infty$.

To ensure that individual databases do not know which message is retrieved and to keep the M cached messages private, we have the following privacy constraint, $\forall n \in [N]$, $\forall \theta, \theta' \in [K]$, $\forall \mathbb{H}, \mathbb{H}' \subset [K]$ such that $|\mathbb{H}| = |\mathbb{H}'| = M$,

$$\begin{aligned} &(Q_n^{[\theta,\mathbb{H}]}, A_n^{[\theta,\mathbb{H}]}, W_1, \ldots, W_K) \\ &\quad \sim (Q_n^{[\theta',\mathbb{H}']}, A_n^{[\theta',\mathbb{H}']}, W_1, \ldots, W_K), \end{aligned} \tag{8}$$

where $A \sim B$ means that A and B are identically distributed.

For a fixed N, K, S and caching scheme $(r_1, \ldots, r_M)$, a pair (D, L) is achievable if there exists a PIR scheme for the message which is of size L symbols satisfying the reliability constraint (7) and the privacy constraint (8), where D represents the expected number of downloaded bits (over all the queries) from the N databases via the answering strings $A_{1:N}^{[\theta,\mathbb{H}]}$, where $A_{1:N}^{[\theta,\mathbb{H}]} = (A_1^{[\theta,\mathbb{H}]}, \ldots, A_N^{[\theta,\mathbb{H}]})$, i.e.,

$$D = \sum_{n=1}^{N} H\left(A_n^{[\theta,\mathbb{H}]}\right). \tag{9}$$

In this work, we aim at characterizing the optimal normalized download cost D^*, where

$$D^* = \inf\left\{\frac{D}{L} : (D, L) \text{ is achievable}\right\}. \tag{10}$$

III. Main Results and Discussions

We characterize the exact normalized download cost for PIR-PSI under a storage constraint in the following theorem.

Theorem 1 *In PIR-PSI under a storage constraint S, the optimal normalized download cost is*

$$\begin{aligned} D^* =& 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}} + \frac{1 - r_M}{N^{K-M}} \\ &+ \frac{1 - r_{M-1}}{N^{K-M+1}} + \cdots + \frac{1 - r_1}{N^{K-1}} \end{aligned} \tag{11}$$

where M is the number of side information messages, r_i is the portion of the ith side information message that is cached with $\sum_{i=1}^{M} r_i = S$, and $r_1 \geq r_2 \geq \cdots \geq r_M$ without loss of generality.

The converse proof for Theorem 1 is given in Section IV, and the achievability proof for Theorem 1 is given in Section V.

Remark 1 *For $S = 0$, by letting $r_i = 0$, for $i = 1, \ldots, M$,* (11) *reduces to*

$$D^* = 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1}}, \tag{12}$$

which is the optimal normalized download cost of the original PIR problem as shown in [12].

Remark 2 *For $S \in [K]$ and $M = S$, by letting $r_i = 1$ for $i = 1, \ldots, M$,* (11) *reduces to*

$$D^* = 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}}, \tag{13}$$

which is the optimal normalized download cost of the PIR with PSI problem as shown in [32]. We can further generalize the result to the PIR with partially known PSI as shown in [33]. Note further that for $M > S$, $(\frac{1-r_M}{N^{K-M}} + \frac{1-r_{M-1}}{N^{K-M+1}} + \cdots + \frac{1-r_1}{N^{K-1}})$ is the penalty to the download cost under the storage constraint.

Corollary 1 *For fixed $M \geq S$, uniform caching scheme achieves the lowest normalized download cost.*

Proof: The user has access to M messages. To achieve a low normalized download cost in (11), we need to solve the following optimization problem,

$$\begin{aligned} \min_{\alpha_i, i=1,\ldots,M} \quad & \alpha_M \frac{1}{N^{K-M}} + \alpha_{M-1} \frac{1}{N^{K-M+1}} + \cdots \\ & + \alpha_1 \frac{1}{N^{K-1}} \\ \text{s.t.} \quad & \alpha_M + \alpha_{M-1} + \cdots + \alpha_1 = M - S, \\ & 1 \geq \alpha_M \geq \alpha_{M-1} \geq \cdots \geq \alpha_1 \geq 0, \end{aligned} \tag{14}$$

which is obtained by replacing $1 - r_i$ in (11) with α_i for $i = 1, \ldots, M$. We prove by contradiction that the minimum is achieved when $\alpha_M = \alpha_{M-1}$. Suppose not, then we have optimum $\alpha_M^* > \alpha_{M-1}^*$. Choose $\delta = \frac{\alpha_M^* - \alpha_{M-1}^*}{3}$, and let $\alpha'_M = \alpha_M^* - \delta$, $\alpha'_{M-1} = \alpha_{M-1}^* + \delta$. Then, with α'_M and α'_{M-1}, we achieve a lower normalized download cost than with α_M^* and α_{M-1}^*, which gives a contradiction. Therefore, we have $\alpha_M = \alpha_{M-1}$. Intuitively, note that the coefficient of α_M is larger than the coefficient of α_{M-1} in the objective function in (14). Therefore, in order to minimize the objective function, we need to choose α_M as small as possible. But, since α_M needs to be larger than α_{M-1} according to the constraint set of (14), the smallest α_M we can choose is $\alpha_M = \alpha_{M-1}$. Using similar arguments, we also have $\alpha_{M-1} = \alpha_{M-2} = \cdots = \alpha_1$. Therefore, uniform caching achieves the lowest normalized download cost for fixed M. ■

Corollary 2 *For fixed S, among all the $K - \lceil S \rceil + 1$ uniform caching schemes, the uniform caching scheme with $M = K$ achieves the lowest normalized download cost.*

Proof: For the uniform caching scheme M, the user caches the first $\frac{S}{M}L$ symbols of each chosen message. From (11), the normalized download cost is

$$\begin{aligned} D^*(M) =& 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}} \\ & + \left(1 - \frac{S}{M}\right)\left(\frac{1}{N^{K-M}} + \cdots + \frac{1}{N^{K-1}}\right). \end{aligned} \tag{15}$$

Considering the difference of the normalized download costs between $D^*(M+1)$ and $D^*(M)$,

$$\begin{aligned} & D^*(M+1) - D^*(M) \\ & = 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-2-M}} + \\ & \quad \left(1 - \frac{S}{M+1}\right)\left(\frac{1}{N^{K-M-1}} + \cdots + \frac{1}{N^{K-1}}\right) \\ & \quad - \left[1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}}\right. \\ & \quad \left. + \left(1 - \frac{S}{M}\right)\left(\frac{1}{N^{K-M}} + \cdots + \frac{1}{N^{K-1}}\right)\right] \qquad (16) \\ & = -\frac{S}{M+1}\left(\frac{1}{N^{K-M-1}} + \cdots + \frac{1}{N^{K-1}}\right) \\ & \quad + \frac{S}{M}\left(\frac{1}{N^{K-M}} + \cdots + \frac{1}{N^{K-1}}\right) \qquad (17) \\ & = -\frac{S}{M+1} \times \frac{1}{N^{K-M-1}} \\ & \quad + \left(\frac{S}{M} - \frac{S}{M+1}\right)\left(\frac{1}{N^{K-M}} + \cdots + \frac{1}{N^{K-1}}\right) \qquad (18) \\ & = \frac{S}{M(M+1)}\left(\frac{1}{N^{K-M}} + \cdots + \frac{1}{N^{K-1}}\right) \\ & \quad - \frac{S}{M(M+1)} \times \frac{M}{N^{K-M-1}} \qquad (19) \\ & \leq 0. \qquad (20) \end{aligned}$$

Thus, the uniform caching scheme with $M = K$ achieves the lowest normalized download cost among all possible uniform caching schemes. ■

Corollary 3 *For fixed S, among all possible caching schemes, the uniform caching scheme with $M = K$ achieves the lowest normalized download cost.*

Proof: From Corollary 1, we know that for fixed M, uniform caching scheme achieves the lowest normalized download cost. From Corollary 2, we know that among all uniform caching schemes, the uniform caching scheme with $M = K$ achieves the lowest normalized download cost. Combining these two corollaries, we conclude that among all possible caching schemes, the uniform caching scheme with $M = K$ achieves the lowest normalized download cost. ■

Remark 3 *In this work, we consider that all the databases know the caching scheme, i.e., the databases know M and r_i for $i = 1, \ldots, M$. Since the user caches the first Lr_i symbols for $i = 1, \ldots, M$, all the databases know the cached symbols' indices, which is different from that in [31], [36], [39]. In [31], [36], the cached symbols' indices are randomly chosen and completely unknown to all the databases, and*

in [39], the cached symbols' indices are partially known to the databases.

Remark 4 *References [31], [39] only considered the case where $M = K$ and $r_i = r$, $i = 1, \ldots, K$, i.e., the user accesses every message and caches the same amount from each message, while in our current work, we relax both conditions such that $M \leq K$ and r_i is arbitrary. We also note that references [31], [39] consider only PIR, while our current paper considers PIR-PSI.*

Remark 5 *A natural extension to this work is to consider the case with randomly chosen indices as in [31], [39]. While we could generalize the schemes in [31], [39], which were developed for PIR-only to the case of PIR-PSI in this paper, we observed two problems with this approach: First, the generalization is standard and does not add any additional insights into this paper but lengthens it and distracts attention from the main focus of this paper which is PIR-PSI with a storage constraint. Second, when symbols are chosen randomly, we do not have a capacity result in general except in special cases (e.g., $K = 2, 3$ messages as emphasized in [31], [39]). Therefore, the case where the user randomly caches Lr_i symbols is an interesting but different formulation, which even without a PSI constraint, has been a problem which is still mostly open.*

IV. Converse Proof

In this section, we provide a lower bound for PIR-PSI under a storage constraint. In the following, without loss of generality, we relabel the messages according to $\mathbb{H}$, such that $W_{1:M}$ are the messages accessed by the user in the prefetching phase, where $W_{1:M} = (W_1, W_2, \ldots, W_M)$. Here, W_i denotes the message whose first Lr_i symbols are cached by the user, for $i = 1, 2, \ldots, M$, and without loss of generality, $r_1 \geq r_2 \geq \cdots \geq r_M$.

We first need the following lemma, which develops a lower bound on the length of the undesired portion of the answering strings as a consequence of the privacy constraint.

Lemma 1 (Interference lower bound) *For PIR-PSI under a storage constraint, the interference from undesired messages within the answering strings, $D - L$, is lower bounded by,*

$$D - L + o(L) \geq I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, W_K\right). \tag{21}$$

If the privacy constraint is absent, the user downloads only L symbols of the desired message, however, when the privacy constraint is present, it should download D symbols. The difference between D and L, i.e., $D - L$, corresponds to the undesired portion of the answering strings. Note that Lemma 1 is an extension of [12, Lemma 5], where $M = 0$, i.e., the user has no PSI. Lemma 1 differs from its counterpart in [31, Lemma 1] in two aspects; first, the left hand side is $D(r) - L(1 - r)$ in [31] as the user requests to download the uncached bits only, and second, [31, Lemma 1] constructs $K-1$ distinct lower bounds by changing k, in contrast to only one bound here. In addition, we note that a similar argument to Lemma 1 can be implied from [32] and [33]. The main difference between Lemma 1 and [32], [33] is that $\mathcal{W}_{\mathbb{H}}$ refers to parts of messages here, while in [32], [33], $\mathcal{W}_{\mathbb{H}}$ refers to full messages.

Proof: We start with the right hand side of (21),

$$\begin{aligned} &I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, W_K\right) \\ &\quad \leq I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]}, W_K | \mathcal{W}_{\mathbb{H}}, \mathbb{H}\right). \end{aligned} \tag{22}$$

For the right hand side of (22), we have

$$\begin{aligned} &I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]}, W_K | \mathcal{W}_{\mathbb{H}}, \mathbb{H}\right) \\ &\quad = I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}\right) \\ &\qquad + I\left(W_{1:K-1}; W_K | Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]}, \mathcal{W}_{\mathbb{H}}, \mathbb{H}\right) && (23) \\ &\quad \overset{(7)}{=} I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}\right) + o(L) && (24) \\ &\quad \overset{(4),(5)}{=} I\left(W_{1:K-1}; A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_{1:N}^{[K,\mathbb{H}]}\right) + o(L) && (25) \\ &\quad = H\left(A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_{1:N}^{[K,\mathbb{H}]}\right) \\ &\qquad - H\left(A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_{1:N}^{[K,\mathbb{H}]}, W_{1:K-1}\right) + o(L) && (26) \\ &\quad \leq D - H\left(A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_{1:N}^{[K,\mathbb{H}]}, W_{1:K-1}\right) + o(L) && (27) \\ &\quad \overset{(7)}{=} D - H\left(A_{1:N}^{[K,\mathbb{H}]}, W_K | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_{1:N}^{[K,\mathbb{H}]}, W_{1:K-1}\right) \\ &\qquad + o(L) && (28) \\ &\quad \leq D - H\left(W_K | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, Q_{1:N}^{[K,\mathbb{H}]}, W_{1:K-1}\right) + o(L) && (29) \\ &\quad \overset{(4),(5)}{=} D - L + o(L) && (30) \end{aligned}$$

where (24), (28) follow from the decodability of W_K given $\left(Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]}, \mathcal{W}_{\mathbb{H}}, \mathbb{H}\right)$, (25), (30) follow from the independence of $W_{1:K}$ and $Q_{1:N}^{[K,\mathbb{H}]}$ given $\mathbb{H}$, and (27) follows from the independence bound. Combining (22) and (30) yields (21). ■

For the conditional mutual information term on the right hand side of (21), we have

$$\begin{aligned} &I\left(W_{1:K-1}; Q_{1:N}^{[K,\mathbb{H}]}, A_{1:N}^{[K,\mathbb{H}]} | \mathcal{W}_{\mathbb{H}}, \mathbb{H}, W_K\right) \\ &\quad = \sum_h p(h) I\left(W_{1:K-1}; Q_{1:N}^{[K,h]}, A_{1:N}^{[K,h]} | \mathcal{W}_h, h, W_K\right) && (31) \\ &\quad = \sum_h p(h) I\left(W_{1:K-1}; Q_{1:N}^{[K,h]}, A_{1:N}^{[K,h]} | \mathcal{W}_h, W_K\right). && (32) \end{aligned}$$

where we have written the mutual information in (21) as an expectation over all possible caching scheme realizations, as the databases do not know which messages are cached.

In the following lemma, we develop an inductive relation for the mutual information term on the right hand side of (32).

Lemma 2 (Fractional induction lemma) *For all $k \in \{1, \ldots, K-1\}$, the mutual information term in* (32) *can be*

inductively lower bounded as,

$$I\left(W_{1:k};Q_{1:N}^{[k+1,h]},A_{1:N}^{[k+1,h]}|\mathcal{W}_h,W_{k+1:K}\right) \geq \frac{1}{N}I\left(W_{1:k-1};Q_{1:N}^{[k,h]},A_{1:N}^{[k,h]}|\mathcal{W}_h,W_{k:K}\right) + \frac{L}{N}(1-r_k)-o(L), \tag{33}$$

where $r_k = 0$ when $k > M$.

Lemma 2 is a generalization of [12, Lemma 6] to our setting. The main difference between Lemma 2 and [12, Lemma 6] is that the cached PSI results in a different induction relation.

Proof: We start with the left hand side of (33),

$$I\left(W_{1:k};Q_{1:N}^{[k+1,h]},A_{1:N}^{[k+1,h]}|\mathcal{W}_h,W_{k+1:K}\right) = \frac{1}{N}\times N\times I\left(W_{1:k};Q_{1:N}^{[k+1,h]},A_{1:N}^{[k+1,h]}|\mathcal{W}_h,W_{k+1:K}\right) \tag{34}$$

$$\geq \frac{1}{N}\sum_{n=1}^{N} I\left(W_{1:k};Q_{n}^{[k+1,h]},A_{n}^{[k+1,h]}|\mathcal{W}_h,W_{k+1:K}\right) \tag{35}$$

$$\overset{(8)}{=} \frac{1}{N}\sum_{n=1}^{N} I\left(W_{1:k};Q_{n}^{[k,h]},A_{n}^{[k,h]}|\mathcal{W}_h,W_{k+1:K}\right) \tag{36}$$

$$\geq \frac{1}{N}\sum_{n=1}^{N} I\left(W_{1:k};A_{n}^{[k,h]}|\mathcal{W}_h,W_{k+1:K},Q_{n}^{[k,h]}\right) \tag{37}$$

$$\overset{(6)}{=} \frac{1}{N}\sum_{n=1}^{N} H\left(A_{n}^{[k,h]}|\mathcal{W}_h,W_{k+1:K},Q_{n}^{[k,h]}\right) \tag{38}$$

$$\geq \frac{1}{N}\sum_{n=1}^{N} H\left(A_{n}^{[k,h]}|\mathcal{W}_h,W_{k+1:K},Q_{1:N}^{[k,h]},A_{1:n-1}^{[k,h]}\right) \tag{39}$$

$$\overset{(6)}{=} \frac{1}{N}\sum_{n=1}^{N} I\left(W_{1:k};A_{n}^{[k,h]}|\mathcal{W}_h,W_{k+1:K},Q_{1:N}^{[k,h]},A_{1:n-1}^{[k,h]}\right) \tag{40}$$

$$= \frac{1}{N}I\left(W_{1:k};A_{1:N}^{[k,h]}|\mathcal{W}_h,W_{k+1:K},Q_{1:N}^{[k,h]}\right) \tag{41}$$

$$\overset{(4),(5)}{=} \frac{1}{N}I\left(W_{1:k};Q_{1:N}^{[k,h]},A_{1:N}^{[k,h]}|\mathcal{W}_h,W_{k+1:K}\right) \tag{42}$$

$$\overset{(7)}{=} \frac{1}{N}I\left(W_{1:k};W_k,Q_{1:N}^{[k,h]},A_{1:N}^{[k,h]}|\mathcal{W}_h,W_{k+1:K}\right)-o(L) \tag{43}$$

$$= \frac{1}{N}I\left(W_{1:k};W_k|\mathcal{W}_h,W_{k+1:K}\right) + \frac{1}{N}I\left(W_{1:k};Q_{1:N}^{[k,h]},A_{1:N}^{[k,h]}|\mathcal{W}_h,W_{k:K}\right)-o(L) \tag{44}$$

$$= \frac{1}{N}I\left(W_{1:k};Q_{1:N}^{[k,h]},A_{1:N}^{[k,h]}|\mathcal{W}_h,W_{k:K}\right) + \frac{L}{N}(1-r_k)-o(L), \tag{45}$$

where (35) and (37) follow from the chain rule and the non-negativity of mutual information, (36) follows from the privacy constraint, (38), (40) follow from the fact that answer strings are deterministic functions of the messages and the queries, (39) follows from the fact that conditioning reduces entropy, (42) follows from the independence of $W_{1:K}$ and $Q_{1:N}^{[k,h]}$, (43) follows from the reliability constraint on W_k, and (45) is due to the fact that $H\left(W_k|\mathcal{W}_h,W_{k+1:K}\right)=L(1-r_k)$, where if $k\notin h$ then $r_k=0$. ■

By applying Lemma 2 recursively to the right hand side of (32)

$$I\left(W_{1:K-1};Q_{1:N}^{[K,h]},A_{1:N}^{[K,h]}|\mathcal{W}_h,W_K\right) \overset{(33)}{\geq} \frac{1}{N}I\left(W_{1:K-2};Q_{1:N}^{[K-1,h]},A_{1:N}^{[K-1,h]}|\mathcal{W}_h,W_{K-1:K}\right) + \frac{L}{N}-o(L) \tag{46}$$

$$\overset{(33)}{\geq} \frac{1}{N^2}I\left(W_{1:K-3};Q_{1:N}^{[K-2,h]},A_{1:N}^{[K-2,h]}|\mathcal{W}_h,W_{K-2:K}\right) + \frac{L}{N^2}+\frac{L}{N}-o(L) \tag{47}$$

$$\overset{(33)}{\geq} \cdots \tag{48}$$

$$\overset{(33)}{\geq} \frac{I\left(W_{1:M};Q_{1:N}^{[M+1,h]},A_{1:N}^{[M+1,h]}|\mathcal{W}_h,W_{M+1:K}\right)}{N^{K-1-M}} + \frac{L}{N^{K-1-M}}+\cdots+\frac{L}{N^2}+\frac{L}{N}-o(L) \tag{49}$$

$$\overset{(33)}{\geq} \frac{1}{N^{K-M}}I\left(W_{1:M-1};Q_{1:N}^{[M,h]},A_{1:N}^{[M,h]}|\mathcal{W}_h,W_{M:K}\right) + \frac{L}{N^{K-M}}(1-r_M)+\frac{L}{N^{K-1-M}}+\cdots+\frac{L}{N^2} + \frac{L}{N}-o(L) \tag{50}$$

$$\overset{(33)}{\geq} \cdots \tag{51}$$

$$\overset{(33)}{\geq} \frac{L(1-r_1)}{N^{K-1}}+\cdots+\frac{L(1-r_M)}{N^{K-M}}+\cdots+\frac{L}{N^2} + \frac{L}{N}-o(L). \tag{52}$$

Note that in (46) to (49), we apply the fractional induction lemma with $r=0$, since $W_{M+1:K}$ are not cached in $\mathcal{W}_h$. In (50) to (52), $r_k>0$ for the fractional induction lemma, since $W_{1:M}$ are cached in $\mathcal{W}_h$ partially.

By combining (21), (32), and (52), and dividing by L on both sides, we obtain a lower bound for the normalized download cost as

$$D^* \geq 1+\frac{1}{N}+\frac{1}{N^2}+\cdots+\frac{1}{N^{K-1-M}} + \frac{1-r_M}{N^{K-M}}+\frac{1-r_{M-1}}{N^{K-M+1}}+\cdots+\frac{1-r_1}{N^{K-1}}, \tag{53}$$

which proves (11).

V. Achievability Proof

Our achievability scheme is based on the PIR schemes in [12] and [32]. For the portion of the messages not cached by the user, we use the PIR scheme in [12], which applies the following three principles recursively: 1) database symmetry, 2) message symmetry within each database, and 3) exploiting undesired messages as side information. For the portion of the messages cached by the user, we use the PIR scheme in [32], which is based on MDS codes and consists of two stages: The first stage determines the systematic part of the MDS code according to the queries generated in [12]. In the second

stage, the user reduces the download cost by downloading the parity part of the MDS code only. By applying the two PIR schemes, the user retrieves the desired message privately while keeping the cached messages private.

A. Motivating Examples

1) $N = 2$ Databases, $K = 5$ Messages, $M = 2$ Accessed Messages, and $S = 1$ with Uniform Caching: In this example, in the prefetching phase, the user randomly chooses two messages to cache, say W_1 and W_4. Since $S = 1$ and the user uses uniform caching scheme, the user caches the first half of W_1 and the first half of W_4. We note that the databases are aware of the caching scheme, i.e., the databases know that two out of five messages are chosen by the user, and the first halves of the chosen messages are cached. However, the databases do not know which are the two chosen messages.

In the retrieval phase, assume that the user wishes to retrieve message W_3 privately. For the first half portion of the message, i.e., for the symbols in the interval $[0, \frac{L}{2}]$, since the user has cached messages W_1 and W_4, the user applies the PIR scheme in [32] with $M = 2$. The total download cost for the first half portion of the message, as shown in (13), is

$$\frac{L}{2} \times \left(1 + \frac{1}{2} + \frac{1}{2^{5-1-2}}\right). \tag{54}$$

For the remaining half portion of the message, i.e., for the symbols in the interval $[\frac{L}{2}, L]$, since the user has not cached any messages, the user applies the PIR scheme in [12]. The total download cost for the remaining half portion of the message, as shown in (12), is

$$\frac{L}{2} \times \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^{5-1}}\right). \tag{55}$$

The overall download cost is the sum of (54) and (55). Therefore, the optimal normalized download cost is $\frac{59}{32}$, which can also be obtained through (11) by letting $r_1 = \frac{1}{2}$ and $r_2 = \frac{1}{2}$. Note that since we have applied the PIR scheme in [32] to retrieve the first half portion of the message, the databases cannot learn which messages are cached by the user. In addition, both PIR schemes in [12] and [32] keep the identity of the desired message private. Therefore, the combination of these two PIR schemes is a feasible PIR scheme for PIR-PSI a under storage constraint [16].

2) $N = 2$ Databases, $K = 5$ Messages, $S = 1$, $M = 3$ with $r_1 = \frac{1}{2}$, and $r_2 = r_3 = \frac{1}{4}$: In this example, see Fig. 2, in the prefetching phase, since $r_1 = \frac{1}{2}$, the user first randomly chooses one message to cache, say W_3, and the user caches the first half of W_3. Since $r_2 = r_3 = \frac{1}{4}$, the user then randomly chooses two other messages to cache, say W_2 and W_5, and the user caches the first $\frac{1}{4}$ portions of W_2 and W_5. Note that $S = 1$ and $\frac{1}{2} \times 1 + \frac{1}{4} \times 2 = 1$, and the local cache memory size constraint is satisfied. We note that the databases are aware of the caching strategy, i.e., the databases know that three out of five messages are chosen by the user, and for one of the chosen message, the first half of the message is cached, and for the remaining two chosen messages, the first $\frac{1}{4}$ portions are cached. However, the databases do not know which three messages are chosen.

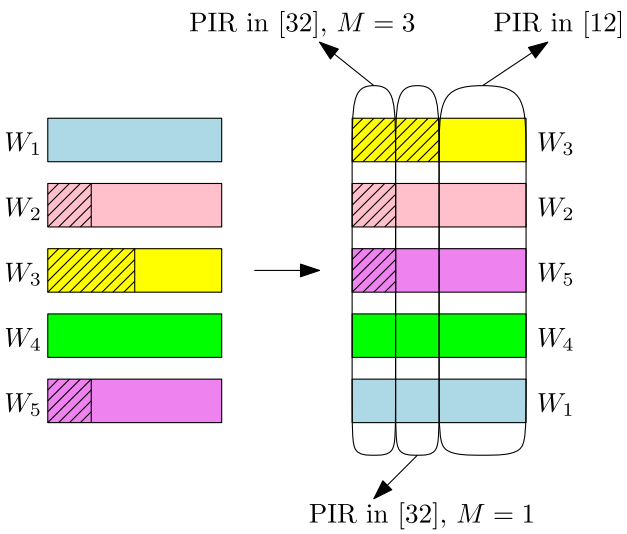

Fig. 2. Achievable scheme: $K = 5$, $S = 1$, and $M = 3$ with $r_1 = \frac{1}{2}$, and $r_2 = r_3 = \frac{1}{4}$.

In the retrieval phase, assume that the user wishes to retrieve message W_1 privately. For the first $\frac{1}{4}$ portion of messages, i.e., for the symbols in the interval $[0, \frac{L}{4}]$, since the user caches messages W_2, W_3 and W_5, the user applies the PIR scheme in [32] with $M = 3$. The total download cost for the first $\frac{1}{4}$ portion of the message, as shown in (13), is

$$\frac{L}{4} \times \left(1 + \frac{1}{2^{5-1-3}}\right). \tag{56}$$

For the following $\frac{1}{4}$ portion of messages, i.e., for the symbols in the interval $[\frac{L}{4}, \frac{L}{2}]$, since the user caches message W_3, the user applies the PIR scheme in [32] with $M = 1$. The total download cost for the second $\frac{1}{4}$ portion of the message, as shown in (13), is

$$\frac{L}{4} \times \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^{5-1-1}}\right). \tag{57}$$

For the last half portion of messages, i.e., for the symbols in the interval $[\frac{L}{2}, L]$, since the user has not cached any messages, the user applies the PIR scheme in [12]. The total download cost for the last half portion of the message, as shown in (12), is

$$\frac{L}{2} \times \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^{5-1}}\right). \tag{58}$$

The overall download cost is the sum of (56), (57) and (58). Therefore, the optimal normalized download cost is $\frac{29}{16}$, which can also be obtained through (11) by letting $r_1 = \frac{1}{2}$, and $r_2 = r_3 = \frac{1}{4}$. Note that by applying the PIR scheme in [32] to retrieve the first $\frac{1}{4}$ portion and the middle $\frac{1}{4}$ portion of the message, the databases cannot learn which messages have been cached by the user. In addition, both PIR schemes in [12] and [32] hide the identity of the desired message. Therefore, the combination of these two PIR schemes is a feasible PIR scheme for PIR-PSI under a storage constraint [16].

B. General Achievable Scheme

We now describe the general achievable scheme for $r_1 \geq r_2 \geq \cdots \geq r_M$. We first consider the first r_M fraction of messages, i.e., for the symbols in the interval $[0, Lr_M]$. Since $r_1 \geq r_2 \geq \cdots \geq r_M$, the user caches M messages for this portion. The user applies the PIR scheme in [32] which results in the download cost

$$Lr_M \times \left(1 + \frac{1}{N} + + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}}\right). \quad (59)$$

Following the same logic, for the symbols in the interval $[Lr_i, Lr_{i-1}]$, $i \geq 2$, the user caches i messages for this portion. The user applies the PIR scheme in [32] which results in the download cost

$$L(r_{i-1} - r_i) \times \left(1 + \frac{1}{N} + + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-i}}\right). \quad (60)$$

Lastly, for the symbols in the interval $[Lr_1, L]$, the user caches no messages for this portion. The user applies the PIR scheme in [12] which results in the download cost

$$L(1 - r_1) \times \left(1 + \frac{1}{N} + + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1}}\right). \quad (61)$$

The overall download cost is the sum of (59), (60) for $i = 2, 3, \ldots, M$, and (61), which is (11). By applying the PIR scheme in [32] to retrieve symbols in the interval of $[0, Lr_1]$, the databases cannot learn which messages have been cached by the user. In addition, both PIR schemes in [12] and [32] protect the identity of the desired message. Therefore, the combination of these two PIR schemes is a feasible PIR scheme for PIR-PSI under a storage constraint [16].

VI. Conclusion

In this paper, we have introduced a new PIR model, namely PIR-PSI under a storage constraint. In this model, the user randomly chooses M messages and caches the first r_i portion of the chosen messages for $i = 1, \ldots, M$ subject to the memory size constraint $\sum_{i=1}^{M} r_i = S$. In the retrieval phase, the user wishes to retrieve a message such that no individual database can learn the identity of the desired message and the identities of the cached messages. For each caching scheme, i.e., $(r_1, \ldots, r_M)$, we characterized the optimal normalized download cost to be $D^* = 1 + \frac{1}{N} + \frac{1}{N^2} + \cdots + \frac{1}{N^{K-1-M}} + \frac{1-r_M}{N^{K-M}} + \frac{1-r_{M-1}}{N^{K-M+1}} + \cdots + \frac{1-r_1}{N^{K-1}}$. In addition, we showed that, for a fixed memory size S, and a fixed number of accessible messages M, uniform caching achieves the lowest normalized download cost, where uniform caching means $r_i = \frac{S}{M}$, $i = 1, \ldots, M$. Then, we showed that, for a fixed memory size S, among all $K - \lceil S \rceil + 1$ uniform caching schemes, the uniform caching scheme caching $M = K$ messages achieves the lowest normalized download cost. Finally, we conclude that for a fixed memory size S, the uniform caching scheme caching K messages achieves the lowest normalized download cost.

References

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

[2] W. Gasarch, "A survey on private information retrieval," in *Proc. Bull. EATCS*, 2004, p. 113.

[3] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Prague, Czech Republic: Springer, 1999, pp. 402–414.

[4] R. Ostrovsky and W. E. Skeith, III, "A survey of single-database private information retrieval: Techniques and applications," in *Proc. Int. Workshop Public Key Cryptogr.* Beijing, China: Springer, 2007, pp. 393–411.

[5] S. Yekhanin, "Private information retrieval," *Commun. ACM*, vol. 53, no. 4, pp. 68–73, Apr. 2010.

[6] N. B. Shah, K. V. Rashmi, and K. Ramchandran, "One extra bit of download ensures perfectly private information retrieval," in *Proc. IEEE ISIT*, Jun./Jul. 2014, pp. 856–860.

[7] G. Fanti and K. Ramchandran, "Efficient private information retrieval over unsynchronized databases," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1229–1239, Oct. 2015.

[8] T. H. Chan, S.-W. Ho, and H. Yamamoto, "Private information retrieval for coded storage," in *Proc. IEEE ISIT*, Jun. 2015, pp. 2842–2846.

[9] A. Fazeli, A. Vardy, and E. Yaakobi, "Codes for distributed PIR with low storage overhead," in *Proc. IEEE ISIT*, Jun. 2015, pp. 2852–2856.

[10] R. Tajeddine, O. W. Gnilke, and S. El Rouayheb, "Private information retrieval from MDS coded data in distributed storage systems," in *Proc. IEEE ISIT*, Jul. 2016, pp. 1411–1415.

[11] H. Sun and S. A. Jafar, "The capacity of private information retrieval," in *Proc. IEEE GLOBECOM*, Dec. 2016, pp. 1–6.

[12] 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.

[13] 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.

[14] 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. 2019.

[15] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1945–1956, Mar. 2018.

[16] H. Sun and S. A. Jafar, "Optimal download cost of private information retrieval for arbitrary message length," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2920–2932, Dec. 2017.

[17] Q. Wang and M. Skoglund, "Symmetric private information retrieval for MDS coded distributed storage," 2016, *arXiv:1610.04530*. [Online]. Available: https://arxiv.org/abs/1610.04530

[18] H. Sun and S. A. Jafar, "Multiround private information retrieval: Capacity and storage overhead," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5743–5754, Aug. 2018.

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

[20] 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.

[21] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, C. Hollanti, and S. El Rouayheb, "Private information retrieval schemes for coded data with arbitrary collusion patterns," 2017, *arXiv:1701.07636*. [Online]. Available: https://arxiv.org/abs/1701.07636

[22] K. Banawan and S. Ulukus, "Multi-message private information retrieval: Capacity results and near-optimal schemes," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6842–6862, Oct. 2018.

[23] Y. Zhang and G. Ge, "A general private information retrieval scheme for MDS coded databases with colluding servers," 2017, *arXiv:1704.06785*. [Online]. Available: https://arxiv.org/abs/1704.06785

[24] Y. Zhang and G. Ge, "Private information retrieval from MDS coded databases with colluding servers under several variant models," 2017, *arXiv:1705.03186*. [Online]. Available: https://arxiv.org/abs/1705.03186

[25] 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.

[26] 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.

[27] Q. Wang and M. Skoglund, "Secure symmetric private information retrieval from colluding databases with adversaries," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2017, pp. 1083–1090.

[28] R. Tajeddine and S. El Rouayheb, "Robust private information retrieval on coded data," in *Proc. IEEE ISIT*, Jun. 2017, pp. 1903–1907.

[29] Q. Wang and M. Skoglund, "Linear symmetric private information retrieval for MDS coded distributed storage with colluding servers," 2017, *arXiv:1708.05673*. [Online]. Available: https://arxiv.org/abs/1708.05673

[30] S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb, and A. Sprintson, "Private information retrieval with side information," 2017, *arXiv:1709.00112*. [Online]. Available: https://arxiv.org/abs/1709.00112

[31] Y.-P. 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.

[32] Z. Chen, Z. Wang, and S. Jafar, "The capacity of T-private information retrieval with private side information," 2017, *arXiv:1709.03022*. [Online]. Available: https://arxiv.org/abs/1709.03022

[33] Y.-P. Wei, K. Banawan, and S. Ulukus, "The capacity of private information retrieval with partially known private side information," *IEEE Trans. Inf. Theory*, to be published.

[34] Q. Wang and M. Skoglund, "Secure private information retrieval from colluding databases with eavesdroppers," in *Proc. IEEE ISIT*, Jun. 2018, pp. 2456–2460.

[35] H. Sun and S. A. Jafar, "The capacity of private computation," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3880–3897, Jun. 2019.

[36] M. Kim, H. Yang, and J. Lee, "Cache-aided private information retrieval," in *Proc. 51st Asilomar Conf. Signals, Syst., Comput.*, Oct./Nov. 2017, pp. 398–402.

[37] M. Mirmohseni and M. A. Maddah-Ali, "Private function retrieval," 2017, *arXiv:1711.04677*. [Online]. Available: https://arxiv.org/abs/1711.04677

[38] M. Abdul-Wahid, F. Almoualem, D. Kumar, and R. Tandon, "Private information retrieval from storage constrained databases–coded caching meets PIR," 2017, *arXiv:1711.05244*. [Online]. Available: https://arxiv.org/abs/1711.05244

[39] Y.-P. Wei, K. Banawan, and S. Ulukus, "Cache-aided private information retrieval with partially known uncoded prefetching: Fundamental limits," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 6, pp. 1126–1139, Jun. 2018.

[40] K. Banawan and S. Ulukus, "Asymmetry hurts: Private information retrieval under asymmetric traffic constraints," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 7628–7645, Nov. 2019.

[41] Z. Chen, Z. Wang, and S. Jafar, "The asymptotic capacity of private search," 2018, *arXiv:1801.05768*. [Online]. Available: https://arxiv.org/abs/1801.05768

[42] K. Banawan and S. Ulukus, "Private information retrieval through wiretap channel II: Privacy meets security," 2018, *arXiv:1801.06171*. [Online]. Available: https://arxiv.org/abs/1801.06171

[43] R. G. L. D'Oliveira and S. El Rouayheb, "Lifting private information retrieval from two to any number of messages," 2018, *arXiv:1802.06443*. [Online]. Available: https://arxiv.org/abs/1802.06443

[44] R. Tajeddine, O. W. Gnilke, and S. El Rouayheb, "Private information retrieval from MDS coded data in distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7081–7093, Nov. 2018.

[45] Q. Wang, H. Sun, and M. Skoglund, "The capacity of private information retrieval with eavesdroppers," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 3198–3214, May 2019.

Yi-Peng Wei (S'15) received the B.Sc. degree in electrical engineering from National Tsing Hua University, Taiwan, in 2009, the M.Sc. degree from the Graduate Institute of Communication Engineering, National Taiwan University, Taiwan, in 2012, and the Ph.D. degree in electrical engineering from the University of Maryland at College Park, MD, USA, in 2019, with his Ph.D. thesis on private information retrieval with side information. In 2019, he joined Google as a software engineer.

Sennur Ulukus (S'90–M'98–SM'15–F'16) is the Anthony Ephremides Professor in Information Sciences and Systems in the Department of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University. Her research interests are in information theory, wireless communications, machine learning, signal processing and networks, with recent focus on private information retrieval, age of information, distributed coded computation, energy harvesting communications, physical layer security, and wireless energy and information transfer.

Dr. Ulukus is a Distinguished Scholar-Teacher of the University of Maryland. She received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2019 IEEE Communications Society Best Tutorial Paper Award, an 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 ECE George Corcoran Outstanding Teaching Award. She is a Distinguished Lecturer of the IEEE Information Theory Society for 2018–2019. She has been on the Editorial Board of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING since 2016. She was an Editor for the IEEE *Journal on Selected Areas in Communications Series on Green Communications and Networking* (2015–2016), the IEEE TRANSACTIONS ON INFORMATION THEORY (2007–2010), and the IEEE TRANSACTIONS ON COMMUNICATIONS (2003–2007). She was a Guest Editor for the IEEE *Journal on Selected Areas in Communications* (2015 and 2008), *Journal of Communications and Networks* (2012), and the IEEE TRANSACTIONS ON INFORMATION THEORY (2011). She is a TPC co-chair of 2019 ITW, 2017 IEEE ISIT, 2016 IEEE Globecom, 2014 IEEE PIMRC, and 2011 IEEE CTW.