X-secure T-private Information Retrieval from MDS Coded Storage with Byzantine and Unresponsive Servers

Zhuqing Jia and Syed A. Jafar

Center for Pervasive Communications and Computing (CPCC), UC Irvine
Email: {zhuqingj, syed}@uci.edu

Abstract

The problem of X-secure T-private information retrieval from MDS coded storage is studied in this paper, where the user wishes to privately retrieve one out of K independent messages that are distributed over N servers according to an MDS code. It is guaranteed that any group of up to X colluding servers learn nothing about the messages and that any group of up to T colluding servers learn nothing about the identity of desired message. A lower bound of achievable rates is proved by presenting a novel scheme based on *cross-subspace alignment* and a successive decoding with interference cancellation strategy. For large number of messages ($K \to \infty$) the achieved rate, which we conjecture to be optimal, improves upon the best known rates previously reported in the literature by Raviv and Karpuk, and generalizes an achievable rate for MDS-TPIR previously found by Freij-Hollanti et al. that is also conjectured to be asymptotically optimal. The setting is then expanded to allow unresponsive and Byzantine servers. Finally, the scheme is applied to find a new lower convex hull of (download, upload) pairs of secure and private distributed matrix multiplication that generalizes, and in certain asymptotic settings strictly improves upon the best known previous results.

1 Introduction

Originating in computer science and cryptography, the problem of private information retrieval (PIR) [1] seeks efficient ways to retrieve desired messages from distributed servers without disclosing to the servers which messages are desired. The *rate* of PIR is the maximum number of bits of desired message that can be retrieved per bit of total download from all servers [2]. PIR has recently attracted much attention in the information theory community, where the focus has been on finding the capacity (maximum rate) [2] or equivalently, minimizing the download cost [3] under various constraints. The study of PIR is important from an information theoretic perspective not only because privacy is important, but also because optimal PIR schemes often reveal novel coding structures, thereby advancing our understanding of structured codes, a cornerstone of network information theory. The fundamental significance of these coding structures is emphasized by the connections between PIR and a number of other important problems such as locally decodable codes [4,5], locally repairable codes [6], batch codes [7], oblivious transfer [8,9], instance hiding [1,10], secret sharing [11], blind interference alignment [12,13], and secure computation [14], including recent works on secure distributed matrix multiplication [15–20]. As the literature on information theoretic PIR continues to grow, it is also valuable to find unified perspectives that combine our understanding of various aspects of PIR and allow generalizations beyond PIR. Against this background, the contribution of this work is summarized in Figure 1.

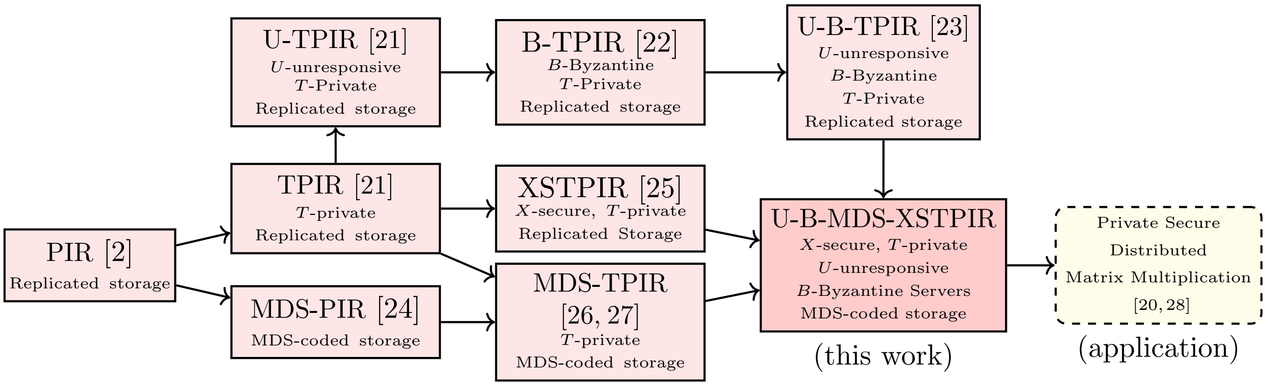

Figure 1: *The U-B-MDS-XSTPIR setting studied in this work generalizes previously studied settings of PIR [2], TPIR [21], MDS-PIR [24], MDS-TPIR [26, 27], XSTPIR [25], U-TPIR [21], B-TPIR [22], and U-B-TPIR [23] as shown, and finds application beyond PIR in the context of Private Secure Distributed Matrix Multiplication (PSDMM).*

The capacity of PIR with K messages, N servers, and replicated storage was characterized in [2] as $C_{\text{PIR}} = \left(1 + \frac{1}{N} + \cdots + \frac{1}{N^{K-1}}\right)^{-1}$. Since the number of messages, K is typically large, of particular interest is the asymptotic value of capacity as $K \to \infty$. Evidently, the asymptotic capacity of PIR is $C_{\text{PIR}}^{\infty} = 1 - \frac{1}{N}$. The asymptotically optimal achievable scheme builds upon a prior construction from [29] and may be seen as a form of blind interference alignment [12]. The capacity of TPIR, i.e., PIR with a T-privacy constraint and replicated storage was characterized in [21]. and its asymptotic value is $C_{\text{TPIR}}^{\infty} = 1 - \frac{T}{N}$. The optimal achievable scheme uses an MDS coded query structure. The T-Privacy constraint requires that no information about the desired message index is leaked to any set of up to T colluding servers. The capacity of MDS-PIR, i.e., PIR with (N, K_c) MDS-coded storage was characterized in [24] and its asymptotic value turns out to be $C^{\infty}_{\text{MDS-PIR}} = 1 - \frac{K_c}{N}$. MDS-TPIR, i.e., PIR with both T-privacy and (N, K_c) MDS coded storage was studied in [26] and while its capacity remains open [27], the asymptotic achievable rate of $R^{\infty}_{\text{MDS-TPIR}} = 1 - \frac{T+K_c-1}{N}$ is expected to be optimal. The novel achievable scheme of [26] is based on star products of GRS (Generalized Reed-Solomon) codes. The asymptotic capacity of XSTPIR, i.e., PIR with X-secure storage, T-private queries, and replicated storage was found in [25] as $1 - (X + T)/N$. The achievable scheme of [25] is based on the novel idea of cross-subspace alignment, which has subsequently found use in the context of secure distributed matrix multiplication [17, 19].

In this work we study the problem of U-B-MDS-XSTPIR, i.e., PIR with X-secure data, T-private queries, (N, K_c) MDS coded storage, where U servers are unresponsive and up to B servers are Byzantine (who may return erroneous responses). In particular we show that a rate of $R^{\infty}_{\text{U-B-MDS-XSTPIR}} = 1 - \left(\frac{K_c+X+T+2B-1}{N-U}\right)$ is achievable for any number of messages K. This rate strictly improves upon the previous best known rate $R = \left(1 - \left(\frac{K_c+X+T+2B-1}{N-U}\right)\right)\left(\frac{K_c}{K_c+X}\right)$ for MDS-XSTPIR, found[1] in [30]. In fact, for MDS-XSTPIR, i.e., with $U = B = 0$, we conjecture that our rate of $R^{\infty}_{\text{MDS-XSTPIR}} = 1 - \left(\frac{K_c+X+T-1}{N}\right)$ is asymptotically optimal as $K \to \infty$, thus generalizing a previous conjecture for MDS-TPIR in [26] that can be obtained by further setting $X = 0$. Remarkably, U-B-MDS-XSTPIR is a generalization of PIR, TPIR, MDS-PIR, XSTPIR, U-TPIR, B-TPIR, and U-B-TPIR and the asymptotically optimal (or the best known) structured coding schemes for all of these problems can be obtained as a special case of the unified scheme for U-B-MDS-XSTPIR that we present in this work. The basis for this unified view, and the central technical contribution of this work, is a scheme that combines the cross-subspace alignment idea of [25] with a layered structure that allows successive decoding and interference cancellation to retrieve multiple layers of symbols from the desired message. The scheme is also shown to be applicable to the problem of secure and private distributed matrix multiplication (PSDMM) that was recently introduced in [20, 28]. Remarkably, the new scheme is able to generalize, and in certain asymptotic settings strictly improve upon the previously best known rates for PSDMM.

Notations: For a positive integer N, $[N]$ stands for the set $\{1, 2, \ldots, N\}$. The notation $X_{[N]}$ denotes the set $\{X_1, X_2, \ldots, X_N\}$. For an index set $\mathcal{I} = \{i_1, i_2, \ldots, i_n\}$, $X_{\mathcal{I}}$ denotes the set $\{X_{i_1}, X_{i_2}, \ldots, X_{i_n}\}$. For variables $\alpha_n, n \in [N]$ and an arbitrary function $f(\cdot)$, we denote the $N \times 1$ vector whose n^{th} term is $f(\alpha_n)$, as $\overrightarrow{f(\alpha)}$.

2 Problem Statement: U-B-MDS-XSTPIR

Consider K independent messages, $W_1, W_2, \ldots, W_K$. Each message is represented by ℓ uniformly random symbols from the finite field $\mathbb{F}_q$.

$$H(W_1) = H(W_2) = \cdots = H(W_K) = \ell, \tag{1}$$

$$H(W_{[K]}) = K\ell, \tag{2}$$

in q-ary units. Note that as is typical in information theory, the message sizes are unbounded, and the coding scheme may freely choose the block size ℓ. The information stored at the n^{th} server is denoted by S_n, $n \in [N]$. Messages are stored among N servers according to an MDS$(N, X + K_c)$

[1] Reference [30] considers the problem of private polynomial computation with Lagrange encoding, which reduces to MDS-XSTPIR in the special case where the functions to be computed are all distinct coordinate projections.

code which codes each message separately. From any $X + K_c$ servers, it must be possible to recover all messages.

$$H(W_{[K]}|S_{\mathcal{M}}) = 0, \quad \forall \mathcal{M} \subset [N], |\mathcal{M}| = X + K_c. \tag{3}$$

The storage requirement at each server is $K\ell/K_c$, i.e.,

$$H(S_n) = \frac{K\ell}{K_c}, \quad \forall n \in [N]. \tag{4}$$

Thus, compared to replicated storage, the storage requirement is reduced by a factor of $1/K_c$. X-secure storage, $0 \leq X \leq N$, guarantees that any X (or fewer) colluding servers learn nothing about the messages.

$$I(S_{\mathcal{X}}; W_{[K]}) = 0, \quad \forall \mathcal{X} \subset [N], |\mathcal{X}| = X. \tag{5}$$

The user privately and uniformly generates the index of his desired message $\theta \in [K]$. To retrieve the desired message privately, the user generates N queries, $Q_{[N]}^{\theta}$. The n^{th} query Q_n^{θ} is sent to the n^{th} server. The user has no prior knowledge of the information stored at the servers, i.e.,

$$I(S_{[N]}; \theta, Q_{[N]}^{\theta}) = 0. \tag{6}$$

T-privacy, $0 \leq T \leq N$, guarantees that any T (or fewer) colluding servers learn nothing about the desired message index θ.

$$I(Q_{\mathcal{T}}^{\theta}, S_{\mathcal{T}}; \theta) = 0, \quad \forall \mathcal{T} \subset [N], |\mathcal{T}| = T. \tag{7}$$

Upon receiving the user's query Q_n^{θ}, the n^{th} server responds with the answer A_n^{θ}.

There exists a set of servers $\mathcal{B}$, $\mathcal{B} \subset [N], |\mathcal{B}| \leq B$, known as Byzantine servers, and another (disjoint) set of servers $\mathcal{U}$, $\mathcal{U} \subset [N], |\mathcal{U}| = U$, known as unresponsive servers. The user knows U, B but the realizations of the sets $\mathcal{U}, \mathcal{B}$, are not known to the user *apriori.* The Byzantine servers respond to the user arbitrarily, possibly introducing errors. The unresponsive servers do not respond at all. However, the remaining servers, i.e., servers in $[N] \setminus (\mathcal{B} \cup \mathcal{U})$, respond to the user truthfully with a function of the query and their stored information.

$$H(A_n^{\theta}|Q_n^{\theta}, S_n) = 0, \quad \forall n \in [N] \setminus (\mathcal{B} \cup \mathcal{U}). \tag{8}$$

The user must be able to recover the desired message W_θ from the responses that he receives.

$$H(W_\theta \mid A_{[N]\setminus\mathcal{U}}^{\theta}, Q_{[N]}^{\theta}, \theta) = 0 \quad \forall \mathcal{U}, \mathcal{B} \subset [N], \mathcal{U} = U, \mathcal{B} = B, \mathcal{U} \cap \mathcal{B} = \emptyset. \tag{9}$$

The rate of a U-B-MDS-XSTPIR scheme is defined by the number of bits of desired message that are retrieved per total bit of download from all servers on average,

$$R_{\text{U-B-MDS-XSTPIR}} = \frac{H(W_\theta)}{\sum_{n\in[N]\setminus\mathcal{U}} A_n^{\theta}} = \frac{\ell}{D}. \tag{10}$$

$D = \sum_{n\in[N]\setminus\mathcal{U}} A_n^{\theta}$ is the expected number of downloaded bits from all servers. When $B = 0, U = 0$, i.e., there are no Byzantine servers and no unresponsive servers, then we refer to the problem simply as MDS-XSTPIR.

3 Result: An Achievable Rate for U-B-MDS-XSTPIR

The following lemma is essentially inherited from [25] with minor notational adjustments. Since this lemma is used extensively in this work, a brief proof is also included for the sake of completeness.

Lemma 1. *If $\underline{1}, \underline{2}, \cdots, \underline{L}, \alpha_1, \alpha_2, \cdots, \alpha_N$ are $N + L$ distinct elements of $\mathbb{F}_q$, with $1 \leq L \leq N-1$, then the following $N \times N$ matrix is invertible over $\mathbb{F}_q$.*

$$\mathbf{M}_{L,N} \triangleq \begin{bmatrix} \frac{1}{\underline{1}-\alpha_1} & \frac{1}{\underline{2}-\alpha_1} & \cdots & \frac{1}{\underline{L}-\alpha_1} & 1 & \alpha_1 & \cdots & \alpha_1^{N-L-1} \\ \frac{1}{\underline{1}-\alpha_2} & \frac{1}{\underline{2}-\alpha_2} & \cdots & \frac{1}{\underline{L}-\alpha_2} & 1 & \alpha_2 & \cdots & \alpha_2^{N-L-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \frac{1}{\underline{1}-\alpha_N} & \frac{1}{\underline{2}-\alpha_N} & \cdots & \frac{1}{\underline{L}-\alpha_N} & 1 & \alpha_N & \cdots & \alpha_N^{N-L-1} \end{bmatrix} \tag{11}$$

Proof. To set up a proof by contradiction, suppose M is not invertible. Then there exist constants $c_n \in \mathbb{F}_q, n \in [N]$, at least one of which is non-zero, such that $\sum_{n\in[N]} c_n \mathbf{M}_{:,n} = \mathbf{0}$, where $\mathbf{M}_{:,n}$ is the n^{th} column of $\mathbf{M}$. Define

$$\Delta \triangleq (\underline{1}-\alpha)(\underline{2}-\alpha)\cdots(\underline{L}-\alpha). \tag{12}$$

Then the polynomial

$$g(\alpha) = \Delta \left(\sum_{l\in[L]} \frac{c_l}{\underline{l}-\alpha} + \sum_{n=L+1}^{N} c_n \alpha^{n-L-1} \right) \tag{13}$$

has at least N distinct roots: $\alpha_1, \alpha_2, \cdots, \alpha_N$. But $g(\alpha)$ has degree no more than $N-1$, so it must be the zero polynomial. This implies that $c_n = 0$ for all $n \in [N]$. The contradiction completes the proof. □

Theorem 1. *The following rate is achievable for U-B-MDS-XSTPIR,*

$$R_{\text{U-B-MDS-XSTPIR}}(N, K_c, X, T, U, B, K) = 1 - \left(\frac{K_c + X + T + 2B - 1}{N - U} \right). \tag{14}$$

The achievability of this rate, proved in Section 4, is the central contribution of this work. It is based on a coding scheme that uses cross-subspace alignment along with a layered structure that allows successive decoding with interference cancellation. Note that previously the best known achievable result for U-B-MDS-XSTPIR for large number of messages ($K \to \infty$) was $R = \left(1 - \left(\frac{K_c+X+T+2B-1}{N-U}\right)\right)\left(\frac{K_c}{K_c+X}\right)$, found in [30]. Evidently our scheme achieves a strictly higher rate. While we conjecture that the rate in Theorem 1 for MDS-XSTPIR ($U = 0, B = 0$) is also the asymptotic capacity of MDS-XSTPIR, a converse proof to this effect remains beyond reach. This is to be expected, because the converse proof has also been unavailable for MDS-TPIR, which is a special case of MDS-XSTPIR. Our final result appears in Section 5 where the result of Theorem 1 is applied to the problem of Private Secure Distributed Matrix Multiplication.

4 Proof of Theorem 1

First we provide the proof of achievability for $U = 0, B = 0$, i.e., with no unresponsive or Byzantine servers. Throughout the scheme, let us define

$$L = N - (K_c + X + T - 1). \tag{15}$$

and let us set

$$\ell = LK_c. \tag{16}$$

Let us start with an illustrative example.

4.1 $X = 1, T = 1, K_c = 2, N = 4$

Here we have $L = 1$ and $\ell = 2$. So let each message consist of $\ell = 2$ symbols from a finite field $\mathbb{F}_q$, where $q \geq L + N = 5$. Let $\mathbf{W}_{11}$ and $\mathbf{W}_{12}$ be two $1 \times K$ row vectors containing the first and second symbol from every message, respectively. Let $\mathbf{Z}_{11}$ be a uniformly distributed random noise vector from $\mathbb{F}_q^{1\times K}$, that will be used to provide $X = 1$ security for the stored data. Let $\mathbf{Z}'^1_{11}$, $\mathbf{Z}'^2_{11}$ be independent, uniformly distributed random noise vectors from $\mathbb{F}_q^{K\times 1}$ that will be used to provide $T = 1$ privacy for the queries. Let $\mathbf{Q}_\theta$ be the θ-th column of the $K \times K$ identity matrix, where θ is the index of desired message. The independence between message, noise vectors, and desired message index θ is formalized as follows.

$$H(\mathbf{W}_{11}, \mathbf{W}_{12}, \mathbf{Z}_{11}, \mathbf{Z}'^1_{11}, \mathbf{Z}'^2_{11}, \theta) = H(\mathbf{W}_{11}) + H(\mathbf{W}_{12}) + H(\mathbf{Z}_{11}) + H(\mathbf{Z}'^1_{11}) + H(\mathbf{Z}'^2_{11}) + H(\theta). \tag{17}$$

Note that by the definition of $\mathbf{W}_{11}$, $\mathbf{W}_{12}$ and $\mathbf{Q}_\theta$, the inner products $\mathbf{W}_{11}\mathbf{Q}_\theta$ and $\mathbf{W}_{12}\mathbf{Q}_\theta$ are precisely the two symbols of the desired message, that the user wishes to retrieve. Let $\underline{1}, \alpha_1, \alpha_2, \cdots, \alpha_N$, represent $N + 1$ distinct elements of $\mathbb{F}_q$. The storage at the n-th server is constructed as follows.

$$S_n = \left(\frac{1}{(\underline{1} - \alpha_n)^2} \mathbf{W}_{11} + \frac{1}{\underline{1} - \alpha_n} \mathbf{W}_{12} + \mathbf{Z}_{11} \right), \tag{18}$$

Thus, the data is coded along with the noise according to an MDS$(N, K_c + X)$, i.e., MDS$(4, 3)$ code. The presence of noise guarantees that the data is $(X = 1)$ secure. The query sent by the user to the n-th server to privately retrieve the θ-th message, consists of $K_c = 2$ rounds, which are denoted as $Q_n^{\theta,1}$ and $Q_n^{\theta,2}$ respectively.

$$Q_n^{\theta,1} = (\underline{1} - \alpha_n)\mathbf{Q}_\theta + (\underline{1} - \alpha_n)^2 \mathbf{Z}'^1_{11}, \tag{19}$$

$$Q_n^{\theta,2} = \mathbf{Q}_\theta + (\underline{1} - \alpha_n)^2 \mathbf{Z}'^2_{11}. \tag{20}$$

Upon receiving the query from user, the answer returned by the n-th server is

$$A_n^\theta = (S_n Q_n^{\theta,1}, S_n Q_n^{\theta,2}). \tag{21}$$

Now let us see why correctness is guaranteed. We rewrite $S_n Q_n^{\theta,1}$ as

$$S_n Q_n^{\theta,1} = \left(\frac{1}{(\underline{1} - \alpha_n)^2} \mathbf{W}_{11} + \frac{1}{\underline{1} - \alpha_n} \mathbf{W}_{12} + \mathbf{Z}_{11} \right) \left((\underline{1} - \alpha_n)\mathbf{Q}_\theta + (\underline{1} - \alpha_n)^2 \mathbf{Z}'^1_{11} \right) \tag{22}$$

$$= \frac{1}{\underline{1} - \alpha_n} \mathbf{W}_{11}\mathbf{Q}_\theta + \underbrace{\left(\mathbf{W}_{11}\mathbf{Z}'^1_{11} + \mathbf{W}_{12}\mathbf{Q}_\theta \right)}_{I_1} + (\underline{1} - \alpha_n) \underbrace{\left(\mathbf{W}_{12}\mathbf{Z}'^1_{11} + \mathbf{Z}_{11}\mathbf{Q}_\theta \right)}_{I_2} + (\underline{1} - \alpha_n)^2 \underbrace{\mathbf{Z}_{11}\mathbf{Z}'^1_{11}}_{I_3}. \tag{23}$$

Now, note that the terms $1, (\underline{1} - \alpha_n), (\underline{1} - \alpha_n)^2$, can each be expanded into weighted sums of the terms $1, \alpha_n, \alpha_n^2$. Re-grouping terms according to this expansion, and collecting $S_n Q_n^{\theta,1}$ terms from the answers received from all $N = 4$ servers, we obtain

$$\begin{bmatrix} S_1Q_1^{\theta,1} \\ S_2Q_2^{\theta,1} \\ S_3Q_3^{\theta,1} \\ S_4Q_4^{\theta,1} \end{bmatrix} = \begin{bmatrix} \frac{1}{\underline{1}-\alpha_1} & 1 & \alpha_1 & \alpha_1^2 \\ \frac{1}{\underline{1}-\alpha_2} & 1 & \alpha_2 & \alpha_2^2 \\ \frac{1}{\underline{1}-\alpha_3} & 1 & \alpha_3 & \alpha_3^2 \\ \frac{1}{\underline{1}-\alpha_4} & 1 & \alpha_4 & \alpha_4^2 \end{bmatrix} \begin{bmatrix} \mathbf{W}_{11}\mathbf{Q}_\theta \\ I_1 + \underline{1}I_2 + \underline{1}^2 I_3 \\ -I_2 - \underline{1}I_3 - \underline{1}I_3 \\ I_3 \end{bmatrix} \tag{24}$$

Since the 4×4 matrix is $\mathbf{M}_{1,4}$ which is invertible according to Lemma 1, the user is able to retrieve his first desired symbol, $\mathbf{W}_{11}\mathbf{Q}_\theta$. Now, in order to retrieve his second desired symbol, $\mathbf{W}_{11}\mathbf{Q}_\theta$, the user will use successive decoding along with cancellation of interference from the previously retrieved desired symbol. Consider the second part of the answer received from each server, $S_nQ_n^{\theta,2}$, which can be written as follows.

$$S_nQ_n^{\theta,2} = \left(\frac{1}{(\underline{1}-\alpha_n)^2}\mathbf{W}_{11} + \frac{1}{\underline{1}-\alpha_n}\mathbf{W}_{12} + \mathbf{Z}_{11}\right)\left(\mathbf{Q}_\theta + (\underline{1}-\alpha_n)^2\mathbf{Z}_{11}'^2\right) \tag{25}$$

$$= \frac{1}{(\underline{1}-\alpha_n)^2}\underbrace{\mathbf{W}_{11}\mathbf{Q}_\theta}_{I_0'} + \frac{1}{\underline{1}-\alpha_n}\mathbf{W}_{12}\mathbf{Q}_\theta + \underbrace{(\mathbf{W}_{11}\mathbf{Z}_{11}'^2 + \mathbf{Z}_{11}\mathbf{Q}_\theta)}_{I_1'} + (\underline{1}-\alpha_n)\underbrace{\mathbf{W}_{12}\mathbf{Z}_{11}'^2}_{I_2'} + (\underline{1}-\alpha_n)^2\underbrace{\mathbf{Z}_{11}\mathbf{Z}_{11}'^2}_{I_3'} \tag{26}$$

Aside from the desired symbol $\mathbf{W}_{12}\mathbf{Q}_\theta$, there are four *interference* terms I_0', I_1', I_2', I_3'. Now, since the user has already retrieved $\mathbf{W}_{11}\mathbf{Q}_\theta$, he can subtract I_0' from $S_nQ_n^{\theta,2}$. Furthermore, like before, the remaining interference terms can be expanded along α_n^t, $t \in \{0, 1, 2\}$. Thus the user is able to obtain

$$\begin{bmatrix} S_1Q_1^{\theta,2} - \frac{I_0'}{(\underline{1}-\alpha_1)^2} \\ S_2Q_2^{\theta,2} - \frac{I_0'}{(\underline{1}-\alpha_2)^2} \\ S_3Q_3^{\theta,2} - \frac{I_0'}{(\underline{1}-\alpha_3)^2} \\ S_4Q_4^{\theta,2} - \frac{I_0'}{(\underline{1}-\alpha_4)^2} \end{bmatrix} = \begin{bmatrix} \frac{1}{\underline{1}-\alpha_1} & 1 & \alpha_1 & \alpha_1^2 \\ \frac{1}{\underline{1}-\alpha_2} & 1 & \alpha_2 & \alpha_2^2 \\ \frac{1}{\underline{1}-\alpha_3} & 1 & \alpha_3 & \alpha_3^2 \\ \frac{1}{\underline{1}-\alpha_4} & 1 & \alpha_4 & \alpha_4^2 \end{bmatrix} \begin{bmatrix} \mathbf{W}_{12}\mathbf{Q}_\theta \\ I_1' + \underline{1}I_2' + \underline{1}^2 I_3' \\ -I_2' - \underline{1}I_3' - \underline{1}I_3' \\ I_3' \end{bmatrix} \tag{27}$$

from which, by inverting the matrix $\mathbf{M}_{1,4}$, the user is able to retrieve his second desired symbol, $\mathbf{W}_{12}\mathbf{Q}_\theta$. This completes the proof of correctness.

For ease of reference, a compact summary of the storage at each server, the queries, and a partitioning of signal and interference dimensions contained in the answers from each server, is provided in Table 1. Queries and answers of each round are partitioned with dashed lines. Recovered desired symbols from previous rounds that can be canceled appear along vectors that are wrapped with rounded-corner boxes.

$T = 1$-privacy and $X = 1$-security follows from the fact that queries and storage are protected by the i.i.d. uniformly distributed noise vectors $\mathbf{Z}_{11}$ and $\mathbf{Z}_{11}'^1$, $\mathbf{Z}_{11}'^2$ respectively. Finally, let us calculate the rate achieved by the scheme. From 8 downloaded q-ary symbols, the user retrieves 2 desired q-ary symbols, so the rate achieved is $R = 2/8 = 1/4 = 1 - 3/4$. This completes the proof of achievability for the setting $U = B = 0, X = 1, T = 1, K_c = 2, N = 4$.

4.1.1 $X = 1, T = 1, K_c = 2, N = 5$

Here we have $L = N - (X + T + K_c - 1) = 2$ and $\ell = LK_c = 4$. So let each message consist of $\ell = 4$ symbols from a finite field $\mathbb{F}_q$, where $q \geq L + N = 7$. Let $\mathbf{W}_{11}, \mathbf{W}_{21}, \mathbf{W}_{12}, \mathbf{W}_{22}$ be four $1 \times K$

	Server 'n' (Replace α with α_n)
Storage(S_n)	$\frac{1}{(\underline{1}-\alpha)^2}\mathbf{W}_{11}+\frac{1}{\underline{1}-\alpha}\mathbf{W}_{12}+\mathbf{Z}_{11}$
Query ($Q_n^{[\theta]}$)	$(\underline{1}-\alpha)\mathbf{Q}_\theta+(\underline{1}-\alpha)^2\mathbf{Z}'^{1}_{11}$ - $\mathbf{Q}_\theta+(\underline{1}-\alpha)^2\mathbf{Z}'^{2}_{11}$
Desired symbols appear along vectors $\overrightarrow{(\underline{1}-\alpha)^{-1}}$ - $\boxed{\overrightarrow{(\underline{1}-\alpha)^{-2}}},\overrightarrow{(\underline{1}-\alpha)^{-1}}$	
Interference appears along vectors $\overrightarrow{1},\overrightarrow{(\underline{1}-\alpha)},\overrightarrow{(\underline{1}-\alpha)^2}\equiv\overrightarrow{1},\overrightarrow{\alpha},\overrightarrow{\alpha^2}$	

Table 1: *A summary of the MDS-XSTPIR scheme for* $X=1,T=1,K_c=2,N=4,U=0,B=0$*, showing storage at each server, the queries, and a partitioning of signal and interference dimensions contained in the answers from each server.*

row vectors containing the four symbols from every message, respectively. Let $\mathbf{Z}_{11},\mathbf{Z}_{21}$ be two independent, uniformly distributed random noise vector from $\mathbb{F}_q^{1\times K}$ that will be used to guarantee $X=1$ security. Similarly, let $\mathbf{Z}'^{1}_{11},\mathbf{Z}'^{1}_{21}$, $\mathbf{Z}'^{2}_{11},\mathbf{Z}'^{2}_{21}$ be independent, uniformly distributed random noise vectors from $\mathbb{F}_q^{K\times 1}$ that will be used to guarantee $T=1$ privacy. As before, let $\mathbf{Q}_\theta$ be the θ-th column of the $K\times K$ identity matrix, where θ is the index of desired message. The desired message W_θ can be represented as

$$\begin{aligned} W_\theta &= (\mathbf{W}_{lk}\mathbf{Q}_\theta)_{l\in[2],k\in[2]} && (28)\\ &= (\mathbf{W}_{11}\mathbf{Q}_\theta,\mathbf{W}_{12}\mathbf{Q}_\theta,\mathbf{W}_{21}\mathbf{Q}_\theta,\mathbf{W}_{22}\mathbf{Q}_\theta). && (29)\end{aligned}$$

The independence between message, noise vectors, and desired message index θ is specified as follows.

$$\begin{aligned} &H(\mathbf{W}_{11},\mathbf{W}_{21},\mathbf{W}_{12},\mathbf{W}_{22},\mathbf{Z}_{11},\mathbf{Z}_{21},\mathbf{Z}'^{1}_{11},\mathbf{Z}'^{1}_{21},\mathbf{Z}'^{2}_{11},\mathbf{Z}'^{2}_{21},\theta)\\ &=\sum_{l\in[2],k\in[2]} H(\mathbf{W}_{lk})+H(\mathbf{Z}_{11})+H(\mathbf{Z}_{21})+H(\mathbf{Z}'^{1}_{11})+H(\mathbf{Z}'^{1}_{21})+H(\mathbf{Z}'^{2}_{11})+H(\mathbf{Z}'^{2}_{21})+H(\theta). \quad (30)\end{aligned}$$

Let $\underline{1},\underline{2},\alpha_1,\alpha_2,\cdots,\alpha_5$ be $L+N=2+5=7$ distinct elements of $\mathbb{F}_q$, $q\geq 7$. The storage at the n-th server is constructed as follows.

$$S_n=(S_{n1},S_{n2}), \quad (31)$$

where

$$S_{n1} = \frac{1}{(\underline{1}-\alpha_n)^2}\mathbf{W}_{11} + \frac{1}{\underline{1}-\alpha_n}\mathbf{W}_{12} + \mathbf{Z}_{11}, \tag{32}$$

$$S_{n2} = \frac{1}{(\underline{2}-\alpha_n)^2}\mathbf{W}_{21} + \frac{1}{\underline{2}-\alpha_n}\mathbf{W}_{22} + \mathbf{Z}_{21} \tag{33}$$

so that each of (32) and (33) codes noise with message symbols across N servers according to an MDS$(N, K_c + X)$ code, guaranteeing $X = 1$ security on top of MDS coded storage. The query sent to the n-th server to retrieve the θ^{th} message consists of $K_c = 2$ rounds, $Q_n^{\theta,1}$ and $Q_n^{\theta,2}$. Furthermore, we will set

$$Q_n^{\theta,1} = (Q_{n1}^{\theta,1}, Q_{n2}^{\theta,1}) \tag{34}$$

$$Q_n^{\theta,2} = (Q_{n1}^{\theta,2}, Q_{n2}^{\theta,2}) \tag{35}$$

where

$$Q_{n1}^{\theta,1} =(\underline{1}-\alpha_n)\mathbf{Q}_\theta + (\underline{1}-\alpha_n)^2\mathbf{Z}_{11}'^{1}, \tag{36}$$

$$Q_{n2}^{\theta,1} =(\underline{2}-\alpha_n)\mathbf{Q}_\theta + (\underline{2}-\alpha_n)^2\mathbf{Z}_{21}'^{1}, \tag{37}$$

$$Q_{n1}^{\theta,2} =\mathbf{Q}_\theta + (\underline{1}-\alpha_n)^2\mathbf{Z}_{11}'^{2}, \tag{38}$$

$$Q_{n2}^{\theta,2} =\mathbf{Q}_\theta + (\underline{2}-\alpha_n)^2\mathbf{Z}_{21}'^{2}. \tag{39}$$

Upon receiving the query from user, the answer returned by the n-th server is comprised of two symbols,

$$\begin{aligned} A_n^\theta &= (A_{n1}^\theta, A_{n2}^\theta) && (40)\\ &= (S_{n1}Q_{n1}^{\theta,1} + S_{n2}Q_{n2}^{\theta,1}, \quad S_{n1}Q_{n1}^{\theta,2} + S_{n2}Q_{n2}^{\theta,2}). && (41) \end{aligned}$$

Now let us see why correctness is guaranteed. Consider the first symbol, A_{n1}^θ.

$$\begin{aligned} A_{n1}^\theta &= S_{n1}Q_{n1}^{\theta,1} + S_{n2}Q_{n2}^{\theta,1}\\ &= \frac{1}{\underline{1}-\alpha_n}\mathbf{W}_{11}\mathbf{Q}_\theta + \frac{1}{\underline{2}-\alpha_n}\mathbf{W}_{21}\mathbf{Q}_\theta + (\mathbf{W}_{11}\mathbf{Z}_{11}'^{1} + \mathbf{W}_{21}\mathbf{Z}_{21}'^{1} + \mathbf{W}_{12}\mathbf{Q}_\theta + \mathbf{W}_{22}\mathbf{Q}_\theta)\\ &\quad + (\underline{1}-\alpha_n)(\mathbf{W}_{12}\mathbf{Z}_{11}'^{1} + \mathbf{Z}_{11}\mathbf{Q}_\theta) + (\underline{2}-\alpha_n)(\mathbf{W}_{22}\mathbf{Z}_{21}'^{1} + \mathbf{Z}_{21}\mathbf{Q}_\theta)\\ &\quad + (\underline{1}-\alpha_n)^2\mathbf{Z}_{11}\mathbf{Z}_{11}'^{1} + (\underline{1}-\alpha_n)^2\mathbf{Z}_{21}\mathbf{Z}_{21}'^{1}. \end{aligned} \tag{42}$$

The first two terms in (42) are desired message symbols. Each of the remaining 5 terms can be expanded into weighted sums of terms of the form α_n^t, $t \in \{0,1,2\}$, allowing the user to represent the symbols A_{n1}^θ downloaded from all $n \in [N]$ servers, as

$$\begin{bmatrix} A_{11}^\theta\\ A_{21}^\theta\\ A_{31}^\theta\\ A_{41}^\theta\\ A_{51}^\theta \end{bmatrix} = \begin{bmatrix} \frac{1}{\underline{1}-\alpha_1} & \frac{1}{\underline{2}-\alpha_1} & 1 & \alpha_1 & \alpha_1^2\\ \frac{1}{\underline{1}-\alpha_2} & \frac{1}{\underline{2}-\alpha_2} & 1 & \alpha_2 & \alpha_2^2\\ \frac{1}{\underline{1}-\alpha_3} & \frac{1}{\underline{2}-\alpha_3} & 1 & \alpha_3 & \alpha_3^2\\ \frac{1}{\underline{1}-\alpha_4} & \frac{1}{\underline{2}-\alpha_4} & 1 & \alpha_4 & \alpha_4^2\\ \frac{1}{\underline{1}-\alpha_5} & \frac{1}{\underline{2}-\alpha_5} & 1 & \alpha_5 & \alpha_5^2 \end{bmatrix} \begin{bmatrix} \mathbf{W}_{11}\mathbf{Q}_\theta\\ \mathbf{W}_{21}\mathbf{Q}_\theta\\ *\\ *\\ * \end{bmatrix} \tag{43}$$

where we have used $*$ to represent various combinations of interference symbols that can be found explicitly by expanding (42), since those forms are not important. What matters is that the 5×5 square matrix in (43) is $\mathbf{M}_{2,5}$ which is invertible according to Lemma 1, so the user can retrieve the two desired symbols, $\mathbf{W}_{11}\mathbf{Q}_\theta$, $\mathbf{W}_{21}\mathbf{Q}_\theta$ by inverting the matrix. Next, the user needs to retrieve the remaining two desired symbols $\mathbf{W}_{12}\mathbf{Q}_\theta$, $\mathbf{W}_{22}\mathbf{Q}_\theta$, for which we will use successive decoding with interference cancellation. Consider the downloaded symbol A^θ_{n2}.

$$\begin{aligned} A^\theta_{n2} &= S_{n1}Q^{\theta,2}_{n1} + S_{n2}Q^{\theta,2}_{n2} \\ &= \frac{1}{(\underline{1}-\alpha_n)^2}\mathbf{W}_{11}\mathbf{Q}_\theta + \frac{1}{(\underline{2}-\alpha_n)^2}\mathbf{W}_{21}\mathbf{Q}_\theta + \frac{1}{\underline{1}-\alpha_n}\mathbf{W}_{12}\mathbf{Q}_\theta + \frac{1}{\underline{2}-\alpha_n}\mathbf{W}_{22}\mathbf{Q}_\theta \\ &\quad + (\mathbf{W}_{11}\mathbf{Z}'^2_{11} + \mathbf{W}_{21}\mathbf{Z}'^2_{21} + \mathbf{Z}_{11}\mathbf{Q}_\theta + \mathbf{Z}_{21}\mathbf{Q}_\theta) + (\underline{1}-\alpha_n)\mathbf{W}_{12}\mathbf{Z}'^2_{11} + (\underline{2}-\alpha_n)\mathbf{W}_{22}\mathbf{Z}'^2_{21} \\ &\quad + (\underline{1}-\alpha_n)^2\mathbf{Z}_{11}\mathbf{Z}'^2_{11} + (\underline{2}-\alpha_n)^2\mathbf{Z}_{21}\mathbf{Z}'^2_{21}. \end{aligned} \tag{44}$$

The first two symbols in (44) are desired symbols that have already been decoded. So these terms can be subtracted out, leaving the user with the following downloaded information from all $N = 5$ servers.

$$\begin{bmatrix} A^\theta_{12} - \frac{1}{(\underline{1}-\alpha_1)^2}\mathbf{W}_{11}\mathbf{Q}_\theta - \frac{1}{(\underline{2}-\alpha_1)^2}\mathbf{W}_{21}\mathbf{Q}_\theta \\ A^\theta_{22} - \frac{1}{(\underline{1}-\alpha_2)^2}\mathbf{W}_{11}\mathbf{Q}_\theta - \frac{1}{(\underline{2}-\alpha_2)^2}\mathbf{W}_{21}\mathbf{Q}_\theta \\ A^\theta_{32} - \frac{1}{(\underline{1}-\alpha_3)^2}\mathbf{W}_{11}\mathbf{Q}_\theta - \frac{1}{(\underline{2}-\alpha_3)^2}\mathbf{W}_{21}\mathbf{Q}_\theta \\ A^\theta_{42} - \frac{1}{(\underline{1}-\alpha_4)^2}\mathbf{W}_{11}\mathbf{Q}_\theta - \frac{1}{(\underline{2}-\alpha_4)^2}\mathbf{W}_{21}\mathbf{Q}_\theta \\ A^\theta_{52} - \frac{1}{(\underline{1}-\alpha_5)^2}\mathbf{W}_{11}\mathbf{Q}_\theta - \frac{1}{(\underline{2}-\alpha_5)^2}\mathbf{W}_{21}\mathbf{Q}_\theta \end{bmatrix} = \begin{bmatrix} \frac{1}{\underline{1}-\alpha_1} & \frac{1}{\underline{2}-\alpha_1} & 1 & \alpha_1 & \alpha_1^2 \\ \frac{1}{\underline{1}-\alpha_2} & \frac{1}{\underline{2}-\alpha_2} & 1 & \alpha_2 & \alpha_2^2 \\ \frac{1}{\underline{1}-\alpha_3} & \frac{1}{\underline{2}-\alpha_3} & 1 & \alpha_3 & \alpha_3^2 \\ \frac{1}{\underline{1}-\alpha_4} & \frac{1}{\underline{2}-\alpha_4} & 1 & \alpha_4 & \alpha_4^2 \\ \frac{1}{\underline{1}-\alpha_5} & \frac{1}{\underline{2}-\alpha_5} & 1 & \alpha_5 & \alpha_5^2 \end{bmatrix} \begin{bmatrix} \mathbf{W}_{12}\mathbf{Q}_\theta \\ \mathbf{W}_{22}\mathbf{Q}_\theta \\ * \\ * \\ * \end{bmatrix} \tag{45}$$

Once again, the 5×5 square matrix in (45) is $\mathbf{M}_{2,5}$ which is invertible according to Lemma 1, so the user can retrieve his remaining two desired symbols, $\mathbf{W}_{12}\mathbf{Q}_\theta$, $\mathbf{W}_{22}\mathbf{Q}_\theta$ by inverting the matrix. This completes the proof of correctness. Let us summarize the storage at each server, the queries, and the partitioning of signal and interference dimensions contained in the answers from each server in Table 2. $T = 1$-privacy and $X = 1$-security follows from the fact that queries and storage are protected by the i.i.d. uniformly distributed noise vectors. Now consider the rate achieved by the scheme. Since the user downloads 2 symbols from each of 5 servers, we note that from a total of 10 downloaded q-ary symbols, the user is able to recover 4 desired q-ary symbols, so the rate achieved is $R = 4/10 = 2/5 = 1 - 3/5$. This completes the construction of the scheme for the setting $U = B = 0, X = 1, T = 1, K_c = 2, N = 5$. We now specify the scheme for $U = B = 0$ and arbitrary X, T, K_c, N parameters.

4.1.2 $U = B = 0$, arbitrary X, T, K_c, N

Let each message consist of $\ell = LK_c$ symbols from a finite field $\mathbb{F}_q$ where $L = N-(X+T+K_c-1)$ and $q \geq L+N$. Let $\mathbf{W}_{lk}, l \in [L], k \in [K_c]$ be $1 \times K$ row vectors. For each value of $l \in [L], k \in [K_c]$, the $1\times K$ row vector $\mathbf{W}_{lk}$ contains the $(L(k-1)+l)^{th}$ symbol from every message. Let $(\mathbf{Z}_{lx})_{l\in[L],x\in[X]}$ be independent, uniformly distributed random noise vectors from $\mathbb{F}_q^{1\times K}$ that will be used to guarantee X-security. Let $(\mathbf{Z}'^{\kappa}_{lt})_{l\in[L],t\in[T],\kappa\in[K_c]}$ be independent, uniformly distributed random noise vectors from $\mathbb{F}_q^{K\times 1}$ that will be used to guarantee that the queries are T-private. As before, let $\mathbf{Q}_\theta$ be the θ-th column of the $K \times K$ identity matrix, where θ is the index of desired message. The desired message W_θ can be represented as,

$$W_\theta = (\mathbf{W}_{lk}\mathbf{Q}_\theta)_{l\in[L],k\in[K_c]} \tag{46}$$

$$= \begin{pmatrix} \mathbf{W}_{11}\mathbf{Q}_\theta, & \mathbf{W}_{12}\mathbf{Q}_\theta, & \cdots, & \mathbf{W}_{1K_c}\mathbf{Q}_\theta \\ \mathbf{W}_{21}\mathbf{Q}_\theta, & \mathbf{W}_{22}\mathbf{Q}_\theta, & \cdots, & \mathbf{W}_{2K_c}\mathbf{Q}_\theta \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{W}_{L1}\mathbf{Q}_\theta, & \mathbf{W}_{L2}\mathbf{Q}_\theta, & \cdots, & \mathbf{W}_{LK_c}\mathbf{Q}_\theta \end{pmatrix}. \tag{47}$$

The independence between messages, noise vectors and θ is formalized as follows.

$$H((\mathbf{W}_{lk})_{l\in[L],k\in[K_c]}, (\mathbf{Z}_{lx})_{l\in[L],x\in[X]}, (\mathbf{Z}'^{\kappa}_{lt})_{l\in[L],t\in[T],\kappa\in[K_c]}, \theta)$$

$$= \sum_{l\in[L],k\in[K_c]} H(\mathbf{W}_{lk}) + \sum_{l\in[L],x\in[X]} H(\mathbf{Z}_{lx}) + \sum_{l\in[L],t\in[T],\kappa\in[K_c]} H(\mathbf{Z}'^{\kappa}_{lt}) + H(\theta). \tag{48}$$

Let $\underline{1}, \underline{2}, \cdots, \underline{L}, \alpha_1, \alpha_2, \cdots, \alpha_N$ be $L+N$ distinct elements of $\mathbb{F}_q$. Since $q \geq N+L$, these constants must exist. The storage at the n^{th} server is comprised of L symbols $(S_{nl})_{l\in[L]}$, i.e.,

$$S_n = (S_{n1}, S_{n,2}, \ldots, S_{nL}). \tag{49}$$

For all $l \in [L]$, S_{nl} is constructed as

$$S_{nl} = \frac{1}{(\underline{l}-\alpha_n)^{K_c}}\mathbf{W}_{l1} + \frac{1}{(\underline{l}-\alpha_n)^{K_c-1}}\mathbf{W}_{l2} + \cdots + \frac{1}{\underline{l}-\alpha_n}\mathbf{W}_{lK_c} + \sum_{x\in[X]} (\underline{l}-\alpha_n)^{x-1}\mathbf{Z}_{lx} \tag{50}$$

$$= \sum_{k\in[K_c]} \frac{1}{(\underline{l}-\alpha_n)^{K_c-k+1}}\mathbf{W}_{lk} + \sum_{x\in[X]} (\underline{l}-\alpha_n)^{x-1}\mathbf{Z}_{lx}. \tag{51}$$

	Server ‘n’ (Replace α with α_n)
Storage (S_n)	$\frac{1}{(\underline{1}-\alpha)^2}\mathbf{W}_{11} + \frac{1}{\underline{1}-\alpha}\mathbf{W}_{12} + \mathbf{Z}_{11}$ $\frac{1}{(\underline{2}-\alpha)^2}\mathbf{W}_{21} + \frac{1}{\underline{2}-\alpha}\mathbf{W}_{22} + \mathbf{Z}_{21}$
Query ($Q_n^{[\theta]}$)	$(\underline{1}-\alpha)\mathbf{Q}_\theta + (\underline{1}-\alpha)^2\mathbf{Z}'^{1}_{11}$ $(\underline{2}-\alpha)\mathbf{Q}_\theta + (\underline{2}-\alpha)^2\mathbf{Z}'^{1}_{21}$ $\mathbf{Q}_\theta + (\underline{1}-\alpha)^2\mathbf{Z}'^{2}_{11}$ $\mathbf{Q}_\theta + (\underline{2}-\alpha)^2\mathbf{Z}'^{2}_{21}$
	Desired symbols appear along vectors $\overrightarrow{(\underline{1}-\alpha)^{-1}}, \overrightarrow{(\underline{2}-\alpha)^{-1}}$
	$\boxed{\overrightarrow{(\underline{1}-\alpha)^{-2}}}, \boxed{\overrightarrow{(\underline{2}-\alpha)^{-2}}}, \overrightarrow{(\underline{1}-\alpha)^{-1}}, \overrightarrow{(\underline{2}-\alpha)^{-1}}$ Interference appears along vectors $\overrightarrow{1}, \overrightarrow{(\underline{1}-\alpha)}, \overrightarrow{(\underline{1}-\alpha)^2}, \overrightarrow{(\underline{2}-\alpha)}, \overrightarrow{(\underline{2}-\alpha)^2} \equiv \overrightarrow{1}, \overrightarrow{\alpha}, \overrightarrow{\alpha^2}$

Table 2: *A summary of the MDS-XSTPIR scheme for $X=1, T=1, K_c=2, N=5, U=0, B=0$, showing storage at each server, the queries, and a partitioning of signal and interference dimensions contained in the answers from each server.*

Thus, for each $l \in [L]$, the values S_{nl} stored across all N servers comprise an MDS$(N, K_c + X)$ code which includes X noise symbols for X-security. The query sent by the user to the n-th server, in order to retrieve the θ^{th} desired message, is comprised of K_c rounds, $(Q_n^{\theta,\kappa})_{\kappa \in [K_c]}$. For each $\kappa \in [K_c]$, the query is constructed as follows.

$$Q_n^{\theta,\kappa} = (Q_{n1}^{\theta,\kappa}, Q_{n2}^{\theta,\kappa}, \ldots, Q_{nL}^{\theta,\kappa}), \tag{52}$$

where $\forall l \in [L]$, let us set

$$Q_{nl}^{\theta,\kappa} = (\underline{l} - \alpha_n)^{K_c - \kappa} \mathbf{Q}_\theta + \sum_{t \in [T]} (\underline{l} - \alpha_n)^{K_c + t - 1} \mathbf{Z}_{lt}'^{\kappa}. \tag{53}$$

Upon receiving the query from the user, the n-th server responds with the following K_c symbols.

$$A_n^\theta = (A_{n1}^\theta, A_{n2}^\theta, \cdots, A_{nK_c}^\theta) \tag{54}$$

where for all $\kappa \in [K_c]$,

$$A_{n\kappa}^\theta = (S_{n1} Q_{n1}^{\theta,\kappa} + S_{n2} Q_{n2}^{\theta,\kappa} + \cdots + S_{nL} Q_{nL}^{\theta,\kappa}). \tag{55}$$

To show that the scheme is correct, for any $\kappa \in [K_c]$, let us rewrite the symbol $A_{n\kappa}^\theta$ as,

$$A_{n\kappa}^\theta = \sum_{l \in [L]} S_{nl} Q_{nl}^{\theta,\kappa} \tag{56}$$

$$= \sum_{l \in [L]} \left(\sum_{k \in [K_c]} \frac{1}{(\underline{l} - \alpha_n)^{K_c - k + 1}} \mathbf{W}_{lk} + \sum_{x \in [X]} (\underline{l} - \alpha_n)^{x-1} \mathbf{Z}_{lx} \right) \left((\underline{l} - \alpha_n)^{K_c - \kappa} \mathbf{Q}_\theta + \sum_{t \in [T]} (\underline{l} - \alpha_n)^{K_c + t - 1} \mathbf{Z}_{lt}'^{\kappa} \right) \tag{57}$$

$$\begin{aligned} &= \sum_{l \in [L]} \sum_{k \in [\kappa]} \frac{1}{(\underline{l} - \alpha_n)^{\kappa - k + 1}} \mathbf{W}_{lk} \mathbf{Q}_\theta + \sum_{l \in [L]} \sum_{k = \kappa + 1}^{K_c} (\underline{l} - \alpha_n)^{k - \kappa - 1} \mathbf{W}_{lk} \mathbf{Q}_\theta \\ &\quad + \sum_{l \in [L]} \sum_{x \in [X]} (\underline{l} - \alpha_n)^{K_c - \kappa + x - 1} \mathbf{Z}_{lx} \mathbf{Q}_\theta + \sum_{l \in [L]} \sum_{k \in [K_c]} \sum_{t \in [T]} (\underline{l} - \alpha_n)^{k + t - 2} \mathbf{W}_{lk} \mathbf{Z}_{lt}'^{\kappa} \\ &\quad + \sum_{l \in [L]} \sum_{x \in [X]} \sum_{t \in [T]} (\underline{l} - \alpha_n)^{K_c + t + x - 2} \mathbf{Z}_{lx} \mathbf{Z}_{lt}'^{\kappa}. \end{aligned} \tag{58}$$

Now we will see why it is possible to recover all desired symbols $(\mathbf{W}_{lk} \mathbf{Q}_\theta)_{l \in [L], k \in [K_c]}$. Consider $\kappa = 1$.

$$A_{n1}^\theta = \sum_{l \in [L]} S_{nl} Q_{nl}^{\theta,1} \tag{59}$$

$$\begin{aligned} &= \sum_{l \in [L]} \frac{1}{\underline{l} - \alpha_n} \mathbf{W}_{l1} \mathbf{Q}_\theta + \sum_{l \in [L]} \sum_{k=2}^{K_c} (\underline{l} - \alpha_n)^{k-2} \mathbf{W}_{lk} \mathbf{Q}_\theta + \sum_{l \in [L]} \sum_{x \in [X]} (\underline{l} - \alpha_n)^{K_c + x - 2} \mathbf{Z}_{lx} \mathbf{Q}_\theta \\ &\quad + \sum_{l \in [L]} \sum_{k \in [K_c]} \sum_{t \in [T]} (\underline{l} - \alpha_n)^{t + k - 2} \mathbf{W}_{lk} \mathbf{Z}_{lt}'^{1} + \sum_{l \in [L]} \sum_{x \in [X]} \sum_{t \in [T]} (\underline{l} - \alpha_n)^{K_c + t + x - 2} \mathbf{Z}_{lx} \mathbf{Z}_{lt}'^{1} \end{aligned} \tag{60}$$

The first term contains the L desired symbols $(\mathbf{W}_{11}\mathbf{Q}_\theta, \ldots, \mathbf{W}_{L1}\mathbf{Q}_\theta)$ that are to be retrieved in the first round, i.e., for $\kappa = 1$. Each of the remaining four terms constitute interference which can be expanded into weighted sums of terms of the form α_n^t, $t \in \{0, 1, \ldots, K_c + X + T - 2\}$. Therefore, collecting the A_{n1}^θ symbols from all N servers, the user obtains

$$\begin{bmatrix} A_{11}^\theta \\ A_{21}^\theta \\ \vdots \\ A_{N1}^\theta \end{bmatrix} = \begin{bmatrix} \frac{1}{\underline{1}-\alpha_1} & \cdots & \frac{1}{\underline{L}-\alpha_1} & 1 & \alpha_1 & \cdots & \alpha_1^{K_c+X+T-2} \\ \frac{1}{\underline{1}-\alpha_2} & \cdots & \frac{1}{\underline{L}-\alpha_2} & 1 & \alpha_2 & \cdots & \alpha_2^{K_c+X+T-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{\underline{1}-\alpha_N} & \cdots & \frac{1}{\underline{L}-\alpha_N} & 1 & \alpha_N & \cdots & \alpha_N^{K_c+X+T-2} \end{bmatrix} \begin{bmatrix} \mathbf{W}_{11}\mathbf{Q}_\theta \\ \mathbf{W}_{21}\mathbf{Q}_\theta \\ \vdots \\ \mathbf{W}_{L1}\mathbf{Q}_\theta \\ * \\ \vdots \\ * \end{bmatrix} \tag{61}$$

where $*$ represents various combinations of interference terms, whose precise forms are inconsequential. What matters is that the $N \times N$ matrix in (61) is $\mathbf{M}_{L,N}$ which is invertible according to Lemma 1, so that the user is able to retrieve the desired symbols $(\mathbf{W}_{11}\mathbf{Q}_\theta, \ldots, \mathbf{W}_{L1}\mathbf{Q}_\theta)$ by inverting the matrix.

The scheme proceeds similarly to retrieves desired symbols $(\mathbf{W}_{1\kappa}\mathbf{Q}_\theta, \ldots, \mathbf{W}_{L\kappa}\mathbf{Q}_\theta)$ with the κ^{th} round of queries. To prove this by induction, let us consider any κ, such that $2 \leq \kappa \leq K_c$, and assume that the desired symbols $(\mathbf{W}_{lk}\mathbf{Q}_\theta)_{l\in[L],k\in[\kappa-1]}$ have already been retrieved. Now we wish to show that the desired symbols $(\mathbf{W}_{l\kappa}\mathbf{Q}_\theta)_{l\in[L]}$ can be retrieved.

$$\begin{aligned} A_{n\kappa}^\theta &= \sum_{l\in[L]} S_{nl} Q_{nl}^{\theta,\kappa} && (62) \\ &= \sum_{l\in[L]} \sum_{k\in[\kappa-1]} \frac{1}{(\underline{l}-\alpha_n)^{\kappa-k+1}} \mathbf{W}_{lk}\mathbf{Q}_\theta + \sum_{l\in[L]} \frac{1}{\underline{l}-\alpha_n} \mathbf{W}_{l\kappa}\mathbf{Q}_\theta \\ &\quad + \sum_{l\in[L]} \sum_{k=\kappa+1}^{K_c} (\underline{l}-\alpha_n)^{k-\kappa-1} \mathbf{W}_{lk}\mathbf{Q}_\theta + \sum_{l\in[L]} \sum_{x\in[X]} (\underline{l}-\alpha_n)^{K_c-\kappa+x-1} \mathbf{Z}_{lx}\mathbf{Q}_\theta && (63) \\ &\quad + \sum_{l\in[L]} \sum_{k\in[K_c]} \sum_{t\in[T]} (\underline{l}-\alpha_n)^{t+k-2} \mathbf{W}_{lk}\mathbf{Z}_{lt}^{\prime\kappa} + \sum_{l\in[L]} \sum_{x\in[X]} \sum_{t\in[T]} (\underline{l}-\alpha_n)^{K_c+t+x-2} \mathbf{Z}_{lx}\mathbf{Z}_{lt}^{\prime\kappa}. && (64) \end{aligned}$$

The first term contains symbols that have already been retrieved, so the user can subtract this term from $A_{n\kappa}^\theta$.

$$A_{n\kappa}^{\theta\prime} = A_{n\kappa}^\theta - \sum_{l\in[L]} \sum_{k\in[\kappa-1]} \frac{1}{(\underline{l}-\alpha_n)^{\kappa-k+1}} \mathbf{W}_{lk}\mathbf{Q}_\theta. \tag{65}$$

The next term is comprised of the L symbols $(\mathbf{W}_{l\kappa}\mathbf{Q}_\theta)_{l\in[L]}$ that the user wishes to retrieve. The remaining 4 terms constitute interference which can be expanded as before into weighted sums of terms of the form $\alpha_n^t, t \in \{0, 1, \ldots, K_c + X + T - 2\}$. Therefore, collecting the $A_{n\kappa}^{\theta\prime}$ symbols from all N servers, the user obtains,

$$\begin{bmatrix} A_{11}^{\theta'} \\ A_{21}^{\theta'} \\ \vdots \\ A_{N1}^{\theta'} \end{bmatrix} = \begin{bmatrix} \frac{1}{1-\alpha_1} & \cdots & \frac{1}{L-\alpha_1} & 1 & \alpha_1 & \cdots & \alpha_1^{K_c+X+T-2} \\ \frac{1}{1-\alpha_2} & \cdots & \frac{1}{L-\alpha_2} & 1 & \alpha_2 & \cdots & \alpha_2^{K_c+X+T-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{1-\alpha_N} & \cdots & \frac{1}{L-\alpha_N} & 1 & \alpha_N & \cdots & \alpha_N^{K_c+X+T-2} \end{bmatrix} \begin{bmatrix} \mathbf{W}_{1\kappa}\mathbf{Q}_\theta \\ \mathbf{W}_{2\kappa}\mathbf{Q}_\theta \\ \vdots \\ \mathbf{W}_{L\kappa}\mathbf{Q}_\theta \\ * \\ \vdots \\ * \end{bmatrix} \tag{66}$$

The desired symbols $(\mathbf{W}_{l\kappa}\mathbf{Q}_\theta)_{l\in[L]}$ can be retrieved by inverting the $N \times N$ square matrix in (66), which is guaranteed to be invertible according to Lemma 1. Thus, the induction argument shows that all $\ell = LK_c$ desired symbols are retrieved successfully. A summary of the storage at each server, the queries, and a partitioning of signal and interference dimensions contained in the answers from each server is provided in Table 3.

T-privacy is guaranteed because $\mathbf{Q}_\theta$ is protected by the noise vectors $(\mathbf{Z}_{lt}^{\prime\kappa})_{l\in[L],t\in[T],\kappa\in[K_c]}$ that are i.i.d. uniform and coded according to an MDS(N,T) code. Similarly, X-security is guaranteed because for each $l \in [L]$, the messages $(\mathbf{W}_{lk})_{k\in[K_c]}$ are protected by the noise vectors $(\mathbf{Z}_{lx})_{x\in[X]}$ that are i.i.d. uniform and coded according to an MDS(N,X) code. Now let us consider the rate achieved by the scheme. From a total of NK_c downloaded q-ary symbols, the user is able to retrieve his $\ell = LK_c$ desired symbols, so the rate achieved is

$$R = \frac{LK_c}{NK_c} = \frac{L}{N} = 1 - \left(\frac{K_c + X + T - 1}{N}\right), \tag{67}$$

which matches the result in Theorem 1.

	Server ‘n’ (Replace α with α_n)
Storage (S_n)	$\frac{1}{(\underline{1}-\alpha)^{K_c}}\mathbf{W}_{11}+\cdots+\frac{1}{\underline{1}-\alpha}\mathbf{W}_{1K_c}+\mathbf{Z}_{11}+\cdots+(\underline{1}-\alpha)^{X-1}\mathbf{Z}_{1X}$ $\frac{1}{(\underline{2}-\alpha)^{K_c}}\mathbf{W}_{21}+\cdots+\frac{1}{\underline{2}-\alpha}\mathbf{W}_{2K_c}+\mathbf{Z}_{21}+\cdots+(\underline{2}-\alpha)^{X-1}\mathbf{Z}_{2X}$ $\vdots$ $\frac{1}{(\underline{L}-\alpha)^{K_c}}\mathbf{W}_{L1}+\cdots+\frac{1}{\underline{L}-\alpha}\mathbf{W}_{L'K_c}+\mathbf{Z}_{L1}+\cdots+(\underline{L}-\alpha)^{X-1}\mathbf{Z}_{LX}$
Query $(Q_n^{[\theta]})$	$(\underline{1}-\alpha)^{K_c-1}\mathbf{Q}_\theta+(\underline{1}-\alpha)^{K_c}\mathbf{Z}'^{1}_{11}+\cdots+(\underline{1}-\alpha)^{K_c+T-1}\mathbf{Z}'^{1}_{1T}$ $(\underline{2}-\alpha)^{K_c-1}\mathbf{Q}_\theta+(\underline{2}-\alpha)^{K_c}\mathbf{Z}'^{1}_{21}+\cdots+(\underline{2}-\alpha)^{K_c+T-1}\mathbf{Z}'^{1}_{2T}$ $\vdots$ $(\underline{L}-\alpha)^{K_c-1}\mathbf{Q}_\theta+(\underline{L}-\alpha)^{K_c}\mathbf{Z}'^{1}_{L1}+\cdots+(\underline{L}-\alpha)^{K_c+T-1}\mathbf{Z}'^{1}_{LT}$ - $(\underline{1}-\alpha)^{K_c-2}\mathbf{Q}_\theta+(\underline{1}-\alpha)^{K_c}\mathbf{Z}'^{2}_{11}+\cdots+(\underline{1}-\alpha)^{K_c+T-1}\mathbf{Z}'^{2}_{1T}$ $(\underline{2}-\alpha)^{K_c-2}\mathbf{Q}_\theta+(\underline{2}-\alpha)^{K_c}\mathbf{Z}'^{2}_{21}+\cdots+(\underline{2}-\alpha)^{K_c+T-1}\mathbf{Z}'^{2}_{2T}$ $\vdots$ $(\underline{L}-\alpha)^{K_c-2}\mathbf{Q}_\theta+(\underline{L}-\alpha)^{K_c}\mathbf{Z}'^{2}_{L'1}+\cdots+(\underline{L}-\alpha)^{K_c+T-1}\mathbf{Z}'^{2}_{LT}$ - $\vdots$ - $\mathbf{Q}_\theta+(\underline{1}-\alpha)^{K_c}\mathbf{Z}'^{K_c}_{11}+\cdots+(\underline{1}-\alpha)^{K_c+T-1}\mathbf{Z}'^{K_c}_{1T}$ $\mathbf{Q}_\theta+(\underline{2}-\alpha)^{K_c}\mathbf{Z}'^{K_c}_{21}+\cdots+(\underline{2}-\alpha)^{K_c+T-1}\mathbf{Z}'^{K_c}_{2T}$ $\vdots$ $\mathbf{Q}_\theta+(\underline{L}-\alpha)^{K_c}\mathbf{Z}'^{K_c}_{f_{L'}1}+\cdots+(\underline{L}-\alpha)^{K_c+T-1}\mathbf{Z}'^{K_c}_{LT}$
	Desired symbols appear along vectors $\overrightarrow{(\underline{1}-\alpha)^{-1}},\cdots,\overrightarrow{(\underline{L}-\alpha)^{-1}}$ - $\boxed{\overrightarrow{(\underline{1}-\alpha)^{-2}}},\cdots,\boxed{\overrightarrow{(\underline{L}-\alpha)^{-2}}},\overrightarrow{(\underline{1}-\alpha)^{-1}},\cdots,\overrightarrow{(\underline{L}-\alpha)^{-1}}$ - $\vdots$ - $\boxed{\overrightarrow{(\underline{1}-\alpha)^{-K_c}}},\cdots,\boxed{\overrightarrow{(\underline{L}-\alpha)^{-K_c}}},\cdots,$ $\boxed{\overrightarrow{(\underline{1}-\alpha)^{-2}}},\cdots,\boxed{\overrightarrow{(\underline{L}-\alpha)^{-2}}},$ $\overrightarrow{(\underline{1}-\alpha)^{-1}},\cdots,\overrightarrow{(\underline{L}-\alpha)^{-1}}$ Interference appears along vectors $\overrightarrow{1},\overrightarrow{(\underline{1}-\alpha)},\cdots,\overrightarrow{(\underline{1}-\alpha)^{X+T+K_c-2}},\cdots,\overrightarrow{(\underline{L}-\alpha)},\cdots,\overrightarrow{(\underline{L}-\alpha)^{X+T+K_c-2}}$ $\equiv\overrightarrow{1},\overrightarrow{\alpha},\cdots,\overrightarrow{\alpha^{X+T+K_c-2}}$

Table 3: *A summary of the general MDS-XSTPIR scheme showing storage at each server, the queries, and a partitioning of signal and interference dimensions contained in the answers from each server.*

4.2 Arbitrary U, B

Now let us generalize the scheme to non-trivial U and B, i.e., for U unresponsive servers and up to B byzantine servers. For this generalization, let us set

$$L = (N-U) - (K_c + X + T + 2B - 1) \tag{68}$$
$$\ell = LK_c. \tag{69}$$

Even though now the values of U, B are non-trivial, the construction of storage, queries and answers remains identical to the description provided previously for $U = B = 0$. So let us consider any $(N-U)$ responsive servers, say servers $n_1, n_2, \cdots, n_{N-U}$. Instead of the $N \times N$ square matrix $\mathbf{M}_{L,N}$ in (66), we now have the $(N-U) \times (N-U-2B)$ decoding matrix,

$$\mathbf{M}_{(N-U)\times(N-U-2B)} = \begin{bmatrix} \frac{1}{\underline{1}-\alpha_{n_1}} & \cdots & \frac{1}{\underline{L}-\alpha_{n_1}} & 1 & \alpha_{n_1} & \cdots & \alpha_{n_1}^{K_c+X+T-2} \\ \frac{1}{\underline{1}-\alpha_{n_2}} & \cdots & \frac{1}{\underline{L}-\alpha_{n_2}} & 1 & \alpha_{n_2} & \cdots & \alpha_{n_2}^{K_c+X+T-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{\underline{1}-\alpha_{n_{N-U}}} & \cdots & \frac{1}{\underline{L}-\alpha_{n_{N-U}}} & 1 & \alpha_{n_{N-U}} & \cdots & \alpha_{n_{N-U}}^{K_c+X+T-2} \end{bmatrix}. \tag{70}$$

Note that if we consider any $N-U-2B$ rows of $\mathbf{M}_{(N-U)\times(N-U-2B)}$ then we obtain an invertible square matrix because of Lemma 1. Therefore, $\mathbf{M}_{(N-U)\times(N-U-2B)}$ is the generator matrix of an MDS$(N-U, N-U-2B)$ code, and it is can correct up to $((N-U)-(N-U-2B))/2 = B$ errors. Thus by this construction, we establish a scheme that works with U unresponsive servers and up to B Byzantine servers, while achieving the rate of

$$R = 1 - \left(\frac{K_c + X + T + 2B - 1}{N-U}\right). \tag{71}$$

This completes the proof of Theorem 1.

5 Private and Secure Distributed Matrix Multiplication

Recently in [20,28], the problem of private and secure matrix multiplication (PSDMM) is proposed, where a user wishes to compute the product of a confidential matrix $\mathbf{A}$ with a matrix $\mathbf{B}_\theta, \theta \in [M]$ with the aid of N distributed servers. In [20], it is assumed that the set of matrices $\mathbf{B}_{[M]}$ are public and available to the N servers, however, the confidential matrix $\mathbf{A}$ is shared secretly among all N servers, such that no information about $\mathbf{A}$ is leaked to any server. Besides, the user wants to keep the index θ private from each server. The goal of the problem is to minimize (i) the upload cost from the source of the confidential matrix $\mathbf{A}$ to the N servers and (ii) the download cost from the N servers to the user. In [20], the authors exploit the MDS-PIR scheme proposed in [24] to construct the PSDMM scheme, and characterize the lower convex hull of (upload, download) pairs.

Using the MDS-XSTPIR scheme present in Section 4, we now present a novel PSDMM scheme for a generalized model. In our model, the index θ is T-private, while the confidential matrix $\mathbf{A}$ is X_A-secure. Furthermore, we also allow matrices $\mathbf{B}_{[M]}$ to be X_B-secure. Note that the model in [20] is obtained as a special case of our generalized model by setting $X_A = T = 1, X_B = 0$.

5.1 PSDMM: Problem Statement

Let $\mathbf{A} = (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_\ell)$ represent ℓ random matrices, each of dimension $\lambda \times \chi$, that are independently and uniformly distributed over $\mathbb{F}_q^{\lambda\times\chi}$. Let $\mathbf{B}_{[M]}$ be M random matrices independently and uniformly distributed over $\mathbb{F}_q^{\chi\times\mu}$. The independence between matrices $\mathbf{A}_{[\ell]}$ and $\mathbf{B}_{[M]}$ is formalized as follows.

$$H(\mathbf{A}, \mathbf{B}_{[M]}) = \sum_{l\in[\ell]} H(\mathbf{A}_l) + \sum_{m\in[M]} H(\mathbf{B}_m). \tag{72}$$

The matrices $\mathbf{A}$ and $\mathbf{B}_{[M]}$ are made available at N distributed servers through secret sharing schemes with security levels X_A and X_B, respectively. That is, any group of up to X_A colluding servers can learn nothing about $\mathbf{A}$, and any group of up to X_B servers can learn nothing about $\mathbf{B}_{[M]}$. To this end, matrices $\mathbf{A}$ and $\mathbf{B}_{[M]}$ are separately coded according to secret sharing schemes that generate shares $\tilde{A}_n$, $\tilde{B}_n, n \in [N]$, and these shares are made available to the n-th server. Furthermore, we assume that the upload cost of $\tilde{A}_{[N]}$ is to be optimized, while that of $\tilde{B}_{[N]}$ and $Q^\theta_{[N]}$ is ignored, presumably because $\mathbf{A}$ matrices are frequently updated while $\mathbf{B}_{[M]}$ are static, and the size of queries does not scale with ℓ.

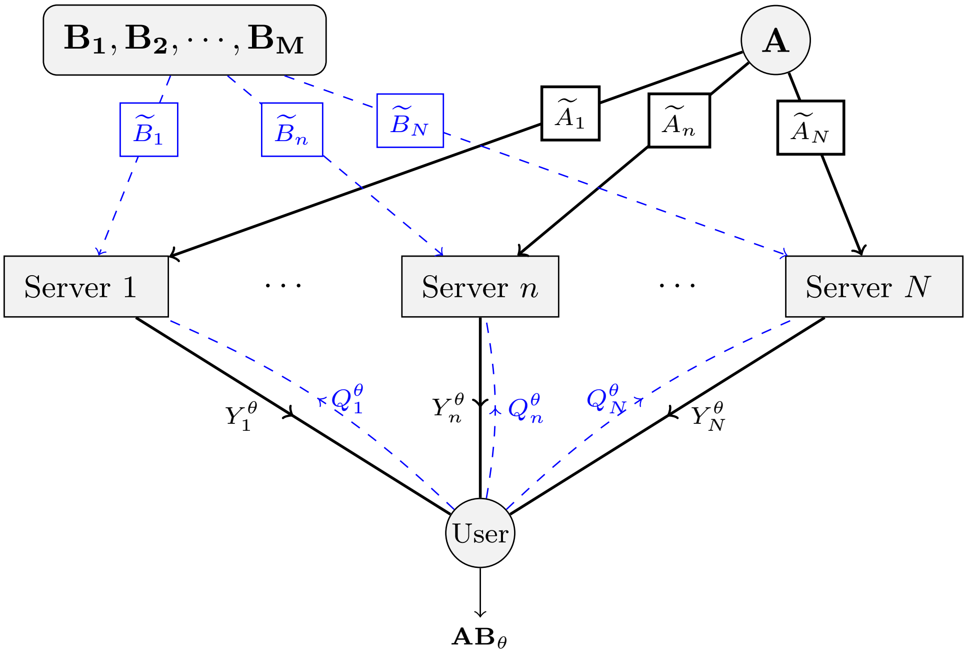

Figure 2: *Model for private secure distributed matrix multiplication (PSDMM).* $\mathbf{A}$ *matrices are* X_A *secure, while* $\mathbf{B}$ *matrices are* X_B *secure. The uploads to be optimized are the* $\widetilde{A}$ *terms and the downloads to be optimized are the* Y^θ *terms.*

The independence between the securely coded matrices is specified as follows.

$$I(\mathbf{A}, \tilde{A}_{[N]}; \mathbf{B}_{[M]}, \tilde{B}_{[N]}) = 0. \tag{73}$$

Matrices must be recoverable from their secret shares.

$$H(\mathbf{A} \mid \tilde{A}_{[N]}) = 0, \tag{74}$$

$$H(\mathbf{B}_{[M]} \mid \tilde{B}_{[N]}) = 0. \tag{75}$$

The matrices must be perfectly secure from any set of secret shares that can be accessed by a set of up to X_A, X_B colluding servers, respectively.

$$I(\mathbf{A}; \tilde{A}_{\mathcal{X}}) = 0 \quad \mathcal{X} \subset [N], |\mathcal{X}| = X_A, \tag{76}$$

$$I(\mathbf{B}_{[M]}; \tilde{B}_{\mathcal{X}}) = 0 \quad \mathcal{X} \subset [N], |\mathcal{X}| = X_B. \tag{77}$$

The user generates an index $\theta \in [M]$ privately and uniformly, and wishes to compute the product

$$\mathbf{AB}_\theta = (\mathbf{A}_1\mathbf{B}_\theta, \mathbf{A}_2\mathbf{B}_\theta, \dots, \mathbf{A}_\ell\mathbf{B}_\theta). \tag{78}$$

To this end, the user generates N queries $Q^\theta_{[N]}$. The n-th query Q^θ_n is sent to the n-th server. The user has no prior knowledge of matrices $\mathbf{A}$ and $\mathbf{B}_{[M]}$ and their secret shares, i.e.,

$$I(\theta, Q^\theta_{[N]}; \tilde{A}_{[N]}, \tilde{B}_{[N]}) = 0. \tag{79}$$

T-privacy, $0 \leq T \leq N$, guarantees that any group of up to T colluding servers learn nothing about θ.

$$I(Q^\theta_{\mathcal{T}}, \tilde{A}_{\mathcal{T}}, \tilde{B}_{\mathcal{T}}; \theta) = 0. \tag{80}$$

Upon receiving the user's query Q^θ_n, the n-th server responds with an answer Y^θ_n, which is a function of all information available to it.

$$H(Y^\theta_n | Q^\theta_n, \tilde{A}_n, \tilde{B}_n) = 0. \tag{81}$$

The user must be able to recover the product $\mathbf{AB}_\theta$ from all N answers, i.e.,

$$H(\mathbf{AB}_\theta | Y^\theta_{[N]}, Q^\theta_{[N]}) = 0. \tag{82}$$

The upload cost and download cost are defined as follows.

$$U = \frac{\sum_{n\in[N]} H(\tilde{A}_n)}{H(\mathbf{A})}, \tag{83}$$

$$D = \frac{\sum_{n\in[N]} H(Y^\theta_n)}{H(\mathbf{AB}_\theta)}. \tag{84}$$

5.2 A New Scheme for PSDMM

In this section, we will present a PSDMM scheme to show that the lower convex hull of (upload, download) pairs

$$(U, D) = \left(\frac{N}{K_c}, \quad \frac{N}{N - (2K_c + X_A + X_B + T - 2)}\right) \tag{85}$$

for

$$K_c = 1, 2, \dots, \lfloor (N + 1 - X_A - X_B - T)/2 \rfloor \tag{86}$$

is achievable when $q \to \infty$ and $\chi \geq \min(\lambda, \mu)$. Furthermore, when $X_B = 0$, i.e., there are no security constraints on matrices $\mathbf{B}_{[M]}$, and $\chi \geq \min(\lambda, \mu)$, then the lower convex hull of (upload, download) pairs

$$(U, D) = \left(\frac{N}{K_c}, \frac{N}{N - (K_c + X_A + T - 1)}\right) \tag{87}$$

for

$$K_c = 1, 2, \dots, (N + 1 - X_A - T) \tag{88}$$

is achievable as $q \to \infty$.

First, let us consider the case $X_B \neq 0$. For this setting, let us set

$$L = N - (X_A + X_B + T + 2K_c - 2), \tag{89}$$

$$\ell = K_c L. \tag{90}$$

For all $l \in [L], k \in [K_c]$, let us define

$$\mathbf{A}_{lk} = \mathbf{A}_{L(k-1)+l}. \tag{91}$$

We will also set

$$\mathbf{B} = \begin{bmatrix} \mathbf{B}_1 & \mathbf{B}_2 & \dots & \mathbf{B}_M \end{bmatrix} \tag{92}$$

to be an $\chi \times M\mu$ matrix that contains all $\mathbf{B}_{[M]}$. Let us also define $\mathbf{Q}_\theta$ be a $M\mu \times \mu$ matrix as follows.

$$\mathbf{Q}_\theta = [\ \underbrace{\mathbf{0}_\mu \quad \dots \quad \mathbf{0}_\mu}_{\text{A total of } (\theta-1)\mathbf{0}_\mu\text{'s}} \quad \mathbf{I}_\mu \quad \underbrace{\mathbf{0}_\mu \quad \dots \quad \mathbf{0}_\mu}_{\text{A total of } (M-\theta)\mathbf{0}_\mu\text{'s}}\ ]^T \tag{93}$$

where $\mathbf{0}_\mu$ is the $\mu \times \mu$ square zero matrix, and $\mathbf{I}_\mu$ is the $\mu \times \mu$ identity matrix. We note that by construction, $\mathbf{A}\mathbf{B}\mathbf{Q}_\theta = (\mathbf{A}_1\mathbf{B}\mathbf{Q}_\theta, \dots, \mathbf{A}_\ell\mathbf{B}\mathbf{Q}_\theta) = (\mathbf{A}_{lk}\mathbf{B}\mathbf{Q}_\theta)_{l\in[L],k\in[K_c]}$ is the desired product. Let $(\mathbf{Z}_{lx})_{l\in[L],x\in[X_A]}$ and $(\mathbf{Z}'_{lx'})_{l\in[L],x'\in[X_B]}$ be independent, uniformly distributed random noise matrices from $\mathbb{F}_q^{\lambda\times\chi}$ and $\mathbb{F}_q^{\chi\times M\mu}$ that will be used to guarantee X_A and X_B security levels for $\mathbf{A}, \mathbf{B}_{[M]}$, respectively. Let $(\mathbf{Z}''^{\kappa}_{lt})_{l\in[L],t\in[T],\kappa\in[K_c]}$ be independent, uniformly distributed random noise matrices from $\mathbb{F}_q^{M\mu\times\mu}$, that will be used to guarantee T-privacy of queries. The independence between $\mathbf{A}, \mathbf{B}_{[M]}$, noise matrices and θ is formalized as follows.

$$\begin{aligned} &H(\mathbf{A}, \mathbf{B}_{[M]}, (\mathbf{Z}_{lx})_{l\in[L],x\in[X_A]}, (\mathbf{Z}'_{lx'})_{l\in[L],x'\in[X_B]}, (\mathbf{Z}''^{\kappa}_{lt})_{l\in[L],t\in[T],\kappa\in[K_c]}, \theta) \\ &= \sum_{l\in[L],k\in[K_c]} H(\mathbf{A}_{lk}) + \sum_{m\in[M]} H(\mathbf{B}_m) + \sum_{l\in[L],x\in[X_A]} H(\mathbf{Z}_{lx}) \\ &\quad + \sum_{l\in[L],x'\in[X_B]} H(\mathbf{Z}'_{lx'}) + \sum_{l\in[L],t\in[T],\kappa\in[K_c]} H(\mathbf{Z}''^{\kappa}_{lt}) + H(\theta). \end{aligned} \tag{94}$$

Let $\underline{1}, \underline{2}, \cdots, \underline{L}, \alpha_1, \alpha_2, \cdots, \alpha_N$ be distinct elements of $\mathbb{F}_q$. We require $q \geq L + N$ so these elements must exist. Now we are ready to construct the scheme. The secret share of $\mathbf{B}_{[M]}$ at the n-th server, $\tilde{B}_n$ is constructed as follows.

$$\tilde{B}_n = (\tilde{B}_{n1}, \tilde{B}_{n2}, \dots, \tilde{B}_{nL}), \tag{95}$$

where $\forall l \in [L]$,

$$\tilde{B}_{nl} = \mathbf{B} + \sum_{x'\in[X_B]} (\underline{l} - \alpha_n)^{K_c+x'-1}\mathbf{Z}'_{lx'}. \tag{96}$$

The secret share of $\mathbf{A}$ at the n^{th} server is constructed as follows.

$$\tilde{A}_n = (\tilde{A}_{n1}, \tilde{A}_{n2}, \dots, \tilde{A}_{nL}), \tag{97}$$

where $\forall l \in [L]$,

$$\tilde{A}_{nl} = \sum_{k\in[K_c]} \frac{1}{(\underline{l}-\alpha_n)^{K_c-k+1}}\mathbf{A}_{lk} + \sum_{x\in[X_A]} (\underline{l}-\alpha_n)^{x-1}\mathbf{Z}_{lx}. \tag{98}$$

The query sent by the user to the n^{th} server, is comprised of K_c rounds, $Q_n^\theta = (Q_n^{\theta,\kappa})_{\kappa\in[K_c]}$. For all $\kappa \in [K_c]$, we construct the queries as follows.

$$Q_n^{\theta,\kappa} = (Q_{n1}^{\theta,\kappa}, Q_{n2}^{\theta,\kappa}, \dots, Q_{nL}^{\theta,\kappa}), \tag{99}$$

where $\forall l \in [L]$, we set

$$Q_{nl}^{\theta,\kappa} = (\underline{l}-\alpha_n)^{K_c-\kappa}\mathbf{Q}_\theta + \sum_{t\in[T]}(\underline{l}-\alpha_n)^{K_c+t-1}\mathbf{Z}_{lt}''^{\kappa}. \tag{100}$$

Upon receiving the query from the user, the n^{th} server responds with the following K_c symbols.

$$Y_n^\theta = (\tilde{A}_{n1}\tilde{B}_{n1}Q_{n1}^{\theta,\kappa} + \tilde{A}_{n2}\tilde{B}_{n2}Q_{n2}^{\theta,\kappa} + \cdots + \tilde{A}_{nL}\tilde{B}_{nL}Q_{nL}^{\theta,\kappa})_{\kappa\in[K_c]}. \tag{101}$$

To show the correctness of the scheme, let us consider $\tilde{A}_{nl}\tilde{B}_{nl}, \forall l \in [L]$.

$$\begin{aligned}
\tilde{A}_{nl}\tilde{B}_{nl} &= \left(\sum_{k\in[K_c]} \frac{1}{(\underline{l}-\alpha_n)^{K_c-k+1}}\mathbf{A}_{lk} + \sum_{x\in[X_A]} (\underline{l}-\alpha_n)^{x-1}\mathbf{Z}_{lx}\right) \\
&\qquad\qquad \left(\mathbf{B} + \sum_{x'\in[X_B]} (\underline{l}-\alpha_n)^{K_c+x'-1}\mathbf{Z}'_{lx'}\right) && (102)\\
&= \sum_{k\in[K_c]} \frac{1}{(\underline{l}-\alpha_n)^{K_c-k+1}}\mathbf{A}_{lk}\mathbf{B} + \sum_{x\in[X_A]} (\underline{l}-\alpha_n)^{x-1}\mathbf{Z}_{lx}\mathbf{B} \\
&\quad + \sum_{k\in[K_c]}\sum_{x'\in[X_B]} (\underline{l}-\alpha_n)^{x'+k-2}\mathbf{A}_{lk}\mathbf{Z}'_{\ell x'} + \sum_{x\in[X_A]}\sum_{x'\in[X_B]} (\underline{l}-\alpha_n)^{K_c+x+x'-2}\mathbf{Z}_{lx}\mathbf{Z}'_{lx'} && (103)\\
&= \sum_{k\in[K_c]} \frac{1}{(\underline{l}-\alpha_n)^{K_c-k+1}}\mathbf{A}_{lk}\mathbf{B} + \sum_{\xi\in[K_c+X_A+X_B-1]} (\underline{l}-\alpha_n)^{\xi-1}\bar{\mathbf{Z}}_{l\xi} && (104)
\end{aligned}$$

In (104) we rearranged the last three terms of (103) grouping them into weighted sums of terms of the form $(\underline{l}-\alpha_n)^i$, $i \in \{0, 1, \dots, K_c + X_A + X_B - 2\}$. The grouped terms $\bar{\mathbf{Z}}_{l\xi}$ can be calculated explicitly but as it turns out the precise form of these terms is inconsequential. Now note that if we regard $(\mathbf{A}_{lk}\mathbf{B})_{l\in[L],k\in[K_c]}$ terms as messages, and other terms as noise, then (104) has the same form as (51), the storage construction in the MDS-XSTPIR scheme presented in Section 4.[2] Also note that the construction of queries is also the same as the MDS-XSTPIR scheme, thus the correctness follows directly from the proof presented in Section 4, which means the user is able to recover the product $\mathbf{ABQ}_\theta = (\mathbf{A}_{lk}\mathbf{BQ}_\theta)_{l\in[L],k\in[K_c]}$. Privacy and security follows from the fact that $\mathbf{Q}_\theta$, $\mathbf{A}$, $\mathbf{B}_{[M]}$ are protected by the i.i.d. uniformly distributed noise matrices coded according

[2] Note that X in (51) corresponds to $K_c + X_A + X_B - 1$ in (104), so that $L = N - (X + T + K_c - 1)$ in Section 4 corresponds to $L = N - (2K_c + X_A + X_B + T - 2)$ in this section. The condition on K_c becomes $K_c = \frac{N-(X_A+X_B+T+L-2)}{2}$. However, since we must have $L \geq 1$ and $K_c \geq 1$ can only take integer values, it follows that the feasible values of K_c are $1 \leq K_c \leq \lfloor \frac{N-(X_A+X_B+T-1)}{2} \rfloor$.

to MDS(N,T), MDS(X_A,T), MDS(X_B,T) codes, respectively. This completes the construction of the scheme for $X_B \neq 0$. Note that when $q \to \infty$ and $\chi \geq \min(\lambda,\mu)$, then $H(\mathbf{A}\mathbf{B}_\theta) = \ell\lambda\mu$ in q-ary units according to ([19], Lemma 2), and the download cost is

$$D = \frac{NK_c\lambda\mu}{\ell\lambda\mu} = \frac{N}{L} = \frac{N}{N-(2K_c+X_A+X_B+T-2)}. \tag{105}$$

Now let us consider the case $X_B = 0$. For this setting, let us set

$$L = N - (X_A + X_B + T + K_c - 1), \tag{106}$$

$$\ell = K_c L. \tag{107}$$

We will continue using other definitions as before, but since there is no security constraint on $\mathbf{B}$ matrices, let us replace $\tilde{B}_n$ as

$$\tilde{B}_n = \mathbf{B}. \tag{108}$$

Now we have

$$\tilde{A}_{nl}\tilde{B}_{nl} = \sum_{k\in[K_c]} \frac{1}{(\underline{l}-\alpha_n)^{K_c-k+1}}\mathbf{A}_{lk}\mathbf{B} + \sum_{x\in[X_A]} (\underline{l}-\alpha_n)^{x-1}\mathbf{Z}_{lx}\mathbf{B}, \tag{109}$$

which is coded according to an MDS(N,K_c+X_A) code. Thus the correctness, privacy and security follows from that proof in Section 4. The download cost is

$$D = \frac{NK_c\lambda\mu}{L\lambda\mu} = \frac{N}{L} = \frac{N}{N-(K_c+X_A+X_B+T-1)}. \tag{110}$$

Now let us consider the upload cost of the scheme. Note that by the construction of $\tilde{A}_n$, it is coded according to an MDS(N,K_c) code. Therefore, the upload cost is $\frac{N}{K_c}$.

It is shown in [20] that when $X_A = T = 1, X_B = 0$, the lower convex hull of (upload, download) pairs

$$(U,D) = \left(\frac{N}{K_c}, \frac{K_c+1}{K_c}\left(1+\left(\frac{K_c+1}{N}\right)+\cdots+\left(\frac{K_c+1}{N}\right)^{M-1}\right)\right) \tag{111}$$

is achievable for $K_c = 1,2,\ldots,N-1$. For the asymptotic setting, i.e., $M \to \infty$, we have from [20] that $D = \frac{K_c+1}{K_c}\frac{N}{N-(K_c+1)}$, which is strictly worse than the (upload, download) pairs characterized in this work. This is because the scheme in [20] allows the user to decode noise matrices protecting $\mathbf{A}$, whereas in our scheme, because of *cross-subspace alignment*, the user is only able to decode desired matrices, thus the penalty term $\frac{K_c+1}{K_c}$ disappears.

6 Conclusion

The problem of U-B-MDS-XSTPIR, i.e., X-secure T-private information retrieval from MDS coded storage, with N servers out of which U are unresponsive and up to B may be Byzantine, is studied in this work. A lower bound on achievable rates of U-B-MDS-XSTPIR is characterized by presenting a *cross-subspace alignment* and successive decoding based scheme. We also adapt the scheme to the problem of private and secure distributed matrix multiplication that is recently proposed in [20,28]. The presented MDS-XSTPIR scheme is shown to be applicable to PSDMM problem, even if we allow security concerns for all constituent matrices. The immediate challenge for future work is to settle the asymptotic capacity conjectures for MDS-TPIR, and also of MDS-XSTPIR, either in the affirmative by finding tight converse bounds or in the negative by finding better asymptotic achievable schemes. Beyond this, settling down the conjecture of asymptotic capacity of U-B-MDS-XSTPIR with unresponsive and Byzantine servers also merits investigation.

References

[1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, 1995, pp. 41–50.

[2] H. Sun and S. A. Jafar, "The Capacity of Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4075–4088, July 2017.

[3] R. Tajeddine, O. W. Gnilke, and S. El Rouayheb, "Private Information Retrieval from MDS Coded Data in Distributed Storage Systems," *IEEE Transactions on Information Theory*, 2018.

[4] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," in *Proceedings of the thirty-second annual ACM symposium on Theory of computing.* ACM, 2000, pp. 80–86.

[5] S. Yekhanin, "Locally Decodable Codes and Private Information Retrieval Schemes," Ph.D. dissertation, Massachusetts Institute of Technology, 2007.

[6] P. Gopalan, C.Huang, H. Simitci, and S. Yekhanin, "On the Locality of Codeword Symbols," *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6925–6934, Nov. 2012.

[7] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Batch codes and their applications," in *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing.* ACM, 2004, pp. 262–271.

[8] M. O. Rabin, "How to exchange secrets with oblivious transfer." 1981.

[9] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," in *Proceedings of the thirtieth annual ACM symposium on Theory of computing.* ACM, 1998, pp. 151–160.

[10] M. Abadi, J. Feigenbaum, and J. Kilian, "On hiding information from an oracle," in *Proceedings of the nineteenth annual ACM symposium on Theory of computing.* ACM, 1987, pp. 195–203.

[11] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[12] S. A. Jafar, "Blind Interference Alignment," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 216–227, June 2012.

[13] H. Sun and S. A. Jafar, "Blind interference alignment for private information retrieval," *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 560–564, 2016.

[14] A. C. Yao, "Protocols for secure computations," in *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on.* IEEE, 1982, pp. 160–164.

[15] W.-T. Chang and R. Tandon, "On the capacity of secure distributed matrix multiplication," *arXiv preprint arXiv:1806.00469*, 2018.

[16] R. G. D'Oliveira, S. E. Rouayheb, and D. Karpuk, "Gasp codes for secure distributed matrix multiplication," *arXiv preprint arXiv:1812.09962*, 2018.

[17] J. Kakar, S. Ebadifar, and A. Sezgin, "Rate-efficiency and straggler-robustness through partition in distributed two-sided secure matrix computation," *arXiv preprint arXiv:1810.13006*, 2018.

[18] M. Aliasgari, O. Simeone, and J. Kliewer, "Distributed and private coded matrix computation with flexible communication load," *arXiv preprint arXiv:1901.07705*, 2019.

[19] Z. Jia and S. Jafar, "On the capacity of secure distributed matrix multiplication," *arXiv preprint arXiv:1908.06957*, 2019.

[20] W. Chang and R. Tandon, "On the upload versus download cost for secure and private matrix multiplication," *arXiv preprint arXiv:1906.10684*, 2019.

[21] H. Sun and S. A. Jafar, "The Capacity of Robust Private Information Retrieval with Colluding Databases," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2361–2370, April 2018.

[22] K. Banawan and S. Ulukus, "The capacity of private information retrieval from byzantine and colluding databases," *arXiv preprint arXiv:1706.01442*, 2017.

[23] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, and C. Hollanti, "Private information retrieval from coded storage systems with colluding, byzantine, and unresponsive servers," *arXiv preprint arXiv:1806.08006*, 2018.

[24] K. Banawan and S. Ulukus, "The Capacity of Private Information Retrieval from Coded Databases," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1945–1956, 2018.

[25] Z. Jia, H. Sun, and S. A. Jafar, "Cross subspace alignment and the asymptotic capacity of x -secure t -private information retrieval," *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5783–5798, Sep. 2019.

[26] R. Freij-Hollanti, O. Gnilke, C. Hollanti, and D. Karpuk, "Private Information Retrieval from Coded Databases with Colluding Servers," *SIAM Journal on Applied Algebra and Geometry*, vol. 1, no. 1, pp. 647–664, 2017.

[27] H. Sun and S. A. Jafar, "Private Information Retrieval from MDS Coded Data with Colluding Servers: Settling a Conjecture by Freij-Hollanti et al." *IEEE Transactions on Information Theory*, vol. 64, no. 2, pp. 1000–1022, February 2018.

[28] M. Kim and J. Lee, "Private secure coded computation," *arXiv preprint arXiv:1902.00167*, 2019.

[29] N. Shah, K. Rashmi, and K. Ramchandran, "One Extra Bit of Download Ensures Perfectly Private Information Retrieval," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 856–860.

[30] N. Raviv and D. Karpuk, "Private Polynomial Computation from Lagrange Encoding," *arXiv preprint arXiv:1812.04142*, 2018.