On the Generic Capacity of K-User Symmetric Linear Computation Broadcast

Yuhang Yao, *Graduate Student Member, IEEE*, and Syed A. Jafar, *Fellow, IEEE*

***Abstract*— Linear computation broadcast (LCBC) refers to a setting with d dimensional data stored at a central server, where K users, each with some prior linear side-information, wish to compute various linear combinations of the data. For each computation instance, the data is represented as a d-dimensional vector with elements in a finite field $\mathbb{F}_{p^n}$ where p^n is a power of a prime. The computation is to be performed many times, and the goal is to determine the minimum amount of information per computation instance that must be broadcast to satisfy all the users. The reciprocal of the optimal broadcast cost per computation instance is the capacity of LCBC. The capacity is known for up to $K = 3$ users. Since LCBC includes index coding as a special case, large K settings of LCBC are at least as hard as the index coding problem. As such the general LCBC problem is beyond our reach and we do not pursue it. Instead of the general setting (*all* cases), by focusing on the *generic* setting (*almost all* cases) this work shows that the generic capacity of the symmetric LCBC (where every user has m' dimensions of side-information and m dimensions of demand) for large number of users ($K \geq d$ suffices) is $C_g = 1/\Delta_g$, where $\Delta_g = \min\left\{\max\{0, d-m'\}, \frac{dm}{m+m'}\right\}$, is the broadcast cost that is both achievable and unbeatable asymptotically almost surely for large n, among all LCBC instances with the given parameters p, K, d, m, m'. Relative to baseline schemes of random coding or separate transmissions, C_g shows an extremal gain by a factor of K as a function of number of users, and by a factor of $\approx d/4$ as a function of data dimensions, when optimized over remaining parameters. For arbitrary number of users, the generic capacity of the symmetric LCBC is characterized within a factor of 2.**

***Index Terms*— Computation broadcast, generic capacity.**

I. Introduction

RECENT observations of 'megatrends' in the communication industry indicate that the number of devices connected to the internet is expected to cross 500 billion, approaching 60 times the estimated human population over the next decade [1]. With machines set to become the dominant users of future communication networks, along with accompanying developments in artificial intelligence and virtual/augmented/mixed reality applications, a major paradigm shift is on the horizon where communication networks increasingly take on a new role, as *computation networks*. The changing paradigm brings with it numerous challenges and opportunities.

One of the distinguishing features of computation networks is their algorithmic nature, which creates *predictable* dependencies and side-information structures. To what extent can such structures be exploited for gains in communication efficiency? Answering this question requires an understanding of the capacity of computation networks.

The study of the capacity of computation networks has a rich history in information theory, spanning a variety of ideas and directions that include zero error capacity and confusability graphs [2], graph entropy [3], [4], conditional graph entropy [5], multiterminal source coding [6], encoding of correlated sources [7], [8], [9], [10], sum-networks [11], [12], [13], computation over acyclic directed networks [14], [15], compute-and-forward [16], federated learning [17], private computation [18], [19], coded computing [20], [21], [22], [23], and distributed matrix multiplication [24], [25], [26], [27], to name a few. However, due to the enormous scope, hardness, and inherent combinatorial complexity of such problems, a *cohesive* foundation is yet to emerge.

Following the ground-up approach of classical network information theory which focuses on elemental scenarios, and taking cues from systems theory that builds on an elegant foundation of *linear* systems, it is conceivable that a cohesive foundation could emerge from the study of the building blocks of *linear computation networks*. Linear computation networks are characterized by the presence of side-information and demands that are linear functions of the data. Linear side information and dependencies are quite valuable as theoretical abstractions because in principle they allow the study of a complex linear computation network by breaking it down into tractable components, while retaining some of the critical relationships between the components in the form of side-information. For example, multi-round/multi-hop linear computation networks may be optimized one-round/hop at a time, by accounting for the information from other rounds/hops as side-information.

As a fundamental building block, the linear computation broadcast (LCBC) problem is introduced in [28]. LCBC refers

Manuscript received 14 December 2022; revised 6 November 2023; accepted 20 March 2024. Date of publication 27 March 2024; date of current version 23 April 2024. This work was supported in part by NSF under Grant CCF-2221379 and in part by Office of Naval Research (ONR) under Grant N00014-21-1-2386. An earlier version of this paper was presented in part at the 2023 IEEE International Conference on Communications (ICC) [DOI: 10.1109/ICC45041.2023.10278932]. *(Corresponding author: Yuhang Yao.)*

The authors are with the Center for Pervasive Communications and Computing (CPCC), Department of Electrical Engineering and Computer Science, University of California at Irvine, Irvine, CA 92697 USA (e-mail: yuhangy5@uci.edu; syed@uci.edu).

Communicated by A. Ramamoorthy, Associate Editor for Coding Techniques.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2024.3382257.

Digital Object Identifier 10.1109/TIT.2024.3382257

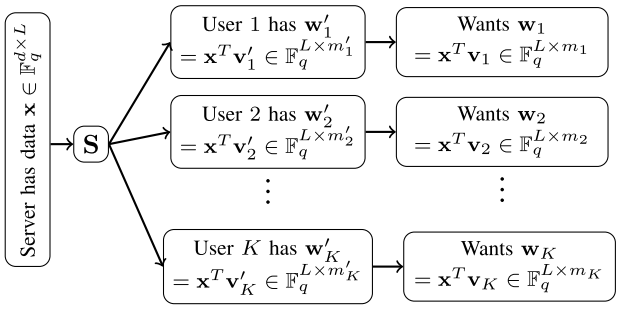

Fig. 1. LCBC$\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)$ with batch-size L. $q = p^n$ is a power of a prime. The coefficient matrices $\mathbf{v}_k \in \mathbb{F}_q^{d\times m_k}$, $\mathbf{v}'_k \in \mathbb{F}_q^{d\times m'_k}$ for all $k \in [K]$ specify the desired computations and side-informations, respectively.

to the setting illustrated in Figure 1, where K users, each with some prior side-information $(\mathbf{w}'_k = \mathbf{x}^T\mathbf{v}'_k)$ comprised of various linear combinations of d-dimensional data $(\mathbf{x})$ over a finite field $(\mathbb{F}_q = \mathbb{F}_{p^n})$, wish to retrieve other individually specialized linear combinations $(\mathbf{w}_k = \mathbf{x}^T\mathbf{v}_k)$ of the data, with the help of a central server that has all the data. The goal is to determine the minimum amount of information that the central server must broadcast in order to satisfy all the users' computational demands. In addition to its significance as an elemental building block of computational networks, the LCBC setting is remarkably powerful by itself, e.g., it includes index coding [29], [30], [31] as a special case, and generalizes linear coded caching [32], [33], [34] to allow arbitrary cached information and demands. The one-to-many topology represented by LCBC arises naturally in any context where distributed nodes coordinate with each other [35], [36] with the help of a master node. Such scenarios may be pervasive in the future as interactive networked VR environments [37] become commonplace.

The capacity of LCBC is characterized for $K = 2$ users in [28]. More recently, in [38] the capacity is fully characterized for the $K = 3$ user LCBC. In addition to such efforts that are aimed at small number of users, it is also important to develop insights into the fundamental limits of larger LCBC networks. However, any such attempt runs into immediate obstacles. In addition to the combinatorial complexity of large networks, the LCBC — because it includes index coding as a special case — is at least as hard as the index coding problem in general. The difficulty of the index coding problem is well recognized [31], [39], [40], [41], [42]. How to overcome this obstacle, is the central question that motivates our work in this paper.

A key idea that makes this work possible is the distinction between the *general* LCBC problem — which includes *all* instances, and the *generic* LCBC problem — which includes *almost all* instances. We focus on the latter. While the general LCBC problem is necessarily at least as hard as the general index coding problem, the generic LCBC problem may still be tractable. Such observations are common in many fields, for example computational complexity theory posits that for many computation problems, the difficult cases are rare and most (generic) instances are much easier, thereby motivating the sub-field of *generic-case complexity* [43], [44]. Drawing parallels to the degrees of freedom (DoF) studies of wireless interference networks, there also the general problem remains open — for arbitrary channel realizations the DoF are not known for even the 3-user interference channel. However, the generic problem is settled for the K-user (any K) interference channel; we know the DoF for *almost all* realizations [45], [46], [47]. For general MIMO interference channels, even maximizing linearly achievable DoF is shown to be NP-hard [48], yet it is tractable in the generic sense [49], [50]. Similarly, while the index coding problem is hard, index coding instances represent a negligible fraction of all possible instances of LCBC. Thus, there remains hope that a foundation for a cohesive theory of linear computation networks may yet be built by studying the *generic capacity* of its building blocks.

With some oversimplification for the sake of intuition, consider the following toy example. We have a $K = 4$ user setting, say over $\mathbb{F}_7$, with $d = 4$ dimensional data represented by $\mathbf{x} = (\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D})^T$. The users each have 1-dimensional side-information and demands,

$$\mathbf{w}'_1 = \mathbf{A} + \mathbf{B} + \mathbf{C} + \mathbf{D}, \qquad \mathbf{w}_1 = \mathbf{A} + 2\mathbf{B} + 3\mathbf{C} + 4\mathbf{D}, \quad (1)$$
$$\mathbf{w}'_2 = \mathbf{A} + 3\mathbf{B} + 2\mathbf{C} + 5\mathbf{D}, \quad \mathbf{w}_2 = 2\mathbf{A} + \mathbf{B} + 4\mathbf{C} + 6\mathbf{D}, \quad (2)$$
$$\mathbf{w}'_3 = 5\mathbf{A} + 4\mathbf{B} + \mathbf{C} + 3\mathbf{D}, \quad \mathbf{w}_3 = 6\mathbf{A} + 3\mathbf{B} + 4\mathbf{C} + \mathbf{D}, \quad (3)$$
$$\mathbf{w}'_4 = 4\mathbf{A} + \mathbf{B} + 5\mathbf{C} + 6\mathbf{D}, \quad \mathbf{w}_4 = 5\mathbf{A} + 2\mathbf{B} + 6\mathbf{C} + 3\mathbf{D}. \quad (4)$$

If we had only the first 2 users to consider, the broadcast cost of 2 would be trivially achieved, e.g., by broadcasting $\mathbf{w}_1, \mathbf{w}_2$ which satisfies both users. If we had only the first 3 users, the solution is less trivial, but we still find (see Section IV-C) that broadcasting $(\mathbf{S}_1, \mathbf{S}_2) = (2\mathbf{A} + 6\mathbf{B} + 3\mathbf{C},\ 4\mathbf{A} + 4\mathbf{B} + \mathbf{C} + \mathbf{D})$ incurs a cost of 2, while satisfying all 3 users' demands – it is easy to verify that User 1 recovers $\mathbf{w}_1 = 2\mathbf{S}_1 - 3\mathbf{w}'_1$, User 2 recovers $\mathbf{w}_2 = 5\mathbf{S}_2 - 4\mathbf{w}'_2$, and User 3 recovers $\mathbf{w}_3 = \mathbf{S}_1 + \mathbf{S}_2$, all operations in $\mathbb{F}_7$, represented as integers modulo 7. However, as the number of users increases, the problem becomes much more challenging. It is far from obvious that a broadcast cost of 2 could still suffice to satisfy all 4 users listed above, and highly counter-intuitive that the optimal broadcast cost may still be only 2 for large number of users, e.g., $K = 100$ users. This surprising conclusion follows from the results found in this work, with the important caveat that the results are shown to be true only asymptotically almost surely for large n. In other words, for this example, suppose we have the 4 dimensional data $(\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D})$ over $\mathbb{F}_q$, $q = p^n$ for any arbitrary prime p, and a large number (say $K = 100$) of users, and the coefficients of the users' 1-dimensional demands and side-informations are chosen uniformly randomly from $\mathbb{F}_{p^n}$, each choice representing a particular instance of this LCBC. Then we prove that as $n \to \infty$, almost all instances have optimal broadcast cost 2 (in q-ary units). The larger the number of users K, the larger n may need to be for the convergence to take effect, but the optimal broadcast cost must ultimately converge in probability to 2 q-ary symbols.

The main result of this work is the characterization of the *generic* capacity, $C_g(p, K, d, m, m') = 1/\Delta_g$, where $\Delta_g = \min\left\{\max\{0, d - m'\}, \frac{dm}{m+m'}\right\}$, for a K user LCBC with d dimensional data over $\mathbb{F}_{p^n}$, in the symmetric setting where every user has m dimensional demands and m' dimensional side-information, for large enough number of users ($K \geq d$ suffices) and large n. Informally, Δ_g represents a broadcast

cost that is both achievable, and unbeatable, asymptotically almost surely for large n, among the class of all LCBC problems with fixed parameters K, p, d, m, m'. Setting aside the trivial regimes $d \leq m+m'$ where random coding is optimal ($\Delta_g = \max\{0, d-m'\}$), and $d \geq K(m+m')$ where separate transmissions for each user are optimal ($\Delta_g = Km$), in the remaining non-trivial regime where $m+m' < d < K(m+m')$, we have $\Delta_g = dm/(m+m')$. Note that this depends only on d, m, m', i.e., the dimensions of the data, demands, and side-information. In particular, our generic capacity results do not depend on the characteristic p of the finite field, and in the non-trivial regime with sufficiently large number of users, the generic capacity also does not depend on the number of users K. The converse proofs are information theoretic and make use of functional submodularity [38], [51], [52]. The achievability arguments build upon the idea of asymptotic interference alignment [45], both by adapting it from the K user wireless interference channel to the K user LCBC context, and by a non-trivial strengthening of the original scheme involving an additional symbol-extension overhead that is needed to harness sufficient *diversity* in the finite field setting. The generic capacity characterization reveals that the capacity can be significantly higher than what is achievable with the baseline schemes of random coding and/or separate transmissions. For example, the extremal gain [53] of generic capacity over baseline schemes, as a function of the number of users (maximized over the remaining parameters) is K, and the extremal gain as a function of the data dimension d is $\approx d/4$ (Observation 3 in Section IV-D). As an immediate corollary of the main result, the generic capacity of the symmetric LCBC is characterized within a factor of 2 for any number of users K (Observation 1). Notably, an exact characterization is found (Theorem 3) for any number of users if the side-information and demands are one-dimensional. Some extensions to asymmetric settings are obtained as well.

II. Notation

A. Miscellaneous

The notation $[a:b]$ represents the set of integers $\{a, a+1, \ldots, b\}$ if $b \geq a$ and $\emptyset$ otherwise. The compact notation $[K]$ is equivalent to $[1:K]$. For a set of indices S, the notation A_S represents $\{A_s, s \in S\}$, e.g., $A_{[K]} = \{A_1, A_2 \cdots, A_K\}$. $|\mathcal{S}|$ denotes the cardinality of a set $\mathcal{S}$. $\mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field with $q = p^n$ a power of a prime. The elements of the prime field $\mathbb{F}_p$ are represented as $\mathbb{Z}/p\mathbb{Z}$, i.e., integers modulo p. The notation $\mathbb{F}_q^{n_1 \times n_2}$ represents the set of $n_1 \times n_2$ matrices with elements in $\mathbb{F}_q$. $\mathbb{F}_q$ is a sub-field of $\mathbb{F}_{q^z}$, and $\mathbb{F}_{q^z}$ is an extension field of $\mathbb{F}_q$ for $z > 1$. $\mathbb{N} = \{1, 2, \cdots\}$ is the set of natural numbers. The greatest common divisor of a, b is denoted $\gcd(a, b)$. $(x)^+ \triangleq \max\{0, x\}$. $\mathsf{Pr}(E)$ stands for the probability of the event E. Given an event E_n that depends on an integer parameter n, we say that Event E_n holds asymptotically almost surely (a.a.s.) if $\lim_{n\to\infty} \mathsf{Pr}(E_n) = 1$. Throughout this work when we use a.a.s., the quantity approaching infinity will be denoted by n. For variables a, b that depend on an integer n, we use the notation $a \overset{\text{a.a.s.}}{=} b$ to represent the statement, $\lim_{n\to\infty} \mathsf{Pr}(a = b) = 1$. Similarly, $a \overset{\text{a.a.s.}}{\geq} b$ represents $\lim_{n\to\infty} \mathsf{Pr}(a \geq b) = 1$; $a \overset{\text{a.a.s.}}{\leq} b$ represents $\lim_{n\to\infty} \mathsf{Pr}(a \leq b) = 1$; $a \overset{\text{a.a.s.}}{<} b$ represents $\lim_{n\to\infty} \mathsf{Pr}(a < b) = 1$, and $a \overset{\text{a.a.s.}}{>} b$ represents $\lim_{n\to\infty} \mathsf{Pr}(a > b) = 1$.

B. Matrix Operations

By default we will consider matrices in a finite field $\mathbb{F}_q$. For two matrices M_1, M_2 with the same number of rows, $[M_1, M_2]$ represents a concatenated matrix which can be partitioned column-wise into M_1 and M_2. $M_{[i]}$ denotes the i-th column of M. The notation $M_{[a:b]}$ stands for the sub-matrix $[M_{[a]}, M_{[a+1]}, \ldots, M_{[b]}]$ if $b \geq a$, and $[\,]$ otherwise. The rank of $M \in \mathbb{F}_q^{m\times n}$ is denoted by $\mathrm{rk}(M)$, and we say that M has *full rank* if and only if $\mathrm{rk}(M) = \min\{m, n\}$. $\langle M \rangle_q$ denotes the $\mathbb{F}_q$-linear vector space spanned by the columns of M. The subscript q will typically be suppressed as it is clear from the context. If M has full column rank, then we say that M forms a basis for $\langle M \rangle$. The notation $M_1 \cap M_2$ represents a matrix whose columns form a basis of $\langle M_1 \rangle \cap \langle M_2 \rangle$. In addition, $\mathbf{0}^{a\times b}$ represents the $a \times b$ zero matrix. $\mathbf{I}^{a\times a}$ represents the $a \times a$ identity matrix.

C. Conditional Matrix Notation: $(M_1|M_2)$

Say $M_1 \in \mathbb{F}_q^{d\times\mu_1}$ and $M_2 \in \mathbb{F}_q^{d\times\mu_2}$. By Steinitz Exchange Lemma, there exists a sub-matrix of M_1 with full column rank, denoted by $(M_1|M_2)$, that is comprised of $\mathrm{rk}(M_1) - \mathrm{rk}(M_1 \cap M_2)$ columns of M_1 such that $[M_1 \cap M_2, (M_1|M_2)]$ forms a basis for $\langle M_1 \rangle$. We have,

$$\begin{aligned} \mathrm{rk}(M_1|M_2) &= \mathrm{rk}(M_1) - \mathrm{rk}(M_1 \cap M_2) \\ &= \mathrm{rk}([M_1, M_2]) - \mathrm{rk}(M_2) \end{aligned} \tag{5}$$

where we made the use of the fact that $\mathrm{rk}([M_1, M_2]) = \mathrm{rk}(M_1) + \mathrm{rk}(M_2) - \mathrm{rk}(M_1 \cap M_2)$.

III. Problem Formulation: Linear Computation Broadcast

A. LCBC$\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)$

An LCBC problem is specified by its parameters as LCBC$\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)$, where $\mathbb{F}_q$ is a finite field with $q = p^n$ a power of a prime, and $\mathbf{v}_k \in \mathbb{F}_q^{d\times m_k}$, $\mathbf{v}'_k \in \mathbb{F}_q^{d\times m'_k}$, for all $k \in [K]$, are matrices with the same number of rows, d. The value K represents the number of users, d represents the data dimension, and m_k, m'_k quantify the amounts of desired computations and side-information corresponding to User k. The context is as follows. A central server stores multiple instances of d dimensional data over a finite field $\mathbb{F}_q$. The ℓ^{th} instance of the data vector is denoted as $\mathbf{x}(\ell) = [x_1(\ell), \ldots, x_d(\ell)]^T \in \mathbb{F}_q^{d\times 1}$, and $\mathbf{x} = [\mathbf{x}(1), \ldots, \mathbf{x}(L)] \in \mathbb{F}_q^{d\times L}$ collects $L \in \mathbb{N}$ data instances.[1] A broadcast link connects K distributed users to the central server. The *coefficient* matrices $\mathbf{v}'_k$ and $\mathbf{v}_k$ specify the side-information and desired computations for the k^{th} user. Specifically, for all $k \in [K]$, User k has side information $\mathbf{w}'_k = \mathbf{x}^T\mathbf{v}'_k \in \mathbb{F}_q^{L\times m'_k}$,

[1]The parameter L is referred to as the batch size and may be chosen freely by a coding scheme.

and wishes to compute $\mathbf{w}_k = \mathbf{x}^T \mathbf{v}_k \in \mathbb{F}_q^{L \times m_k}$. For compact notation in the sequel it is useful to define,

$$\mathbf{u}_k \triangleq [\mathbf{v}'_k, \mathbf{v}_k]. \tag{6}$$

A coding scheme for an LCBC problem is denoted by a tuple $(L, \Phi, \Psi_{[K]}, \mathcal{S})$, which specifies a batch size L, an encoding function $\Phi : \mathbb{F}_q^{L \times d} \to \mathcal{S}$ that maps the data to the broadcast information $\mathbf{S}$ over some alphabet $\mathcal{S}$, i.e.,

$$\Phi(\mathbf{x}) = \mathbf{S} \tag{7}$$

and decoders, $\Psi_k : \mathcal{S} \times \mathbb{F}_q^{L \times m'_k} \to \mathbb{F}_q^{L \times m_k}$, that allow the k^{th} user to retrieve $\mathbf{w}_k$ from the broadcast information $\mathbf{S}$ and the side-information $\mathbf{w}'_k$ for all $k \in [K]$, i.e.,

$$\mathbf{w}_k = \Psi_k(\mathbf{S}, \mathbf{w}'_k) = \Psi_k(\Phi(\mathbf{x}), \mathbf{w}'_k), \qquad \forall k \in [K]. \tag{8}$$

A coding scheme that allows successful decoding for all data realizations, i.e., satisfies (8) for all $\mathbf{x} \in \mathbb{F}_q^{d \times L}$, is called an *achievable* scheme. Let us define $\mathcal{A}\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)$ as the set of all achievable schemes for LCBC$\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)$.

The broadcast cost (normalized by L and measured in q-ary units) for an achievable scheme is defined as $\Delta = \log_q |\mathcal{S}|/L$. The optimal broadcast cost $\Delta^*\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)$ for an LCBC problem is defined as,

$$\Delta^*\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right) = \inf_{(L, \Phi, \Psi_{[K]}, \mathcal{S}) \in \mathcal{A}\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right)} \Delta. \tag{9}$$

The capacity, C^*, of an LCBC problem is the reciprocal of its optimal broadcast cost,

$$C^*\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right) = 1/\Delta^*\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right). \tag{10}$$

Note that although the side information and demands are linear functions of the data, the achievable schemes, i.e., the encoding and decoding operations are not restricted to be linear.

B. Generic Capacity

Define

$$\mathcal{L}_n\left(p, K, d, m_{[K]}, m'_{[K]}\right) = \left\{ \text{LCBC}\left(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\right) \;\middle|\; \begin{array}{rcl} q & = & p^n \\ \mathbf{v}_k & \in & \mathbb{F}_q^{d \times m_k} \\ \mathbf{v}'_k & \in & \mathbb{F}_q^{d \times m'_k} \\ \forall k & \in & [K] \end{array} \right\}, \tag{11}$$

or $\mathcal{L}_n$ in short, as the set of all LCBC instances with the 'dimensional' parameters p, n, K, $m_{[K]}$, $m'_{[K]}$. Let Λ_n be a uniformly randomly chosen instance from $\mathcal{L}_n$, and $\Delta^*(\Lambda_n)$ be the optimal download cost of Λ_n. In order to define generic capacity, let us fix the parameters $(p, K, d, m_{[K]}, m'_{[K]})$ and allow n to approach infinity.

The generic optimal broadcast cost Δ_g, if exists, is defined as the value that $\Delta^*(\Lambda_n)$ converges to in probability, i.e.,

$$\lim_{n \to \infty} \mathsf{Pr}\Big(\big|\Delta^*(\Lambda_n) - \Delta_g\big| < \varepsilon\Big) = 1, \qquad \forall \varepsilon > 0. \tag{12}$$

The generic capacity is then defined as the reciprocal, i.e.,

$$C_g = 1/\Delta_g. \tag{13}$$

Since Δ_g, C_g may not always exist, we further define the following upper and lower extremal metrics, which always exist and help in the analysis of generic capacity. We say that Δ is achievable asymptotically almost surely (a.a.s) (cf. Definition 1.1.2(v) [54]) if,

$$\lim_{n \to \infty} \mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq \Delta\Big) = 1, \tag{14}$$

which is expressed compactly as $\Delta^*(\Lambda_n) \overset{\text{a.a.s.}}{\leq} \Delta$. Define the smallest such Δ as $\Delta_u^*\left(p, K, d, m_{[K]}, m'_{[K]}\right)$, or Δ_u^* in short, i.e.,

$$\Delta_u^* \triangleq \inf\left\{\Delta : \Delta^*(\Lambda_n) \overset{\text{a.a.s.}}{\leq} \Delta\right\}. \tag{15}$$

Similarly, define Δ_l^* as,

$$\Delta_l^* \triangleq \sup\left\{\Delta : \Delta^*(\Lambda_n) \overset{\text{a.a.s.}}{>} \Delta\right\}. \tag{16}$$

Thus, Δ_u^* is the infimum of broadcast costs that are achievable a.a.s. (tightest upper bound), and Δ_l^* is the supremum of broadcast costs that are *not* achievable a.a.s. (tightest lower bound). By definition, $\Delta_u^* \geq \Delta_l^*$. If[2] $\Delta_u^* = \Delta_l^*$, then they are equal to the generic optimal broadcast cost Δ_g, i.e.,

$$\Delta_g = \Delta_u^* = \Delta_l^* \tag{17}$$

and $C_g = 1/\Delta_g$ exists. If $\Delta_u^* \neq \Delta_l^*$, then Δ_g, C_g do not exist.

Remark 1: It is worth noting that the definition of 'generic capacity' connects to the notion of generic subsets in the literature on generic case complexity [55]. To briefly point out this connection, following along the lines of Definition 3.1 and Lemma 3.2 of [55], we may define a generic subset as follows: Let I be a set of inputs with size[3] function σ. Define I_r, the sphere of radius r, by $I_r = \{w \mid w \in I, \sigma(w) = r\}$, the set of inputs of size r. A subset $R \subset I$ is said to have asymptotic density α, written $\rho'(R) = \alpha$, if $\lim_{r \to \infty} |R \cap I_r|/|I_r| = \alpha$ where $|X|$ denotes the size of a set X. If R has asymptotic density 1, it is called generic; and if it has asymptotic density 0, it is negligible. Now, for our problem, the set $I = \cup_{n \in \mathbb{N}} \mathcal{L}_n$ is the set of all LCBC instances for fixed $p, K, m_{[K]}, m'_{[K]}$. The size function $\sigma = n$, and the sphere $I_n = \mathcal{L}_n$. Let $R_u(\Delta) = \{\mathcal{L} \in I \mid \Delta \geq \Delta^*(\mathcal{L})\}$ be the subset of LCBC instances for which the broadcast cost Δ is achievable. Then Δ_u^* is the infimum of the values of Δ for which $R_u(\Delta)$ is generic. Similarly, Δ_l^* is the supremum of the values of Δ for which $R_l(\Delta) = \{\mathcal{L} \in I \mid \Delta < \Delta^*(\mathcal{L})\}$ is generic. In plain words, Δ_u^* is the infimum of broadcast costs that are generically achievable, while Δ_l^* is the supremum of broadcast costs that are generically not achievable. When they match, we have the generic optimal broadcast cost, and as its reciprocal notion, the generic capacity.

[2]Note that the definition does not automatically preclude strict inequality, e.g., as a thought experiment suppose one half of all instances have $\Delta^* = 1$ and the other half have $\Delta^* = 2$, then $\Delta_u^* = 2$ and $\Delta_l^* = 1$.

[3]A size function for a set I is a map $\sigma : I \to \mathbb{N}$, the nonnegative integers, such that the preimage of each integer is finite (Definition 2.4 of [55]).

IV. Results: Generic Capacity

In this work we mainly focus on the *symmetric* LCBC, where we have,

$$m_1 = m_2 = \ldots = m_K = m,$$
$$m'_1 = m'_2 = \ldots = m'_K = m'. \tag{18}$$

Note that the generic capacity (if it exists) can only be a function of (p, K, d, m, m'), since these are the only parameters left.

A. $K = 1, 2, 3$ Users

While we are interested primarily in LCBC settings with large number of users (large K), it is instructive to start with the generic capacity characterizations for $K = 1, 2, 3$ users. Recall that the LCBC problem is already fully solved for $K = 2$ in [28] and $K = 3$ in [38]. Therefore, the following theorem essentially follows from [28] and [38]. The $K = 1$ case is trivial and is included for the sake of completeness.

Theorem 1: The generic capacity $C_g = 1/\Delta_g$ for the symmetric LCBC with $K = 1, 2, 3$ users is characterized as follows.

$K = 1$ user:

$$\Delta_g = \begin{cases} 0, & d \le m'; \\ d - m', & m' \le d \le m + m'; \\ m, & m + m' \le d. \end{cases} \tag{19}$$

$K = 2$ users:

$$\Delta_g = \begin{cases} 0, & d \le m'; \\ d - m', & m' \le d \le m + m'; \\ m, & m + m' \le d \le m + 2m'; \\ d - 2m', & m + 2m' \le d \le 2(m + m'); \\ 2m, & 2(m + m') \le d. \end{cases} \tag{20}$$

$K = 3$ users:

$$\Delta_g = \begin{cases} 0, & d \le m'; \\ d - m', & m' \le d \le m' + m; \\ m, & m' + m \le d \le m + 1.5m'; \\ d - 1.5m', & m + 1.5m' \le d \le 1.5(m + m'); \\ 1.5m, & 1.5(m + m') \le d \le 1.5m + 2m'; \\ d - 2m', & 1.5m + 2m' \le d \le 2(m + m'); \\ 2m, & 2(m' + m) \le d \le 2m + 3m'; \\ d - 3m', & 2m + 3m' \le d \le 3(m + m'); \\ 3m, & 3(m + m') \le d. \end{cases} \tag{21}$$

The proof of Theorem 1 is relegated to Appendix III. The task left for the proof is to correctly account for the generic cases (non-trivial for $K = 3$), after which the capacity results from [28] and [38] can be directly applied.

B. Large K

The main result of this work appears in the following theorem.

Theorem 2: For the symmetric LCBC with the number of users satisfying

$$K \ge d/\gcd(d, m + m'), \tag{22}$$

the generic capacity $C_g = 1/\Delta_g$ is characterized as follows,

$$\Delta_g = \begin{cases} 0, & d \le m'; \\ d - m', & m' \le d \le m + m'; \\ dm/(m + m'), & m + m' < d \le K(m + m'). \end{cases} \tag{23}$$

The proof of converse for Theorem 2 appears in Section VI while the achievability is proved in Appendix I. The main technical challenge is to show the achievability of $dm/(m + m') + \varepsilon, \forall \varepsilon > 0$ in the non-trivial regime, $m + m' < d \le K(m + m')$. Remarkably, in this regime we are able to show that $\forall \varepsilon > 0$, a broadcast cost of $dm/(m + m') + \varepsilon$ is achievable a.a.s., regardless of the number of users K, based on an asymptotic interference alignment (IA) scheme. Examples to illustrate the asymptotic IA construction are provided in Section V. The condition (22) on the number of users in Theorem 2 is needed for our converse bound in Section VI to match the achievability.

Next, let us briefly address arbitrary number of users and asymmetric settings through the following corollary of Theorem 2.

Corollary 1: For the (not necessarily symmetric) LCBC with arbitrary number of users,

$$\Delta_l^* \ge \max_{\mathcal{K} \subset [K]} \min \left\{ d - \sum_{k \in \mathcal{K}} m'_k, \ \sum_{k \in \mathcal{K}} m_k \right\}, \tag{24}$$

$$\Delta_u^* \le \min \left\{ \frac{m_{\max} d}{m_{\max} + m'_{\min}}, (d - m'_{\min})^+, \sum_{k \in [K]} m_k \right\}, \tag{25}$$

where $m_{\max} \triangleq \max_{k \in [K]} m_k$, and $m'_{\min} \triangleq \min_{k \in [K]} m'_k$.

Proof: (24) follows from a simple cooperation bound. Consider any LCBC instance $\Lambda_n \in \mathcal{L}_n$. For any subset $\mathcal{K} \subset [K]$ let the users in $\mathcal{K}$ fully cooperate as one user, and eliminate all other users $[K] \setminus \mathcal{K}$, to obtain a single user LCBC instance $\Lambda_{n,\mathcal{K}}$ with optimal broadcast cost $\Delta^*(\Lambda_{n,\mathcal{K}}) \le \Delta^*(\Lambda_n)$. The combined user has demand coefficient matrix $\mathbf{v}_{\mathcal{K}} \triangleq [\mathbf{v}_k, k \in \mathcal{K}]$ with d rows and $m_{\mathcal{K}} \triangleq \sum_{k \in \mathcal{K}} m_k$ columns, and the side-information coefficient matrix $\mathbf{v}'_{\mathcal{K}} \triangleq [\mathbf{v}'_k, k \in \mathcal{K}]$ with d rows and $m'_{\mathcal{K}} \triangleq \sum_{k \in \mathcal{K}} m'_k$ columns. From Theorem 1, based on the generic capacity for the single user case, we immediately obtain (24). For (25) note that $\Delta^*(\Lambda_n) \le \sum_{k \in [K]} m_k$ because serving the users separately is always an option. $\Delta^*(\Lambda_n) \le (d - m'_{\min})^+$ also holds because broadcasting $(d - m'_{\min})$ generic linear combinations (over a sufficiently large field extension) of the data allows each user a total number of generic equations $(d - m'_{\min})^+ + m'_k \ge d$, which suffices for each user to recover all d data dimensions. Finally, it is always possible to mimic a symmetric setting by adding superfluous demands and discarding some of the side-information at each user until every user has $m'_{\min}$ generic linear combinations of side-information and $m_{\max}$ generic

linear combinations of demand. Note that if $d \leq m_{\max}+m'_{\min}$ then $\frac{m_{\max}d}{m_{\max}+m'_{\min}} > (d - m'_{\min})^+$, and if $d > K(m_{\max} + m'_{\min})$, then $\frac{m_{\max}d}{m_{\max}+m'_{\min}} > \sum_{k\in[K]} m_k$. The only remaining case is $m_{\max} + m'_{\min} < d \leq K(m_{\max} + m'_{\min})$, in which case the achievability of $\frac{m_{\max}d}{m_{\max}+m'_{\min}}$ is shown in the proof of Theorem 2. □

C. One Dimensional Case: $m = m' = 1$

In the special case where the side-information and demands are one-dimensional, the generic capacity is characterized for *any* number of users, as follows.

Theorem 3: For LCBC with $m = m' = 1$, the generic capacity $C_g = 1/\Delta_g$ is characterized as follows.

1) For even d,

$$\Delta_g = \begin{cases} d/2, & 2 \leq d \leq 2K; \\ K, & d \geq 2K. \end{cases} \tag{26}$$

2) For odd d,

$$\Delta_g = \begin{cases} 0, & d = 1; \\ d/2, & 3 \leq d < 2K-1; \\ K-1, & d = 2K-1; \\ K, & d > 2K-1. \end{cases} \tag{27}$$

The result for even d follows directly from Theorem 2 and Corollary 1. Specifically, note that for even d we have $d/\text{gcd}(d,2) = d/2$, and thus (23) finds the generic capacity for even d when $K \geq d/2$. Meanwhile, letting $\mathcal{K} = [K]$ in (24), together with (25) proves the capacity for $K \leq d/2$.

For cases with odd d, (24) and (25) provide the capacity for $d = 1$ and $d > 2K-1$ (equivalently, $d \geq 2K$). For the remaining 2 regimes, (25) shows achievability for $1 \leq d < 2K-1$. (24) provides the converse for $d = 2K-1$ by specifying $\mathcal{K} = [1 : (d-1)/2]$, since $\min\{d-(d-1)/2, (d-1)/2\} = (d-1)/2 = K-1$. To complete the proof of Theorem 3, it remains to show the converse for $3 \leq d < 2K-1$, and the achievability for $d = 2K-1$. These proofs are provided in Section VII.

D. Observations

1) The following observations follow directly by specializing Corollary 1 to the symmetric LCBC with arbitrary number of users K.

$$d \leq m' \implies \Delta_g = 0; \tag{28}$$

$$m' \leq d \leq m+m' \implies \Delta_g = d - m'; \tag{29}$$

$$1 < \frac{d}{m+m'} \leq K \implies \text{if } \Delta_g \text{ exists, then}$$
$$\max\left\{d - m'\left\lceil\frac{d}{(m+m')}\right\rceil, m\left\lfloor\frac{d}{m+m'}\right\rfloor\right\}$$
$$\leq \Delta_g \leq \frac{md}{(m+m')}; \tag{30}$$

$$K(m+m') \leq d \implies \Delta_g = Km. \tag{31}$$

Regarding (30), where Δ_g is not fully established, note that in this regime, if $(m+m')$ divides d, then $\Delta_g = md/(m+m')$ is settled. On the other hand, if $(m+m')$ does not divide d, and if Δ_g exists, then we have its value within a multiplicative factor of 2 because in this regime,

$$\frac{md/(m+m')}{m\lfloor d/(m+m')\rfloor} = \frac{d/(m+m')}{\lfloor d/(m+m')\rfloor} \leq 2. \tag{32}$$

Thus, the generic capacity of the symmetric LCBC is characterized within a factor of 2 when it exists, for arbitrary number of users K.

2) Theorem 2 and Corollary 1 lead to sharp generic capacity results for various asymmetric cases as well. For example, from Corollary 1 we find that for any number of users, if $m'_k \leq d \leq m_k + m'_k$ for all $k \in [K]$, then $\Delta_g = d - \min_{k\in[K]} m'_k$. If $d \geq \sum_{k\in[K]}(m_k + m'_k)$ then $\Delta_g = \sum_{k\in[K]} m_k$. In Theorem 2 the optimal broadcast cost $\Delta_g = dm/(m+m')$ for the non-trivial regime $(m+m') < d \leq K(m+m')$, remains unchanged if we include another K' users, say Users $K+1, K+2, \cdots, K+K'$, with asymmetric demands and side-information such that $m_{k'} \geq m'$ and $m_k \leq m$ for all $k' \in [K+1 : K+K']$. The original converse still holds because additional users cannot help. The original achievability still holds because the additional users have more side-information and less demands than original users, so they can pretend to be like the original users by discarding some of their side-information and adding superfluous demands. This creates a symmetric setting with $K+K'$ users, but in this regime $\Delta_g = dm/(m+m')$ does not depend on the number of users.

3) The generic capacity of the symmetric LCBC $C_g(p,K,d,m,m')$ can be quite significantly higher than the best of the rates achievable through the baseline schemes of random coding $(1/(d-m'))$ and separate transmissions $(1/(Km))$. Gains up to the order of K and d in the number of users and data dimensions are observed. To make this precise, consider the *extremal* gain [53] of generic capacity over the baseline schemes as a function of the number of users, K,

$$\eta_K \triangleq \sup_{p,d,m,m'} \frac{C_g(p,K,d,m,m')}{\max\left\{\frac{1}{(d-m')^+}, \frac{1}{Km}\right\}}$$
$$= \sup_{d,m,m'} \frac{\frac{m+m'}{md}}{\max\left\{\frac{1}{(d-m')^+}, \frac{1}{Km}\right\}}$$
$$= K, \tag{33}$$

and as a function of the data dimension d,

$$\eta_d \triangleq \sup_{p,K,m,m'} \frac{C_g(p,K,d,m,m')}{\max\left\{\frac{1}{(d-m')^+}, \frac{1}{Km}\right\}}$$
$$= \sup_{K,m,m'} \frac{\frac{m+m'}{md}}{\max\left\{\frac{1}{(d-m')^+}, \frac{1}{Km}\right\}}$$
$$\in [d/4, d/4+1]. \tag{34}$$

To see (33) note that it is trivial that $\eta_K \leq K$, whereas with $d = Km + m'$ and $m = 1, m' \to \infty$, we have $\eta_K \geq \lim_{m'\to\infty} K(1+m')/(K+m') = K$. For (34), setting $m = 1, m' = \lfloor d/2 \rfloor$ and $K > \lceil d/2 \rceil$, we have

$\eta_d \geq (1+\lfloor d/2 \rfloor)(d-\lfloor d/2 \rfloor)/d \geq d/4$, whereas we also have $\eta_d \leq (1+m')(1-m'/d) \leq (d+1)^2/(4d) \leq d/4+1$. The strong gains are indicative of the crucial role of interference alignment in the capacity of linear computation networks, especially when side-information is abundant.

4) In all cases where the question of *existence* of generic capacity is settled, the answer is in the affirmative. However, it remains unknown whether this is always true, e.g., for all p, d, K, m, m', must we have $\Delta_u^* = \Delta_l^*$? We conjecture that this is indeed the case.
5) In all cases where the generic capacity of the LCBC is known, it does not depend on the characteristic, p, i.e., for a fixed K, the generic optimal broadcast cost can be expressed as $\Delta_g(d, m, m')$. The capacity of the *general* LCBC should depend on the characteristic, because there exist examples of network coding problems where such dependence has been demonstrated, and there exists an equivalence between network coding and index coding, which in turn is a special case of the LCBC. However, it remains unknown whether the *generic* capacity of LCBC could depend on the characteristic p.
6) The functional form of $\Delta_g(d, m, m')$ is plotted in Figure 2 for $K = 2$, $K = 3$ and for large K. While $\Delta_g(d, m, m')$ characterizations are only defined for non-negative integer values of d, m, m', the functional form is shown as a continuous plot for simplicity. There exist three slightly different forms of the plot for $K = 3$, depending on the relationship between m and m'. The $K = 3$ plot shown in Figure 2 assumes $m < m'$. While the lengths of the steps for $K = 3$ are determined by the relative sizes of m, m', d, the plot always takes the shape of a staircase function with alternating horizontal (slope = 0) and slanted (slope = 1) edges. The slope of the outer envelope is $m/(m'+m)$.
7) A remarkable *scale-invariance* property is evident in $\Delta_g(d, m, m')$, in the sense that scaling d, m, m' by the same constant results in a scaling of $\Delta_g(d, m, m')$ by the same constant as well. Specifically,

$$\Delta_g(\lambda d, \lambda m, \lambda m') = \lambda \Delta_g(d, m, m'). \tag{35}$$

This is reminiscent of scale-invariance noted in DoF studies of wireless networks [56].
8) The initial (where $d \leq m+m'$) and final stages ($d \geq K(m+m')$) represent somewhat trivial regimes that are the same for all K. In the remaining non-trivial regime, while Δ_g for $K = 2$ and $K = 3$ takes the shape of a slanted staircase function, for large number of users we obtain a smooth ramp function instead. A comparison of $K = 2$ with $K = 3$ suggests that the number of steps in the staircase increases with K, bringing the staircase closer to its upper linear envelope ($md/(m+m')$), until K exceeds a threshold, beyond which the stairs disappear and Δ_g is equal to that linear envelope.
9) In the non-trivial regime $1 < d/(m+m') < K$ for large K (e.g., $K \geq d$) it is remarkable that Δ_g does not depend on K. In other words, once the number of users exceeds a threshold (e.g., $K \geq d$), additional users do not add to the generic broadcast cost of the LCBC. The achievable scheme in this parameter regime relies on linear asymptotic interference alignment (IA) [45] over a sub-field of $\mathbb{F}_q$, and while Δ_g remains unaffected by additional users, the cost of additional users may be reflected in the need for larger n values to approach the same broadcast cost, as the number of users increases. As usual with asymptotic IA schemes, the achievable scheme is far from practical, and serves primarily to establish the fundamental limit of an asymptotic metric, in this case Δ_g. What is possible with practical schemes, e.g., with limited n and other coding-theoretic complexity constraints, remains an important open problem.
10) The generic capacity explored in this work is for LCBC instances over $\mathbb{F}_{p^n}$ where we allow large n but p is arbitrary. This formulation is appealing because the large n limit allows $\mathbb{F}_{p^n}$ to be interpreted as high dimensional vector subspaces over subfields of $\mathbb{F}_{p^n}$, e.g., $\mathbb{F}_p$. This facilitates linear vector coding schemes, allows dimensional analysis from vector space perspectives, and leads to new insights from linear interference alignment schemes, that may be broadly applicable. The alternative, where p is allowed to be large but n is arbitrary (especially $n = 1$) remains unexplored. By analogy with wireless DoF studies, the latter is somewhat reminiscent of algebraic interference alignment schemes based on rational dimensions [46], i.e., non-linear IA schemes.
11) Linear asymptotic IA has been used previously for network coding problems, e.g., distributed storage exact repair [57], and K user multiple unicast [58], under the assumption of large 'q'. Note that since $q = p^n$, a large-q assumption is more general than a large-n assumption, e.g., large-q also allows $n = 1$ with large p. So at first sight it may seem that our IA schemes that require large-n are weaker than conventional asymptotic IA schemes that only require large-q. This interpretation however misses a crucial aspect of our construction, which is somewhat subtle but technically quite significant. Conventional (large-q) constructions of asymptotic IA schemes rely on a diagonal structure of underlying linear transformations (matrices), based on symbol extensions (batch processing), and most importantly require these diagonal matrices to have sufficient diversity, which is possible with *time-varying* coefficients [45]. In fact, such constructions are also possible for LCBC if we allow time-varying demands and side-information, e.g., new coefficient matrices are drawn i.i.d. uniform for each $\ell \in [L]$. However, for the LCBC with fixed demands and side-information, i.e., fixed coefficient matrices $\mathbf{v}_k, \mathbf{v}'_k$, symbol extensions only give rise to diagonal matrices that are scaled versions of the identity matrix (consider large p and $n = 1$), i.e., they lack the diversity that is needed for linear asymptotic IA schemes. Our construction works with fixed coefficient matrices, consistent with the original LCBC definition. In this regard, a key technical contribution of this work is to show that the large-n assumption allows sufficient

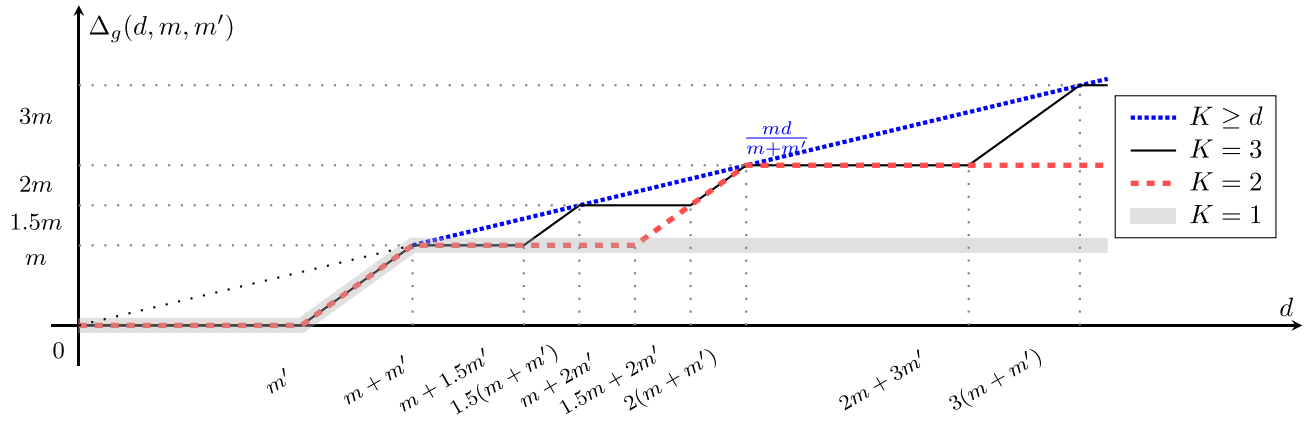

Fig. 2. Functional form of Δ_g. The large K setting listed as $K \geq d$ for brevity, also allows more general K as in (22).

diversity for linear asymptotic IA. For this we modify the conventional asymptotic IA construction to include an additional overhead (see Remark 2 in Section V-A), and then show that while this overhead has a negligible impact on Δ_g, it gives us sufficient diversity a.a.s.

V. Examples

In this section let us present two examples to convey the main ideas of our asymptotic IA constructions, with somewhat simplified notation. The complete achievability proof for Theorem 2 appears later, in Appendix I. The first example that is presented in Section V-A is perhaps the smallest example where asymptotic alignment is needed. However, the proof in this limited case hides too many of the details that are needed in the general case, so we provide a larger example in the following subsection which may be more useful in understanding the general proof.

A. Example 1: $(p, K, d = 4, m = 1, m' = 1)$

Let $L = 1$. For $q = p^n$, we will interpret $\mathbb{F}_q$ as an n-dimensional vector space over $\mathbb{F}_p$, and design a linear scheme over $\mathbb{F}_p$. Accordingly, let us clarify the notation as follows.

1) The elements of the data and coefficient matrices are chosen from $\mathbb{F}_q = \mathbb{F}_{p^n}$.
2) The data $\mathbf{x}^T = [x_1, x_2, x_3, x_4] \in \mathbb{F}_q^{1\times 4}$, is equivalently represented over $\mathbb{F}_p$ as $\mathbf{X}^T = [X_1^T, X_2^T, X_3^T, X_4^T] \in \mathbb{F}_p^{1\times 4n}$, where $X_i \in \mathbb{F}_p^{n\times 1}$ is the $n \times 1$ vector representation of x_i over $\mathbb{F}_p$.
3) User k has side information $\mathbf{x}^T\mathbf{v}'_k \in \mathbb{F}_q$ and wishes to compute $\mathbf{x}^T\mathbf{v}_k \in \mathbb{F}_q$, where the elements of $(\mathbf{v}'_k)^T = [v'_{k1}, v'_{k2}, v'_{k3}, v'_{k4}]$, $\mathbf{v}_k^T = [v_{k1}, v_{k2}, v_{k3}, v_{k4}]$, are drawn i.i.d. uniform in $\mathbb{F}_q$. Equivalently, over $\mathbb{F}_p$, User k has side information $\mathbf{X}^T\mathbf{V}'_k \in \mathbb{F}_p^{1\times n}$ and wishes to compute $\mathbf{X}^T\mathbf{V}_k \in \mathbb{F}_p^{1\times n}$, where $(\mathbf{V}'_k)^T = \left[(V'_{k1})^T, (V'_{k2})^T, (V'_{k3})^T, (V'_{k4})^T\right] \in \mathbb{F}_p^{n\times 4n}$, $(\mathbf{V}_k)^T = \left[(V_{k1})^T, (V_{k2})^T, (V_{k3})^T, (V_{k4})^T\right] \in \mathbb{F}_p^{n\times 4n}$ and $\mathbf{V}'_{ki}, \mathbf{V}_{ki}$ are the $n \times n$ matrix representations in $\mathbb{F}_p$ of v'_{ki} and v_{ki}, respectively.
4) Let r be uniformly randomly chosen in $\mathbb{F}_q$, and denote by $R \in \mathbb{F}_p^{n\times n}$ the matrix representation of r in $\mathbb{F}_p$.
5) Define the set of variables,

$$\mathcal{V} \triangleq \left\{v_{ki} : k \in [K], i \in [4]\right\} \cup \left\{v'_{ki} : k \in [K], i \in [4]\right\} \cup \left\{r\right\}, \tag{36}$$

and note that $|\mathcal{V}| = 8K + 1$.

Our goal is to show that $\Delta_u^* \leq dm/(m + m') = 2$. For all $k \in [K]$ and for all $i \in [4]$, let us define $t_{ki} \in \mathbb{F}_q$ as,

$$t_{ki} \triangleq v'_{ki} - v_{ki}r, \tag{37}$$

so that we have

$$\begin{bmatrix} v'_{k1} \\ v'_{k2} \\ v'_{k3} \\ v'_{k4} \end{bmatrix} = \begin{bmatrix} v_{k1} \\ v_{k2} \\ v_{k3} \\ v_{k4} \end{bmatrix} r + \begin{bmatrix} t_{k1} \\ t_{k2} \\ t_{k3} \\ t_{k4} \end{bmatrix}. \tag{38}$$

Let $T_{ki} \in \mathbb{F}_p^{n\times n}$ denote the $n \times n$ matrix representation of t_{ki} in $\mathbb{F}_p$, so that we have in $\mathbb{F}_p$,

$$\underbrace{\begin{bmatrix} V'_{k1} \\ V'_{k2} \\ V'_{k3} \\ V'_{k4} \end{bmatrix}}_{\mathbf{V}'_k \in \mathbb{F}_p^{4n\times n}} = \underbrace{\begin{bmatrix} V_{k1} \\ V_{k2} \\ V_{k3} \\ V_{k4} \end{bmatrix}}_{\mathbf{V}_k \in \mathbb{F}_p^{4n\times n}} R + \underbrace{\begin{bmatrix} T_{k1} \\ T_{k2} \\ T_{k3} \\ T_{k4} \end{bmatrix}}_{\mathbf{T}_k \in \mathbb{F}_p^{4n\times n}}, \tag{39}$$

and $\mathbf{T}_k$ is defined as in (39).

Next let us construct a matrix, $\mathbf{H} \in \mathbb{F}_p^{n\times\eta}$, whose column-span over $\mathbb{F}_p$ is almost invariant under linear transformations $\mathbf{V}_{ki}$ and $\mathbf{T}_{ki}$ for all $k \in [K], i \in [4]$, i.e., $\langle V_{ki}\mathbf{H}\rangle_p \approx \langle\mathbf{H}\rangle_p$ and $\langle\mathbf{T}_{ki}\mathbf{H}\rangle_p \approx \langle\mathbf{H}\rangle_p$. In addition, we want $\eta/n \approx 1/2$, so that the columns of $\mathbf{H}$ span approximately half of the n-dimensional vector space. For this, we invoke the asymptotic IA scheme of [45].

For a natural number N whose value (as a function of n) will be specified later, let us start first by constructing the vector $\mathbf{h} \in \mathbb{F}_q^{1\times\eta}$ as follows,

$$\mathbf{h} = \left[\prod_{k=1}^{K}\prod_{i=1}^{4} v_{ki}^{\alpha_{ki}} t_{ki}^{\beta_{ki}},\ \text{s.t. } 0 \leq \alpha_{ki}, \beta_{ki} \leq N-1\right] \tag{40}$$

$$\triangleq (h_1, h_2, \ldots, h_\eta), \tag{41}$$

and similarly define $\overline{\mathbf{h}} \in \mathbb{F}_q^{1\times\overline{\eta}}$ as follows,

$$\overline{\mathbf{h}} = \left[\prod_{k=1}^{K}\prod_{i=1}^{4} v_{ki}^{\alpha_{ki}} t_{ki}^{\beta_{ki}},\ \text{s.t. } 0 \le \alpha_{ki}, \beta_{ki} \le N\right] \tag{42}$$

$$\triangleq (\overline{h}_1, \overline{h}_2, \ldots, \overline{h}_{\overline{\eta}}). \tag{43}$$

Note that we have,

$$\eta = N^{8K}, \quad \overline{\eta} = (N+1)^{8K}. \tag{44}$$

This construction ensures that the elements of $v_{ki}\mathbf{h}$ and $t_{ki}\mathbf{h}$ are contained among the elements of $\overline{\mathbf{h}}$ for all $k \in [K], i \in [4]$. Now let $H_1, H_2, \ldots, H_\eta \in \mathbb{F}_p^{n\times n}$ be the matrix representations in $\mathbb{F}_p$ of $h_1, h_2, \ldots, h_\eta \in \mathbb{F}_q$, and $\overline{H}_1, \overline{H}_2, \ldots, \overline{H}_\eta \in \mathbb{F}_p^{n\times n}$ be the matrix representations in $\mathbb{F}_p$ of $\overline{h}_1, \overline{h}_2, \ldots, \overline{h}_{\overline{\eta}} \in \mathbb{F}_q$. Define,

$$\mathbf{H} = \left[H_1\mathbf{1}, H_2\mathbf{1}, \ldots, H_\eta\mathbf{1}\right] \quad \in \mathbb{F}_p^{n\times\eta}, \tag{45}$$

and

$$\overline{\mathbf{H}} = \left[\overline{H}_1\mathbf{1}, \overline{H}_2\mathbf{1}, \ldots, \overline{H}_{\overline{\eta}}\mathbf{1}\right] \quad \in \mathbb{F}_p^{n\times\overline{\eta}}, \tag{46}$$

where $\mathbf{1}$ denotes the $n \times 1$ vector of 1's. By construction, the columns of $V_{ki}\mathbf{H}$ and $T_{ki}\mathbf{H}$ are subsets of the columns of $\overline{\mathbf{H}}$, which implies that $\forall k \in [K],\ i \in [4]$,

$$\langle V_{ki}\mathbf{H}\rangle_p \subset \langle\overline{\mathbf{H}}\rangle_p, \quad \langle T_{ki}\mathbf{H}\rangle_p \subset \langle\overline{\mathbf{H}}\rangle_p. \tag{47}$$

Consider the matrix $[\mathbf{H}, R\mathbf{H}] \in \mathbb{F}_p^{n\times 2\eta}$, and define the event E_n as,

$$E_n \triangleq \Big(\text{rk}([\mathbf{H}, R\mathbf{H}]) = 2\eta\Big). \tag{48}$$

The next steps, (49)-(64) show that E_n holds a.a.s., which will subsequently be essential to guarantee successful decoding by each user.

$[\mathbf{H}, R\mathbf{H}] \in \mathbb{F}_p^{n\times 2\eta}$ has full column rank if and only if for all $\mathbf{c} = [c_1, \ldots, c_\eta]^T, \mathbf{c}' = [c'_1, \ldots, c'_\eta]^T \in \mathbb{F}_p^{\eta\times 1}$ such that $\left[\mathbf{c}^T, \mathbf{c}'^T\right] \neq \mathbf{0}^{1\times 2\eta}$,

$$\mathbf{0}^{n\times 1}$$

$$\neq [\mathbf{H}, R\mathbf{H}]\begin{bmatrix}\mathbf{c}\\ \mathbf{c}'\end{bmatrix} \tag{49}$$

$$= \left[H_1\mathbf{1}, H_2\mathbf{1}, \ldots, H_\eta\mathbf{1}, RH_1\mathbf{1}, RH_2\mathbf{1}, \ldots, RH_\eta\mathbf{1}\right]\begin{bmatrix}\mathbf{c}\\ \mathbf{c}'\end{bmatrix} \tag{50}$$

$$= \left(c_1H_1\mathbf{1} + c_2H_2\mathbf{1} + \cdots + c_\eta H_\eta\mathbf{1}\right) + \left(c'_1RH_1\mathbf{1} + c'_2RH_2\mathbf{1} + \ldots + c'_\eta RH_\eta\mathbf{1}\right) \tag{51}$$

$$= \big(c_1H_1 + c_2H_2 + \ldots + c_\eta H_\eta + c'_1RH_1 + c'_2RH_2 + \ldots + c'_\eta RH_\eta\big)\mathbf{1} \tag{52}$$

$$\triangleq F_{\mathbf{c},\mathbf{c}'}\mathbf{1} \tag{53}$$

where $F_{\mathbf{c},\mathbf{c}'}$ is an $n \times n$ matrix in $\mathbb{F}_p$, which has a scalar representation in $\mathbb{F}_q$ as,

$$f_{\mathbf{c},\mathbf{c}'} = \underbrace{c_1h_1 + c_2h_2 + \ldots + c_\eta h_\eta}_{\eta} + \underbrace{c'_1rh_1 + c'_2rh_2 + \ldots + c'_\eta rh_\eta}_{\eta} \ \in \mathbb{F}_q. \tag{54}$$

Note that since $\mathbb{F}_p$ is a sub-field of $\mathbb{F}_q$, the scalars c_i, c'_i in $\mathbb{F}_p$, are also scalars c_i, c'_i in $\mathbb{F}_q$. Thus, $F_{\mathbf{c},\mathbf{c}'}\mathbf{1} \in \mathbb{F}_p^{n\times 1}$ can be equivalently represented in $\mathbb{F}_q$ as the product of $f_{\mathbf{c},\mathbf{c}'}$ with the scalar representation in $\mathbb{F}_q$, of $\mathbf{1}$ (the all 1 vector in $\mathbb{F}_p$). Since the $\mathbb{F}_q$ representation of $\mathbf{1}$ is not 0, we obtain that

$$F_{\mathbf{c},\mathbf{c}'}\mathbf{1} \neq \mathbf{0}^{n\times 1} \iff f_{\mathbf{c},\mathbf{c}'} \neq 0. \tag{55}$$

Therefore, $[\mathbf{H}, R\mathbf{H}]$ has full column rank if and only if,

$$P \triangleq \prod_{[\mathbf{c}^T,\mathbf{c}'^T]\in\mathbb{F}_p^{1\times 2\eta}\setminus\{\mathbf{0}\}} f_{\mathbf{c},\mathbf{c}'} \neq 0. \tag{56}$$

To distinguish polynomials from polynomial functions, let us indicate polynomials with square parentheses around them. For example, $[f_{\mathbf{c},\mathbf{c}'}] \in \mathbb{F}_p[\mathcal{V}]$ is a polynomial in the indeterminate variables $\mathcal{V}$, with coefficients in $\mathbb{F}_p$, and $f_{\mathbf{c},\mathbf{c}'}(\mathcal{V}) : \mathbb{F}_q^{|\mathcal{V}|} \to \mathbb{F}_q$ is a function that maps the variables $\mathcal{V}$, which take values in $\mathbb{F}_q$, to a scalar value in $\mathbb{F}_q$. Similarly, $[P] \in \mathbb{F}_p[\mathcal{V}]$ is a polynomial, whereas $P(\mathcal{V}) : \mathbb{F}_q^{|\mathcal{V}|} \to \mathbb{F}_q$ is a function. The condition (56), which is equivalent to the event E_n, says that a uniformly random evaluation of the function $P(\mathcal{V})$ produces a non-zero value. We will show that this is true a.a.s. in n.

First let us show that $[f_{\mathbf{c},\mathbf{c}'}] \in \mathbb{F}_p[\mathcal{V}]$ is a non-zero polynomial for all $\left[\mathbf{c}^T, \mathbf{c}'^T\right] \in \mathbb{F}_p^{1\times 2\eta} \setminus \mathbf{0}$. We consider two cases.

1) Case I: At least one of $c_1, c_2, \ldots, c_\eta$ is not zero. Let us set $r = 0$, which implies $t_{ki} = v'_{ki}$ by (38). Meanwhile, $h_1, h_2, \ldots, h_\eta$ are different monomials in the elements of v'_{ki} and v_{ki} due to (40). Since different monomials are linearly independent, we have that $[f_{\mathbf{c},\mathbf{c}'}] = c_1h_1 + c_2h_2 + \ldots + c_\eta h_\eta$ is a non-zero polynomial.
2) Case II: $c_1 = c_2 = \ldots = c_\eta = 0$ and thus at least one of $c'_1, c'_2, \ldots, c'_\eta \neq 0$. For this case, we have $[f_{\mathbf{c},\mathbf{c}'}] = r(c'_1h_1 + c'_2h_2 + \ldots + c'_\eta h_\eta)$, which is also a non-zero polynomial since it is a product of r with a non-zero polynomial.

Thus, $[f_{\mathbf{c},\mathbf{c}'}] \in \mathbb{F}_p[\mathcal{V}]$ is a non-zero polynomial. It has degree not more than $12K(N-1)+1$. Therefore, $[P] \in \mathbb{F}_p[\mathcal{V}]$ is a non-zero polynomial with degree not more than $(p^{2\eta}-1)[12K(N-1)+1]$. By Schwartz-Zippel Lemma, when all the variables $\mathcal{V}$ are assigned i.i.d. uniformly chosen values in $\mathbb{F}_q$,

$$\Pr\Big(P(\mathcal{V}) \neq 0\Big) \ge 1 - \frac{(p^{2\eta}-1)[12K(N-1)+1]}{q} \tag{57}$$

$$= 1 - \frac{(p^{2\eta}-1)[12K(N-1)+1]}{p^n} \tag{58}$$

$$\ge 1 - 12K\frac{N}{p^{n-2\eta}} \tag{59}$$

$$\to 1 \tag{60}$$

as $n \to \infty$ if $\lim_{n\to\infty} \frac{N}{p^{(n-2\eta)}} = 0$.

Now let us specify the value of N as follows,

$$N = \left\lfloor \left(\frac{n-\sqrt{n}}{2}\right)^{1/(8K)} \right\rfloor, \tag{61}$$

from which it follows that,

$$N \le \left(\frac{n-\sqrt{n}}{2}\right)^{1/(8K)} \tag{62}$$

and

$$n - 2\eta = n - 2N^{8K} \geq \sqrt{n}. \tag{63}$$

Therefore,

$$\lim_{n\to\infty} \frac{N}{p^{n-2\eta}} \leq \lim_{n\to\infty} \frac{\left(\frac{n-\sqrt{n}}{2}\right)^{1/(8K)}}{p^{\sqrt{n}}} = 0 \tag{64}$$

and since $N \geq 0$, we have $\lim_{n\to\infty} \frac{N}{p^{n-2\eta}} = 0$. Thus, we have shown that E_n holds a.a.s., i.e., $[\mathbf{H}, R\mathbf{H}] \in \mathbb{F}_p^{n\times 2\eta}$ has full column rank 2η, a.a.s.

Now let $\mathbf{Z} = (\mathbf{I}^{n\times n} | [\mathbf{H}, R\mathbf{H}]) \in \mathbb{F}_p^{n\times(n-2\eta)}$, so that $[\mathbf{H}, R\mathbf{H}, \mathbf{Z}] \in \mathbb{F}_p^{n\times n}$ has full rank n. Let the server broadcast $\mathbf{S} = (\mathbf{S}_0, \mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_K) \in \mathbb{F}_p^{1\times(4\overline{\eta}+K(n-2\eta))}$, such that,

$$\mathbf{S}_0 = \mathbf{X}^T \begin{bmatrix} \overline{\mathbf{H}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}} \end{bmatrix} \quad \in \mathbb{F}_p^{1\times 4\overline{\eta}} \tag{65}$$

and for all $k \in [K]$,

$$\mathbf{S}_k = \mathbf{X}^T \mathbf{V}_k \mathbf{Z} \quad \in \mathbb{F}_p^{1\times(n-2\eta)}. \tag{66}$$

Remark 2: From (63) we note that $n \geq 2\eta + \sqrt{n}$. The $\sqrt{n}$ term represents an overhead that is not present in conventional asymptotic IA constructions. The overhead is evident in the separate transmissions, of the projections of the desired information along the columns of $\mathbf{Z}$, for each of the K users, as in $\mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_K$. Digging deeper, this overhead is essential for our scheme to ensure that E_n holds a.a.s. Note that it is because of this $\sqrt{n}$ overhead that we have $\lim_{n\to\infty} \frac{N}{p^{(n-2\eta)}} = 0$ in (60),(64), because in the fraction $\frac{N}{p^{n-2\eta}}$, the numerator is sub-linear in n (roughy $n^{1/8K}$), while the denominator is super-polynomial in n, roughly $(p^{\sqrt{n}})$. Fortunately, the extra broadcast cost of $K\sqrt{n}$ due to this overhead, is negligible compared to n for large n, so it does not affect the asymptotic achievability.

The decoding process works as follows. User k is able to compute $\mathbf{X}^T\mathbf{V}'_k\mathbf{H}$ directly from its side information $\mathbf{X}^T\mathbf{V}'_k$. The user is able to compute $\mathbf{X}^T\mathbf{V}_k\mathbf{H}$ and $\mathbf{X}^T\mathbf{T}_k\mathbf{H}$ from $\mathbf{S}_0$, since,

$$\langle \mathbf{V}_k\mathbf{H} \rangle_p = \left\langle \begin{bmatrix} V_{k1}\mathbf{H} \\ V_{k2}\mathbf{H} \\ V_{k3}\mathbf{H} \\ V_{k4}\mathbf{H} \end{bmatrix} \right\rangle_p \subset \left\langle \begin{bmatrix} \overline{\mathbf{H}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}} \end{bmatrix} \right\rangle_p \tag{67}$$

and

$$\langle \mathbf{T}_k\mathbf{H} \rangle_p = \left\langle \begin{bmatrix} T_{k1}\mathbf{H} \\ T_{k2}\mathbf{H} \\ T_{k3}\mathbf{H} \\ T_{k4}\mathbf{H} \end{bmatrix} \right\rangle_p \subset \left\langle \begin{bmatrix} \overline{\mathbf{H}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}} \end{bmatrix} \right\rangle_p \tag{68}$$

due to (47). Thus, User k is able to compute

$$\mathbf{X}^T\mathbf{V}_k R\mathbf{H} = \mathbf{X}^T\mathbf{V}'_k\mathbf{H} - \mathbf{X}^T\mathbf{T}_k\mathbf{H} \tag{69}$$

according to (39). Together with $\mathbf{S}_k$, User k thus obtains,

$$[\mathbf{X}^T\mathbf{V}_k\mathbf{H},\ \mathbf{X}^T\mathbf{V}_k R\mathbf{H},\ \mathbf{S}_k] = \mathbf{X}^T\mathbf{V}_k[\mathbf{H}, R\mathbf{H}, \mathbf{Z}] \tag{70}$$

and since $[\mathbf{H}, R\mathbf{H}, \mathbf{Z}] \in \mathbb{F}_p^{n\times n}$ is invertible (has full rank) a.a.s., User k is able to retrieve its desired computation, $\mathbf{X}^T\mathbf{V}_k \in \mathbb{F}_p^{1\times n}$ a.a.s.

For $q = p^n$, the cost of broadcasting each p-ary symbol is $1/n$ in q-ary units. Thus, the broadcast cost of this scheme is,

$$\Delta_n = \frac{4\overline{\eta} + K(n-2\eta)}{n}. \tag{71}$$

The next few steps (72)-(77) show that $\lim_{n\to\infty} \Delta_n = 2$.

By (61), we have that,

$$\eta = N^{8K} \leq \frac{n-\sqrt{n}}{2} \leq (N+1)^{8K} = \overline{\eta} \tag{72}$$

which implies that

$$\lim_{n\to\infty} \frac{\eta}{n} = \lim_{n\to\infty} \frac{N^{8K}}{n} \leq \lim_{n\to\infty} \frac{n-\sqrt{n}}{2n} = \frac{1}{2}. \tag{73}$$

On the other hand,

$$\begin{aligned} \lim_{n\to\infty} \frac{\eta}{n} &= \lim_{n\to\infty} \frac{(N+1)^{8K}/((1+1/N)^{8K})}{n} \\ &\geq \lim_{N\to\infty} \frac{1}{(1+1/N)^{8K}} \lim_{n\to\infty} \frac{n-\sqrt{n}}{2n} \\ &= 1 \times \frac{1}{2} = \frac{1}{2}. \end{aligned} \tag{74}$$

Thus, we have that

$$\lim_{n\to\infty} \frac{\eta}{n} = \frac{1}{2}, \tag{75}$$

which also implies that

$$\lim_{n\to\infty} \frac{\overline{\eta}}{n} = \lim_{n\to\infty} \frac{\eta}{n} \times \lim_{N\to\infty} (1+1/N)^{8K} = \frac{1}{2} \times 1 = \frac{1}{2}. \tag{76}$$

Combining (71) with (75) and (76) we have

$$\lim_{n\to\infty} \Delta_n = 4 \times \frac{1}{2} + 0 = 2 \tag{77}$$

since K is independent of n. Thus, for any $\varepsilon > 0$, $\exists n_0 > 0$ such that $\Delta_n \leq 2+\varepsilon$ for all $n \geq n_0$. Recall that the broadcast cost Δ_n is achievable if E_n holds, i.e., $\Delta^*(\Lambda_n) \leq \Delta_n \leq 2+\epsilon$ if $n \geq n_0$ and E_n holds. Now let us show that $2+\epsilon$ is achievable a.a.s., by evaluating the limit in (14) as follows,

$$\begin{aligned} &\lim_{n\to\infty} \mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq 2+\epsilon\Big) \\ &\geq \lim_{n\to\infty} \mathsf{Pr}\Big(\Big(\Delta^*(\Lambda_n) \leq 2+\epsilon\Big) \wedge E_n\Big) \qquad (78) \\ &= \lim_{n\to\infty} \mathsf{Pr}(E_n)\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq 2+\epsilon \;\Big|\; E_n\Big) \qquad (79) \\ &= 1 \qquad (80) \end{aligned}$$

which implies that $\lim_{n\to\infty} \mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq 2+\epsilon\Big) = 1$. Since this is true for all $\varepsilon > 0$, according to (15) we have $\Delta_u^* \leq \inf\{2+\epsilon \mid \epsilon > 0\} = 2$. □

B. Example 2: $(p, K, d = 4, m = 2, m' = 1)$

Let $L = 1$. For $q = p^n$, we will interpret $\mathbb{F}_q$ as an n-dimensional vector space over $\mathbb{F}_p$, and design a linear scheme over $\mathbb{F}_p$. Accordingly, let us clarify the notation as follows.

1) The elements of the data and coefficient matrices are chosen from $\mathbb{F}_q = \mathbb{F}_{p^n}$.
2) The data $\mathbf{x}^T = [x_1, x_2, x_3, x_4] \in \mathbb{F}_q^{1\times 4}$, is equivalently represented over $\mathbb{F}_p$ as $\mathbf{X}^T = [X_1^T, X_2^T, X_3^T, X_4^T] \in \mathbb{F}_p^{1\times 4n}$, where $X_i \in \mathbb{F}_p^{n\times 1}$ is the $n \times 1$ vector representation of x_i over $\mathbb{F}_p$.
3) User k has side information $\mathbf{x}^T\mathbf{v}'_k \in \mathbb{F}_q$ and wishes to compute $\mathbf{x}^T\mathbf{v}_k = \mathbf{x}^T[\mathbf{v}_k^1, \mathbf{v}_k^2] \in \mathbb{F}_q^{1\times 2}$, where the elements of $(\mathbf{v}'_k)^T = [v'_{k1}, v'_{k2}, v'_{k3}, v'_{k4}]$, $(\mathbf{v}_k^\mu)^T = [v_{k1}^\mu, v_{k2}^\mu, v_{k3}^\mu, v_{k4}^\mu], \mu \in [2]$ are drawn i.i.d. uniform in $\mathbb{F}_q$. Equivalently, over $\mathbb{F}_p$, User k has side information $\mathbf{X}^T\mathbf{V}'_k$ and wishes to compute $\mathbf{X}^T\mathbf{V}_k$, where $(\mathbf{V}'_k)^T = [(V'_{k1})^T, (V'_{k2})^T, (V'_{k3})^T, (V'_{k4})^T] \in \mathbb{F}_p^{n\times 4n}$, $\mathbf{V}_k = [\mathbf{V}_k^1, \mathbf{V}_k^2]$ and $(\mathbf{V}_k^\mu)^T = [(V_{k1}^\mu)^T, (V_{k2}^\mu)^T, (V_{k3}^\mu)^T, (V_{k4}^\mu)^T] \in \mathbb{F}_p^{n\times 4n}$. $V'_{ki}, V_{ki}^\mu, \mu \in [2]$ are the $n \times n$ matrix representations in $\mathbb{F}_p$ of v'_{ki} and v_{ki}^μ, respectively.
4) Let r, θ_1, θ_2 be uniformly randomly chosen in $\mathbb{F}_q$. Denote by R the matrix representations of r, θ_1, θ_2 in $\mathbb{F}_p$, respectively.
5) Define the set of variables,

$$\mathcal{V} \triangleq \left\{v_{ki}^j : k \in [K], i \in [4], j \in [2]\right\} \cup \left\{v'_{ki} : k \in [K], i \in [4]\right\} \cup \left\{r, \theta_1, \theta_2\right\}, \quad (81)$$

and note that $|\mathcal{V}| = 12K + 3$.

Our goal is to show that $\Delta_u^* \le dm/(m + m') = \frac{8}{3}$. For all $k \in [K], i \in [4], \mu \in [2]$, let us define t_{ki}^μ such that

$$\begin{bmatrix} v'_{k1} \\ v'_{k2} \\ v'_{k3} \\ v'_{k4} \end{bmatrix} = \begin{bmatrix} v_{k1}^\mu \\ v_{k2}^\mu \\ v_{k3}^\mu \\ v_{k4}^\mu \end{bmatrix} r + \begin{bmatrix} t_{k1}^\mu \\ t_{k2}^\mu \\ t_{k3}^\mu \\ t_{k4}^\mu \end{bmatrix}. \quad (82)$$

Let $T_{ki}^\mu \in \mathbb{F}_p^{n\times n}$ denote the $n \times n$ matrix representations of t_{ki}^μ in $\mathbb{F}_p$, so that we have in $\mathbb{F}_p$,

$$\underbrace{\begin{bmatrix} V'_{k1} \\ V'_{k2} \\ V'_{k3} \\ V'_{k4} \end{bmatrix}}_{\mathbf{V}'_k \in \mathbb{F}_p^{4n\times n}} = \underbrace{\begin{bmatrix} V_{k1}^\mu \\ V_{k2}^\mu \\ V_{k3}^\mu \\ V_{k4}^\mu \end{bmatrix}}_{\mathbf{V}_k^\mu \in \mathbb{F}_p^{4n\times n}} R + \underbrace{\begin{bmatrix} T_{k1}^\mu \\ T_{k2}^\mu \\ T_{k3}^\mu \\ T_{k4}^\mu \end{bmatrix}}_{\mathbf{T}_k^\mu \in \mathbb{F}_p^{4n\times n}} \quad (83)$$

for all $k \in [K], \mu \in [2]$, and $\mathbf{T}_k^\mu, \mu \in [2]$ are defined as in (83).

Since $m = 2 > 1$ in this example, unlike what we did in the previous $m = 1$ example, this time we will need to create two $\mathbf{H}$ matrices, namely, $\mathbf{H}_1$ and $\mathbf{H}_2$, such that $\mathbf{H}_1$ is almost invariant under linear transformations V_{ki}^j and $T_{ki}^1, \forall k \in [K], i \in [4], j \in [2]$, i.e., $\langle V_{ki}^j \mathbf{H}_1\rangle_p \approx \langle \mathbf{H}_1\rangle_p$ and $\langle T_{ki}^1 \mathbf{H}_1\rangle_p \approx \langle \mathbf{H}_1\rangle_p$. $\mathbf{H}_2$ is almost invariant under linear transformations V_{ki}^j and $T_{ki}^2, \forall k \in [K], i \in [4], j \in [2]$, i.e., $\langle V_{ki}^j \mathbf{H}_2\rangle_p \approx \langle \mathbf{H}\rangle_p$ and $\langle T_{ki}^2 \mathbf{H}_2\rangle_p \approx \langle \mathbf{H}_2\rangle_p$. In addition, we want $\eta/n \approx 1/3$ so that the columns of $\mathbf{H}_\mu, \mu \in [2]$ span approximately one third of the n-dimensional vector space. Moreover, $\mathbf{H}_1$ and $\mathbf{H}_2$ are required to be linearly independent a.a.s. For these, we invoke the asymptotic IA scheme of [45], and design $\mathbf{h}_\mu, \overline{\mathbf{h}}_\mu, \mu \in [2]$ in the following way,

$$\mathbf{h}_\mu^{1\times\eta} = \left[\theta_\mu \prod_{k=1}^{K}\left(\left(\prod_{i=1}^{4}\prod_{j=1}^{2}(v_{ki}^j)^{\alpha_{ki}^j}\right)\left(\prod_{i=1}^{4}(t_{ki}^\mu)^{\beta_{ki}^\mu}\right)\right), \text{ s.t. } 0 \le \alpha_{ki}^j, \beta_{ki}^\mu \le N-1\right] \quad (84)$$

$$\triangleq (h_\mu^1, h_\mu^2, \ldots, h_\mu^\eta), \qquad \forall \mu \in [2], \quad (85)$$

$$\overline{\mathbf{h}}_\mu^{1\times\eta} = \left[\theta_\mu \prod_{k=1}^{K}\left(\left(\prod_{i=1}^{4}\prod_{j=1}^{2}(v_{ki}^j)^{\alpha_{ki}^j}\right)\left(\prod_{i=1}^{4}(t_{ki}^\mu)^{\beta_{ki}^\mu}\right)\right), \text{ s.t. } 0 \le \alpha_{ki}^j, \beta_{ki}^\mu \le N\right] \quad (86)$$

$$\triangleq (\overline{h}_\mu^1, \overline{h}_\mu^2, \ldots, \overline{h}_\mu^{\overline{\eta}}), \qquad \forall \mu \in [2]. \quad (87)$$

Note that we have,

$$\eta = N^{12K}, \quad \overline{\eta} = (N+1)^{12K}. \quad (88)$$

This construction ensures that for $\mu \in [2]$, the elements of $v_{ki}^j \mathbf{h}_\mu$ and $t_{ki}^\mu \mathbf{h}_\mu$ are contained among the elements of $\overline{\mathbf{h}}_\mu$ for all $i \in [4], j \in [2]$. Now let $H_1, H_2, \ldots, H_\eta \in \mathbb{F}_p^{n\times n}$ be the matrix representations in $\mathbb{F}_p$ of $h_1, h_2, \ldots, h_\eta \in \mathbb{F}_q$, and $\overline{H}_1, \overline{H}_2, \ldots, \overline{H}_{\overline{\eta}} \in \mathbb{F}_p^{n\times n}$ be the matrix representations in $\mathbb{F}_p$ of $\overline{h}_1, \overline{h}_2, \ldots, \overline{h}_{\overline{\eta}} \in \mathbb{F}_q$. Define,

$$\mathbf{H}_\mu = \left[H_\mu^1\mathbf{1}, H_\mu^2\mathbf{1}, \ldots, H_\mu^\eta\mathbf{1}\right] \in \mathbb{F}_p^{n\times\eta}, \qquad \mu \in [2] \quad (89)$$

and

$$\overline{\mathbf{H}}_\mu = \left[\overline{H}_\mu^1\mathbf{1}, \overline{H}_\mu^2\mathbf{1}, \ldots, \overline{H}_\mu^{\overline{\eta}}\mathbf{1}\right] \in \mathbb{F}_p^{n\times\overline{\eta}}, \qquad \mu \in [2], \quad (90)$$

where $\mathbf{1}$ denotes the $n \times 1$ vector of 1's. By construction, the columns of $V_{ki}^j \mathbf{H}_\mu$ and $T_{ki}^\mu \mathbf{H}_\mu$ are subsets of the columns of $\mathbf{H}_\mu$, which implies that $\forall \mu \in [2], k \in [K], i \in [4], j \in [2]$,

$$\langle V_{ki}^j \mathbf{H}_\mu\rangle_p \subset \langle \overline{\mathbf{H}}_\mu\rangle_p, \quad \langle T_{ki}^\mu \mathbf{H}_\mu\rangle_p \subset \langle \overline{\mathbf{H}}_\mu\rangle_p. \quad (91)$$

Consider the $m = 2$ matrices, $[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1] \in \mathbb{F}_p^{n\times 3\eta}$ and $[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_2] \in \mathbb{F}_p^{n\times 3\eta}$, and define the event E_n as,

$$E_n \triangleq (\text{rk}([\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1]) = 3\eta) \wedge (\text{rk}([\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_2]) = 3\eta). \quad (92)$$

The next steps (93)-(108), show that E_n holds a.a.s., which will subsequently be essential to guarantee successfully decoding by each user. In fact, due to symmetry, it suffices to prove that $\text{rk}([\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1]) \overset{\text{a.a.s.}}{=} 3\eta$.

$[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1] \in \mathbb{F}_p^{n\times 3\eta}$ has full column rank if and only if for all $\mathbf{c}_1 = [c_1^1, c_1^2, \ldots, c_1^\eta]^T, \mathbf{c}_2 = [c_2^1, c_2^2, \ldots, c_2^\eta]^T, \mathbf{c}' = [c'^1, c'^2, \ldots, c'^\eta]^T \in \mathbb{F}_p^{\eta\times 1}$ such that $\overline{\mathbf{c}}^T = [\mathbf{c}_1^T, \mathbf{c}_2^T, \mathbf{c}'^T] \neq \mathbf{0}^{1\times 3\eta}$,

$$\mathbf{0}^{n\times 1} \neq [\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1]\overline{\mathbf{c}} \quad (93)$$

$$= \mathbf{H}_1\mathbf{c}_1 + \mathbf{H}_2\mathbf{c}_2 + R\mathbf{H}_1\mathbf{c}' \quad (94)$$

$$= \sum_{j=1}^{\eta} c_1^j H_1^j\mathbf{1} + \sum_{j=1}^{\eta} c_2^j H_2^j\mathbf{1} + \sum_{j=1}^{\eta} c'^j R H_1^j\mathbf{1} \quad (95)$$

$$= \left(\sum_{j=1}^{\eta} c_1^j H_1^j + \sum_{j=1}^{\eta} c_2^j H_2^j + \sum_{j=1}^{\eta} c'^j R H_1^j\right)\mathbf{1} \quad (96)$$

$$\triangleq F_{\overline{\mathbf{c}}}\mathbf{1} \quad (97)$$

where $F_{\overline{\mathbf{c}}}$ is an $n \times n$ matrix in $\mathbb{F}_p$, which has a scalar representation in $\mathbb{F}_q$ as,

$$f_{\overline{\mathbf{c}}} = \sum_{j=1}^{\eta} c_1^j h_1^j + \sum_{j=1}^{\eta} c_2^j h_2^j + \sum_{j=1}^{\eta} c'^j r h_1^j \quad \in \mathbb{F}_q. \tag{98}$$

Note that since $\mathbb{F}_p$ is a sub-field of $\mathbb{F}_q$, the scalars c_1^j, c_2^j, c'^j in $\mathbb{F}_p$ are also scalars c_1^j, c_2^j, c'^j in $\mathbb{F}_q$.

Thus, $F_{\overline{\mathbf{c}}} \in \mathbb{F}_p^{n\times 1}$ can be equivalently represented in $\mathbb{F}_q$ as the product of $f_{\overline{\mathbf{c}}}$ with the scalar representation in $\mathbb{F}_q$, of $\mathbf{1}$ (the all 1 vector in $\mathbb{F}_p$). Since the $\mathbb{F}_q$ representation of $\mathbf{1}$ is not 0, we obtain that

$$F_{\overline{\mathbf{c}}}\mathbf{1} \neq \mathbf{0}^{n\times 1} \Longleftrightarrow f_{\overline{\mathbf{c}}} \neq 0. \tag{99}$$

Therefore, $[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1] \in \mathbb{F}_p^{n\times 3\eta}$ has full column rank if and only if,

$$P \triangleq \prod_{\overline{\mathbf{c}}\in\mathbb{F}_p^{3\eta\times 1}\setminus\{\mathbf{0}\}} f_{\overline{\mathbf{c}}} \neq 0. \tag{100}$$

The condition of (100), which is equivalent to the event E_n, says that a uniformly random evaluation of the function $P(\mathcal{V})$ produces a non-zero value. We will show that this is true a.a.s. in n.

1) Case I: $\mathbf{c}_1$ or $\mathbf{c}_2$ is not the zero vector. Let us set $r = 0$, which implies $f_{\overline{\mathbf{c}}} = \sum_{j=1}^{\eta} c_1^j h_1^j + \sum_{j=1}^{\eta} c_2^j h_2^j$, and that $t_{ki}^{\mu} = v'_{ki}, \forall \mu \in [2], i \in [4]$ by (82). Meanwhile, $h_1^1, h_1^2, \ldots, h_1^\eta$ are different monomials in the elements of v_{ki}^j, v'_{ki} and θ_1. Similarly, $h_2^1, h_2^2, \ldots, h_2^\eta$ are different monomials in the elements of v_{ki}^j, v'_{ki} and θ_2 due to (84). Moreover, since any h_1^j has the factor θ_1 but does not have the factor θ_2, and any h_2^j has the factor θ_2 but does not have the factor θ_1, it follows that $h_1^1, h_1^2, \ldots, h_1^\eta, h_2^1, h_2^2, \ldots, h_2^\eta$ are different monomials. Since different monomials are linearly independent, we have that $[f_{\overline{\mathbf{c}}}]$ is a non-zero polynomial.
2) Case II: $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{0}$ and thus $\mathbf{c}' \neq \mathbf{0}$. For this case, we have $[f_{\overline{\mathbf{c}}}] = r(c'^1 h_1^1 + c'^2 h_1^2 + \ldots + c'^\eta h_1^\eta)$, which is also a non-zero polynomial since it is a product of r with a non-zero polynomial (since $h_1^1, h_1^2, \ldots, h_1^\eta$ are linearly independent).

Thus, $[f_{\overline{\mathbf{c}}}]$ is a non-zero polynomial. Since h_i^j has degree not more than $16(N-1)K+1$, $[f_{\overline{\mathbf{c}}}]$ has degree not more than $16NK+2$. Therefore, $[P] \in \mathbb{F}_p[\mathcal{V}]$ is a non-zero polynomial with degree not more than $(p^{3\eta}-1)(16NK+2)$. By Schwartz-Zippel Lemma, when all the variables $\mathcal{V}$ are assigned i.i.d. uniformly chosen values in $\mathbb{F}_q$,

$$\begin{aligned}
\mathsf{Pr}\big(P \neq 0\big) &\geq 1 - \frac{(p^{3\eta}-1)[16(N-1)K+2]}{q} && (101)\\
&= 1 - \frac{(p^{3\eta}-1)[16(N-1)K+2]}{p^n} && (102)\\
&\geq 1 - 16K\frac{N}{p^{n-3\eta}} && (103)\\
&\to 1 && (104)
\end{aligned}$$

as $n \to \infty$ if $\lim_{n\to\infty} \frac{N}{p^{n-3\eta}} = 0$.

Now let us specify the value of N as follows,

$$N = \left\lfloor \left(\frac{n-\sqrt{n}}{3}\right)^{1/(12K)} \right\rfloor, \tag{105}$$

from which it follows that,

$$N \leq \left(\frac{n-\sqrt{n}}{3}\right)^{1/(12K)} \tag{106}$$

and

$$n - 3\eta = n - 3N^{12K} \geq \sqrt{n}. \tag{107}$$

Therefore,

$$\lim_{n\to\infty} \frac{N}{p^{n-3\eta}} \leq \lim_{n\to\infty} \frac{\left(\frac{n-\sqrt{n}}{3}\right)^{1/(12K)}}{p^{\sqrt{n}}} = 0, \tag{108}$$

and since $N \geq 0$, we have $\lim_{n\to\infty} \frac{N}{p^{n-3\eta}} = 0$. Thus, $\mathrm{rk}([\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1]) \overset{\text{a.a.s.}}{=} 3\eta$, and due to symmetry it can be proved that $\mathrm{rk}([\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_2]) \overset{\text{a.a.s.}}{=} 3\eta$. Thus, we have shown that E_n holds a.a.s. Now for $\mu \in [2]$, let $(\mathbf{Z}_\mu = \mathbf{I}^{n\times n} | [\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_\mu]) \in \mathbb{F}_p^{n\times(n-3\eta)}$, so that

$$\big[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_\mu, \mathbf{Z}_\mu\big] \tag{109}$$

has full column rank n. Let the server broadcast $\mathbf{S} = \big(\mathbf{S}_0, \mathbf{S}_{[K]}^1, \mathbf{S}_{[K]}^2\big) \in \mathbb{F}_p^{1\times(8\overline{\eta}+2K(n-3\eta))}$, where

$$\mathbf{S}_0 = \mathbf{X}^T \begin{bmatrix} \overline{\mathbf{H}}_1 & \overline{\mathbf{H}}_2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_1 & \overline{\mathbf{H}}_2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_1 & \overline{\mathbf{H}}_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_1 & \overline{\mathbf{H}}_2 \end{bmatrix} \in \mathbb{F}_p^{1\times 8\overline{\eta}} \tag{110}$$

and for $k \in [K], \mu \in [2]$,

$$\mathbf{S}_k^\mu = \mathbf{X}^T \mathbf{V}_k^\mu \mathbf{Z}_\mu. \tag{111}$$

The decoding process works as follows. User k is able to compute

$$\mathbf{X}^T \mathbf{V}'_k \mathbf{H}_\mu, \qquad \mu \in [2] \tag{112}$$

directly from its side information $\mathbf{X}^T\mathbf{V}'_k$. Meanwhile, it is able to compute

$$\mathbf{X}^T \mathbf{V}_k^j \mathbf{H}_\mu, \qquad j \in [2], \quad \mu \in [2] \tag{113}$$

and

$$\mathbf{X}^T \mathbf{T}_k^\mu \mathbf{H}_\mu, \qquad \mu \in [2] \tag{114}$$

from $\mathbf{S}_0$, since for $j \in [2], \mu \in [2]$,

$$\begin{aligned}
\left\langle \mathbf{V}_k^j \mathbf{H}_\mu \right\rangle_p &= \left\langle \begin{bmatrix} V_{k1}^j \mathbf{H}_\mu \\ V_{k2}^j \mathbf{H}_\mu \\ V_{k3}^j \mathbf{H}_\mu \\ V_{k4}^j \mathbf{H}_\mu \end{bmatrix} \right\rangle_p \\
&\subset \left\langle \begin{bmatrix} \overline{\mathbf{H}}_\mu & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}}_\mu & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_\mu & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_\mu \end{bmatrix} \right\rangle_p, && (115)
\end{aligned}$$

and for $\mu \in [2]$,

$$\left\langle \begin{bmatrix} T_{k1}^{\mu}\mathbf{H}_{\mu} \\ T_{k2}^{\mu}\mathbf{H}_{\mu} \\ T_{k3}^{\mu}\mathbf{H}_{\mu} \\ T_{k4}^{\mu}\mathbf{H}_{\mu} \end{bmatrix} \right\rangle_p \subset \left\langle \begin{bmatrix} \overline{\mathbf{H}}_{\mu} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}}_{\mu} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_{\mu} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_{\mu} \end{bmatrix} \right\rangle_p \tag{116}$$

due to (91). Thus, User k is able to compute

$$\mathbf{X}^T\mathbf{V}_k^{\mu}R\mathbf{H}_{\mu} = \mathbf{X}^T\mathbf{V}_k'\mathbf{H}_{\mu} - \mathbf{X}^T\mathbf{T}_k^{\mu}\mathbf{H}_{\mu}, \quad \mu \in [2] \tag{117}$$

according to (83). Together with $\mathbf{S}_k^{\mu}$, User k thus obtains,

$$\left[\mathbf{X}^T\mathbf{V}_k^{j}\mathbf{H}_{\mu}, \mathbf{X}^T\mathbf{V}_k^{\mu}R\mathbf{H}_{\mu}, \mathbf{S}_k^{\mu}\right], \quad j \in [2], \quad \mu \in [2] \tag{118}$$

which are

$$\mathbf{X}^T\mathbf{V}_k^1\left[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1, \mathbf{Z}_1\right], \ \mathbf{X}^T\mathbf{V}_k^2\left[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_2, \mathbf{Z}_2\right] \tag{119}$$

and since $\left[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_1, \mathbf{Z}_1\right] \in \mathbb{F}_p^{n\times n}$ and $\left[\mathbf{H}_1, \mathbf{H}_2, R\mathbf{H}_2, \mathbf{Z}_2\right] \in \mathbb{F}_p^{n\times n}$ are invertible (have full rank) a.a.s., User k is able to retrieve its desired computation, $\mathbf{X}^T\mathbf{V}_k = \left[\mathbf{X}^T\mathbf{V}_k^1, \mathbf{X}^T\mathbf{V}_k^2\right] \in \mathbb{F}_p^{1\times 2n}$ a.a.s.

For $q = p^n$, the cost of broadcasting each p-ary symbol is $1/n$ in q-ary units. Thus, the broadcast cost of this scheme is,

$$\Delta_n = \frac{8\overline{\eta} + 2K\big(n - 3\eta\big)}{n}. \tag{120}$$

The next few steps (121)-(128) show that $\lim_{n\to\infty}\Delta_n = \frac{8}{3}$.

By (105), we have that

$$\eta = N^{12K} \leq \frac{n-\sqrt{n}}{3} \leq (N+1)^{12K} = \overline{\eta} \tag{121}$$

which implies that

$$\lim_{n\to\infty}\frac{\eta}{n} = \lim_{n\to\infty}\frac{N^{12K}}{n} \leq \lim_{n\to\infty}\frac{n-\sqrt{n}}{n}\times\frac{1}{3} = \frac{1}{3}. \tag{122}$$

On the other hand,

$$\lim_{n\to\infty}\frac{\eta}{n} = \lim_{n\to\infty}\frac{(N+1)^{12K}/(1+1/N)^{12K}}{n} \tag{123}$$

$$\geq \lim_{N\to\infty}\frac{1}{(1+1/N)^{12K}}\lim_{n\to\infty}\frac{n-\sqrt{n}}{n}\times\frac{1}{3} \tag{124}$$

$$= \frac{1}{3}. \tag{125}$$

Thus, we have that

$$\lim_{n\to\infty}\frac{\eta}{n} = \frac{1}{3} \tag{126}$$

which also implies that

$$\lim_{n\to\infty}\frac{\overline{\eta}}{n} = \lim_{n\to\infty}\frac{\eta}{n}\times\lim_{N\to\infty}(1+1/N)^{12K} = \frac{1}{3}. \tag{127}$$

Combining (120) with (126) and (127) we have

$$\lim_{n\to\infty}\Delta_n = 8\times\frac{1}{3} + 0 = \frac{8}{3} \tag{128}$$

since K is independent of n. Thus, for any $\varepsilon > 0$, $\exists n_0 > 0$ such that $\Delta_n \leq \frac{8}{3} + \varepsilon$ for all $n \geq n_0$. Recall that the broadcast cost Δ_n is achievable if E_n holds, i.e., $\Delta^*(\Lambda_n) \leq \Delta_n \leq \frac{8}{3} + \epsilon$ if $n \geq n_0$ and E_n holds. Now let us show that $\frac{8}{3} + \epsilon$ is achievable a.a.s., by evaluating the limit in (14) as follows,

$$\lim_{n\to\infty}\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq \frac{8}{3} + \epsilon\Big)$$

$$\geq \lim_{n\to\infty}\mathsf{Pr}\left(\Big(\Delta^*(\Lambda_n) \leq \frac{8}{3} + \epsilon\Big) \wedge E_n\right) \tag{129}$$

$$= \lim_{n\to\infty}\mathsf{Pr}(E_n)\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq \frac{8}{3} + \epsilon \ \Big|\ E_n\Big) \tag{130}$$

$$= 1 \tag{131}$$

which implies that $\lim_{n\to\infty}\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \leq \frac{8}{3} + \epsilon\Big) = 1$. Since this is true for all $\varepsilon > 0$, according to (15) we have $\Delta_u^* \leq \inf\{\frac{8}{3} + \epsilon \mid \epsilon > 0\} = \frac{8}{3}$. □

VI. Proof of Converse: Theorem 2

Recall that $\mathbf{u}_k \triangleq [\mathbf{v}_k', \mathbf{v}_k], \forall k \in [K]$, and the data $\mathbf{x} \in \mathbb{F}_q^{d\times L}$ for a scheme with batch size equal to L. Since a scheme must work for all data realizations, it must work if $\mathbf{x}$ is uniformly distributed. The decoding constraint (8) implies

$$H(\mathbf{S}, \mathbf{x}^T\mathbf{v}_k') = H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_k), \ \forall k \in [K]. \tag{132}$$

The converse for $d \geq K(m+m')$ is obtained trivially by allowing all K users to cooperate fully, see proof of (24) in Corollary 1. The converse for $d \leq m + m'$ is obtained as

$$\Delta^*(\Lambda_n) \geq H(\mathbf{S})/L \tag{133}$$

$$\geq H(\mathbf{S} \mid \mathbf{x}^T\mathbf{v}_1')/L \tag{134}$$

$$= H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_1 \mid \mathbf{x}^T\mathbf{v}_1')/L \tag{135}$$

$$\geq H(\mathbf{x}^T\mathbf{u}_1 \mid \mathbf{x}^T\mathbf{v}_1')/L \tag{136}$$

$$\geq \big(H(\mathbf{x}^T\mathbf{u}_1) - H(\mathbf{x}^T\mathbf{v}_1')\big)/L \tag{137}$$

$$= \mathrm{rk}(\mathbf{u}_1) - \mathrm{rk}(\mathbf{v}_1') \overset{\text{a.a.s.}}{=} (d-m')^+ \tag{138}$$

Step (133) is due to Shannon's source coding theorem. Steps (134), (136) and (137) follow from basic information inequalities. Step (135) is because User 1 must decode $\mathbf{x}^T\mathbf{u}_1$ from $\mathbf{S}$ and $\mathbf{x}^T\mathbf{v}_1'$. Step (138) applies the useful connection between entropy and ranks, that $H(\mathbf{x}^T\mathbf{u}) = L\cdot\mathrm{rk}(\mathbf{u})$ for a uniformly distributed $\mathbf{x}$ and a deterministic matrix $\mathbf{u}$. This leaves us with the only non-trivial regime, $(m+m') < d < K(m+m')$, for which we will show that $\Delta^*(\Lambda_n) \overset{\text{a.a.s.}}{\geq} dm/(m+m')$ in the remainder of this section.

Let us provide an intuitive outline before launching into the technical details. Recall that Theorem 2 considers $K \geq d/\gcd(d, m+m')$. If $m+m'$ divides d, it immediately follows that $K \geq d/\gcd(d, m+m') = d/(m+m') \implies d \geq K(m+m')$. Therefore, the non-trivial cases must be that $m+m'$ does not divide d. What we want for the converse argument, intuitively, is to still have the first $d/(m+m')$ users cooperate fully. This is not directly possible because $d/(m+m')$ is not a natural number, but let us set that concern aside for a moment. The $d/(m+m')$ users together already have side information that is equivalent to $m'd/(m+m')$ dimensional projection of the data, which together with the broadcast symbol $\mathbf{S}$ allows them to recover $(m+m')d/(m+m') = d$ dimensions of the data. If so, then we would have that $H(\mathbf{S})/L \geq d - m'd(m+m') = dm/(m+m')$ as the desired converse bound. Now, how

do we overcome the obstacle that we cannot have a fractional number of users? Intuitively, this is achieved by invoking functional submodularity (Lemma 1 of [38], [51], [52]). The idea is that functional submodularity helps to identify and introduce additional entropic terms of certain (linear) functions of the side information and demands. These functions are essentially the projection of the data into finer subspaces. If we regard the entropies of the subsets of the side information and demands as a set of regular building blocks, the additional entropies introduced by functional submodularity are similar to finer fragments. By rearranging and combining these regular building blocks and fragments in a more efficient way, we are able to derive a better converse bound. To make the details concrete, the readers may refer to the following proof sketch for the example with $m+m'=6, d=10$ and $K=d/\gcd(d,m+m')=5$. For this example, we want to show that $\Delta^*(\Lambda_n) \overset{\text{a.a.s.}}{\geq} md/(m+m')=5m/3$.

In the following, steps labeled $(*)$ uses functional submodularity (Lemma 1 of [38], [51], [52]). We proceed as follows.

$$\begin{aligned}
&\underbrace{H(\mathbf{S},\mathbf{x}^T\mathbf{v}_1')+H(\mathbf{S},\mathbf{x}^T\mathbf{v}_2')}_{T_{12}}\\
&\overset{(132)}{=} H(\mathbf{S},\mathbf{x}^T\mathbf{u}_1)+H(\mathbf{S},\mathbf{x}^T\mathbf{u}_2) && (139)\\
&\overset{(*)}{\geq} H(\mathbf{S},\mathbf{x}^T[\mathbf{u}_1,\mathbf{u}_2])+H(\mathbf{S},\mathbf{x}^T(\mathbf{u}_1\cap\mathbf{u}_2)) && (140)\\
&\geq H(\mathbf{x}^T[\mathbf{u}_1,\mathbf{u}_2])+H(\mathbf{S},\mathbf{x}^T(\mathbf{u}_1\cap\mathbf{u}_2)) && (141)\\
&\overset{\text{a.a.s.}}{=} 10L+H(\mathbf{S},\mathbf{x}^T(\mathbf{u}_1\cap\mathbf{u}_2)) && (142)
\end{aligned}$$

The last step is because as $n\to\infty$ the rank of $[\mathbf{u}_1,\mathbf{u}_2]$ is equal to 10 a.a.s. (The proof is omitted here but can be found in the proof for the general case). Then,

$$\begin{aligned}
&\underbrace{T_{12}+H(\mathbf{S},\mathbf{x}^T\mathbf{v}_3')}_{T_{123}}\\
&\overset{(132)}{=} T_{12}+H(\mathbf{S},\mathbf{x}^T\mathbf{u}_3) && (143)\\
&\overset{(*)}{\geq} 10L+H(\mathbf{S},\mathbf{x}^T[\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3])+H(\mathbf{S}) && (144)
\end{aligned}$$

It follows that,

$$\begin{aligned}
&\underbrace{T_{123}+H(\mathbf{S},\mathbf{x}^T\mathbf{v}_4')}_{T_{1234}}\\
&\overset{(132)}{=} T_{123}+H(\mathbf{S},\mathbf{x}^T\mathbf{u}_4) && (145)\\
&\overset{(*)}{\geq} 10L+H(\mathbf{S})+H(\mathbf{S},\mathbf{x}^T[\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3,\mathbf{u}_4])\\
&\quad+H(\mathbf{S},\mathbf{x}^T[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4]) && (146)\\
&\geq 10L+H(\mathbf{S})+H(\mathbf{x}^T[\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3,\mathbf{u}_4])\\
&\quad+H(\mathbf{S},\mathbf{x}^T[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4]) && (147)\\
&\overset{\text{a.a.s.}}{=} 20L+H(\mathbf{S})+H(\mathbf{S},\mathbf{x}^T[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4]) && (148)
\end{aligned}$$

The last step is because as $n\to\infty$ the rank of $[\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3,\mathbf{u}_4]$ is equal to 10 a.a.s. Then,

$$\begin{aligned}
&\underbrace{T_{1234}+H(\mathbf{S},\mathbf{x}^T\mathbf{v}_5')}_{T_{12345}}\\
&\overset{(132)}{=} T_{1234}+H(\mathbf{S},\mathbf{x}^T\mathbf{u}_5) && (149)\\
&\geq 20L+H(\mathbf{S})+H(\mathbf{S},\mathbf{x}^T[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4])\\
&\quad+H(\mathbf{S},\mathbf{x}^T\mathbf{u}_5) && (150)\\
&\overset{(*)}{\geq} 20L+2H(\mathbf{S})+H(\mathbf{S},\mathbf{x}^T[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4,\mathbf{u}_5]) && (151)\\
&\geq 20L+2H(\mathbf{S})+H(\mathbf{x}^T[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4,\mathbf{u}_5]) && (152)\\
&\overset{\text{a.a.s.}}{=} 30L+2H(\mathbf{S}) && (153)
\end{aligned}$$

The last step is because as $n\to\infty$ the rank of $[(\mathbf{u}_1\cap\mathbf{u}_2,\mathbf{u}_3)\cap\mathbf{u}_4,\mathbf{u}_5]$ is equal to 10 a.a.s.

On the other hand,

$$\begin{aligned}
T_{12345}&=H(\mathbf{S},\mathbf{x}^T\mathbf{v}_1')+H(\mathbf{S},\mathbf{x}^T\mathbf{v}_2')+\cdots+H(\mathbf{S},\mathbf{x}^T\mathbf{v}_5') && (154)\\
&\leq H(\mathbf{S})+H(\mathbf{x}^T\mathbf{v}_1')+H(\mathbf{S})+H(\mathbf{x}^T\mathbf{v}_2')+\cdots\\
&\quad+H(\mathbf{S})+H(\mathbf{x}^T\mathbf{v}_5') && (155)\\
&\leq 5H(\mathbf{S})+5m'L && (156)
\end{aligned}$$

We thus obtain

$$\begin{aligned}
&5H(\mathbf{S})+5m'L\overset{\text{a.a.s.}}{\geq}30L+2H(\mathbf{S})\\
&\implies \Delta^*(\Lambda_n)\geq H(\mathbf{S})/L\overset{\text{a.a.s.}}{\geq}(30-5m')/3=5m/3 \quad (157)
\end{aligned}$$

as desired.

The general proof starts as follows. Let us start with a useful lemma, whose proof is relegated to Appendix IV.

Lemma 1: Consider any $M'\in\mathbb{F}_{p^n}^{d\times\mu'},(\mu'\leq d)$ that has full column rank μ'. Let $M\in\mathbb{F}_{p^n}^{d\times\mu}$. If the elements of M are chosen i.i.d uniform in $\mathbb{F}_{p^n}$, then $[M',M]$ has rank $\min\{d,\mu'+\mu\}$ a.a.s.

Define $\overline{m}$, and the constants $K_0,K_1,\cdots,K_{\overline{m}}$ as follows,

$$\overline{m}\triangleq\frac{m+m'}{\gcd(d,m+m')}, \quad (158)$$

$$K_i\triangleq\left\lceil\frac{id}{m+m'}\right\rceil,\quad \forall i\in[0:\overline{m}], \quad (159)$$

so that,

$$\begin{aligned}
&1)\ K_0=0,\ K_{\overline{m}}=\left\lceil\frac{\overline{m}d}{m+m'}\right\rceil=\frac{d}{\gcd(d,m+m')}, && (160)\\
&2)\ (K_i-1)(m+m')<id\leq K_i(m+m'),\forall i\in[\overline{m}], && (161)\\
&3)\ K_i-K_{i-1}>0,\ \forall i\in[\overline{m}]. && (162)
\end{aligned}$$

Define the matrices $\Upsilon_0,\cdots,\Upsilon_{\overline{m}}$, $\Pi_1,\cdots,\Pi_{\overline{m}}$, and $\Gamma_1,\cdots,\Gamma_{\overline{m}}$, as follows,

$$\begin{aligned}
&\Upsilon_0\triangleq[\,] && (163)\\
&\Gamma_1\triangleq[\Upsilon_0,\mathbf{u}_{K_0+1},\mathbf{u}_{K_0+2},\ldots,\mathbf{u}_{K_1-1}],\\
&\Upsilon_1\triangleq\Gamma_1\cap\mathbf{u}_{K_1},\quad \Pi_1\triangleq[\Gamma_1,\mathbf{u}_{K_1}], && (164)\\
&\Gamma_2\triangleq[\Upsilon_1,\mathbf{u}_{K_1+1},\mathbf{u}_{K_1+2},\ldots,\mathbf{u}_{K_2-1}],\\
&\Upsilon_2\triangleq\Gamma_2\cap\mathbf{u}_{K_2},\quad \Pi_2\triangleq[\Gamma_2,\mathbf{u}_{K_2}] && (165)\\
&\quad\vdots\\
&\Gamma_{i+1}\triangleq[\Upsilon_i,\mathbf{u}_{K_i+1},\mathbf{u}_{K_i+2},\ldots,\mathbf{u}_{K_{i+1}-1}],\\
&\Upsilon_{i+1}\triangleq\Gamma_{i+1}\cap\mathbf{u}_{K_{i+1}},\quad \Pi_{i+1}\triangleq[\Gamma_{i+1},\mathbf{u}_{K_{i+1}}] && (166)\\
&\quad\vdots
\end{aligned}$$

$$\Gamma_{\overline{m}} \triangleq [\Upsilon_{\overline{m}-1}, \mathbf{u}_{K_{\overline{m}-1}+1}, \mathbf{u}_{K_{\overline{m}-1}+2}, \ldots, \mathbf{u}_{K_{\overline{m}}-1}],$$
$$\Upsilon_{\overline{m}} \triangleq \Gamma_{\overline{m}} \cap \mathbf{u}_{K_{\overline{m}}}, \quad \Pi_{\overline{m}} \triangleq [\Gamma_{\overline{m}}, \mathbf{u}_{K_{\overline{m}}}] \tag{167}$$

so that for all $i \in [\overline{m}]$,

$$\Gamma_i \in \mathbb{F}_q^{d \times (\mathbf{rk}(\Upsilon_{i-1})+(K_i-K_{i-1}-1)(m+m'))}, \tag{168}$$
$$\Pi_i \in \mathbb{F}_q^{d \times (\mathbf{rk}(\Upsilon_{i-1})+(K_i-K_{i-1})(m+m'))}. \tag{169}$$

Define the event E_n as follows,

$$E_n \triangleq \Big(\mathrm{rk}(\mathbf{v}'_k) = m', \quad \forall k \in [K]\Big) \wedge \Big(\mathrm{rk}(\Pi_i) = d, \quad \forall i \in [\overline{m}]\Big). \tag{170}$$

The next steps (171)-(179) show that E_n holds a.a.s.

From Lemma 1 (let $M' = [\,]$, $M = \mathbf{v}'_k$), we have $\mathrm{rk}(\mathbf{v}'_k) \overset{\text{a.a.s.}}{=} m'$, since $m' \le m + m' \le d$. Similarly by Lemma 1, (letting $M' = [\,]$ and $M = \Gamma_1$, $M = \mathbf{u}_{K_1}$, $M = \Pi_1$, respectively), we have

$$\mathrm{rk}(\Gamma_1) \overset{\text{a.a.s.}}{=} (K_1 - 1)(m + m'), \tag{171}$$
$$\mathrm{rk}(\mathbf{u}_{K_1}) \overset{\text{a.a.s.}}{=} m + m', \tag{172}$$
$$\mathrm{rk}(\Pi_1) \overset{\text{a.a.s.}}{=} d, \tag{173}$$

where (171) and (173) are due to (161), and (172) follows from $m+m' \le d$. Then since $\mathrm{rk}(\Upsilon_1) = \mathrm{rk}(\Gamma_1)+\mathrm{rk}(\mathbf{u}_{K_1})-\mathrm{rk}(\Pi_1)$, we have that

$$\mathrm{rk}(\Upsilon_1) \overset{\text{a.a.s.}}{=} K_1(m + m') - d. \tag{174}$$

Next, to set up an inductive argument, suppose for some i, $1 \le i < \overline{m}$,

$$\mathrm{rk}(\Upsilon_i) \overset{\text{a.a.s.}}{=} K_i(m + m') - id. \tag{175}$$

Conditioned on $\Big(\mathrm{rk}(\Upsilon_i) = K_i(m + m') - id\Big)$, from Lemma 1 and (161),(168),(169) we have

$$\mathrm{rk}(\Gamma_{i+1}) \overset{\text{a.a.s.}}{=} (K_{i+1} - 1)(m + m') - id, \tag{176}$$
$$\mathrm{rk}(\Pi_{i+1}) \overset{\text{a.a.s.}}{=} d, \tag{177}$$
$$\mathrm{rk}(\mathbf{u}_{K_{i+1}}) \overset{\text{a.a.s.}}{=} m + m', \tag{178}$$
$$\mathrm{rk}(\Upsilon_{i+1}) \overset{\text{a.a.s.}}{=} K_{i+1}(m + m') - (i + 1)d. \tag{179}$$

where in order to obtain (179), we used the property $\mathrm{rk}(\Upsilon_{i+1}) = \mathrm{rk}(\Gamma_{i+1}) + \mathrm{rk}(\mathbf{u}_{K_{i+1}}) - \mathrm{rk}(\Pi_{i+1})$, along with (176), (177) and (178). By induction, we obtain $\mathrm{rk}(\Pi_i) \overset{\text{a.a.s.}}{=} d, \quad \forall i \in [\overline{m}]$, which implies that E_n holds a.a.s.

Figure 3 may be useful in understanding the construction above and the proof.

For the next stage of the proof, we consider any given $\mathrm{LCBC}\big(\mathbb{F}_{p^n}, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\big)$ where E_n holds. Note that $\mathbf{v}_{[K]}, \mathbf{v}'_{[K]}$ are now arbitrary *constant* matrices that satisfy E_n. Our goal now is to bound the optimal broadcast cost $\Delta^*\big(\mathbb{F}_q, \mathbf{v}_{[K]}, \mathbf{v}'_{[K]}\big)$. Let $\mathbf{x}$ be uniformly distributed to facilitate entropic accounting. Recall that there is no loss of generality in this assumption, because $\mathbf{x}$ is independent of E_n and any achievable scheme must work for all data realizations, so it must also work for all data distributions. Thus, we have,

$$2\overline{m}H(\mathbf{S}) + K_{\overline{m}}Lm' \tag{180}$$
$$\overset{(a)}{=} 2\overline{m}H(\mathbf{S}) + \sum_{k=1}^{K_{\overline{m}}} H(\mathbf{x}^T\mathbf{v}'_k) \tag{181}$$

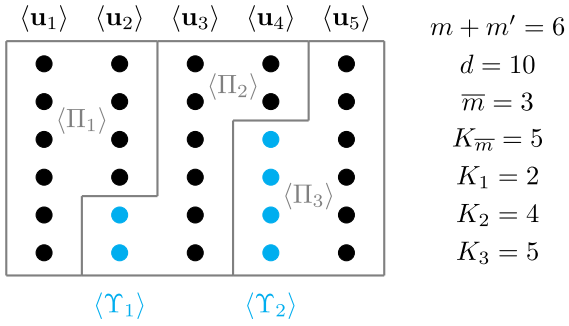

Fig. 3. Illustration of the converse proof for $m + m' = 6, d = 10$. Each dot represents one dimension. The number of dots represents the dimension for the corresponding space a.a.s. $\langle \mathbf{u}_k \rangle, k \in [5]$ has dimension 6 a.a.s. $\langle \Upsilon_1 \rangle$ is the intersection of $\langle \mathbf{u}_1 \rangle$ and $\langle \mathbf{u}_2 \rangle$, which has dimension 2 a.a.s. $\langle \Upsilon_2 \rangle$ is the intersection of $\langle [\Upsilon_1, \mathbf{u}_3] \rangle$ and $\langle \mathbf{u}_4 \rangle$, which has dimension 4 a.a.s. $\langle \Pi_1 \rangle$ is the union of $\langle \mathbf{u}_1 \rangle$ and $\langle \mathbf{u}_2 \rangle$, which has dimension 10 a.a.s. $\langle \Pi_2 \rangle$ is the union of $\langle [\Upsilon_1, \mathbf{u}_3] \rangle$ and $\langle \mathbf{u}_4 \rangle$, which has dimension 10 a.a.s. $\langle \Pi_3 \rangle$ is the union of $\langle \Upsilon_2 \rangle$ and $\langle \mathbf{u}_5 \rangle$, which has dimension 10 a.a.s.

$$= \sum_{i=0}^{\overline{m}-1} \Big[\Big(H(\mathbf{S}) + H(\mathbf{x}^T\mathbf{v}'_{K_i+1}) + H(\mathbf{x}^T\mathbf{v}'_{K_i+2}) + \ldots + H(\mathbf{x}^T\mathbf{v}'_{K_{i+1}-1})\Big) + \Big(H(\mathbf{S}) + H(\mathbf{x}^T\mathbf{v}'_{K_{i+1}})\Big)\Big]$$
$$\ge \sum_{i=0}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{v}'_{K_i+1}, \mathbf{v}'_{K_i+2}, \ldots, \mathbf{v}'_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{v}'_{K_{i+1}})\Big) \tag{182}$$
$$\overset{(b)}{=} \sum_{i=0}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_i+1}, \mathbf{u}_{K_i+2}, \ldots, \mathbf{u}_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_{i+1}})\Big) \tag{183}$$
$$= H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{K_1-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_1}) + \sum_{i=1}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_i+1}, \mathbf{u}_{K_i+2}, \ldots, \mathbf{u}_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_{i+1}})\Big) \tag{184}$$
$$= H(\mathbf{S}, \mathbf{x}^T\Gamma_1) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_1}) + \sum_{i=1}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_i+1}, \mathbf{u}_{K_i+2}, \ldots, \mathbf{u}_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_{i+1}})\Big) \tag{185}$$
$$\overset{(c)}{\ge} H(\mathbf{x}^T\Pi_1) + H(\mathbf{S}, \mathbf{x}^T\Upsilon_1) + \sum_{i=1}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_i+1}, \mathbf{u}_{K_i+2}, \ldots, \mathbf{u}_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_{i+1}})\Big) \tag{186}$$
$$= H(\mathbf{x}^T\Pi_1) + H(\mathbf{S}, \mathbf{x}^T\Upsilon_1) + H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_1+1}, \mathbf{u}_{K_1+2}, \ldots, \mathbf{u}_{K_2-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_2}) + \sum_{i=2}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_i+1}, \mathbf{u}_{K_i+2}, \ldots, \mathbf{u}_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_{i+1}})\Big) \tag{187}$$
$$\overset{(c)}{\ge} \Big(H(\mathbf{x}^T\Pi_1) + H(\mathbf{S})\Big) + H(\mathbf{S}, \mathbf{x}^T\Gamma_2) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_2}) + \sum_{i=2}^{\overline{m}-1} \Big(H(\mathbf{S}, \mathbf{x}^T[\mathbf{u}_{K_i+1}, \mathbf{u}_{K_i+2}, \ldots, \mathbf{u}_{K_{i+1}-1}]) + H(\mathbf{S}, \mathbf{x}^T\mathbf{u}_{K_{i+1}})\Big) \tag{188}$$

$$\vdots$$
$$\geq \Big(H(\mathbf{x}^T\Pi_1)+H(\mathbf{S})\Big)+\ldots+\Big(H(\mathbf{x}^T\Pi_{\overline{m}-1})+H(\mathbf{S})\Big) + H(\mathbf{S},\mathbf{x}^T\Gamma_{\overline{m}})+H(\mathbf{S},\mathbf{x}^T\mathbf{u}_{K_{\overline{m}}}) \quad (189)$$
$$\overset{(c)}{\geq} \Big(H(\mathbf{x}^T\Pi_1)+H(\mathbf{S})\Big)+\ldots+\Big(H(\mathbf{x}^T\Pi_{\overline{m}})+H(\mathbf{S})\Big) \quad (190)$$
$$\overset{(a)}{\geq} \overline{m}\big(Ld+H(\mathbf{S})\big) \quad (191)$$
$$\Longrightarrow \overline{m}H(\mathbf{S})+K_{\overline{m}}Lm' \geq \overline{m}Ld \quad (192)$$

Steps labeled (a) hold because E_n holds. Steps labeled (b) follow from the decodability constraint, i.e., $H(\mathbf{S},\mathbf{x}^T\mathbf{u}_k)=H(\mathbf{S},\mathbf{x}^T\mathbf{v}'_k)$. Steps labeled (c) use functional submodularity (Lemma 1 of [38], [51], [52]).

Note that (160) implies that

$$\frac{K_{\overline{m}}}{\overline{m}}=\frac{d}{m+m'}. \quad (193)$$

Thus, we obtain that

$$\Delta \geq \frac{H(\mathbf{S})}{L} \geq d-\frac{K_{\overline{m}}}{\overline{m}}m'=d-\frac{d}{m+m'}m'=\frac{md}{m+m'}. \quad (194)$$

This in turn implies that for any $\varepsilon>0$,

$$\lim_{n\to\infty}\mathsf{Pr}\left(\Delta^*(\Lambda_n)>\frac{md}{m+m'}-\epsilon\right) \quad (195)$$
$$\geq \lim_{n\to\infty}\mathsf{Pr}\left(\left[\Delta^*(\Lambda_n)>\frac{md}{m+m'}-\epsilon\right]\wedge E_n\right) \quad (196)$$
$$= \lim_{n\to\infty}\mathsf{Pr}(E_n)\mathsf{Pr}\Big(\Delta^*(\Lambda_n)>\frac{md}{m+m'}-\epsilon \;\Big|\; E_n\Big) \quad (197)$$
$$=1. \quad (198)$$

Thus $\Delta^*(\Lambda_n)\overset{\text{a.a.s.}}{>} md/(m+m')-\varepsilon$. Since this is true for all $\varepsilon>0$, according to (16) we have $\Delta_l^*\geq md/(m+m')$. □

VII. Proof of Theorem 3

In this section, let us show the converse for odd d with $3\leq d<2K-1$, and the achievability for $d=2K-1$.

A. Converse for Odd d With $3\leq d<2K-1$

The condition for this regime is equivalent to $2\leq\frac{d+1}{2}<K$. Since the generic capacity for this regime is only a function of d, and assuming a smaller K will not hurt the converse, it suffices to show the converse for $K=\frac{d+1}{2}+1$, that is, $\Delta_l^*\geq d/2$. We start with the following lemma.

Lemma 2: For LCBC($\mathbb{F}_q,\mathbf{v}_{[K]},\mathbf{v}'_{[K]}$), the broadcast cost Δ satisfies,

$$\Delta\geq\frac{1}{2}\Big(\mathrm{rk}(\mathbf{v}'_1\cap[\mathbf{u}_1\cap\mathbf{u}_{\mathcal{K}_1},\mathbf{u}_1\cap\mathbf{u}_{\mathcal{K}_2}])+\mathrm{rk}([\mathbf{u}_1,\mathbf{u}_{\mathcal{K}_1}]) + \mathrm{rk}([\mathbf{u}_1,\mathbf{u}_{\mathcal{K}_2}])-2\mathrm{rk}(\mathbf{v}'_1)-\mathrm{rk}(\mathbf{v}'_{\mathcal{K}_1})-\mathrm{rk}(\mathbf{v}'_{\mathcal{K}_2})\Big), \quad (199)$$

where $\mathcal{K}_1$ and $\mathcal{K}_2$ are subsets of $[K]$.

Proof: For simplicity, we will make use of the converse in [59]. Denote the original LCBC as Λ and its optimal download cost as $\Delta^*(\Lambda)$. Now, consider another LCBC setting L' with 3 users, where User 1 has side information $\mathbf{x}^T\mathbf{v}'_1$ and desires $\mathbf{x}^T\mathbf{v}_1$; User 2 has side information $\mathbf{x}^T\mathbf{v}'_{\mathcal{K}_1}$ and desires $\mathbf{x}^T\mathbf{v}_{\mathcal{K}_1}$; User 3 has side information $\mathbf{x}^T\mathbf{v}'_{\mathcal{K}_2}$ and desires $\mathbf{x}^T\mathbf{v}_{\mathcal{K}_2}$. Denote by $\Delta^*(\Lambda')$ the optimal download cost of Λ'. We have $\Delta^*(\Lambda)\geq\Delta^*(\Lambda')$ since for any scheme that works for Λ, we can construct another scheme that works for Λ' with a same download cost by letting the users in $\mathcal{K}_1$ cooperate, and the users in $\mathcal{K}_2$ cooperate. Note that $\mathcal{K}_1$ and $\mathcal{K}_2$ can have a non-empty intersection. Also note that although the capacity result in [59] is only for $m_k=m'_k=1,\forall k\in[3]$, the converse holds for any LCBC with 3 users. Now let us make use of the converse in [59]. Since $\Delta^*(\Lambda)\geq\Delta^*(\Lambda')$, by (7) of [59], and by rearranging the terms, we have the desired bound. ■

Next we show the converse for the generic capacity, i.e., $\Delta_l^*\geq d/2$ for $K=\frac{d+1}{2}+1$. Note that $\frac{d+1}{2}+1=3+\frac{d-3}{2}$. Let $\mathcal{K}_0=[K-\frac{d-3}{2}+1:K]$, $\mathcal{K}_1=\{2\}\cup\mathcal{K}_0$ and $\mathcal{K}_2=\{3\}\cup\mathcal{K}_0$. Note that $\mathcal{K}_0=\emptyset$ if $d=3$. Since the converse bound in Lemma 2 is composed of ranks of certain matrices, we then finds these ranks in the a.a.s. sense.

First, since $2(1+|\mathcal{K}_1|)=2(1+|\mathcal{K}_2|)=d+1>d$, by Lemma 1,

$$\mathrm{rk}([\mathbf{u}_1,\mathbf{u}_{\mathcal{K}_1}])\overset{\text{a.a.s.}}{=}d,\quad \mathrm{rk}([\mathbf{u}_1,\mathbf{u}_{\mathcal{K}_2}])\overset{\text{a.a.s.}}{=}d, \quad (200)$$

and

$$\mathrm{rk}(\mathbf{v}'_1)\overset{\text{a.a.s.}}{=}1,\quad \mathrm{rk}(\mathbf{v}'_{\mathcal{K}_1})\overset{\text{a.a.s.}}{=}\frac{d-1}{2},\quad \mathrm{rk}(\mathbf{v}'_{\mathcal{K}_2})\overset{\text{a.a.s.}}{=}\frac{d-1}{2}. \quad (201)$$

This leaves us the only non-trivial term, $\mathrm{rk}(\mathbf{v}'_1\cap[\mathbf{u}_1\cap\mathbf{u}_{\mathcal{K}_1},\mathbf{u}_1\cap\mathbf{u}_{\mathcal{K}_2}])$. To avoid complex notations, within this section let

$$A=\mathbf{u}_1\in\mathbb{F}_q^{d\times 2}, \quad (202)$$
$$B=\mathbf{u}_{\mathcal{K}_1}=[\mathbf{u}_{\mathcal{K}_0},\mathbf{u}_2]\in\mathbb{F}_q^{d\times(d-1)}, \quad (203)$$
$$C=\mathbf{u}_{\mathcal{K}_2}=[\mathbf{u}_{\mathcal{K}_0},\mathbf{u}_3]\in\mathbb{F}_q^{d\times(d-1)}. \quad (204)$$

Then let

$$D=[A,\mathbf{0}^{d\times(d-2)}]\big([A,B_{[1:d-2]}]\big)^*B_{[d-1]}\in\mathbb{F}_q^{d\times 1}, \quad (205)$$
$$E=[A,\mathbf{0}^{d\times(d-2)}]\big([A,C_{[1:d-2]}]\big)^*C_{[d-1]}\in\mathbb{F}_q^{d\times 1}, \quad (206)$$

where M^* denotes the adjugate matrix of a square matrix M such that $MM^*=\det(M)\mathbf{I}$. By construction, we have $\langle D\rangle\subset\langle A\rangle$ and $\langle E\rangle\subset\langle A\rangle$. Then note that

$$D+[\mathbf{0}^{d\times 2},B_{[1:d-2]}]\big([A,B_{[1:d-2]}]\big)^*B_{[d-1]} = \det([A,B_{[1:d-2]}])B_{[d-1]}. \quad (207)$$

We obtain that $\langle D\rangle\subset\langle B\rangle$. Similarly, we have $\langle E\rangle\subset\langle C\rangle$. Therefore, $\langle D\rangle\subset\langle A\cap B\rangle$ and $\langle E\rangle\subset\langle A\cap C\rangle$. Next, let $Z\in\mathbb{F}_q^{d\times(d-2)}$. We claim that

$$P=\det([D,E,Z]) \quad (208)$$

is a non-zero polynomial in the elements of $\mathbf{u}_{[K]},Z$. To see this, specify

$$\mathbf{u}_1=\mathbf{I}^{d\times d}_{[1:2]},\quad \mathbf{u}_{\mathcal{K}_0}=\mathbf{I}_{[3:d-1]}, \quad (209)$$
$$\mathbf{u}_2=[\mathbf{I}^{d\times d}_{[d]},\mathbf{I}^{d\times d}_{[1]}], \quad (210)$$

$$\mathbf{u}_3 = [\mathbf{I}_{[d]}^{d\times d}, \mathbf{I}_{[2]}^{d\times d}], \tag{211}$$

$$Z = \mathbf{I}_{[3:d]}^{d\times d}. \tag{212}$$

We then have

$$[A, B_{[1:d-2]}] = [A, C_{[1:d-2]}] = \mathbf{I}^{d\times d}, \tag{213}$$

and it follows that

$$D = \mathbf{I}_{[1]}, \quad E = \mathbf{I}_{[2]} \implies \det([D, E, Z]) = \det(\mathbf{I}^{d\times d}) = 1. \tag{214}$$

Therefore, P is a non-zero polynomial, with degree not more than $2(d+1)+(d-2)$. By Schwartz-Zippel Lemma, the probability of P evaluating to a non-zero value is not less than

$$1 - \frac{2(d+1)+(d-2)}{p^n} \tag{215}$$

which approaches 1 as $n \to \infty$. Thus,

$$\text{rk}([D, E]) \overset{\text{a.a.s.}}{\geq} 2 \implies \text{rk}([\mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_1}, \mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_2}]) \overset{\text{a.a.s.}}{\geq} 2. \tag{216}$$

Since $\langle [\mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_1}, \mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_2}] \rangle \subset \langle \mathbf{u}_1 \rangle$, and $\text{rk}(\mathbf{u}_1) \leq 2$, we have that

$$\langle [\mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_1}, \mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_2}] \rangle \overset{\text{a.a.s.}}{=} \langle \mathbf{u}_1 \rangle. \tag{217}$$

Since $\langle \mathbf{v}_1' \rangle \subset \langle \mathbf{u}_1 \rangle$, we obtain that

$$\text{rk}(\mathbf{v}_1' \cap [\mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_1}, \mathbf{u}_1 \cap \mathbf{u}_{\mathcal{K}_2}]) \overset{\text{a.a.s.}}{=} \text{rk}(\mathbf{v}_1') \overset{\text{a.a.s.}}{=} 1. \tag{218}$$

Now let us consider (199) in the a.a.s. sense. We have

$$\Delta_n \overset{\text{a.a.s.}}{\geq} \frac{1+2d-2-(d-1)}{2} = \frac{d}{2}, \tag{219}$$

or, equivalently,

$$\Delta_l^* \geq \frac{d}{2}, \tag{220}$$

which proves the desired converse. □

B. Achievability for Odd d With $d = 2K-1$

Consider the following K matrices

$$M_k = [\mathbf{v}'_{[K]}, \mathbf{v}_{[K]\setminus\{k\}}] \in \mathbb{F}_q^{d\times d}, \quad k \in [K]. \tag{221}$$

By Lemma 1, we have,

$$\text{rk}(M_k) \overset{\text{a.a.s.}}{=} d, \quad \forall k \in [K]. \tag{222}$$

For any LCBC instance that satisfies $\text{rk}(M_k) = d, \ \forall k \in [K]$, we are able to find non-zero $\mathbb{F}_q$ elements $\alpha_1, \alpha_2, \ldots, \alpha_{K-1}$ and $\mathbb{F}_q$ elements $\alpha_1', \alpha_2', \ldots, \alpha_K'$ such that

$$\mathbf{v}_K = \sum_{k=1}^{K-1} \alpha_k \mathbf{v}_k + \sum_{k=1}^{K} \alpha_k' \mathbf{v}_k'. \tag{223}$$

To see this, first note that since $\text{rk}(M_K) = d$, $\mathbf{v}_K$ can be represented by a linear combination of the $2K-1$ vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{K-1}, \mathbf{v}_1', \mathbf{v}_2', \ldots, \mathbf{v}_K'$. Now let us show that the coefficients $\alpha_1, \alpha_2, \ldots, \alpha_{K-1}$ are non-zero. We prove by contradiction. Suppose $\alpha_i = 0$. We then have

$$\sum_{k\in[1:K-1]\setminus\{i\}} \alpha_k \mathbf{v}_k + \sum_{k=1}^{K} \alpha_k' \mathbf{v}_k' - \mathbf{v}_K = 0, \tag{224}$$

which implies that M_i does not have full column rank d. This contradiction proves that $\alpha_k \neq 0, \forall k \in [1:K-1]$. Let the batch size $L = 1$. The server broadcasts $\mathbf{S} = \mathbf{S}_{[K-1]}$, where

$$\mathbf{S}_k = \mathbf{x}^T(\alpha_k \mathbf{v}_k + \alpha_k' \mathbf{v}_k') \in \mathbb{F}_q, \quad k \in [K-1]. \tag{225}$$

User $k, k \in [K-1]$ can get its desired computation by $\mathbf{x}^T\mathbf{v}_k = (1/\alpha_k)(\mathbf{S}_k - \alpha_k' \mathbf{x}^T\mathbf{v}_k')$. User K can get its desired computation by $\mathbf{x}^T\mathbf{v}_K = \sum_{k=1}^{K-1} \mathbf{S}_k + \alpha_K' \mathbf{x}^T\mathbf{v}_K'$. The broadcast cost is then $\Delta = K-1$. By (222), we conclude that

$$\Delta_u^* \leq K-1. \tag{226}$$

which is the desired upper bound. □

VIII. Conclusion

The take home message of this work is optimistic. While a general capacity characterization of the LCBC for large number of users remains out of reach because it includes recognized hard problems such as index coding, a generic capacity characterization is shown to be tractable. As such, the LCBC setting that generalizes index coding, combined with the generic capacity formulation that focuses on *almost all* instances of the LCBC, presents a promising path forward for future progress. This is analogous to DoF studies of wireless networks where much progress has come about by focusing on generic settings ('almost all' channel realizations rather than 'all' channel realizations) while the DoF of arbitrary instances still remain largely open.

The latter limitation is worth emphasizing. While a generic capacity characterization reveals the capacity of most LCBC settings, it is notable that the LCBC settings that have received the most attention thus far, say index coding and coded caching for example, have specialized demand and side-information structures that are not generic. Thus, open questions in index coding and caching remain open and as important as ever for future work. The study of generic capacity is not intended to supersede the studies of caching, index coding or other specialized applications, but to complement those efforts with an understanding of what is missed in the study of specializations — the generic case. Understanding the capacity limits for structureless, i.e., generic side-information and demands is especially important because the scope of possible linear computation scenarios that may arise in future applications is far too broad to be understood through studies of specialized structures alone. For example, arbitrary linear filters may be applied by different users on large datasets held by a central server, with side-information arising from previously retrieved outputs of other filtering operations on the same datasets. Depending on the application, there may be little or no freedom to optimize the structure of the demand and side-information. Also, a theory cannot be built out of special cases while ignoring the generic case. So if a cohesive information theoretical understanding of communication networks used for computation tasks is to ever emerge, the generic case has to be at its foundation.

Promising directions for future work include the exploration of generic capacity for asymmetric settings, analysis of the LCBC download cost vs complexity tradeoff, and generic

capacity in the large q sense (especially for $n = 1$). Extensions of finite field results to degrees of freedom (DoF) results over real/complex numbers, and studies of the tradeoffs between precision and communication cost in the GDoF sense (as in [60]) are promising as well. Last but not the least, while the capacity results in this work establish the information theoretic fundamental limits, asymptotic IA schemes are far from practical. Therefore, the extent to which the fundamental limit can be approached with *practical* coding schemes, is a most interesting open question where future coding-theoretic analysis can shed light.

APPENDIX I
THEOREM 2: PROOF OF ACHIEVABILITY

Let us recall the compact notation $\mathbf{u}_k \triangleq [\mathbf{v}'_k, \mathbf{v}_k], \forall k \in [K]$. For $d \geq K(m+m')$, the broadcast cost Km is trivially achievable, simply by broadcasting each user's demand separately, i.e., $\mathbf{S} = \mathbf{x}^T[\mathbf{v}_1, \ldots, \mathbf{v}_K]$. The achievability for the remaining regimes is shown next.

A. Achievability for $d \leq m + m'$

Define the event

$$E_n \triangleq \Big(\text{rk}(\mathbf{v}'_k) = \min\{m', d\}\Big) \wedge \Big(\text{rk}(\mathbf{u}_k) = d\Big). \tag{227}$$

In Lemma 1, letting $M' = [\ ]$, $M = \mathbf{v}'_k$ and $M = \mathbf{u}_k$, respectively, we obtain that E_n holds a.a.s. The following argument is true if E_n holds.

1) If $d \leq m'$, each of the K users is able to compute $\mathbf{x}$, since $\text{rk}(\mathbf{v}'_k) = d$. This implies that $\Delta^* = 0$.
2) Using field extensions (cf. Appendix II of [38]), let us consider the equivalent LCBC with field size $q^z = p^{nz}$. If $m' < d \leq m + m'$, for each $k \in [K]$, let $\mathbf{u}^c \in \mathbb{F}_{q^z}^{d\times(d-m')}$. We claim that $P_k = \det([\mathbf{u}_k, \mathbf{u}^c])$ is a non-zero polynomial in the elements of $\mathbf{u}_k, \mathbf{u}^c$. To see this, for each k, we can choose $\mathbf{u}^c = (\mathbf{I}^{d\times d}|\mathbf{u}_k) \in \mathbb{F}_{q^z}^{d\times(d-m')}$ such that $[\mathbf{u}_k, \mathbf{u}^c]$ spans $\langle \mathbf{I}^{d\times d}\rangle$. It follows that $P = \prod_k P_k$ is a non-zero polynomial in the elements of $\mathbf{u}_{[K]}, \mathbf{u}^c$. By Schwartz-Zippel Lemma, if the elements of $\mathbf{u}^c$ are chosen uniformly in $\mathbb{F}_{q^z}$, the probability of P evaluating to zero is not more than $\frac{\text{degree of } P}{q^z} \leq \frac{K(d-m')}{q^z}$. Thus, by choosing $z > \log_q(K(d-m'))$, we ensure that there exists such $\mathbf{u}^c$ that satisfies $\det([\mathbf{u}_k, \mathbf{u}^c]) \neq 0$ for all $k \in [K]$. Broadcasting $\mathbf{S} = \mathbf{x}^T\mathbf{u}^c$, we have $\Delta = d - m'$, and each User k is able to compute $\mathbf{x}$ with $\mathbf{S}$ and its side information $\mathbf{x}^T\mathbf{v}'_k$.

Thus we have the desired achievability, $\Delta^*(\Lambda_n) \overset{\text{a.a.s.}}{\leq} \max\{0, d - m'\}$.

B. Achievability for $(m + m') < d < K(m + m')$

Let $L = 1$. For $q = p^n$, we will interpret $\mathbb{F}_q$ as an n-dimensional vector space over $\mathbb{F}_p$, and design a linear scheme over $\mathbb{F}_p$. Accordingly, let us clarify the notation as follows.

1) The elements of the data and coefficient matrices are chosen from $\mathbb{F}_q = \mathbb{F}_{p^n}$.
2) The data $\mathbf{x}^T = [x_1, x_2, \ldots, x_d] \in \mathbb{F}_q^{1\times d}$, is equivalently represented over $\mathbb{F}_p$ as $\mathbf{X}^T = [X_1^T, X_2^T, \ldots, X_d^T] \in \mathbb{F}_p^{1\times dn}$, where $X_i \in \mathbb{F}_p^{n\times 1}$ is the $n \times 1$ vector representation of x_i over $\mathbb{F}_p$.
3) User k has side information $\mathbf{x}^T\mathbf{v}'_k \in \mathbb{F}_q^{1\times m'}$ and wishes to compute $\mathbf{x}^T\mathbf{v}_k \in \mathbb{F}_q^{1\times m}$, where

$$\mathbf{v}_k = \begin{bmatrix} \mathbf{v}_k^1 & \mathbf{v}_k^2 & \ldots & \mathbf{v}_k^m \end{bmatrix} \tag{228}$$

$$= \begin{bmatrix} v_{k1}^1 & v_{k1}^2 & \ldots & v_{k1}^m \\ v_{k2}^1 & v_{k2}^2 & \ldots & v_{k2}^m \\ \vdots & \vdots & \ddots & \vdots \\ v_{kd}^1 & v_{kd}^2 & \ldots & v_{kd}^m \end{bmatrix} \in \mathbb{F}_q^{d\times m} \tag{229}$$

and

$$\mathbf{v}'_k = \begin{bmatrix} \mathbf{v}_k'^1 & \mathbf{v}_k'^2 & \ldots & \mathbf{v}_k'^{m'} \end{bmatrix} \tag{230}$$

$$= \begin{bmatrix} v_{k1}'^1 & v_{k1}'^2 & \ldots & v_{k1}'^{m'} \\ v_{k2}'^1 & v_{k2}'^2 & \ldots & v_{k2}'^{m'} \\ \vdots & \vdots & \ddots & \vdots \\ v_{kd}'^1 & v_{kd}'^2 & \ldots & v_{kd}'^{m'} \end{bmatrix} \in \mathbb{F}_q^{d\times m'} \tag{231}$$

4) Let $r_1, r_2, \ldots, r_{m'}, \theta_1, \theta_2, \ldots, \theta_m$ be chosen i.i.d uniformly in $\mathbb{F}_q$.
5) Define the set of variables,

$$\begin{aligned} \mathcal{V} \triangleq &\Big\{v_{ki}^j : k \in [K], i \in [d], j \in [m]\Big\} \\ &\cup \Big\{v_{ki}'^{j'} : k \in [K], i \in [d], j' \in [m']\Big\} \\ &\cup \Big\{r_1, r_2, \ldots, r_{m'}, \theta_1, \theta_2, \ldots, \theta_m\Big\}, \end{aligned} \tag{232}$$

and note that $|\mathcal{V}| = (m + m')(dK + 1)$.
6) We will also introduce the corresponding $n \times n$ matrix representations in $\mathbb{F}_p$ for several $\mathbb{F}_q$ variables (some of the $\mathbb{F}_q$ variables will be introduced later). The following table specifies them.

$\mathbb{F}_q$ variable	$\mathbb{F}_p^{n\times n}$ matrix representation	Comment
v_{ki}^j	V_{ki}^j	$k \in [K]$, $i \in [d]$, $j \in [m]$
$v_{ki}'^{j'}$	$V_{ki}'^{j'}$	$k \in [K]$, $i \in [d]$, $j' \in [m']$
$r_{j'}$	$R_{j'}$	$j' \in [m']$
$t_{ki}^{\mu j'}$	$T_{ki}^{\mu j'}$	$k \in [K]$, $i \in [d]$, $\mu \in [m]$, $j' \in [m']$
h_μ^j	H_μ^j	$j \in [\eta]$, $\mu \in [m]$
$\overline{h}_\mu^j$	$\overline{H}_\mu^j$	$j \in [\overline{\eta}]$, $\mu \in [m]$

Our goal is to show that $\Delta_u^* \leq dm/(m + m')$. Note that if $d = 0$ or $m = 0$, $\Delta = 0$ is trivially achieved for all cases. If $m' = 0$, then $\Delta \leq d$ is trivially achieved for all cases by broadcasting $\mathbf{S} = \mathbf{X}$. Thus, in the following we consider the

cases when $d > 0, m > 0, m' > 0$. First, for $k \in [K], \mu \in [m], j' \in [m']$, let us define

$$\begin{bmatrix} v_{k1}^{\prime j'} \\ v_{k2}^{\prime j'} \\ \vdots \\ v_{kd}^{\prime j'} \end{bmatrix} = \begin{bmatrix} v_{k1}^{\mu} \\ v_{k2}^{\mu} \\ \vdots \\ v_{kd}^{\mu} \end{bmatrix} r_{j'} + \begin{bmatrix} t_{k1}^{\mu j'} \\ t_{k2}^{\mu j'} \\ \vdots \\ t_{kd}^{\mu j'} \end{bmatrix}. \tag{233}$$

We have

$$\underbrace{\begin{bmatrix} V_{k1}^{\prime j'} \\ V_{k2}^{\prime j'} \\ \vdots \\ V_{kd}^{\prime j'} \end{bmatrix}}_{\mathbf{V}_k^{\prime j'} \in \mathbb{F}_p^{dn \times n}} = \underbrace{\begin{bmatrix} V_{k1}^{\mu} \\ V_{k2}^{\mu} \\ \vdots \\ V_{kd}^{\mu} \end{bmatrix}}_{\mathbf{V}_k^{\mu} \in \mathbb{F}_p^{dn \times n}} R_{j'} + \underbrace{\begin{bmatrix} T_{k1}^{\mu j'} \\ T_{k2}^{\mu j'} \\ \vdots \\ T_{kd}^{\mu j'} \end{bmatrix}}_{\mathbf{T}_k^{\mu j'} \in \mathbb{F}_p^{dn \times n}} \tag{234}$$

by (233), and $\mathbf{T}_k^{\mu, j'}, \mu \in [m], j' \in [m']$ are defined as in (234).

Next, construct $\mathbf{h}_\mu \in \mathbb{F}_q^{\eta \times 1}, \overline{\mathbf{h}}_\mu \in \mathbb{F}_q^{\overline{\eta} \times 1}, \mu \in [m]$ as,

$$\mathbf{h}_\mu^{1 \times \eta} = \Bigg[\theta_\mu \prod_{k=1}^{K} \Bigg(\Big(\prod_{i=1}^{d} \prod_{j=1}^{m} (v_{ki}^j)^{\alpha_{ki}^j} \Big) \Big(\prod_{i=1}^{d} \prod_{j'=1}^{m'} (t_{ki}^{\mu j'})^{\beta_{ki}^{\mu j'}} \Big) \Bigg), \quad \text{s.t. } 0 \le \alpha_{ki}^j, \beta_{ki}^{\mu j'} \le N-1 \Bigg] \tag{235}$$

$$\triangleq (h_\mu^1, h_\mu^2, \ldots, h_\mu^\eta), \qquad \forall \mu \in [m]. \tag{236}$$

$$\overline{\mathbf{h}}_\mu^{1 \times \eta} = \Bigg[\theta_\mu \prod_{k=1}^{K} \Bigg(\Big(\prod_{i=1}^{d} \prod_{j=1}^{m} (v_{ki}^j)^{\alpha_{ki}^j} \Big) \Big(\prod_{i=1}^{d} \prod_{j'=1}^{m'} (t_{ki}^{\mu j'})^{\beta_{ki}^{\mu j'}} \Big) \Bigg), \quad \text{s.t. } 0 \le \alpha_{ki}^j, \beta_{ki}^{\mu j'} \le N \Bigg] \tag{237}$$

$$\triangleq (\overline{h}_\mu^1, \overline{h}_\mu^2, \ldots, \overline{h}_\mu^{\overline{\eta}}), \qquad \forall \mu \in [m]. \tag{238}$$

Note that we have,

$$\eta = N^{Kd(m+m')}, \quad \overline{\eta} = (N+1)^{Kd(m+m')}. \tag{239}$$

This construction ensures that for $\mu \in [m]$, the elements of $v_{ki}^j \mathbf{h}_\mu$ and $t_{ki}^{\mu, j'} \mathbf{h}_\mu$ are contained among the elements of $\overline{\mathbf{h}}_\mu$ for all $i \in [d], j \in [m], j' \in [m']$. Define,

$$\mathbf{H}_\mu = \left[H_\mu^1 \mathbf{1}, H_\mu^2 \mathbf{1}, \ldots, H_\mu^\eta \mathbf{1} \right] \quad \in \mathbb{F}_p^{n \times \eta}, \qquad \mu \in [m] \tag{240}$$

and

$$\overline{\mathbf{H}}_\mu = \left[\overline{H}_\mu^1 \mathbf{1}, \overline{H}_\mu^2 \mathbf{1}, \ldots, \overline{H}_\mu^{\overline{\eta}} \mathbf{1} \right] \quad \in \mathbb{F}_p^{n \times \overline{\eta}}, \qquad \mu \in [m], \tag{241}$$

where $\mathbf{1}$ denotes the $n \times 1$ vector of 1's. By construction, the columns of $V_{ki}^j \mathbf{H}$ and $T_{ki}^\mu \mathbf{H}$ are subsets of the columns of $\mathbf{H}_\mu$, which implies that $\forall \mu \in [m], k \in [K], i \in [d], j \in [m], j' \in [m']$,

$$\langle V_{ki}^j \mathbf{H}_\mu \rangle_p \subset \langle \overline{\mathbf{H}}_\mu \rangle_p, \qquad \langle T_{ki}^\mu \mathbf{H}_\mu \rangle_p \subset \langle \overline{\mathbf{H}}_\mu \rangle_p. \tag{242}$$

Consider the m matrices,

$$\left[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1 \mathbf{H}_1, R_2 \mathbf{H}_1, \ldots, R_{m'} \mathbf{H}_1 \right] \in \mathbb{F}_p^{n \times (m+m')\eta} \tag{243}$$

$$\left[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1 \mathbf{H}_2, R_2 \mathbf{H}_2, \ldots, R_{m'} \mathbf{H}_2 \right] \in \mathbb{F}_p^{n \times (m+m')\eta} \tag{244}$$

$$\vdots$$

$$\left[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1 \mathbf{H}_m, R_2 \mathbf{H}_m, \ldots, R_{m'} \mathbf{H}_m \right] \in \mathbb{F}_p^{n \times (m+m')\eta}. \tag{245}$$

Define event E_n as,

$$E_n = \bigwedge_{\mu=1}^{m} \Big(\text{rk}\big([\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1 \mathbf{H}_\mu, R_2 \mathbf{H}_\mu, \ldots, R_{m'} \mathbf{H}_\mu] \big) = (m+m')\eta \Big). \tag{246}$$

The following lemma establishes a sufficient condition when E_n holds a.a.s., which will subsequently be essential to guarantee successfully decoding by each user.

Lemma 3: If $\lim_{n \to \infty} \frac{N}{p^{[n-(m+m')\eta]}} = 0$, then E_n holds a.a.s.

Proof: See Appendix II. ∎

Let us specify the value of N as follows,

$$N = \left\lfloor \left(\frac{n - \sqrt{n}}{m+m'} \right)^{\frac{1}{Kd(m+m')}} \right\rfloor, \tag{247}$$

from which it follows that

$$N \le \left(\frac{n - \sqrt{n}}{m+m'} \right)^{\frac{1}{Kd(m+m')}} \tag{248}$$

and

$$n - (m+m')\eta \ge \sqrt{n}. \tag{249}$$

Therefore,

$$\lim_{n \to \infty} \frac{N}{p^{n-(m+m')\eta}} \le \lim_{n \to \infty} \frac{\left(\frac{n-\sqrt{n}}{m+m'} \right)^{\frac{1}{Kd(m+m')}}}{p^{\sqrt{n}}} = \lim_{n \to \infty} \frac{\mathcal{O}(n^\alpha)}{p^{\sqrt{n}}} = 0 \tag{250}$$

where α is independent of n. Since $N \ge 0$, we have $\lim_{n \to \infty} \frac{N}{p^{n-(m+m')\eta}} = 0$. Applying Lemma 3, we have that E_n holds a.a.s. Now for $\mu \in [1:m]$, let $\mathbf{Z}_\mu = (\mathbf{I}^{n \times n} | [\mathbf{H}_1, \ldots, \mathbf{H}_\mu, R_1 \mathbf{H}, \ldots, R_{m'} \mathbf{H}]) \in \mathbb{F}_p^{n \times (n-(m+m')\eta)}$, so that

$$\left[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1 \mathbf{H}_\mu, R_2 \mathbf{H}_\mu, \ldots, R_{m'} \mathbf{H}_\mu, \mathbf{Z}_\mu \right] \tag{251}$$

has full rank n. For compact notation, let

$$\overline{\mathcal{H}} \triangleq [\overline{\mathbf{H}}_1, \overline{\mathbf{H}}_2, \ldots, \overline{\mathbf{H}}_m]^{n \times m\overline{\eta}}. \tag{252}$$

Let the server broadcast $\mathbf{S} = \left(\mathbf{S}_0, \mathbf{S}_{[K]}^1, \ldots, \mathbf{S}_{[K]}^m \right) \in \mathbb{F}_p^{1 \times [md\overline{\eta} + Km(n-(m+m')\eta)]}$, where

$$\mathbf{S}_0 = \mathbf{X}^T \begin{bmatrix} \overline{\mathcal{H}} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \overline{\mathcal{H}} & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & \overline{\mathcal{H}} \end{bmatrix} \quad \in \mathbb{F}_p^{nd \times md\overline{\eta}} \tag{253}$$

and for $k \in [K], \mu \in [m]$,

$$\mathbf{S}_k^\mu = \mathbf{X}^T \mathbf{V}_k^\mu \mathbf{Z}_\mu. \tag{254}$$

The decoding process works as follows. User k is able to compute

$$\mathbf{X}^T\mathbf{V}_k'^{j'}\mathbf{H}_\mu, \qquad j' \in [m'], \quad \mu \in [m] \tag{255}$$

directly from its side information. Meanwhile, it is able to compute

$$\mathbf{X}^T\mathbf{V}_k^{j}\mathbf{H}_\mu, \qquad j \in [m], \quad \mu \in [m] \tag{256}$$

and

$$\mathbf{X}^T\mathbf{T}_k^{\mu j'}\mathbf{H}_\mu, \qquad j' \in [m'], \quad \mu \in [m] \tag{257}$$

from $\mathbf{S}_0$, since for $j \in [m], \mu \in [m]$,

$$\left\langle \mathbf{V}_k^j\mathbf{H}_\mu \right\rangle_p = \left\langle \begin{bmatrix} V_{k1}^j\mathbf{H}_\mu \\ V_{k2}^j\mathbf{H}_\mu \\ \vdots \\ V_{kd}^j\mathbf{H}_\mu \end{bmatrix} \right\rangle_p \subset \left\langle \begin{bmatrix} \overline{\mathbf{H}}_\mu & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}}_\mu & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_\mu \end{bmatrix} \right\rangle_p, \tag{258}$$

and for $j' \in [m'], \mu \in [m]$,

$$\left\langle \begin{bmatrix} T_{k1}^{\mu j'}\mathbf{H}_\mu \\ T_{k2}^{\mu j'}\mathbf{H}_\mu \\ \vdots \\ T_{kd}^{\mu j'}\mathbf{H}_\mu \end{bmatrix} \right\rangle_p \subset \left\langle \begin{bmatrix} \overline{\mathbf{H}}_\mu & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \overline{\mathbf{H}}_\mu & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \overline{\mathbf{H}}_\mu \end{bmatrix} \right\rangle_p \tag{259}$$

due to (242). Thus, User k is then able to compute

$$\mathbf{X}^T\mathbf{V}_k^\mu R_{j'}\mathbf{H}_\mu = \mathbf{X}^T\mathbf{V}_k'^{j'}\mathbf{H}_\mu - \mathbf{X}^T\mathbf{T}_k^{\mu j'}\mathbf{H}_\mu \tag{260}$$

for all $j' \in [m'], \mu \in [m]$ according to (234). Together with $\mathbf{S}_k^\mu$, User k is able to compute

$$\mathbf{X}^T\mathbf{V}_k^j\mathbf{H}_\mu, \quad \mathbf{X}^T\mathbf{V}_k^\mu R_{j'}\mathbf{H}_\mu \text{ and } \mathbf{S}_k^\mu, \tag{261}$$

for all $j \in [m], j' \in [m'], \mu \in [m]$, which are

$$\mathbf{X}^T\mathbf{V}_k^1\big[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_1, R_2\mathbf{H}_1, \ldots, R_{m'}\mathbf{H}_1, \mathbf{Z}_1\big], \tag{262}$$

$$\mathbf{X}^T\mathbf{V}_k^2\big[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_2, R_2\mathbf{H}_2, \ldots, R_{m'}\mathbf{H}_2, \mathbf{Z}_2\big], \tag{263}$$

$$\vdots$$

$$\mathbf{X}^T\mathbf{V}_k^m\big[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_m, R_2\mathbf{H}_m, \ldots, R_{m'}\mathbf{H}_m, \mathbf{Z}_m\big]. \tag{264}$$

Since $\big[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_\mu, R_2\mathbf{H}_\mu, \ldots, R_{m'}\mathbf{H}_\mu, \mathbf{Z}_\mu\big]$ is invertible (has full rank) a.a.s. for $\mu \in [m]$, User k is able to compute its desired computation, $\mathbf{X}^T\mathbf{V}_k = \mathbf{X}^T\big[\mathbf{V}_k^1, \mathbf{V}_k^2, \ldots, \mathbf{V}_k^m\big]$ a.a.s.

For $q = p^n$, the cost of broadcasting each p-ary symbol is $1/n$ in q-ary units. Thus, the broadcast cost of this scheme is,

$$\Delta_n = \frac{md\overline{\eta} + Km\big(n - (m+m')\eta\big)}{n}. \tag{265}$$

By (247), we have that

$$\eta = N^{Kd(m+m')} \le \frac{n-\sqrt{n}}{m+m'} \le (N+1)^{Kd(m+m')} = \overline{\eta} \tag{266}$$

which implies that

$$\lim_{n\to\infty}\frac{\eta}{n} = \lim_{n\to\infty}\frac{N^{Kd(m+m')}}{n}$$

$$\le \lim_{n\to\infty}\frac{n-\sqrt{n}}{n} \times \frac{1}{m+m'}$$

$$= \frac{1}{m+m'}. \tag{267}$$

On the other hand,

$$\lim_{n\to\infty}\frac{\eta}{n} = \lim_{n\to\infty}\frac{(N+1)^{Kd(m+m')}/(1+1/N)^{Kd(m+m')}}{n} \tag{268}$$

$$\ge \lim_{N\to\infty}\frac{1}{(1+1/N)^{Kd(m+m')}} \times \lim_{n\to\infty}\frac{n-\sqrt{n}}{n} \times \frac{1}{m+m'} \tag{269}$$

$$= \frac{1}{m+m'}. \tag{270}$$

Thus, we have that

$$\lim_{n\to\infty}\frac{\eta}{n} = \frac{1}{m+m'} \tag{271}$$

which also implies that

$$\lim_{n\to\infty}\frac{\overline{\eta}}{n} = \lim_{n\to\infty}\frac{\eta}{n} \times \lim_{N\to\infty}(1+1/N)^{Kd(m+m')} = \frac{1}{m+m'}. \tag{272}$$

Combining (265) with (271) and (272) we have

$$\lim_{n\to\infty}\Delta_n = md \times \frac{1}{m+m'} + 0 = \frac{md}{m+m'} \tag{273}$$

since K, m, m', d are independent of n. Thus, for any $\varepsilon > 0$, $\exists n_0 > 0$ such that $\Delta_n \le \frac{md}{m+m'} + \varepsilon$ for all $n \ge n_0$. Recall that the broadcast cost Δ_n is achievable if E_n holds, i.e., $\Delta^*(\Lambda_n) \le \Delta_n \le \frac{md}{m+m'} + \epsilon$ if $n \ge n_0$ and E_n holds. Now let us show that $\frac{md}{m+m'} + \epsilon$ is achievable a.a.s., by evaluating the limit in (14) as follows,

$$\lim_{n\to\infty}\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \le \frac{md}{m+m'} + \epsilon\Big)$$

$$\ge \lim_{n\to\infty}\mathsf{Pr}\left(\Big(\Delta^*(\Lambda_n) \le \frac{md}{m+m'} + \epsilon\Big) \wedge E_n\right) \tag{274}$$

$$= \lim_{n\to\infty}\mathsf{Pr}(E_n)\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \le \frac{md}{m+m'} + \epsilon \;\Big|\; E_n\Big) \tag{275}$$

$$= 1 \tag{276}$$

which implies that $\lim_{n\to\infty}\mathsf{Pr}\Big(\Delta^*(\Lambda_n) \le \frac{md}{m+m'} + \epsilon\Big) = 1$. Since this is true for all $\varepsilon > 0$, according to (15) we have $\Delta_u^* \le \inf\{\frac{md}{m+m'} + \epsilon \mid \epsilon > 0\} = \frac{md}{m+m'}$. □

Appendix II
Proof of Lemma 3

By Lemma 1.1.3(v) [54], it suffices to prove that $\forall \mu \in [m]$,

$$\mathrm{rk}\big(\big[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_\mu, R_2\mathbf{H}_\mu, \ldots, R_{m'}\mathbf{H}_\mu\big]\big) \overset{\text{a.a.s.}}{=} (m+m')\eta. \tag{277}$$

Due to symmetry, without loss of generality, we will show the proof for $\mu = 1$, which is

$$\mathrm{rk}\big(\big[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_1, R_2\mathbf{H}_1, \ldots, R_{m'}\mathbf{H}_1\big]\big) \overset{\text{a.a.s.}}{=} (m+m')\eta. \tag{278}$$

Note that $\left[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_1, R_2\mathbf{H}_1, \ldots, R_{m'}\mathbf{H}_1\right]$ has full column rank $(m+m')\eta$ if and only if for all $\mathbf{c}_i = [c_i^1, c_i^2, \ldots, c_i^\eta]^T \in \mathbb{F}_p^{\eta\times 1}, i \in [m]$, and $\mathbf{c}'_i = [c_i'^1, c_i'^2, \ldots, c_i'^\eta]^T \in \mathbb{F}_p^{\eta\times 1}, i \in [m']$ such that $\overline{\mathbf{c}}^T = \left[\mathbf{c}_1^T, \mathbf{c}_2^T, \ldots, \mathbf{c}_m^T, \mathbf{c}_1'^T, \mathbf{c}_2'^T, \ldots, \mathbf{c}_{m'}'^T\right] \neq \mathbf{0}^{1\times(m+m')\eta}$,

$$\mathbf{0}^{n\times 1} \neq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_1, R_2\mathbf{H}_1, \ldots, R_{m'}\mathbf{H}_1]\overline{\mathbf{c}} \tag{279}$$

$$= \mathbf{H}_1\mathbf{c}_1 + \mathbf{H}_2\mathbf{c}_2 + \ldots + \mathbf{H}_m\mathbf{c}_m + R_1\mathbf{H}_1\mathbf{c}'_1 + R_2\mathbf{H}_1\mathbf{c}'_2 + \ldots + R_{m'}\mathbf{H}_1\mathbf{c}'_{m'} \tag{280}$$

$$= \sum_{j=1}^{\eta} c_1^j H_1^j\mathbf{1} + \ldots + \sum_{j=1}^{\eta} c_m^j H_m^j\mathbf{1} + \sum_{j=1}^{\eta} c'^j R_1 H_1^j\mathbf{1} + \ldots + \sum_{j=1}^{\eta} c'^j R_{m'} H_1^j\mathbf{1} \tag{281}$$

$$= \left(\sum_{j=1}^{\eta} c_1^j H_1^j + \ldots + \sum_{j=1}^{\eta} c_m^j H_m^j + \sum_{j=1}^{\eta} c'^j R_1 H_1^j + \ldots + \sum_{j=1}^{\eta} c'^j R_{m'} H_1^j\right)\mathbf{1} \tag{282}$$

$$\triangleq F_{\overline{\mathbf{c}}}\mathbf{1} \tag{283}$$

where $F_{\overline{\mathbf{c}}}$ is an $n\times n$ matrix in $\mathbb{F}_p$, which has a scalar representation in $\mathbb{F}_q$ as,

$$f_{\overline{\mathbf{c}}} = \sum_{j=1}^{\eta} c_1^j h_1^j + \ldots + \sum_{j=1}^{\eta} c_m^j h_m^j + \sum_{j=1}^{\eta} c_1'^j r_1 h_1^j + \ldots + \sum_{j=1}^{\eta} c_{m'}'^j r_{m'} h_1^j \quad \in \mathbb{F}_q. \tag{284}$$

Note that since $\mathbb{F}_p$ is a sub-field of $\mathbb{F}_q$, the elements of $\overline{\mathbf{c}}$ in $\mathbb{F}_p$ are also in $\mathbb{F}_q$. Thus, $F_{\overline{\mathbf{c}}} \in \mathbb{F}_p^{n\times 1}$ can be equivalently represented in $\mathbb{F}_q$ as the product of $f_{\overline{\mathbf{c}}}$ with the scalar representation in $\mathbb{F}_q$, of $\mathbf{1}$ (the all 1 vector in $\mathbb{F}_p$). Since the $\mathbb{F}_q$ representation of $\mathbf{1}$ is not 0, we obtain that

$$F_{\overline{\mathbf{c}}}\mathbf{1} \neq \mathbf{0}^{n\times 1} \iff f_{\overline{\mathbf{c}}} \neq 0. \tag{285}$$

Therefore, $[\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_m, R_1\mathbf{H}_1, R_2\mathbf{H}_1, \ldots, R_{m'}\mathbf{H}_1] \in \mathbb{F}_p^{n\times(m+m')\eta}$ has full column rank if and only if,

$$P \triangleq \prod_{\overline{\mathbf{c}}\in\mathbb{F}_p^{(m+m')\eta\times 1}\setminus\{\mathbf{0}\}} f_{\overline{\mathbf{c}}} \neq 0. \tag{286}$$

The condition of (286), which is equivalent to the event E_n, says that a uniformly random evaluation of the function $P(\mathcal{V})$ produces a non-zero value. We will show that this is true a.a.s. in n.

1) Case I: At least one of $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m\}$ is not $\mathbf{0}^{\eta\times 1}$, then set $r_1 = r_2 = \ldots = r_{m'} = 0$, which implies $f_{\overline{\mathbf{c}}} = \sum_{j=1}^{\eta} c_1^j h_1^j + \ldots + \sum_{j=1}^{\eta} c_m^j h_m^j$, and that $t_{ki}^{\mu,j'} = v_{ki}'^{j'}, \forall \mu \in [m], i \in [d], j' \in [m']$ by (233). Meanwhile, $h_\mu^1, h_\mu^2, \ldots, h_\mu^\eta$ are different monomials in the elements of v_{ki}^j, $v_{ki}'^{j'}$ and θ_μ. Moreover, since any h_μ^j has the factor θ_μ but does not have the factor $\theta_{\mu'}$ if $\mu' \neq \mu$, it follows that $h_1^1, h_1^2, \ldots, h_1^\eta, h_2^1, h_2^2, \ldots, h_2^\eta, \ldots, h_m^1, h_m^2, \ldots, h_m^\eta$ ($m\eta$ in total) are different monomials. Since different monomials are linearly independent, we have that $[f_{\overline{\mathbf{c}}}]$ is a non-zero polynomial.
2) Case II: $\mathbf{c}_1 = \mathbf{c}_2 = \ldots = \mathbf{c}_m = \mathbf{0}$ and thus at least one of $\{\mathbf{c}'_1, \mathbf{c}'_2, \ldots, \mathbf{c}'_{m'}\}$ is not $\mathbf{0}^{n\times 1}$. For this case, we have $f_{\overline{\mathbf{c}}} = \sum_{j=1}^{\eta} c_1'^j r_1 h_1^j + \ldots + \sum_{j=1}^{\eta} c_{m'}'^j r_{m'} h_1^j$. From the discussion in the previous case, we know that $h_1^1, h_1^2, \ldots, h_1^\eta$ are non-zero polynomials, and none of them has a factor in $\{r_1, r_2, \ldots, r_{m'}\}$ (because otherwise letting $r_1 = r_2 = \ldots = r_{m'} = 0$ would evaluate that polynomial to 0, which is a contradiction). Thus, we obtain that $r_1h_1^1, r_1h_1^2, \ldots, r_1h_1^\eta, r_2h_1^1, r_2h_1^2, \ldots, r_2h_1^\eta, \ldots, r_{m'}h_1^1, r_{m'}h_1^2, \ldots, r_{m'}h_1^\eta$ are linearly independent. It then follows that $[f_{\overline{\mathbf{c}}}]$ is a non-zero polynomial.

Thus, $[f_{\overline{\mathbf{c}}}]$ is a non-zero polynomial. Since h_i^j has degree not more than $(N-1)Kd(2m'+m)+1$, $[f_{\overline{\mathbf{c}}}]$ has degree not more than $(N-1)Kd(2m'+m)+2$. Therefore, $[P] \in \mathbb{F}_p[\mathcal{V}]$ is a non-zero polynomial with degree not more than $(p^{(m+m')\eta}-1)[(N-1)Kd(2m'+m)+2]$. By Schwartz-Zippel Lemma, when all the variables $\mathcal{V}$ are assigned i.i.d. uniformly chosen values in $\mathbb{F}_q$,

$$\mathsf{Pr}\big(P \neq 0\big) \geq 1 - \frac{(p^{(m+m')\eta}-1)[(N-1)Kd(2m'+m)+2]}{q} \tag{287}$$

$$= 1 - \frac{(p^{(m+m')\eta}-1)[(N-1)Kd(2m'+m)+2]}{p^n} \tag{288}$$

$$\geq 1 - Kd(2m'+m)\frac{N}{p^{n-(m+m')\eta}} \tag{289}$$

$$\to 1 \tag{290}$$

as $n\to\infty$ if $\lim_{n\to\infty}\frac{N}{p^{n-(m+m')\eta}} = 0$.

Appendix III
Proof of Theorem 1

For compact notation, let us define,

$$\gamma_1 \triangleq \big(\min\{3(m+m')-d, m+m', d\}\big)^+ \tag{291}$$

$$\gamma_2 \triangleq \big(\min\{2(m+m')-d, m+m', d\}\big)^+ \tag{292}$$

$$\gamma_3 \triangleq \big(\min\{3(m+m')-2d, m+m', d\}\big)^+ \tag{293}$$

and define $E_n \triangleq \mathbf{C1} \wedge \mathbf{C2} \wedge \cdots \wedge \mathbf{C6}$ as the event that the following conditions hold. We will show that E_n holds a.a.s. The values of Δ_g for $K = 1, 2, 3$ then follow by evaluating the capacity expression from [38] by applying conditions **C1** to **C6** for the symmetric LCBC with $K \leq 3$.

- **C1** $\mathrm{rk}(\mathbf{v}'_k) = \min\{m', d\}, \quad \forall k \in [1:K]$;
- **C2** $\mathrm{rk}(\mathbf{u}_k) = \min\{m+m', d\}, \quad \forall k \in [1:K]$;
- **C3** $\mathrm{rk}([\mathbf{v}'_i, \mathbf{u}_{ij}]) = \min\{m'+\gamma_2, m+m', d\}, \quad \forall i \neq j, i, j \in [1:K], \ K \geq 2$;
- **C4** $\mathrm{rk}([\mathbf{v}'_k, \mathbf{u}_{123}]) = \min\{m'+\gamma_3, m+m', d\}, \quad \forall k \in [1:3], \quad K = 3$;
- **C5** $\mathrm{rk}([\mathbf{v}'_i, \mathbf{u}_{ij}, \mathbf{u}_{ik}]) = \min\{m'+2\gamma_2, m+m', d\}$, for distinct $i, j, k \in [1:3], \quad K = 3$;
- **C6** $\mathrm{rk}([\mathbf{v}'_i, \mathbf{u}_{i(j,k)}]) = \min\{m'+\gamma_1, m+m', d\}$, for distinct $i, j, k \in [1:3], \quad K = 3$,

where

$$\mathbf{u}_{ij} \triangleq \mathbf{u}_i \cap \mathbf{u}_j, \qquad \forall i,j \in [1:K], i \neq j, \tag{294}$$

$$\mathbf{u}_{123} \triangleq \mathbf{u}_1 \cap \mathbf{u}_2 \cap \mathbf{u}_3, \qquad \text{if } K = 3. \tag{295}$$

By Lemma 1.1.3(v) [54], we then show that E_n holds a.a.s. by showing that each of the conditions **C1** to **C6** holds a.a.s.

A. Conditions C1, C2, C3 and C6

In Lemma 1, let $M' = [\ ]$, $M = \mathbf{v}'_k, \mathbf{u}_k$, respectively. We obtain that Conditions **C1** and **C2** hold a.a.s. Then let $M = [\mathbf{u}_j, \mathbf{v}'_i]$, $M = [\mathbf{u}_i, \mathbf{u}_j]$, respectively. We obtain that

$$\text{rk}([\mathbf{u}_j, \mathbf{v}'_i]) \overset{\text{a.a.s.}}{=} \min\{m + 2m', d\}, \tag{296}$$

$$\text{rk}([\mathbf{u}_i, \mathbf{u}_j]) \overset{\text{a.a.s.}}{=} \min\{2(m + m'), d\}. \tag{297}$$

Since

$$\begin{aligned}
&\text{rk}([\mathbf{u}_i, \mathbf{u}_j]) - \text{rk}([\mathbf{u}_j, \mathbf{v}'_i]) \\
&= \text{rk}(\mathbf{u}_i) + \text{rk}(\mathbf{u}_j) - \text{rk}(\mathbf{u}_{ij}) \\
&\quad - [\text{rk}(\mathbf{u}_j) + \text{rk}(\mathbf{v}'_i) - \text{rk}(\mathbf{u}_j \cap \mathbf{v}'_i)] && (298) \\
&= \text{rk}(\mathbf{u}_i) + \text{rk}(\mathbf{u}_j) - \text{rk}(\mathbf{u}_{ij}) \\
&\quad - [\text{rk}(\mathbf{u}_j) + \text{rk}(\mathbf{v}'_i) - \text{rk}(\mathbf{u}_j \cap \mathbf{u}_i \cap \mathbf{v}'_i)] && (299) \\
&= \text{rk}(\mathbf{u}_i) - [\text{rk}(\mathbf{u}_{ij}) + \text{rk}(\mathbf{v}'_i) - \text{rk}(\mathbf{u}_{ij} \cap \mathbf{v}'_i)] && (300) \\
&= \text{rk}(\mathbf{u}_i) - \text{rk}([\mathbf{v}'_i, \mathbf{u}_{ij}]), && (301)
\end{aligned}$$

it follows that

$$\begin{aligned}
&\text{rk}([\mathbf{v}'_i, \mathbf{u}_{ij}]) \\
&\overset{\text{a.a.s.}}{=} \min\{m + m', d\} - \min\{2(m + m'), d\} + \min\{m + 2m', d\} && (302) \\
&= \min\{m' + \gamma_2, m + m', d\} && (303)
\end{aligned}$$

which proves the result for **C3**. Next, let $M = [\mathbf{u}_j, \mathbf{u}_k, \mathbf{v}'_i]$, $M = [\mathbf{u}_i, \mathbf{u}_j, \mathbf{u}_k]$, respectively. We obtain that

$$\text{rk}([\mathbf{u}_j, \mathbf{u}_k, \mathbf{v}'_i]) \overset{\text{a.a.s.}}{=} \min\{2m + 3m', d\}, \tag{304}$$

$$\text{rk}([\mathbf{u}_i, \mathbf{u}_j, \mathbf{u}_k]) \overset{\text{a.a.s.}}{=} \min\{3(m + m'), d\}. \tag{305}$$

Since

$$\begin{aligned}
&\text{rk}([\mathbf{u}_i, \mathbf{u}_j, \mathbf{u}_k]) - \text{rk}([\mathbf{u}_j, \mathbf{u}_k, \mathbf{v}'_i]) \\
&= \text{rk}([\mathbf{u}_j, \mathbf{u}_k]) + \text{rk}(\mathbf{u}_i) - \text{rk}(\mathbf{u}_{i(j,k)}) \\
&\quad - [\text{rk}([\mathbf{u}_j, \mathbf{u}_k]) + \text{rk}(\mathbf{v}'_i) - \text{rk}([\mathbf{u}_j, \mathbf{u}_k] \cap \mathbf{v}'_i)] && (306) \\
&= \text{rk}([\mathbf{u}_j, \mathbf{u}_k]) + \text{rk}(\mathbf{u}_i) - \text{rk}(\mathbf{u}_{i(j,k)}) - \\
&\quad [\text{rk}([\mathbf{u}_j, \mathbf{u}_k]) + \text{rk}(\mathbf{v}'_i) - \text{rk}([\mathbf{u}_j, \mathbf{u}_k] \cap \mathbf{u}_i \cap \mathbf{v}'_i)] && (307) \\
&= \text{rk}(\mathbf{u}_i) - [\text{rk}(\mathbf{u}_{i(j,k)}) + \text{rk}(\mathbf{v}'_i) - \text{rk}(\mathbf{u}_{i(j,k)} \cap \mathbf{v}'_i)] && (308) \\
&= \text{rk}(\mathbf{u}_i) - \text{rk}([\mathbf{v}'_i, \mathbf{u}_{i(j,k)}]), && (309)
\end{aligned}$$

it follows that

$$\begin{aligned}
&\text{rk}([\mathbf{v}'_i, \mathbf{u}_{i(j,k)}]) \\
&\overset{\text{a.a.s.}}{=} \min\{m + m', d\} - \min\{3(m + m'), d\} \\
&\qquad + \min\{2m + 3m', d\} && (310) \\
&= \min\{m' + \gamma_1, m + m', d\} && (311)
\end{aligned}$$

which proves the result for **C6**.

B. Condition C4

To see that **C4** holds a.a.s., we need the following lemma.

Lemma 4: Let $A \in \mathbb{F}_{p^n}^{d \times \mu'}$, $B, C \in \mathbb{F}_{p^n}^{d \times \mu}$, such that $\mu' \leq \mu$. Denote

$$M = \begin{bmatrix} A & B & \mathbf{0} \\ A & \mathbf{0} & C \end{bmatrix}. \tag{312}$$

If the elements of A, B, C are chosen i.i.d uniform, then M has full rank $\min\{2d, \mu' + 2\mu\}$ a.a.s.

Proof: Consider the following cases.

1) If $2d \geq \mu' + 2\mu$, which implies $\mu' \leq \mu \leq d$ and thus $\mu' + \mu \leq 2d$. Let $P_1 = \det([M, Z])$, where $Z \in \mathbb{F}_q^{2d \times (2d - (\mu' + 2\mu))}$, be a polynomial in the elements of A, B, C, Z. To verify that it is not the zero polynomial, consider the following realizations of A, B, C, Z for which $P_1 \neq 0$. Let $A = \mathbf{I}^{d \times d}_{[1:\mu']}$, $B = C = \mathbf{I}^{d \times d}_{[\mu'+1:\mu]}$. Let $v_a \in \mathbb{F}_q^{\mu' \times 1}$, $v_b, v_c \in \mathbb{F}_q^{\mu \times 1}$. Then $M[v_a, v_b, v_c]^T = \mathbf{0} \implies ([A, B][v_a, v_b]^T = \mathbf{0}) \wedge ([A, C][v_a, v_c]^T = \mathbf{0}) \implies v_a = v_b = v_c = \mathbf{0}$. Therefore, M has independent columns. Let $Z = (\mathbf{I}^{d \times d} | M) \in \mathbb{F}_q^{2d \times [2d - (\mu' + 2\mu)]}$, so that $[M, Z]$ has full rank, which yields a non-zero evaluation for P_1. Now, since P_1 is not the zero-polynomial, if the elements of A, B, C, Z are chosen i.i.d uniform, then by Schwartz-Zippel Lemma, we obtain that as $n \to \infty$, the evaluation of P_1 is almost surely non-zero, which implies that $\text{rk}(M) \overset{\text{a.a.s.}}{=} \mu' + 2\mu$.
2) If $2\mu \leq 2d < \mu' + 2\mu$, then we have $2\mu - d > d - \mu' \geq d - \mu \geq 0$. Let $P_2 = \det([M^T, Z^T]^T)$, where $Z \in \mathbb{F}_q^{(\mu' + 2\mu - 2d) \times (\mu' + 2\mu)}$. Let $I_1 = \mathbf{I}^{d \times d}_{[1:2\mu - d]}$, $I_2 = \mathbf{I}^{d \times d}_{[2\mu - d + 1:\mu]}$, $I_3 = \mathbf{I}^{d \times d}_{[\mu + 1:d]}$, $B = [I_1, I_2]$, $C = [I_1, I_3]$, $A_0 = [I_2, I_3]$. Then we have $\langle A_0 \cap B \cap C \rangle = \{\mathbf{0}\}$, which implies that the following matrix has full rank.

$$M_0^{2d \times 2d} = \begin{bmatrix} A_0 & B & \mathbf{0} \\ A_0 & \mathbf{0} & C \end{bmatrix}. \tag{313}$$

To see this, let $v_a \in \mathbb{F}_q^{(2d - 2\mu) \times 1}$, $v_b, v_c \in \mathbb{F}_q^{\mu \times 1}$. Then $M_0 v = M_0[v_a, v_b, v_c]^T = 0 \implies A_0 v_a = -B v_b = -C v_c \in \langle A_0 \cap B \cap C \rangle$. Since A_0, B, C have only trivial intersection, the only solution for v is 0. Letting $A = [\mathbf{0}^{d \times (\mu' + 2\mu - 2d)}, A_0]$, we obtain that M has $2d$ linearly independent rows. Let $Z^T = (\mathbf{I}^{d \times d} | M^T) \in \mathbb{F}_q^{(\mu' + 2\mu - 2d) \times (\mu' + 2\mu)}$, which is constituted by $(\mu' + 2\mu - 2d)$ rows of $\mathbf{I}^{(\mu' + 2\mu) \times (\mu' + 2\mu)}$, so that $\left[M^T, Z^T\right]^T$ has full rank. Therefore, P_2 is not the zero polynomial. By Schwartz-Zippel Lemma, we obtain that for i.i.d. uniform A, B, C, Z, as $n \to \infty$, P_2 will evaluate to a non-zero value almost surely, which implies that $\text{rk}(M) \overset{\text{a.a.s.}}{=} 2d$.
3) If $d < \mu$, then by Lemma 1, we have that $\text{rk}(B) = \text{rk}(C) = d \implies \text{rk}(M) \geq 2d$ holds asymptotically almost surely. Since M has $2d$ rows, we conclude that $\text{rk}(M) \overset{\text{a.a.s.}}{=} 2d$.

■

In Lemma 4 let

$$M = \begin{bmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \mathbf{0} \\ \mathbf{u}_1 & \mathbf{0} & \mathbf{u}_3 \end{bmatrix}. \tag{314}$$

We obtain that $\text{rk}(M) \overset{\text{a.a.s.}}{=} \min\{3(m+m'), 2d\}$. It then follows from [61] that,

$$\begin{aligned}
&\text{rk}(\mathbf{u}_{123}) = \text{rk}(\mathbf{u}_1 \cap \mathbf{u}_2 \cap \mathbf{u}_3) && (315)\\
&= \text{rk}(\mathbf{u}_1) + \text{rk}(\mathbf{u}_2) + \text{rk}(\mathbf{u}_3) - \text{rk}(M) && (316)\\
&\overset{\text{a.a.s.}}{=} 3\min\{(m+m'), d\} - \min\{3(m+m'), 2d\} && (317)\\
&= \gamma_3, && (318)
\end{aligned}$$

Then applying Lemma 4 to

$$M = \begin{bmatrix} \mathbf{v}_1' & \mathbf{u}_2 & \mathbf{0} \\ \mathbf{v}_1' & \mathbf{0} & \mathbf{u}_3 \end{bmatrix}, \tag{319}$$

we obtain that $\text{rk}(M') \overset{\text{a.a.s.}}{=} \min\{2m+3m', 2d\}$. By [61],

$$\begin{aligned}
&\text{rk}(\mathbf{v}_1' \cap \mathbf{u}_{123}) = \text{rk}(\mathbf{v}_1' \cap \mathbf{u}_2 \cap \mathbf{u}_3) && (320)\\
&= \text{rk}(\mathbf{v}_1') + \text{rk}(\mathbf{u}_2) + \text{rk}(\mathbf{u}_3) - \text{rk}(M') && (321)
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\text{rk}([\mathbf{v}_1', \mathbf{u}_{123}]) && (322)\\
&= \text{rk}(\mathbf{v}_1') + \text{rk}(\mathbf{u}_{123}) - \text{rk}(\mathbf{v}_1' \cap \mathbf{u}_{123}) && (323)\\
&= \text{rk}(\mathbf{u}_{123}) - \text{rk}(\mathbf{u}_2) - \text{rk}(\mathbf{u}_3) + \text{rk}(M') && (324)\\
&\overset{\text{a.a.s.}}{=} \gamma_3 - 2\min\{m+m', d\} + \min\{2m+3m', 2d\} && (325)\\
&= \min\{m' + \gamma_3, m+m', d\} && (326)
\end{aligned}$$

C. Condition C5

Finally let us prove for **C5**. In Lemma 1, let $M = [\mathbf{u}_i, \mathbf{u}_j]$. We have

$$\text{rk}([\mathbf{u}_i, \mathbf{u}_j]) \overset{\text{a.a.s.}}{=} \min\{2(m+m'), d\}, \tag{327}$$

By the result for **C2** and (327), we have that for distinct $i, j \in [1:3]$,

$$\begin{aligned}
&\text{rk}(\mathbf{u}_{ij}) = \text{rk}(\mathbf{u}_i) + \text{rk}(\mathbf{u}_j) - \text{rk}([\mathbf{u}_i, \mathbf{u}_j]) && (328)\\
&\overset{\text{a.a.s.}}{=} 2\min\{m+m', d\} - \min\{2(m+m'), d\} && (329)\\
&= \big(\min\{2(m+m') - d, m+m', d\}\big)^+ && (330)\\
&= \gamma_2 && (331)
\end{aligned}$$

To prove that **C5** holds asymptotically almost surely, due to symmetry, it suffices to prove for $i=1, j=2, k=3$. Let us consider the following cases.

If $\gamma_2 = 0$, then we almost surely have $\text{rk}([\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]) = \text{rk}(\mathbf{v}_1') = \min\{m', d\} = \min\{m'+2\gamma_2, m+m', d\}$, as desired. Otherwise, let us consider two sub-cases.

1) $\gamma_2 = \min\{m+m', d\} > 0$. By **C2**,

$$\text{rk}([\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]) \le \text{rk}(\mathbf{u}_1) \overset{\text{a.a.s.}}{=} \min\{m+m', d\} \tag{332}$$

On the other hand, by **C3**,

$$\begin{aligned}
\text{rk}([\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]) &\ge \text{rk}([\mathbf{v}_1', \mathbf{u}_{12}])\\
&\overset{\text{a.a.s.}}{=} \min\{m+\gamma_2, m+m', d\} && (333)\\
&= \min\{m+m', d\} && (334)
\end{aligned}$$

This implies that

$$\begin{aligned}
\text{rk}([\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]) &\overset{\text{a.a.s.}}{=} \min\{m+m', d\}\\
&= \min\{m' + 2\gamma_2, m+m', d\} && (335)
\end{aligned}$$

as desired.

2) $\gamma_2 = 2(m+m') - d > 0$. This implies that $m+m' \le d < 2(m+m')$. Denote $A = \mathbf{u}_1$, $B = \mathbf{u}_2$, $C = \mathbf{u}_3$. Then $\mathbf{v}_1' = A_{[1:m']}$. Denote $a = d - (m+m')$, and let

$$\begin{aligned}
D &= [A, \mathbf{0}^{d\times a}][A, B_{[1:a]}]^* B_{[a+1:m+m']}, && (336)\\
E &= [A, \mathbf{0}^{d\times a}][A, C_{[1:a]}]^* C_{[a+1:m+m']}. && (337)
\end{aligned}$$

Recall that M^* denotes the adjoint matrix of the square matrix M. We claim that $\langle D\rangle \subset \langle \mathbf{u}_{12}\rangle$ and $\langle E\rangle \subset \langle \mathbf{u}_{13}\rangle$. It is obvious that $\langle D\rangle \subset \langle \mathbf{u}_1\rangle$ and $\langle E\rangle \subset \langle \mathbf{u}_1\rangle$. To see that $\langle D\rangle \subset \langle \mathbf{u}_2\rangle$ and $\langle E\rangle \subset \langle \mathbf{u}_3\rangle$, note that

$$\begin{aligned}
&D + [\mathbf{0}^{d\times(m+m')}, B_{[1:a]}][A, B_{[1:a]}]^* B_{[a+1:m+m']} && (338)\\
&= [A, B_{[1:a]}][A, B_{[1:a]}]^* B_{[a+1:m+m']} && (339)\\
&= \det([A, B_{[1:a]}]) B_{[a+1:m+m']}, && (340)
\end{aligned}$$

where we used the fact that for any square matrix M, the product of M and its adjoint M^* is equal to the product of the determinant of M and the identity matrix. Thus, every column of D is a linear combination of the columns of $B = \mathbf{u}_2$, which implies that $\langle D\rangle \subset \langle \mathbf{u}_2\rangle$. Similarly,

$$\begin{aligned}
&E + [\mathbf{0}^{d\times(m+m')}, C_{[1:a]}][A, C_{[1:a]}]^* C_{[a+1:m+m']} && (341)\\
&= \det([A, C_{[1:a]}]) C_{[a+1:m+m']}, && (342)
\end{aligned}$$

which implies that $\langle E\rangle \subset \langle \mathbf{u}_3\rangle$.

Let us now show that $\text{rk}([A_{[1:m']}, D, E]) \ge \min\{m' + 2\gamma_2, m+m'\}$ holds asymptotically almost surely. Denote $b = \min\{m, \gamma_2\}$ and $c = \min\{m, 2\gamma_2\}$. Let $Z \in \mathbb{F}_q^{d\times(d-m'-c)}$. The following determinant is a polynomial in the elements of (A, B, C, Z).

$$P = \det([A_{[1:m']}, D_{[1:b]}, E_{[1:(c-b)]}, Z]). \tag{343}$$

To prove that this is not the zero polynomial, let

$$\begin{aligned}
&I_1 = \mathbf{I}^{d\times d}_{[1:m']}, && I_2 = \mathbf{I}^{d\times d}_{[m'+1:m'+b]},\\
&I_3 = \mathbf{I}^{d\times d}_{[m'+b+1:m'+c]}, && I_4 = \mathbf{I}^{d\times d}_{[m'+c+1:m'+m]},\\
&I_5 = \mathbf{I}^{d\times d}_{[m+m'+1:d]}, && (344)
\end{aligned}$$

and then consider the following evaluation,

$$\begin{aligned}
A = [I_1, I_2, I_3, I_4] &\implies A' = I_1, && (345)\\
B &= [I_5, I_2, \mathbf{0}^{d\times(\gamma_2-b)}], && (346)\\
C &= [I_5, I_3, \mathbf{0}^{d\times(\gamma_2-c+b)}], && (347)\\
Z &= [I_4, I_5]. && (348)
\end{aligned}$$

Note that $[A, B_{[1:a]}] = [A, C_{[1:a]}] = [I_1, I_2, I_3, I_4, I_5] = \mathbf{I}^{d\times d}$. Thus,

$$\begin{aligned}
D &= [A, \mathbf{0}] B_{[a+1:m+m']} && (349)\\
&= [I_1, I_2, I_3, I_4, \mathbf{0}^{d\times a}][I_2, \mathbf{0}^{d\times(\gamma_2-b)}] && (350)\\
&= [I_2, \mathbf{0}^{d\times(\gamma_2-b)}], && (351)
\end{aligned}$$

which implies that $D_{[1:b]} = I_2$. Similarly,

$$\begin{aligned}
E &= [A, \mathbf{0}] C_{[a+1:m+m']} && (352)\\
&= [I_1, I_2, I_3, I_4, \mathbf{0}][I_3, \mathbf{0}^{d\times(\gamma_2-c+b)}] && (353)\\
&= [I_3, \mathbf{0}^{d\times(\gamma_2-c+b)}], && (354)
\end{aligned}$$

which implies that $E_{[1:(c-b)]} = I_3$.

Therefore $P = \det([I_1, I_2, I_3, I_4, I_5]) = \det(\mathbf{I}^{d\times d}) = 1 \neq 0$. Since P is not the zero polynomial, by Schwartz-Zippel Lemma, we obtain that $\text{rk}([A', D, E]) \geq m' + b + (c - b) = m' + c = \min\{m' + 2\gamma_2, m + m'\}$ holds asymptotically almost surely. This implies that $\text{rk}([\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]) \overset{\text{a.a.s.}}{\geq} \min\{m' + 2\gamma_2, m + m'\}$. Since $\text{rk}(\mathbf{v}_1') \overset{\text{a.a.s.}}{=} m'$, $\text{rk}(\mathbf{u}_{12}) = \text{rk}(\mathbf{u}_{13}) \overset{\text{a.a.s.}}{=} \gamma_2$, from the result for **C1** and (328) and note that $\langle[\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]\rangle \subset \langle \mathbf{u}_1\rangle$, we conclude that $\text{rk}([\mathbf{v}_1', \mathbf{u}_{12}, \mathbf{u}_{13}]) \overset{\text{a.a.s.}}{=} \min\{m' + 2\gamma_2, m + m'\} = \min\{m' + 2\gamma_2, m + m', d\}$.

Therefore, $\mathbf{Ci}, \mathbf{i} \in [6]$ holds asymptotically almost surely. We conclude that E_n holds asymptotically almost surely. The proof is completed by evaluating (15) of [38] with conditions **C1** to **C6** to get Δ_g^* for the symmetric GLCBC with $K \leq 3$.

Appendix IV
Proof of Lemma 1

If $d \geq \mu' + \mu$, let $Z \in \mathbb{F}_{p^n}^{d\times(d-\mu'-\mu)}$. Then $P = \det([M', M, Z])$ is a non-zero polynomial in the elements of M and Z. To see this, let $[M, Z] = \mathbf{I}^{d\times d}|M'$, which will then yield that $\det([M', M, Z]) \neq 0$ since $\langle[M', (\mathbf{I}^{d\times d}|M')]\rangle = \langle\mathbf{I}^{d\times d}\rangle$. By Schwartz-Zippel Lemma, if the elements of M and Z are chosen i.i.d uniform, $\Pr(P \neq 0) \geq 1 - \frac{\text{degree of } P}{p^n} \geq 1 - \frac{d}{p^n} \to 1$ as $n \to \infty$, which implies that the probability that $[M', M]$ has full rank $\mu' + \mu$ goes to 1 as $n \to \infty$. If $d < \mu' + \mu$, denote by M_1 the first $d - \mu'$ columns of M. It suffices to show that $\text{rk}([M', M_1]) \overset{\text{a.a.s.}}{=} d$. Note that $P = \det([M', M_1])$ is a non-zero polynomial in the elements of M_1, and thus M. To see this, let $M_1 = \mathbf{I}^{d\times d}|M'$, which will then similarly yield that $\det([M', M_1]) \neq 0$. By Schwartz-Zippel Lemma, if the elements of M_1 are chosen i.i.d uniform, $\Pr(P \neq 0) \geq 1 - \frac{\text{degree of } P}{p^n} \geq 1 - \frac{d}{p^n} \to 1$ as $n \to \infty$, which implies that $\text{rk}([M', M_1]) \overset{\text{a.a.s.}}{=} d$ as desired. □

References

[1] S. Research. (Jul. 2020). *The Next Hyper—Connected Experience for All*. [Online]. Available: https://cdn.codeground.org/nsr/downloads/researchareas/6GVision.pdf

[2] C. Shannon, "The zero error capacity of a noisy channel," *IEEE Trans. Inf. Theory*, vol. IT-2, no. 3, pp. 8–19, Sep. 1956.

[3] J. Körner, "Coding of an information source having ambiguous alphabet and the entropy of graphs," in *Proc. 6th Prague Conf. Inf. Theory*, 1973, pp. 411–425.

[4] H. Witsenhausen, "The zero-error side information problem and chromatic numbers (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 5, pp. 592–593, Sep. 1976.

[5] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[6] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.

[7] V. Doshi, D. Shah, M. Médard, and M. Effros, "Functional compression through graph coloring," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3901–3917, Aug. 2010.

[8] S. Feizi and M. Medard, "On network functional compression," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5387–5401, Sep. 2014.

[9] S. Choi and S. S. Pradhan, "A graph-based framework for transmission of correlated sources over broadcast channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 2841–2856, Jul. 2008.

[10] T. Han and M. Costa, "Broadcast channels with arbitrarily correlated sources," *IEEE Trans. Inf. Theory*, vol. IT-33, no. 5, pp. 641–650, Sep. 1987.

[11] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 2, pp. 219–221, Mar. 1979.

[12] B. K. Rai and B. K. Dey, "On network coding for sum-networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 50–63, Jan. 2012.

[13] A. Tripathy and A. Ramamoorthy, "Sum-networks from incidence structures: Construction and capacity analysis," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3461–3480, May 2018.

[14] C. Huang, Z. Tan, S. Yang, and X. Guang, "Comments on cut-set bounds on network function computation," *IEEE Trans. Inf. Theory*, vol. 64, no. 9, pp. 6454–6459, Sep. 2018.

[15] X. Guang, R. W. Yeung, S. Yang, and C. Li, "Improved upper bound on the network function computing capacity," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3790–3811, Jun. 2019.

[16] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[17] S. Kadhe, N. Rajaraman, O. O. Koyluoglu, and K. Ramchandran, "FastSecAgg: Scalable secure aggregation for privacy-preserving federated learning," 2020, *arXiv:2009.11248*.

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

[19] A. Heidarzadeh and A. Sprintson, "Private computation with side information: The single-server case," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1657–1661.

[20] V. Cadambe and P. Grover, "Codes for distributed computing: A tutorial," *IEEE Inf. Theory Soc. Newslett.*, vol. 67, no. 4, pp. 3–15, Dec. 2017.

[21] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and S. Avestimehr, "Lagrange coded computing: Optimal design for resiliency, security and privacy," 2018, *arXiv:1806.00939*.

[22] J. S. Ng et al., "A comprehensive survey on coded distributed computing: Fundamentals, challenges, and networking applications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1800–1837, 3rd Quart., 2021.

[23] S. Li, M. A. Maddah-Ali, Q. Yu, and A. S. Avestimehr, "A fundamental tradeoff between computation and communication in distributed computing," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 109–128, Jan. 2018.

[24] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "Straggler mitigation in distributed matrix multiplication: Fundamental limits and optimal coding," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1920–1933, Mar. 2020.

[25] S. Dutta, M. Fahim, F. Haddadpour, H. Jeong, V. Cadambe, and P. Grover, "On the optimal recovery threshold of coded matrix multiplication," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 278–301, Jan. 2020.

[26] S. Dutta, Z. Bai, H. Jeong, T. Meng Low, and P. Grover, "A unified coded deep neural network training strategy based on generalized PolyDot codes for matrix multiplication," 2018, *arXiv:1811.10751*.

[27] Z. Jia and S. A. Jafar, "On the capacity of secure distributed batch matrix multiplication," *IEEE Trans. Inf. Theory*, vol. 67, no. 11, pp. 7420–7437, Nov. 2021.

[28] H. Sun and S. A. Jafar, "On the capacity of computation broadcast," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3417–3434, Jun. 2020.

[29] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, "Index coding with side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.

[30] H. Maleki, V. R. Cadambe, and S. A. Jafar, "Index coding—An interference alignment perspective," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5402–5432, Sep. 2014.

[31] F. Arbabjolfaei and Y.-H. Kim, "Fundamentals of index coding," *Found. Trends Commun. Inf. Theory*, vol. 14, nos. 3–4, pp. 163–346, 2018, doi: 10.1561/0100000094.

[32] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "The exact rate-memory tradeoff for caching with uncoded prefetching," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 1281–1296, Feb. 2018.

[33] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, May 2014.

[34] K. Wan, H. Sun, M. Ji, D. Tuninetti, and G. Caire, "Cache-aided general linear function retrieval," *Entropy*, vol. 23, no. 1, p. 25, Dec. 2020. [Online]. Available: https://www.mdpi.com/1099-4300/23/1/25

[35] P. W. Cuff, H. H. Permuter, and T. M. Cover, "Coordination capacity," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4181–4206, Sep. 2010.

[36] P. Fei, Z. Chen, Z. Wang, and S. A. Jafar, "Communication-efficient clock synchronization," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 2592–2597.

[37] J. Ruan and D. Xie, "Networked VR: State of the art, solutions, and challenges," *Electronics*, vol. 10, no. 2, p. 166, Jan. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/2/166

[38] Y. Yao and S. A. Jafar, "The capacity of 3 user linear computation broadcast," 2022, *arXiv:2206.10049*.

[39] M. Effros, S. E. Rouayheb, and M. Langberg, "An equivalence between network coding and index coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2478–2487, May 2015.

[40] E. Lubetzky and U. Stav, "Nonlinear index coding outperforming the linear optimum," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3544–3551, Aug. 2009.

[41] S. E. Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.

[42] H. Sun and S. A. Jafar, "Index coding capacity: How far can one go with only Shannon inequalities?" *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3041–3055, Jun. 2015.

[43] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, "Generic-case complexity, decision problems in group theory, and random walks," *J. Algebra*, vol. 264, no. 2, pp. 665–694, Jun. 2003.

[44] A. R. Meyer and M. S. Paterson, "With what frequency are apparently intractable problems difficult?" MIT, Cambridge, MA, USA, Tech. Rep. MIT/LCS/TM-126, 1979.

[45] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of the K user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[46] A. S. Motahari, S. Oveis-Gharan, M.-A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4799–4810, Aug. 2014.

[47] R. Gül, D. Stotz, S. A. Jafar, H. Bölcskei, and S. Shamai (Shitz), "Canonical conditions for $K/2$ degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 68, no. 3, pp. 1716–1730, Mar. 2022.

[48] M. Razaviyayn, M. Sanjabi, and Z. Luo, "Linear transceiver design for interference alignment: Complexity and computation," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2896–2910, May 2012.

[49] C. Wang, T. Gou, and S. A. Jafar, "Subspace alignment chains and the degrees of freedom of the three-user MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2432–2479, May 2014.

[50] C. Wang, H. Sun, and S. A. Jafar, "Genie chains: Exploring outer bounds on the degrees of freedom of MIMO interference networks," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5573–5602, Oct. 2016.

[51] T. Tao, "Sumset and inverse sumset theory for Shannon entropy," *Combinatorics, Probab. Comput.*, vol. 19, no. 4, pp. 603–639, Jul. 2010.

[52] I. Kontoyiannis and M. Madiman, "Sumset and inverse sumset inequalities for differential entropy and mutual information," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4503–4514, Aug. 2014.

[53] Y.-C. Chan, J. Wang, and S. A. Jafar, "Toward an extremal network theory—Robust GDoF gain of transmitter cooperation over TIN," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3827–3845, Jun. 2020.

[54] T. Tao, *Topics in Random Matrix Theory*, vol. 132. Providence, RI, USA: American Mathematical Society, 2012.

[55] R. Gilman, A. G. Miasnikov, A. Myasnikov, and A. Ushakov, "Report on generic case complexity," 2007, *arXiv:0707.1364*.

[56] H. Sun, T. Gou, and S. Jafar, "Degrees of freedom of MIMO X networks: Spatial scale invariance, one-sided decomposability and linear feasibility," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8377–8385, Dec. 2013.

[57] V. R. Cadambe, S. A. Jafar, H. Maleki, K. Ramchandran, and C. Suh, "Asymptotic interference alignment for optimal repair of MDS codes in distributed storage," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2974–2987, May 2013.

[58] C. Meng, A. K. Das, A. Ramakrishnan, S. A. Jafar, A. Markopoulou, and S. Vishwanath, "Precoding-based network alignment for three unicast sessions," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 426–451, Jan. 2015.

[59] Y. Yao and S. A. Jafar, "Capacity of 3-user linear computation broadcast over F_q with 1D demand and side-information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2022, pp. 1151–1156.

[60] J. Wang, Z. Jia, and S. A. Jafar, "Price of precision in coded distributed matrix multiplication: A dimensional analysis," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2021, pp. 1–6.

[61] Y. Tian, "The dimension of intersection of k subspaces," *Missouri J. Math. Sci.*, vol. 14, no. 2, pp. 92–95, May 2002.

Yuhang Yao (Graduate Student Member, IEEE) received the B.E. degree in communications engineering from Sun Yat-sen University, China, in 2021, and the M.S. degree in electrical and computer engineering from the University of California at Irvine, CA, USA, in 2024, where he is currently pursuing the Ph.D. degree. His research interests include information theory, quantum information theory and their applications to distributed computation, security, and privacy.

Syed A. Jafar (Fellow, IEEE) received the B.Tech. degree in electrical engineering from IIT Delhi, India, in 1997, the M.S. degree in electrical engineering from Caltech, USA, in 1999, and the Ph.D. degree in electrical engineering from Stanford University, USA, in 2003. His industry experience includes positions with the Lucent Bell Laboratories and Qualcomm. He is currently a Chancellor's Professor in electrical engineering and computer science with the University of California at Irvine, Irvine, CA, USA. His research interests include multiuser information theory, wireless communications, and network coding.

He was a recipient of New York Academy of Sciences Blavatnik National Laureate in Physical Sciences and Engineering, the NSF CAREER Award, the ONR Young Investigator Award, the UCI Academic Senate Distinguished Mid-Career Faculty Award for Research, the School of Engineering Mid-Career Excellence in Research Award, and the School of Engineering Maseeh Outstanding Research Award. His coauthored papers have received the IEEE Information Theory Society Paper Award, IEEE Communication Society and Information Theory Society Joint Paper Award, IEEE Communications Society Best Tutorial Paper Award, IEEE Communications Society Heinrich Hertz Award, IEEE Signal Processing Society Young Author Best Paper Award, IEEE Information Theory Society Jack Wolf ISIT Best Student Paper Award, and three IEEE GLOBECOM Best Paper Awards. He received the UC Irvine EECS Professor of the Year award six times from the Engineering Students Council, the School of Engineering Teaching Excellence Award in 2012, and the Senior Career Innovation in Teaching Award in 2018. He was an University of Canterbury Erskine Fellow, an IEEE Communications Society Distinguished Lecturer, an IEEE Information Theory Society Distinguished Lecturer, and a Thomson Reuters/Clarivate Analytics Highly Cited Researcher. He served as an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS (2004–2009), IEEE COMMUNICATIONS LETTERS (2008–2009), and IEEE TRANSACTIONS ON INFORMATION THEORY (2009–2012).