

# Quantum $X$ -Secure $T$ -Private Information Retrieval From MDS Coded Storage With Unresponsive and Byzantine Servers

Yuxiang Lu and Syed A. Jafar

Center for Pervasive Communications and Computing (CPCC)

University of California Irvine, Irvine, CA 92697

*Email: {yuxiang.lu, syed}@uci.edu*

## Abstract

A communication-efficient protocol is introduced over a many-to-one quantum network for Q-E-B-MDS-X-TPIR, i.e., quantum private information retrieval with MDS- $X$ -secure storage and  $T$ -private queries. The protocol is resilient to any set of up to  $E$  unresponsive servers (erased servers or stragglers) and any set of up to  $B$  Byzantine servers. The underlying coding scheme incorporates an enhanced version of a Cross Subspace Alignment (CSA) code, namely a Modified CSA (MCSA) code, into the framework of CSS codes. The error-correcting capabilities of CSS codes are leveraged to encode the dimensions that carry desired computation results from the MCSA code into the error space of the CSS code, while the undesired interference terms are aligned into the stabilized code space. The challenge is to do this efficiently while also correcting quantum erasures and Byzantine errors. The protocol achieves superdense coding gain over comparable classical baselines for Q-E-B-MDS-X-TPIR, recovers as special cases the state of art results for various other quantum PIR settings previously studied in the literature, and paves the way for applications in quantum coded distributed computation, where CSA code structures are important for communication efficiency, while security and resilience to stragglers and Byzantine servers are critical.

## Index Terms

Coded storage, PIR, QMAC, security.

The results of this work were presented in part at IEEE ICC 2024 [34]. See Section I-B for details.

## I. INTRODUCTION

Recent interest in entanglement assisted computation over quantum many to one (also referred to as quantum multiple access (QMAC)) networks adds fundamentally novel dimensions to the rapidly expanding theory of distributed communication and computation, beyond its classical cornerstones such as secret-sharing [1]–[4], private information retrieval (PIR) [5]–[11], coded distributed computation and computation networks [12]–[14], and secure multiparty computation [15]–[19]. Ideas from these diverse perspectives are encapsulated in a variety of specialized coding structures — Reed-Solomon (RS) codes [20], Cross Subspace Alignment (CSA) codes [21], Lagrange Coded Computing [12], and CSS codes [22], [23], to name a few. Assimilating the specialized coding structures is essential for a *unified* theory that can facilitate a broader array of applications. This work represents such an endeavor, with the goal of developing a communication-efficient coding scheme (i.e., an efficient protocol) for Q-E-B-MDS-X-TPIR [21], i.e., quantum  $X$ -secure<sup>1</sup>  $T$ -private information retrieval from MDS coded storage that is resilient to up to  $E$  unresponsive servers (equivalently referred to as erased servers) and up to  $B$  Byzantine servers.<sup>2</sup>

In the Q-E-B-MDS-X-TPIR [21] setting as shown in Fig. 1 there are  $N$  servers equipped *beforehand* (independent of the classical data) with optimally entangled quantum systems. Upon the commencement of the protocol, there are  $K$  *classical* messages  $W_1, \dots, W_K$  (files, datasets) that are distributed among the servers in an MDS coded and  $X$ -secure fashion. MDS coding implies that the messages together with some classical randomness  $Z$  (needed for security) are coded such that the storage size at each server is only a fraction  $1/K_c$  of the original size of the  $K$  messages.  $X$ -security means that even if any set of up to  $X$  servers collude they can learn nothing about the messages. A user (with its own private randomness  $Z'$ ) wishes to

<sup>1</sup> $X$ -security is a secret-sharing constraint. The messages are the secret and the storage at each server is its share of the secret, such that any set of up to  $X$  shares reveal nothing about the secret. There is another form of security, server secrecy [4], [9], [10], which requires that the user must not learn anything about any other message besides its desired message (also referred to as DB-privacy or symmetric privacy). Note that  $X$ -security is not related to server secrecy, and that we consider only the former ( $X$ -security) in this work.

<sup>2</sup>When assembled with ‘PIR’, the abbreviation ‘Q’ stands for ‘Quantum’ (without ‘Q’, the setting is classical by default), ‘E’ stands for upto  $E$  erased servers ( unresponsive servers), ‘B’ stands for upto  $B$  Byzantine servers, ‘MDS’ stands for MDS coded storage, ‘X’ stands for  $X$ -secure storage (so that up to  $X$  colluding servers can learn nothing about the realizations of the **stored messages**) and ‘T’ stands for  $T$ -privacy constraint (so that up to  $T$  colluding servers can learn nothing about which message is desired).

efficiently retrieve the  $\theta^{th}$  message ( $\theta \in [K]$ ) by querying the  $N$  servers in a  $T$ -private fashion.  $T$ -privacy means that even if any set of up to  $T$  servers collude they can learn nothing about which message is desired by the user. The efficiency of the protocol is measured by the *rate*, defined as the number of desired message bits retrieved per *qubit* (a  $d$ -dimensional quantum system (sometimes called a *qudit*) corresponds to  $\log_2(d)$  qubits) of total download from the servers. Each server generates its response based on the user's queries and the storage available to that server, and encodes it into its own quantum system through local quantum operations. The quantum systems are then sent as answers from the servers to the user. The protocol must tolerate up to  $E$  unresponsive servers, i.e., any set of up to  $E$  servers may be unresponsive, equivalently their answers are erased over the QMAC. The protocol must also tolerate any set of up to  $B$  Byzantine servers whose answers are subject to *arbitrary* errors. Note that while the user's queries are sent without knowledge of which servers may turn out to be unresponsive, once the user receives the quantum systems in response, it knows which servers' answers were erased (known-position error), i.e, which servers did not respond. The identities of the Byzantine servers are not directly revealed to the user from the answers. This corresponds to unknown-position errors in the context of error correcting codes. Resilience to unresponsive and Byzantine servers means that we require that regardless of which  $E$  servers are erased, and which  $B$  servers are Byzantine, the protocol must allow the user to recover its desired message by measuring the received quantum systems.

Our solution centers around CSS codes and the classical CSA coding scheme originally introduced for X-TPIR, i.e., PIR with  $X$ -secure storage and  $T$ -private queries [24], and subsequently applied to a number of classical variants of PIR, coded computing and private read-write designs for federated submodel learning [25]. The classical CSA scheme was generalized to a quantum CSA scheme for Q-MDS-X-TPIR over the quantum many-to-one network in [26], [27], and its resilience to eavesdroppers was explored in [11].

#### A. Challenges and Contributions

While we focus on Q-E-B-MDS-X-TPIR to motivate the protocol developed in this work, we expect the protocol to be much more broadly relevant. This is because the underlying challenge is how to efficiently transmit CSA coded classical symbols when there are quantum resources shared among servers, some of which can be unresponsive (stragglers) and/or Byzantine. CSA code structures are not limited to PIR. For example, CSA codes feature prominently in the broad

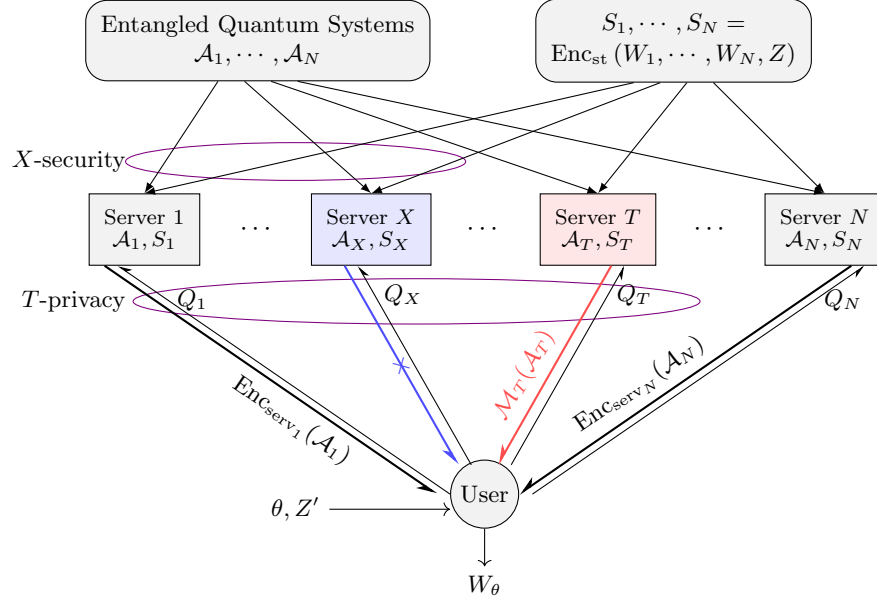


Fig. 1. Q-E-B-MDS-X-TPIR. Quantum systems  $\mathcal{A}_1, \dots, \mathcal{A}_N$  are prepared in an optimally entangled state and distributed to servers in advance. Messages  $W_1, \dots, W_K$ , together with randomness  $Z$  are encoded into  $S_1, \dots, S_N$  in an  $X$ -secure fashion and distributed to  $N$  servers as their storage. To privately retrieve a desired message  $W_\theta$ ,  $\theta \in [K]$ , a user sends to the servers random (based on its local randomness  $Z'$ ) queries  $Q_1, \dots, Q_N$  that are  $T$ -private. Each server locally encodes its response into its quantum system and sends it back to the user. In the figure, unresponsive (blue) server's quantum system is not received, and the Byzantine (red) server applies an arbitrary quantum channel to its quantum system.

area of *coded distributed computation* (CDC) [12], [28]–[30]. Thus, the protocol from this work could potentially be a useful stepping stone towards future studies of quantum CDC (QCDC).<sup>3</sup> Byzantine servers are more challenging in the quantum setting, because the same quantum entanglement that allows gains in communication efficiency under ideal conditions, also makes entangled protocols more susceptible to stragglers and Byzantine adversaries, as their actions impact not only their own quantum systems, but also the overall state of all entangled quantum systems. The challenges are listed as follows.

1) Compared with [26], [27] that studied Q-MDS-X-TPIR, the main challenge is to achieve resilience to unresponsive and Byzantine servers. In classical settings, this is done by having the answers form an error correcting code (ECC) of the desired message symbols (and interfering

<sup>3</sup>The MDS storage can be viewed as coded matrix  $A$ , and the  $T$  private queries as coded matrix  $B$ . The computation of  $AB$  is distributed among servers. The MDS constraint limits upload cost,  $X$ -security/ $T$ -privacy protect against curious servers, and resilience to unresponsive/Byzantine servers guarantees robustness of the distributed computation.

symbols introduced due to various constraints such as  $X$ -security,  $T$ -privacy and MDS storage) so that erasures or errors can be corrected first, after which the desired message symbols can be recovered. This idea is not directly applicable to quantum PIR schemes. Even though QPIR schemes are typically based on the stabilizer formalism [9], [10], [26], the error-correcting capabilities of stabilizer codes are *not* utilized to correct errors. Specifically, instead of the code space of a stabilizer code, in QPIR the information is encoded into the *error space* [31], and is extracted by the user by measuring the qudits (quantum digits, a specific representation of quantum systems that will be explained in Section II-A) with stabilizers to reveal the syndromes. Thus, the received  $N$  answer qudits in QPIR are not in the stabilizer code space, even in the absence of erasures or errors.

2) Compared with [4] that explored Q-TPIR with general access structure that involves resilience to  $E$  unresponsive servers as a special case, the main challenge is to come up with an *efficient* scheme that satisfies  $X$ -security and *MDS storage* constraints. Unlike the random coding based scheme that appears in [4], the CSA code structure is important to accommodate  $X$ -security and *MDS storage*. Note that even in the classical setting, CSA codes allow higher communication rates in PIR with these two constraints (e.g., the CSA code based scheme [21], [24] can achieve higher rates than those achieved without CSA codes in [28], [32]).

3) Utilizing CSA codes further prevents us from placing the answering qudits in the code space of a stabilizer code (without considering the erasure or Byzantine errors). Specifically, the CSA code is the direct sum of a Reed-Solomon code of *interfering/undesired* symbols and a Cauchy RS code of *desired* symbols. It is non-trivial to construct a CSS code upon two CSA codes  $CSA_X, CSA_Z$ , such that  $CSA_X^\perp \subset CSA_Z$ . This is because the dual code of a CSA code should be dual to both the RS part and the Cauchy RS part, whose structures are not trivially compatible. Thus, our main *contribution* is a protocol that utilizes the error-correcting capabilities of CSS codes, i.e., the information carrying ability of their syndromes as the underlying framework. Within this framework, the protocol exploits the RS sub-code of CSA codes to efficiently retrieve the desired computation results (desired message symbols in the PIR problem) that are encoded by *classical* codes,<sup>4</sup> while also tolerating *quantum* erasures and Byzantine errors. Intuitively, in the underlying classical CSA code based protocol, the answers from the servers are viewed

<sup>4</sup>We refer to the desired message symbols as the computation results to emphasize that they are the outcome of the *computation task*, e.g., PIR.

as the RS sub-code of *interfering* symbols, with Cauchy RS code of *desired* message symbols added as “error.” The syndrome of the RS sub-code uniquely identifies the “error” in the Cauchy RS code space together with the actual errors introduced by unresponsive or Byzantine servers. From the quantum perspective, the shared qudits are initially in the code space of the CSS code constructed from the RS sub-codes of two instances of CSA codes. Servers apply Pauli operators to their qudits to encode the answers generated according to the two instances of the CSA code based classical scheme. The Pauli operators’ components that correspond to RS sub-codes of interfering symbols are not detectable since they commute with stabilizers, while the component corresponding to desired message symbols, together with the errors introduced by unresponsive and Byzantine servers, are identified through syndrome measurement. In a nutshell, dimensions that carry desired computation results from the CSA code are encoded into the error space of the CSS code, while the undesired interference terms are aligned into the stabilized code space. A technicality worth noting is that a key enhancement is made to the CSA code, transforming it into a Modified CSA (MCSA) code — whereby the RS sub-code is turned into a GRS sub-code whose dual code is still a GRS code, so that a CSS code can be easily constructed on  $\text{GRS}_X, \text{GRS}_Z$  that are sub-codes of two MCSA codes, where  $\text{GRS}_X^\perp \subset \text{GRS}_Z$ . This ‘MCSA-CSS’ construction can be found in Protocol 3 in this work.

While there is entanglement shared beforehand among the distributed servers (transmitters), it is important to note that the servers do *not* share any entanglement in advance with the user (the receiver). Intuitively, the shared entanglement among transmitters leads to a superdense coding gain in quantum PIR schemes allowing them to achieve in some cases twice the rate of their classical counterparts [9], [10], [26]. The quantum scheme proposed in this paper also achieves the factor of 2 superdense coding gain compared with the classical scheme proposed in [21]. It is also noteworthy that the quantum PIR setting addressed in this paper recovers as *special cases* various other settings considered in the literature, such as Q-B-X-TPIR in [33], Q-E-TPIR in [4], Q-MDS-X-TPIR in [26], Q-MDS-TPIR in [10], and Q-TPIR in [9]. Indeed, the protocol presented in this work achieves the state-of-the-art rates across all of the aforementioned special case scenarios.

### B. Comparison to related works

The most closely related work is the conference version of this paper in [34], [35] where Q-E-X-TPIR problem is studied based on the  $N$ -sum box abstraction of [26]. The conference

version allows neither MDS storage nor resilience to Byzantine servers. The conference version was then developed into a preliminary ArXiv version [36] of this paper where the approach taken for resilience to Byzantine servers that apply arbitrary Pauli errors is to guess the identities of Byzantine servers, treat them as erasures and decode, and check if there exists a set of decoding results that agree. However, the resilience to *arbitrary* Byzantine errors (rather than just Pauli errors) is not explicit under the  $N$ -sum box abstraction. The present version further develops our approach, making the Byzantine resilience explicit. Instead of the  $N$ -sum box abstraction, here we directly utilize the fact that the syndrome measurement of a CSS code can reduce *arbitrary* errors (that affect fewer qudits than its minimum distance) to Pauli errors (Lemma 1).

Let us also note the parallel and independent work in [33] that studies Q-B-X-TPIR through the lens of the  $N$ -sum box abstraction, as further evidence of interest in this problem.

### C. Organization

Section II introduces the notation together with some basic concepts of quantum systems, classical error correcting codes and quantum information. Section III formalizes the Q-E-B-MDS-X-TPIR problem. Section IV presents our main result as Theorem 1. Section V revisits the CSA code based classical E-B-MDS-X-TPIR scheme which is crucial to our construction. A modified CSA code (MCSA code) is presented in Section VI. The quantum protocol, namely MCSA-CSS, that builds upon the MCSA code and a CSS code, is presented in Section VII. Section VIII concludes the paper.

## II. PRELIMINARIES

### A. Miscellaneous

For two integers  $a, b$ , the set  $\{a, a+1, \dots, b\}$  is denoted as  $[a : b]$ . For compact notation,  $[1 : b]$  is denoted as  $[b]$ . For a set  $\mathcal{S}$ ,  $|\mathcal{S}|$  denotes its cardinality, and for any  $k \leq |\mathcal{S}|$ ,  $\binom{\mathcal{S}}{k} \triangleq \{S \mid S \subset \mathcal{S}, |S| = k\}$ . For an  $r \times c$  matrix  $\mathbf{A}$ ,  $\mathbf{A}(\mathcal{A}, \mathcal{B})$  denotes the sub-matrix of  $\mathbf{A}$  whose row indices are in  $\mathcal{A}$  and column indices in  $\mathcal{B}$ .  $\mathcal{A}$  or  $\mathcal{B}$  will be replaced by ‘:’ if they contain all the rows or columns, respectively. If  $\mathbf{A}$  is a vector, we simply write  $\mathbf{A}(\mathcal{S})$  to denote the sub-vector of  $\mathbf{A}$  whose indices are in  $\mathcal{S}$ . For two column vectors  $\mathbf{c}_1, \mathbf{c}_2$ ,  $[\mathbf{c}_1; \mathbf{c}_2] \triangleq [\mathbf{c}_1^\top \ \mathbf{c}_2^\top]^\top$ , i.e., a longer column vector with  $\mathbf{c}_1$  stacked above  $\mathbf{c}_2$ .  $\text{colspan}(\mathbf{A})$  denotes the vector subspace spanned by the columns of  $\mathbf{A}$ . If  $\mathbf{A}$  is a projection matrix, then  $\text{Im}(\mathbf{A}) = \text{colspan}(\mathbf{A})$ .  $\text{ker}(\mathbf{A})$  is the kernel space of  $\mathbf{A}$ .  $\mathbf{A}^\dagger$  is the conjugate transpose of  $\mathbf{A}$ . For a length  $n$  vector  $\mathbf{v} = [v_1 \ v_2 \ \dots \ v_n]^\top$ ,  $\text{Diag}(\mathbf{v})$  denotes

the diagonal  $n \times n$  matrix whose diagonal elements are entries of  $\mathbf{v}$ .  $\text{supp}(\mathbf{v}) \triangleq \{i \mid v_i \neq 0\}$  and  $\text{wt}(\mathbf{v}) \triangleq |\text{supp}(\mathbf{v})|$ .  $\mathbf{I}_N$  is the  $N \times N$  identity matrix. For any random variable that is written in upper case (say,  $Z$ ), we use the corresponding lower case ( $z$ ) to denote its realization. The state of a quantum system  $A$  defined on Hilbert space  $\mathcal{H}_A$  is represented by a density operator  $\rho_A \in \mathcal{D}_A$  where  $\mathcal{D}_A$  is a set of all positive semi-definite operators with trace 1 acting on  $\mathcal{H}_A$ . A pure state can also be represented by a unit vector in  $\mathcal{H}_A$ . For a classical-quantum system  $XA$ ,  $\rho_{A|X=x}$ , or simply  $\rho_{A|x}$ , denotes the density operator of  $A$  conditioned on the realization  $X = x$ . The label of the quantum system in the subscript may be omitted for compact notation if it is clear from the context.  $\mathbb{F}_q$  is a finite field with order  $q$  where  $q = p^r$  is a prime power. The field trace  $\text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\cdot): \mathbb{F}_q \rightarrow \mathbb{F}_p$  is an  $\mathbb{F}_p$ -linear map from  $\mathbb{F}_q$  to  $\mathbb{F}_p$ , and  $\omega \triangleq e^{2\pi\sqrt{-1}/p}$ . If a quantum system  $A$  has dimension  $|A| = q$ , with  $\{|a\rangle\}_{a \in \mathbb{F}_q}$  being its computational basis, we call it a  $q$ -dimensional qudit.

### B. Classical Error Correcting Codes

**Definition 1.**  $[n, k, d]$  Code: An  $[n, k, d]$  classical code over  $\mathbb{F}_q$  is the **column space** of a rank  $k$  generator matrix  $\mathbf{G} \in \mathbb{F}_q^{n \times k}$ , i.e.,  $\mathcal{C} = \text{colspan}(\mathbf{G})$ . It has a rank  $n - k$  parity-check matrix  $\mathbf{H} \in \mathbb{F}_q^{n \times n-k}$  such that  $\mathbf{H}^\top \mathbf{G} = \mathbf{0}$ . The dual code of  $\mathcal{C}$  is  $\mathcal{C}^\perp = \text{colspan}(\mathbf{H})$ . If an  $[n, k, d]$  code satisfies  $d = n - k + 1$ , we call it an  $[n, k]$  MDS (maximum distance separable) code.

**Definition 2.** GRS Code: A Generalized Reed-Solomon Code  $\mathcal{C} = \text{GRS}_{n,k}^{q,(\boldsymbol{\alpha}, \mathbf{u})}$  over  $\mathbb{F}_q$  is the column space of the generator matrix defined in (1) where  $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$  are  $n$  distinct elements in  $\mathbb{F}_q$  and  $\mathbf{u} = (u_1, u_2, \dots, u_n)$  are  $n$  non-zero elements in  $\mathbb{F}_q$ . By definition,  $q \geq n$ .

$$\mathbf{G}_{\text{GRS}_{n,k}^{q,(\boldsymbol{\alpha}, \mathbf{u})}} \triangleq \begin{bmatrix} u_1 & u_1\alpha_1 & \cdots & u_1\alpha_1^{k-1} \\ u_2 & u_2\alpha_2 & \cdots & u_2\alpha_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ u_n & u_n\alpha_n & \cdots & u_n\alpha_n^{k-1} \end{bmatrix} \quad (1)$$

**Definition 3.** CRS Code: A Cauchy Reed-Solomon Code  $\mathcal{C} = \text{CRS}_{n,k}^{q,(\boldsymbol{\alpha}, \mathbf{f}, \mathbf{u})}$  over  $\mathbb{F}_q$  is the column space of the generator matrix defined in (2) where  $(\boldsymbol{\alpha}, \mathbf{f}) = (\alpha_1, \alpha_2, \dots, \alpha_n, f_1, f_2, \dots, f_k)$  are  $n + k$  distinct elements and  $\mathbf{u} = (u_1, u_2, \dots, u_n)$  are  $n$  non-zero elements. By definition,



$$q \geq n + k.$$

$$\mathbf{G}_{\text{CRS}_{n,k}^{g,(\alpha,f,u)}} \triangleq \begin{bmatrix} \frac{u_1}{f_1-\alpha_1} & \frac{u_1}{f_1-\alpha_1} & \cdots & \frac{u_1}{f_k-\alpha_1} \\ \frac{u_2}{f_1-\alpha_2} & \frac{u_2}{f_1-\alpha_2} & \cdots & \frac{u_2}{f_k-\alpha_2} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{u_n}{f_1-\alpha_n} & \frac{u_n}{f_1-\alpha_n} & \cdots & \frac{u_n}{f_k-\alpha_n} \end{bmatrix} \quad (2)$$

### C. Quantum Information

**Definition 4.** Quantum Channel: A quantum channel with input quantum system  $A$  and output quantum system  $B$  is a completely positive trace preserving mapping (CPTP)  $\mathcal{M}: \mathcal{D}_A \rightarrow \mathcal{D}_B$ . It can be represented by Kraus Operators  $\{K_i\}$  such that  $\sum_i K_i^\dagger K_i$  is an identity matrix and  $\mathcal{M}(\rho) = \sum_i K_i \rho K_i^\dagger$ .

**Definition 5.** Pauli Operators for Qudits [37]: For any  $a, b \in \mathbb{F}_q$ , define the single qudit Pauli Operators  $X^b, Z^b \in \mathbb{C}^{q \times q}$  so that

$$X^b |a\rangle = |a + b\rangle, \quad Z^b |a\rangle = \omega^{\text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(ba)} |a\rangle.$$

For  $n \in \mathbb{N}$  and any  $\mathbf{x} = [x_1 \ \cdots \ x_n]^\top, \mathbf{z} = [z_1 \ \cdots \ z_n]^\top \in \mathbb{F}_q^{n \times 1}$ , let the  $n$ -qudit Pauli Operators be defined as

$$X^{\mathbf{x}} Z^{\mathbf{z}} \triangleq \bigotimes_{i \in [n]} X^{x_i} Z^{z_i}.$$

Note that

$$\begin{aligned} (X^{\mathbf{x}} Z^{\mathbf{z}}) (X^{\mathbf{x}'} Z^{\mathbf{z}'}) &= \omega^{\text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{z}^\top \mathbf{x}' - \mathbf{x}^\top \mathbf{z}')} (X^{\mathbf{x}'} Z^{\mathbf{z}'}) (X^{\mathbf{x}} Z^{\mathbf{z}}) \\ &= \omega^{\text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{z}^\top \mathbf{x}')} X^{\mathbf{x}+\mathbf{x}'} Z^{\mathbf{z}+\mathbf{z}'} \end{aligned} \quad (3)$$

**Definition 6.** CSS Code [22], [23], [38]: A  $\mathcal{C} = \text{CSS}(\mathcal{C}_X, \mathcal{C}_Z)$  code encodes the state space of  $k$   $q$ -dimensional qudits into a code space of  $n$   $q$ -dimensional qudits

$$\text{CSS}(\mathcal{C}_X, \mathcal{C}_Z) = \text{colspan} \left( \sum_{\mathbf{x}^\perp \in \mathcal{C}_X^\perp} |\mathbf{x}^\perp + \mathbf{z}\rangle \mid \mathbf{z} \in \mathcal{C}_Z \right), \quad (4)$$

where  $\mathcal{C}_X, \mathcal{C}_Z$  are classical  $[n, k_X, d_X], [n, k_Z, d_Z]$  linear codes with generator matrices  $\mathbf{G}_{\mathcal{C}_X} \in \mathbb{F}_q^{n \times k_X}, \mathbf{G}_{\mathcal{C}_Z} \in \mathbb{F}_q^{n \times k_Z}$  respectively, that satisfy  $\mathcal{C}_X^\perp \subset \mathcal{C}_Z$ . The  $\text{CSS}(\mathcal{C}_X, \mathcal{C}_Z)$  is a stabilizer code with stabilizers  $S = \{X^{\mathbf{a}} Z^{\mathbf{b}} \mid \mathbf{a} \in \mathcal{C}_X^\perp, \mathbf{b} \in \mathcal{C}_Z^\perp\}$ . Its minimum distance is  $d \geq \min(d_X, d_Z)$ .

**Definition 7.** Stabilizer Measurement: For the CSS code in Definition 6, for any  $\mathbf{a} \in \mathcal{C}_X^\top$ ,  $\mathbf{b} \in \mathcal{C}_Z^\top$ , according to [9, Appendix C, Fact 2)], the stabilizer  $X^{\mathbf{a}}Z^{\mathbf{b}}$  can be decomposed as

$$X^{\mathbf{a}}Z^{\mathbf{b}} = \sum_{i \in \mathbb{F}_p} \omega^i \mathbf{P}_i^{\mathbf{a}, \mathbf{b}} \quad (5)$$

where  $\{\mathbf{P}_i^{\mathbf{a}, \mathbf{b}}\}_{i \in \mathbb{F}_p}$  are orthogonal projections such that

$$\mathbf{P}_i^{\mathbf{a}, \mathbf{b}} \mathbf{P}_j^{\mathbf{a}, \mathbf{b}} = \mathbf{0} \quad \forall i \neq j, \quad (6)$$

$$\sum_{i \in \mathbb{F}_p} \mathbf{P}_i^{\mathbf{a}, \mathbf{b}} = \mathbf{I}. \quad (7)$$

Then the stabilizer measurement  $X^{\mathbf{a}}Z^{\mathbf{b}}$  is defined as the *Projection-Valued Measurement* (PVM, [39]) with projections  $\{\mathbf{P}_i^{\mathbf{a}, \mathbf{b}}\}_{i \in \mathbb{F}_p}$ .

**Definition 8.** Syndrome Measurement: For the CSS code defined in Definition 6, a syndrome measurement is the stabilizer measurement corresponding to all the (generator) stabilizers according to Definition 7.

**Proposition 1.** (Well known) For any  $|\psi\rangle \in \text{CSS}(\mathcal{C}_X, \mathcal{C}_Z)$  and any  $\mathbf{x}, \mathbf{z} \in \mathbb{F}_q^{n \times 1}$ , the  $n$ -qudit pure state  $X^{\mathbf{x}}Z^{\mathbf{z}}|\psi\rangle$  is an eigenvector for all the stabilizers, and its syndrome measurement outcome is as follows, with  $\mathbf{H}_{\mathcal{C}_X}$ ,  $\mathbf{H}_{\mathcal{C}_Z}$  being parity-check matrices for  $\mathcal{C}_X, \mathcal{C}_Z$  respectively.

$$\mathbf{s}_X = \mathbf{H}_{\mathcal{C}_Z}^\top \mathbf{x}, \quad \mathbf{s}_Z = \mathbf{H}_{\mathcal{C}_X}^\top \mathbf{z} \quad (8)$$

The following lemma will be useful.

**Lemma 1.** Consider any  $n$ -qudit state  $|\psi\rangle \in \text{CSS}(\mathcal{C}_X, \mathcal{C}_Z)$  with the  $n$  qudits labeled as  $\mathcal{A}_{[n]}$ . For any  $\mathbf{x}, \mathbf{z} \in \mathbb{F}_q^{n \times 1}$ ,  $\mathcal{S} \subset [n]$ ,  $|\mathcal{S}| \leq \min(d_X, d_Z) - 1$  where  $d_X, d_Z$  are distances of  $\mathcal{C}_X, \mathcal{C}_Z$  respectively, suppose the  $n$ -qudit Pauli gate  $X^{\mathbf{x}}Z^{\mathbf{z}}$  is first applied to  $\mathcal{A}_{[n]}$ . Then for any quantum channel  $\mathcal{M}_{\mathcal{S}}: \mathcal{D}_{\mathcal{A}_{\mathcal{S}}} \rightarrow \mathcal{D}_{\mathcal{A}_{\mathcal{S}}}$  that is applied to qudits  $\mathcal{A}_{\mathcal{S}}$ , the syndrome measurement reduces the

quantum channel to some Pauli operators only affecting qudits  $\mathcal{A}_S$ , i.e.,

$$\begin{aligned}
& \forall |\psi\rangle \in \text{CSS}(\mathcal{C}_X, \mathcal{C}_Z); \mathbf{x}, \mathbf{z} \in \mathbb{F}_q^{n \times 1}; \\
& \mathcal{S} \subset [n], |\mathcal{S}| \leq \min(d_X, d_Z) - 1, \mathcal{M}_S: \mathcal{D}_{\mathcal{A}_S} \rightarrow \mathcal{D}_{\mathcal{A}_S}, \\
& \left( \text{id}_{[n] \setminus \mathcal{S}} \otimes \mathcal{M}_S \right) \left( X^{\mathbf{x}} Z^{\mathbf{z}} |\psi\rangle \langle \psi| (X^{\mathbf{x}} Z^{\mathbf{z}})^\dagger \right) \\
& \xrightarrow{\text{synd.meas.}} X^{\epsilon_S^X} Z^{\epsilon_S^Z} \left( X^{\mathbf{x}} Z^{\mathbf{z}} |\psi\rangle \langle \psi| (X^{\mathbf{x}} Z^{\mathbf{z}})^\dagger \right) \left( X^{\epsilon_S^X} Z^{\epsilon_S^Z} \right)^\dagger \\
& \stackrel{(3)}{=} X^{\mathbf{x} + \epsilon_S^X} Z^{\mathbf{z} + \epsilon_S^Z} |\psi\rangle \langle \psi| \left( X^{\mathbf{x} + \epsilon_S^X} Z^{\mathbf{z} + \epsilon_S^Z} \right)^\dagger,
\end{aligned} \tag{9}$$

with the outcome being

$$\mathbf{s}_X = \mathbf{H}_{\mathcal{C}_Z}^\top (\mathbf{x} + \epsilon_S^X), \quad \mathbf{s}_Z = \mathbf{H}_{\mathcal{C}_X}^\top (\mathbf{z} + \epsilon_S^Z), \tag{10}$$

where  $\text{supp}(\epsilon_S^X) = \text{supp}(\epsilon_S^Z) = \mathcal{S}$ .

Though the lemma is conceptually somewhat standard, we provide a proof in Appendix A for the sake of completeness.

### III. PROBLEM STATEMENT

Let us start with the classical setting defined in [21]. There are  $K$  messages  $W_1, \dots, W_K$  that are i.i.d. uniform over  $[\mathbf{M}]$ . They are securely encoded with randomness  $Z \in \mathcal{Z}$  to form the storage at  $N$  servers. For  $\theta \in [K]$ , the user wishes to privately retrieve the message  $W_\theta$  by querying the  $N$  servers. Local randomness  $Z' \in \mathcal{Z}'$  is available to the user to generate private queries. For any  $n \in [N]$ , the *random variables* regarding the storage, query and answer (in the classical setting) at server  $n$ , denoted as  $S_n, Q_n^{[\theta]}$  and  $A_n$  with realizations being  $s_n, q_n, a_n$ , are deterministic functions of the following 3 independent random variables, whose realizations will be denoted as  $w_{[K]}, z, z'$  respectively.

$$\begin{aligned}
& [\text{Messages}] : W_{[K]} \in [\mathbf{M}]^K, \\
& [\text{Storage Randomness}] : Z \in \mathcal{Z}, \\
& [\text{User Randomness}] : Z' \in \mathcal{Z}'.
\end{aligned} \tag{11}$$

The classical problem is similar to the quantum problem in Fig. 1, but there are no entangled quantum systems shared among servers and the answers from servers are classical symbols. Byzantine servers will return arbitrary classical symbols. Next we specify the storage, queries, servers' answers, and the user's decoding for both classical and quantum settings.

### A. Classical Setting

**MDS and  $X$ -Secure Storage:** The storage at server  $n, n \in [N]$  is denoted as  $S_n \in [\mathcal{S}]$ . With encoding function  $\text{Enc}_{\text{st}}: [\mathcal{M}]^K \times \mathcal{Z} \rightarrow [\mathcal{S}]^N$ , the storage  $S_{[N]} = \text{Enc}_{\text{st}}(W_{[K]}, Z)$  forms an  $[N, X + K_c]$  MDS code, such that

$$\begin{aligned} [\text{MDS Storage}] \quad & H(W_{[K]} \mid S_{\mathcal{S}}) = 0, \\ & \forall \mathcal{S} \subset [N], |\mathcal{S}| = X + K_c, \end{aligned} \quad (12)$$

$$\begin{aligned} & H(S_n) = \log_2 \mathcal{S} = K \log_2(\mathcal{M}) / K_c, \\ & \forall n \in [N] \end{aligned} \quad (13)$$

$$\begin{aligned} [X - \text{Security}] \quad & I(W_{[K]}; S_{\mathcal{X}}) = 0, \\ & \forall \mathcal{X} \subset [N], |\mathcal{X}| \leq X. \end{aligned} \quad (14)$$

i.e., any  $X + K_c$  servers must be able to recover all the  $K$ -messages, the storage size at each server is  $1/K_c$  of the total size of the  $K$  messages, and any  $X$  or fewer servers can learn nothing about the messages. The encoding is done by, e.g., sources of the messages.

**Remark 1.** *The storage forms a ramp secret sharing [40] of the  $K$ -message database. We call it MDS and secure storage for comparison with Quantum MDS-PIR [10], as when  $X = 0$ , the above entropic constraints hold for an  $[N, K_c]$  MDS code where  $K_c$  message symbols are encoded into  $N$  codeword symbols such that any  $K_c$  codeword symbols recover the message and each codeword symbol is  $1/K_c$  of the message size (since there are  $K_c$  message symbols). When  $K_c = 1$ , there is no MDS storage constraint.*

**Queries:** A user wishes to retrieve the  $\theta^{\text{th}}, \theta \in [K]$ , message  $W_\theta$  from the servers by sending the  $T$ -private queries  $Q_1^{[\theta]}, Q_2^{[\theta]}, \dots, Q_N^{[\theta]} \in \mathcal{Q}$  to the  $N$  servers such that any  $T$  or fewer servers learn nothing about  $\theta$ . Mathematically, using the encoding function  $\text{Enc}_{\text{user}}: [K] \times \mathcal{Z}' \rightarrow \mathcal{Q}^N$ , the user generates queries,

$$(Q_1^{[\theta]}, Q_2^{[\theta]}, \dots, Q_N^{[\theta]}) = \text{Enc}_{\text{user}}(\theta, Z') \quad (15)$$

where  $Z' \in \mathcal{Z}'$  is the user's local randomness. Meanwhile, the  $T$ -privacy constraint must be satisfied such that

$$\begin{aligned} [T - \text{Privacy}] \quad & (S_{\mathcal{T}}, Q_{\mathcal{T}}^{[\theta]}) \sim (S_{\mathcal{T}}, Q_{\mathcal{T}}^{[\theta']}) , \\ & \forall \theta, \theta' \in [K], \mathcal{T} \subset [N], |\mathcal{T}| \leq T. \end{aligned} \quad (16)$$

That is to say, for any  $\theta \in [K]$ , the joint distribution of the storage and queries at  $T$  or fewer servers are identical.

**Answers:** There is a set  $\mathcal{E} \subset [N]$  of unresponsive servers and another set  $\mathcal{B} \subset [N]$  of Byzantine servers.  $\mathcal{B}, \mathcal{E}$  are not necessarily disjoint. The user does not know  $\mathcal{E}, \mathcal{B}$  *a priori*, except that

$$|\mathcal{E}| \leq E, |\mathcal{B}| \leq B. \quad (17)$$

Each server  $n \in [N] \setminus (\mathcal{E} \cup \mathcal{B})$  generates the answer  $A_n \in [d]$  using the encoding function  $\text{Enc}_{\text{serv}_n} : [S] \times \mathcal{Q} \rightarrow [d]$  according to its storage and received query, i.e.,

$$A_n = \text{Enc}_{\text{serv}_n}(S_n, Q_n^{[\theta]}), \forall n \in [N] \setminus (\mathcal{E} \cup \mathcal{B}). \quad (18)$$

However, any unresponsive or Byzantine server  $\bar{n} \in \mathcal{E} \cup \mathcal{B}$  generates an arbitrary answer  $A_{\bar{n}} \in [d]$ .

**Decoding:** Upon receiving the answers  $A_{[N] \setminus \mathcal{E}}$ , the user decodes the desired message using a function that depends on  $\mathcal{E}$  (since unresponsive servers can be identified by the user),  $\text{Dec}_{\mathcal{E}} : [K] \times [d]^{N-|\mathcal{E}|} \times \mathcal{Z}' \rightarrow [M]$ , i.e.,

$$\hat{W} = \text{Dec}_{\mathcal{E}}(\theta, A_{[N] \setminus \mathcal{E}}, Z). \quad (19)$$

Thus, an E-B-MDS-X-TPIR scheme, is defined as

$$\Psi^C \left( \text{Enc}_{\text{st}}, \text{Enc}_{\text{user}}, \text{Enc}_{\text{serv}}, \{\text{Dec}_{\mathcal{E}}\}_{\mathcal{E} \subset [N], |\mathcal{E}| \leq E} \right). \quad (20)$$

The rate of a classical E-B-MDS-X-TPIR scheme is defined as the number of desired message bits recovered per answer bit that is downloaded from the servers, i.e.,

$$R^C \triangleq \frac{\log(M)}{N \log(d)}. \quad (21)$$

A rate  $R^C$  is said to be achievable if and only if there exists a scheme  $\Psi^C$  with this rate such that

$$\begin{aligned} \Pr(\hat{W} \neq W_{\theta}) &= 0, \\ \forall \theta \in [K], \mathcal{E}, \mathcal{B} \subset [N], |\mathcal{E}| \leq E, |\mathcal{B}| \leq B. \end{aligned} \quad (22)$$

### B. Quantum Setting

**Shared Entanglement:** In quantum setting, a composite quantum system  $\mathcal{A}_{[N]} = \mathcal{A}_1 \mathcal{A}_2 \cdots \mathcal{A}_N$ , with underlying Hilbert Space  $\mathcal{H}_{\mathcal{A}_{[N]}} = \bigotimes_{n \in [N]} \mathbb{C}^d$  is initialized in the state  $\rho_{\mathcal{A}_{[N]}}^0$  *a priori*, and the subsystem  $\mathcal{A}_n$  is given to server  $n, n \in [N]$ .

**MDS and Secure Storage:** Same as the classical setting.

**Queries:** Same as the classical setting.

**Answer:** Again, there are unresponsive servers  $\mathcal{E}$  and Byzantine servers  $\mathcal{B}$  with  $\mathcal{E}, \mathcal{B} \subset [N]$ ,  $|\mathcal{E}| \leq E$ ,  $|\mathcal{B}| \leq B$ . Any reliable server applies to its own quantum subsystem a completely-positive and trace-preserving (CPTP) map as its encoder, based on the realizations of its storage  $S_n = s_n$  and received query  $Q_n^{[\theta]} = q_n$ , i.e.,

$$\text{Enc}_{\text{serv}_n}^{[s_n, q_n]}: \mathcal{D}_{\mathcal{A}_n} \rightarrow \mathcal{D}_{\mathcal{A}_n}. \quad (23)$$

Unresponsive and Byzantine servers apply an arbitrary CPTP map,

$$\mathcal{M}_{\mathcal{E} \cup \mathcal{B}}: \mathcal{D}_{\mathcal{A}_{\mathcal{E} \cup \mathcal{B}}} \rightarrow \mathcal{D}_{\mathcal{A}_{\mathcal{E} \cup \mathcal{B}}} \quad (24)$$

to their quantum subsystems. Note that Byzantine servers do not change their quantum systems' dimension, as otherwise the user can tell which servers are Byzantine and treat them as erasures instead.

**Decoding:** Upon receiving the quantum system  $\mathcal{A}_{[N] \setminus \mathcal{E}}$  with state  $\rho'_{\mathcal{A}_{[N] \setminus \mathcal{E}}}$ , the user measures with POVM  $\text{Dec}_{\mathcal{E}}^{[\theta, z']} = \{\Pi_{\mathcal{E}}^{\theta, z'}(\hat{w}), \hat{w} \in [M]\}$  that depends on  $\theta$  and the realization of its local randomness  $Z' = z'$ , with outcome random variable  $\hat{W}$  as the decoding result.

**Remark 2.** Both unresponsive and Byzantine servers apply arbitrary CPTP maps to their quantum systems. The difference is that the indices in  $\mathcal{E}$  are directly known to the user after collecting all the answers since unresponsive servers do not respond, while the indices in  $\mathcal{B}$  are unknown before decoding. Thus, the decoding POVM  $\text{Dec}_{\mathcal{E}}^{[\theta, z']}$  depends on  $\mathcal{E}$ .

Thus, an E-B-MDS-X-TPIR scheme, is defined as

$$\Psi^Q \left( \rho^0, \text{Enc}_{\text{st}}, \text{Enc}_{\text{user}}, \text{Enc}_{\text{serv}}, \{\text{Dec}_{\mathcal{E}}\}_{\mathcal{E} \subset [N], |\mathcal{E}| \leq E} \right). \quad (25)$$

The rate of a Quantum E-B-MDS-X-TPIR scheme is defined as the number of desired message bits recovered per qubit that is downloaded from the servers, i.e.,

$$R^Q \triangleq \frac{\log(M)}{N \log(d)}. \quad (26)$$

A rate  $R^Q$  is said to be achievable if there exists a scheme  $\Psi^Q$  with this rate such that for any  $\theta \in [K]$ ,

$$\begin{aligned} \Pr(\hat{W} \neq W_{\theta}) &= 0, \\ \forall \theta \in [K], \mathcal{E}, \mathcal{B} \subset [N], |\mathcal{E}| \leq E, |\mathcal{B}| \leq B. \end{aligned} \quad (27)$$

A (quantum) E-B-MDS-X-TPIR problem is parameterized by  $(E, B, K_c, X, T, N, K)$  where  $N, K$  are number of servers and messages respectively. We define the following constants for any  $E, B, K_c, X, T, N, K$  that will be used throughout this paper, where in the last line of (28), we pick  $N + L$  distinct elements in  $\mathbb{F}_q$ .

$$\begin{aligned} L &\triangleq N - (K_c + E + 2B + X + T - 1), \\ V &\triangleq K_c + X + T - 1, \\ \mathbb{F}_q, q = p^r, q &\geq L + N, \\ (\boldsymbol{\alpha}, \mathbf{f}) &\triangleq (\alpha_1, \dots, \alpha_N, f_1, \dots, f_L) \in \mathbb{F}_q^{N+L}. \end{aligned} \tag{28}$$

**Remark 3.** *Since  $T$ -privacy is for the index  $\theta$ , and  $X$ -security is for the shares of messages, both of which are classical even in the quantum setting, quantum analysis is not required while proving the privacy and security of the quantum protocol. Quantum considerations (e.g., CSS code formalism in Lemma 1), are essential only in the proof of correctness of the decoding process.*

#### IV. MAIN RESULTS

The main result of this paper is a Q-E-B-MDS-X-TPIR scheme/protocol, namely MCSA-CSS. This protocol interprets the classical CSA code based E-B-MDS-X-TPIR scheme of [21] in such a way that desired message symbols appear as “errors” added to a code, combines the classical scheme with a CSS code, and decodes the desired message symbols, erasures and Byzantine errors simultaneously through the syndrome decoding of the CSS code. The scheme achieves a higher rate compared with its classical counterpart. As noted, our Q-E-B-MDS-X-TPIR protocol yields the state-of-art achievable rates under the various special cases corresponding to recently studied quantum PIR settings, e.g., Q-B-X-TPIR [33], Q-E-TPIR [4], Q-MDS-X-TPIR [26], Q-MDS-TPIR [10], and Q-TPIR [9], without server secrecy constraints. We have the following theorem<sup>5</sup>, where setting  $E = 0$  or  $B = 0$  corresponds to the case of no resilience to erasures or Byzantine servers, respectively, while setting  $K_c = 1$  or  $X = 0$  corresponds to the case of no MDS or  $X$ -secure storage constraints, respectively.

<sup>5</sup>For ease of comparison with quantum PIR problems, similar to [4] but unlike [21], the unreceived qudits from unresponsive servers are also counted in the download cost.

**Theorem 1.** *For quantum  $K_c$  MDS  $X$ -secure  $T$ -private information retrieval with  $N$  servers out of which at most  $E$  servers are unresponsive and  $B$  servers are Byzantine, the rate*

$$R^Q = \begin{cases} \frac{2(N-E-2B-K_c-X+1)}{N}, \\ (N-E-2B) > (K_c+X+T-1) \geq N/2 \\ \max\left(\frac{N-2E-4B}{N}, \frac{N-E-2B-K_c-X-T+1}{N}\right), \\ (N-E-2B) \geq N/2 > (K_c+X+T-1) \\ \frac{N-E-2B-K_c-X-T+1}{N}, \\ N/2 > (N-E-2B) > (K_c+X+T-1) \end{cases} \quad (29)$$

is achievable.

*Proof.* The achievability of the third regime  $N/2 > (N-E-2B) > (K_c+X+T-1)$  is trivial since a  $q$ -dimensional qudit can always be used to transmit a classical  $q$ -ary symbol and the classical scheme in [21] can be directly applied. The achievability of the first regime  $(N-E-2B) > (K_c+X+T-1) \geq N/2$  will be established by the scheme presented in Section VII.

The achievability of the second regime,  $(N-E-2B) \geq N/2 > (K_c+X+T-1)$ , follows from a combination of the schemes for the first and third regimes, an idea that appears in the preliminary ArXiv version of this paper [36, Theorem 1, Remark 6] and in the subsequent  $2^{nd}$  version of [33]. First of all,  $\frac{N-E-2B-K_c-X-T+1}{N}$  is always achievable by the classical scheme. For the achievability of  $\frac{N-2E-4B}{N}$ , intuitively, when  $N/2 > (K_c+X+T-1)$ , one can always use the scheme that has more demanding privacy constraints, i.e., the scheme with  $\bar{T}$ -privacy such that  $K_c+X+\bar{T}-1 = N/2$  and  $\bar{T} \geq T$ . The Q-MDS-X- $\bar{T}$ PIR falls into the first regime and the rate can be calculated accordingly. Note that such a choice of  $\bar{T}$  needs  $N$  to be even so that  $N/2$  is an integer. The odd case will be resolved by Remark 8.  $\square$

**Remark 4.** *In the first regime, we note the rate of the quantum scheme is twice of the classical scheme, which matches the maximal superdense coding gain observed thus far in other quantum settings of PIR [9], [10], [26] (compared with [6], [7] and [21] without unresponsive and Byzantine servers), secret sharing [4] (compared with [1]).*



## V. CLASSICAL E-B-MDS-X-TPIR: CSA CODE

The classical version of this problem has been studied in [21], and the CSA code based classical scheme there is an essential building block of its quantum version. Let us briefly summarize it here, starting with an example.

*A. Example 1:  $E = 1, B = 0, K_c = 2, X = 1, T = 1$  with  $N = 6$  Servers [21]*

Let  $L = N - (K_c + E + X + T - 1) = 2$  and  $\alpha_1, \dots, \alpha_{N=6}, f_1, f_{L=2}$  be 8 distinct elements over  $\mathbb{F}_q$  ( $q \geq 8$ ). Let  $w_{[K]}$  be the realizations of all the  $K$  messages  $W_{[K]}$ . Each message has  $L \times K_c = 4$  symbols from  $\mathbb{F}_q$ , i.e., for any  $k \in [K]$ , message  $w_k = \{w_k(i, j)\}_{i \in [2], j \in [2]}$  contains 4 symbols from  $\mathbb{F}_q$ . Let  $\dot{\mathbf{w}}_{1,1}, \dot{\mathbf{w}}_{1,2}, \dot{\mathbf{w}}_{2,1}, \dot{\mathbf{w}}_{2,2} \in \mathbb{F}_q^{1 \times K}$  denote the row vectors that contain the 4 symbols of the  $K$  messages, respectively, i.e.,

$$w_k = \begin{bmatrix} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^k & \dot{\mathbf{w}}_{1,2} \mathbf{e}_K^k \\ \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^k & \dot{\mathbf{w}}_{2,2} \mathbf{e}_K^k \end{bmatrix} \quad (30)$$

where  $\mathbf{e}_K^k$  is the  $k^{th}$  column vector of  $\mathbf{I}_K$ .

Let the storage randomness  $Z = \{\mathbf{Z}_{1,1}, \mathbf{Z}_{2,1}\}$  be uniform over  $\mathbb{F}_q^{1 \times K} \times \mathbb{F}_q^{1 \times K}$  and user randomness  $Z' = \{\mathbf{Z}'_{l,t}(\kappa)\}_{l \in [2], \kappa \in [2], t=1}$  be uniform over  $(\mathbb{F}_q^{K \times 1})^4$ .

**Storage:** The storage at server  $n$ ,  $n \in [6]$ , conditioned on the realization of messages and storage randomness, is  $S_n = s_n$  where

$$\begin{aligned} s_n &= \begin{bmatrix} s_n(1) & s_n(2) \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{(f_1 - \alpha_n)^2} \dot{\mathbf{w}}_{1,1} + \frac{1}{f_1 - \alpha_n} \dot{\mathbf{w}}_{1,2} + \mathbf{z}_{1,1} \\ \frac{1}{(f_2 - \alpha_n)^2} \dot{\mathbf{w}}_{2,1} + \frac{1}{f_2 - \alpha_n} \dot{\mathbf{w}}_{2,2} + \mathbf{z}_{2,1} \end{bmatrix}. \end{aligned} \quad (31)$$

Here  $\mathbf{z}_{1,1}, \mathbf{z}_{2,1} \in \mathbb{F}_q^{1 \times K}$  are the realizations of random vectors  $\mathbf{Z}_{1,1}, \mathbf{Z}_{2,1}$  respectively. It is not difficult to see that for any  $l \in [2]$ ,  $(s_1(l), s_2(l), \dots, s_6(l))$   $l \in [2]$  is a  $[6, 3]$  MDS code for  $(\dot{\mathbf{w}}_{l,1}, \dot{\mathbf{w}}_{l,2}, \mathbf{z}_{l,1})$ , and the storage cost at each server is  $1/K_c = 1/2$  of the  $K$  messages  $(s_n(1), s_n(2)) \in \mathbb{F}_q^{1 \times K}$  while each of  $K$  messages contains 4 symbols from  $\mathbb{F}_q$ . At the same time we have a secret sharing of  $\frac{1}{(\alpha_n - f_1)^2} \dot{\mathbf{w}}_{l,1} + \frac{1}{\alpha_n - f_1} \dot{\mathbf{w}}_{l,2}$  with threshold 1, thus the MDS and  $X = 1$  security constraint is satisfied.

**Queries:** The query generation contains  $K_c = 2$  iterations. The query sent from the user to server  $n$ ,  $n \in [6]$ , conditioned on the realization of the user's local randomness, is  $Q_n^{[\theta]} = q_n$  where

$$q_n = \{q_n^{(1)}, q_n^{(2)}\}, \quad (32)$$

with the superscript indicating the iteration number, and

$$q_n^{(1)} = \begin{bmatrix} q_n^{(1)}(1) \\ q_n^{(1)}(2) \end{bmatrix} = \begin{bmatrix} (f_1 - \alpha_n) \mathbf{e}_K^\theta + (f_1 - \alpha_n)^2 \mathbf{z}_{1,1}'^{(1)} \\ (f_2 - \alpha_n) \mathbf{e}_K^\theta + (f_2 - \alpha_n)^2 \mathbf{z}_{2,1}'^{(1)} \end{bmatrix} \quad (33)$$

$$q_n^{(2)} = \begin{bmatrix} q_n^{(2)}(1) \\ q_n^{(2)}(2) \end{bmatrix} = \begin{bmatrix} \mathbf{e}_K^\theta + (f_1 - \alpha_n)^2 \mathbf{z}_{1,1}'^{(2)} \\ \mathbf{e}_K^\theta + (f_2 - \alpha_n)^2 \mathbf{z}_{2,1}'^{(2)} \end{bmatrix} \quad (34)$$

Here,  $\mathbf{e}_{K,\theta}$  is the  $\theta^{th}$  column of  $\mathbf{I}_K$ , used for choosing the  $\theta^{th}$  entry of  $\dot{\mathbf{w}}$ , and  $\mathbf{z}_{l,t}'^{(\kappa)} \in \mathbb{F}_q^{K \times 1}$ ,  $l \in [2]$ ,  $\kappa \in [2]$ ,  $t = 1$  is the realization of corresponding user randomness  $\mathbf{Z}_{l,t}'^{(\kappa)}$ . It is again not difficult to verify that the queries form secret sharing of  $\mathbf{e}_K^\theta$  with threshold 1. Thus, the query is 1-private.

**Answer:** The answer generation takes  $K_c = 2$  iterations. Conditioned on the realization of messages, storage and user randomness, the answer sent from server  $n$  is  $A_n = a_n = \{a_n^{(1)}, a_n^{(2)}\}$  where in iteration  $\kappa \in [2]$ , the answer  $a_n^{(\kappa)}$  is just a symbol from  $\mathbb{F}_q$ . Specifically, in the first iteration,

$$\begin{aligned} a_n^{(1)} &= s_n q_n^{(1)} = s_n(1) q_n^{(1)}(1) + s_n(2) q_n^{(1)}(2) \\ &= \frac{1}{f_1 - \alpha_n} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^\theta + \frac{1}{f_2 - \alpha_n} \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^\theta \\ &\quad + \left( \dot{\mathbf{w}}_{1,1} \mathbf{z}_{1,1}'^{(1)} + \dot{\mathbf{w}}_{2,1} \mathbf{z}_{2,1}'^{(1)} + \dot{\mathbf{w}}_{1,2} \mathbf{e}_K^\theta + \dot{\mathbf{w}}_{2,2} \mathbf{e}_K^\theta \right) \\ &\quad + (f_1 - \alpha_n) \left( \dot{\mathbf{w}}_{1,2} \mathbf{z}_{1,1}'^{(1)} + \mathbf{z}_{1,1} \mathbf{e}_K^\theta \right) \\ &\quad + (f_2 - \alpha_n) \left( \dot{\mathbf{w}}_{2,2} \mathbf{z}_{2,1}'^{(1)} + \mathbf{z}_{2,1} \mathbf{e}_K^\theta \right) \\ &\quad + (f_1 - \alpha_n)^2 \mathbf{z}_{1,1} \mathbf{z}_{1,1}'^{(1)} + (f_2 - \alpha_n)^2 \mathbf{z}_{2,1} \mathbf{z}_{2,1}'^{(1)} \end{aligned} \quad (35)$$

$$\begin{aligned} &= \frac{1}{f_1 - \alpha_n} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^\theta + \frac{1}{f_2 - \alpha_n} \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^\theta \\ &\quad + * + \alpha_n * + \alpha_n^2 * \end{aligned} \quad (36)$$

where the coefficients for rational terms are desired message symbols and the coefficients for  $\alpha_n^0, \alpha_n^1, \alpha_n^2$  are interfering symbols whose specific forms are not important. The collection of the answers from the 6 servers can be represented as,

$$\begin{bmatrix} a_1^{(1)} \\ a_2^{(1)} \\ a_3^{(1)} \\ a_4^{(1)} \\ a_5^{(1)} \\ a_6^{(1)} \end{bmatrix} = \begin{bmatrix} \frac{1}{f_1 - \alpha_1} & \frac{1}{f_2 - \alpha_1} & 1 & \alpha_1 & \alpha_1^2 \\ \frac{1}{f_1 - \alpha_2} & \frac{1}{f_2 - \alpha_2} & 1 & \alpha_2 & \alpha_2^2 \\ \frac{1}{f_1 - \alpha_3} & \frac{1}{f_2 - \alpha_3} & 1 & \alpha_3 & \alpha_3^2 \\ \frac{1}{f_1 - \alpha_4} & \frac{1}{f_2 - \alpha_4} & 1 & \alpha_4 & \alpha_4^2 \\ \frac{1}{f_1 - \alpha_5} & \frac{1}{f_2 - \alpha_5} & 1 & \alpha_5 & \alpha_5^2 \\ \frac{1}{f_1 - \alpha_6} & \frac{1}{f_2 - \alpha_6} & 1 & \alpha_6 & \alpha_6^2 \end{bmatrix} \begin{bmatrix} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^\theta \\ \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^\theta \\ * \\ * \\ * \end{bmatrix}. \quad (37)$$

Due to the fact that any 5 rows of the matrix in (37) form an invertible sub-matrix according to [21], the answers form a  $[6, 5]$  MDS code such that one erasure can be corrected and 2 desired message symbols  $w_\theta(:, 1) = [\dot{\mathbf{w}}_{1,1} \mathbf{e}_K^\theta \quad \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^\theta]^\top$  (together with the interfering symbols) can be decoded.

In the second iteration, the answer from each server is still a symbol in  $\mathbb{F}_q$ , where

$$\begin{aligned} a_n^{(2)} &= s_n q_n^{(2)} = s_n(1) q_n^{(2)}(1) + s_n(2) q_n^{(2)}(2) \\ &= \frac{1}{(f_1 - \alpha_n)^2} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^\theta + \frac{1}{(f_2 - \alpha_n)^2} \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^\theta \\ &\quad + \frac{1}{f_1 - \alpha_n} \dot{\mathbf{w}}_{1,2} \mathbf{e}_K^\theta + \frac{1}{f_2 - \alpha_n} \dot{\mathbf{w}}_{2,2} \mathbf{e}_K^\theta \\ &\quad + * + \alpha_n * + \alpha_n^2 *. \end{aligned} \quad (38)$$

The details of derivation can be found in [21] and are omitted here. Note that the first two terms in (38) are already known from the first iteration of decoding. The 6 answers together can now

be written as,

$$\begin{aligned}
 \begin{bmatrix} a_1^{(2)} \\ a_2^{(2)} \\ a_3^{(2)} \\ a_4^{(2)} \\ a_5^{(2)} \\ a_6^{(2)} \end{bmatrix} &= \begin{bmatrix} \frac{1}{f_1-\alpha_1} & \frac{1}{f_2-\alpha_1} & 1 & \alpha_1 & \alpha_1^2 \\ \frac{1}{f_1-\alpha_2} & \frac{1}{f_2-\alpha_2} & 1 & \alpha_2 & \alpha_2^2 \\ \frac{1}{f_1-\alpha_3} & \frac{1}{f_2-\alpha_3} & 1 & \alpha_3 & \alpha_3^2 \\ \frac{1}{f_1-\alpha_4} & \frac{1}{f_2-\alpha_4} & 1 & \alpha_4 & \alpha_4^2 \\ \frac{1}{f_1-\alpha_5} & \frac{1}{f_2-\alpha_5} & 1 & \alpha_5 & \alpha_5^2 \\ \frac{1}{f_1-\alpha_6} & \frac{1}{f_2-\alpha_6} & 1 & \alpha_6 & \alpha_6^2 \end{bmatrix} \begin{bmatrix} \dot{\mathbf{w}}_{1,2} \mathbf{e}_K^\theta \\ \dot{\mathbf{w}}_{2,2} \mathbf{e}_K^\theta \\ * \\ * \\ * \end{bmatrix} \\
 &+ \underbrace{\begin{bmatrix} \sum_{l \in [2]} \frac{1}{(f_l-\alpha_1)^2} \dot{\mathbf{w}}_{l,1} \mathbf{e}_K^\theta \\ \sum_{l \in [2]} \frac{1}{(f_l-\alpha_2)^2} \dot{\mathbf{w}}_{l,1} \mathbf{e}_K^\theta \\ \sum_{l \in [2]} \frac{1}{(f_l-\alpha_3)^2} \dot{\mathbf{w}}_{l,1} \mathbf{e}_K^\theta \\ \sum_{l \in [2]} \frac{1}{(f_l-\alpha_4)^2} \dot{\mathbf{w}}_{l,1} \mathbf{e}_K^\theta \\ \sum_{l \in [2]} \frac{1}{(f_l-\alpha_5)^2} \dot{\mathbf{w}}_{l,1} \mathbf{e}_K^\theta \\ \sum_{l \in [2]} \frac{1}{(f_l-\alpha_6)^2} \dot{\mathbf{w}}_{l,1} \mathbf{e}_K^\theta \end{bmatrix}}_{\sigma^{(1), \text{known}}}. \tag{39}
 \end{aligned}$$

After subtracting  $\sigma^{(1)}$ ,  $w_\theta(:, 2) = [\dot{\mathbf{w}}_{1,2} \mathbf{e}_K^\theta \quad \dot{\mathbf{w}}_{2,2} \mathbf{e}_K^\theta]^\top$  can be decoded similarly. The  $2 \times 2$  desired message symbols are retrieved by downloading  $6 \times 2$  answer symbols from the servers. The rate achieved is  $1/3$ .

### B. CSA Code for E-B-MDS-X-TPIR

Recall the constants defined in (28). Each message has  $L \times K_c$  symbols from  $\mathbb{F}_q$ , i.e., for any  $k \in [K]$ , the realization of message  $W_k$ ,  $w_k = (w_k(i, j))_{l \in [L], \kappa \in [K_c]}$ . Let us define the length- $K$  vector that contains the  $(l, \kappa)^{th}$  symbol of all the  $K$  messages as

$$\dot{\mathbf{w}}_{l, \kappa} \triangleq \begin{bmatrix} w_1(l, \kappa) & w_2(l, \kappa) & \cdots & w_K(l, \kappa) \end{bmatrix}, \forall l \in [L], \kappa \in [K]. \tag{40}$$

Then for any  $k \in [K]$ , message  $w_k$  can be represented as

$$w_k = \begin{bmatrix} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^k & \dot{\mathbf{w}}_{1,2} \mathbf{e}_K^k & \cdots & \dot{\mathbf{w}}_{1,K_c} \mathbf{e}_K^k \\ \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^k & \dot{\mathbf{w}}_{2,2} \mathbf{e}_K^k & \cdots & \dot{\mathbf{w}}_{2,K_c} \mathbf{e}_K^k \\ \vdots & \vdots & \vdots & \vdots \\ \dot{\mathbf{w}}_{L,1} \mathbf{e}_K^k & \dot{\mathbf{w}}_{L,2} \mathbf{e}_K^k & \cdots & \dot{\mathbf{w}}_{L,K_c} \mathbf{e}_K^k \end{bmatrix} \in \mathbb{F}_q^{L \times K_c}. \tag{41}$$

The sources of randomness included in this scheme, uniform over their respective alphabet, are as follows,

$$\begin{aligned} Z &= \{\mathbf{Z}_{l,x}\}_{l \in [L], x \in [X]}, \mathbf{Z}_{l,x} \in \mathbb{F}_q^{K \times 1}, \\ Z' &= \{\mathbf{Z}'_{l,t}^{(\kappa)}\}_{l \in [L], \kappa \in [K_c], t \in [T]}, \mathbf{Z}'_{l,t}^{(\kappa)} \in \mathbb{F}_q^{1 \times K}. \end{aligned} \quad (42)$$

We let  $z = \{\mathbf{z}_{l,x}\}_{l \in [L], x \in [X]}$ ,  $z' = \{\mathbf{z}'_{l,t}^{(\kappa)}\}_{l \in [L], \kappa \in [K_c], t \in [T]}$  be the realizations.

The CSA scheme in [21] is summarized in the following protocol. The specific forms of storage, queries and answers generation functions can be found in Appendix B.

**Protocol 1. E-B-MDS-X-TPIR:**

CSA  $\left(\{\dot{\mathbf{w}}_{l,\kappa}\}_{l \in [L], \kappa \in [K_c]}, z, z'\right)$  (Classical)

- 1) **Storage:**  $s_{[N]} \leftarrow \text{StoreGen}(\{\dot{\mathbf{w}}_{l,\kappa}\}_{l \in [L], \kappa \in [K_c]}, z)$
- 2) **Queries:**  $q_{[N]} \leftarrow \text{QueryGen}(\theta, z')$
- 3) **Answers:**  $a_{[N]} = \{a_{[N]}^{(\kappa)}\}_{\kappa \in [K_c]} \leftarrow \text{AnsGen}(s_{[N]}, q_{[N]})$ . Note that for all  $\kappa \in [K_c]$ , the answers at iteration  $\kappa$  are specified in (43),

$$\underbrace{\begin{bmatrix} a_1^{(1)} \\ \vdots \\ a_N^{(1)} \end{bmatrix}}_{\triangleq \mathbf{a}^{(\kappa)}} = \underbrace{\begin{bmatrix} \frac{1}{f_1 - \alpha_1} & \cdots & \frac{1}{f_L - \alpha_1} & 1 & \alpha_1 & \cdots & \alpha_1^{V-1} \\ \frac{1}{f_1 - \alpha_2} & \cdots & \frac{1}{f_L - \alpha_2} & 1 & \alpha_2 & \cdots & \alpha_2^{V-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{f_1 - \alpha_N} & \cdots & \frac{1}{f_L - \alpha_N} & 1 & \alpha_N & \cdots & \alpha_N^{V-1} \end{bmatrix}}_{\triangleq \mathbf{G}_{\text{CSA}_{N,L,V}}^{q,(\alpha,\mathbf{f})}} \underbrace{\begin{bmatrix} \dot{\mathbf{w}}_{1,\kappa} \mathbf{e}_K^\theta \\ \vdots \\ \dot{\mathbf{w}}_{L,\kappa} \mathbf{e}_K^\theta \\ * \\ \vdots \\ * \end{bmatrix}}_{=[w_\theta(\cdot, \kappa); *]} + \underbrace{\begin{bmatrix} \sum_{l \in [L], k \in [\kappa-1]} \frac{\dot{\mathbf{w}}_{l,k} \mathbf{e}_K^\theta}{(f_l - \alpha_1)^{\kappa-k+1}} \\ \sum_{l \in [L], k \in [\kappa-1]} \frac{\dot{\mathbf{w}}_{l,k} \mathbf{e}_K^\theta}{(f_l - \alpha_2)^{\kappa-k+1}} \\ \vdots \\ \sum_{l \in [L], k \in [\kappa-1]} \frac{\dot{\mathbf{w}}_{l,k} \mathbf{e}_K^\theta}{(f_l - \alpha_N)^{\kappa-k+1}} \end{bmatrix}}_{\triangleq \sigma^{(\kappa-1)}, \text{ known}} \quad (43)$$

- 4) **Corrupted Answers:** In each iteration  $\kappa \in [K_c]$ , the user receives  $\hat{\mathbf{a}}^{(\kappa)}$  (answers from unresponsive servers can be replaced by 0).

$$\begin{aligned} \hat{\mathbf{a}}^{(\kappa)} &= \mathbf{a}^{(\kappa)} + \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} = \\ &= \mathbf{G}_{\text{CSA}_{N,L,V}}^{q,(\alpha,\mathbf{f})} [w_\theta(\cdot, \kappa); *] + \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} + \sigma^{(\kappa-1)} \end{aligned} \quad (44)$$

where  $\text{supp}(\boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)}) = \mathcal{E} \cup \mathcal{B}$  denotes the errors introduced by unresponsive and Byzantine servers.

5) **Decoding:** For each  $\kappa \in [K_c]$ , the user decodes  $w(:, \kappa) = \Phi_{\mathcal{E}}^{\text{CSA}}(\hat{\mathbf{a}}^{(\kappa)} - \boldsymbol{\sigma}^{(\kappa-1)})$ .

**In the 1<sup>st</sup> iteration,**  $\boldsymbol{\sigma}^{(0)} = \mathbf{0}$  and the answers from  $N$  servers can be regarded as a codeword from  $\mathcal{C} = \text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}$  code with  $\mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}}$  being the generator matrix, added with errors introduced by unresponsive and Byzantine servers as shown in (44). The generator matrix is defined in (43), and the vector  $*$  contains  $V = K_c + X + T - 1$  symbols that are regarded as *interference* that arises due to MDS, security and privacy constraints. The specific forms of the interference terms are not important. According to the following proposition that states the CSA code is an  $[N, L + V]$  MDS code with minimum distance  $d = N - (L + V) + 1 \stackrel{(28)}{=} E + 2B + 1$ , the  $|\mathcal{E}| \leq E$  erasures and  $|\mathcal{B}| \leq B$  Byzantine errors can be corrected and the user is able to recover desired message symbols  $w_{\theta}(:, 1)$  by the decoding scheme of CSA code  $\Phi_{\mathcal{E}}^{\text{CSA}}$ .

**Proposition 2.** Any  $L + V$  rows of  $\mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}}$  defined in (43) form an invertible matrix, i.e.,  $\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})} \triangleq \text{colspan}(\mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}})$  code is an  $[N, L + V]$  MDS code [21].

**In the  $\kappa^{\text{th}}$  iteration,**  $\kappa \in [K_c]$ , the received  $N$  answers, after subtracting  $\boldsymbol{\sigma}^{(\kappa-1)}$  which solely depends on the decoding result in the previous iterations, again form a codeword from  $\mathcal{C} = \text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}$  code, added with errors. Again, according to Proposition 2, the user is able to decode  $w_{\theta}(:, \kappa)$  in the  $\kappa^{\text{th}}$  iteration.

The communication rate of the CSA code based scheme is

$$R^C = \frac{K_c L}{K_c N} \stackrel{(28)}{=} \frac{N - E - 2B - K_c - X - T + 1}{N}. \quad (45)$$

## VI. MODIFIED CSA (MCSA) CODE

In this section, we propose a Modified CSA (MCSA) Code which is still a classical error correction code, that is intended for classical E-B-MDS-X-TPIR protocol, but more compatible with our eventual Q-E-B-MDS-X-TPIR protocol construction, by turning the RS sub-code of CSA code into a GRS code and leveraging the fact that the dual code of a GRS code is still a GRS code.

### A. MCSA Code for E-B-MDS-X-TPIR

**Definition 9. MCSA Code (Classical):** A Modified Cross Subspace Alignment code  $\mathcal{C} = \text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}$  over  $\mathbb{F}_q$  is the column space of the generator matrix defined in (46) where  $\mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}}$  is defined in (43),  $(\alpha, \mathbf{f}) = (\alpha_1, \alpha_2, \dots, \alpha_N, f_1, f_2, \dots, f_L)$  are  $N + L$  distinct

elements and  $\mathbf{u} = (u_1, u_2, \dots, u_N)$  are  $N$  non-zero elements in  $\mathbb{F}_q$ . By definition,  $N \geq L + V$  and  $q \geq N + L$ .

$$\mathbf{G}_{\text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \triangleq \text{Diag}(\mathbf{u}) \mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}}. \quad (46)$$

The specific form of the generator matrix can be found in (48). For this MCSA code, we have the following proposition.

**Proposition 3.** Any  $L + V$  rows of  $\mathbf{G}_{\text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}}$  form an invertible matrix, i.e.,  $\text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}$  code is an  $[N, L + V]$  MDS code.

*Proof.* For any  $\mathcal{R} \subset [N], |\mathcal{R}| = L + V$ , the  $L + V$  rows

$$\mathbf{G}_{\text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}}(\mathcal{R}, :) = \text{Diag}(\mathbf{u}(\mathcal{R})) \mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}}(\mathcal{R}, :) \quad (47)$$

form an invertible matrix since  $\text{Diag}(\mathbf{u}(\mathcal{R}))$  is invertible as  $u_i \neq 0, \forall i \in [N]$ , and  $\mathbf{G}_{\text{CSA}_{N,L,V}^{q,(\alpha,\mathbf{f})}}$  is invertible according to Proposition 2.  $\square$

Let us specify the form of the **answers** from an MCSA based classical E-B-MDS-X-TPIR scheme next. Note that for all  $\kappa \in [K_c]$ , the answers at iteration  $\kappa$  are specified in (48).

$$\begin{aligned} \underbrace{\begin{bmatrix} a_1^{(1)} \\ \vdots \\ a_N^{(1)} \end{bmatrix}}_{\triangleq \mathbf{a}^{(\kappa)}} &= \underbrace{\begin{bmatrix} \frac{u_1}{f_1 - \alpha_1} & \cdots & \frac{u_1}{f_L - \alpha_1} \\ \frac{u_2}{f_1 - \alpha_2} & \cdots & \frac{u_2}{f_L - \alpha_2} \\ \vdots & \vdots & \vdots \\ \frac{u_N}{f_1 - \alpha_N} & \cdots & \frac{u_N}{f_L - \alpha_N} \end{bmatrix}}_{\triangleq \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}}} \underbrace{\begin{bmatrix} u_1 & u_1 \alpha_1 & \cdots & u_1 \alpha_1^{V-1} \\ u_2 & u_2 \alpha_2 & \cdots & u_2 \alpha_2^{V-1} \\ \vdots & \vdots & \vdots & \vdots \\ u_N & u_N \alpha_N & \cdots & u_N \alpha_N^{V-1} \end{bmatrix}}_{\triangleq \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}}} \underbrace{\begin{bmatrix} \dot{\mathbf{w}}_{1,\kappa} \mathbf{e}_K^\theta \\ \vdots \\ \dot{\mathbf{w}}_{L,\kappa} \mathbf{e}_K^\theta \\ * \\ \vdots \\ * \end{bmatrix}}_{\triangleq [\mathbf{w}_\theta(:, \kappa); *]} + \underbrace{\begin{bmatrix} \sum_{l \in [L], k \in [\kappa-1]} \frac{u_1 \dot{\mathbf{w}}_{l,k} \mathbf{e}_K^\theta}{(f_l - \alpha_1)^{\kappa-k+1}} \\ \sum_{l \in [L], k \in [\kappa-1]} \frac{u_2 \dot{\mathbf{w}}_{l,k} \mathbf{e}_K^\theta}{(f_l - \alpha_2)^{\kappa-k+1}} \\ \vdots \\ \sum_{l \in [L], k \in [\kappa-1]} \frac{u_N \dot{\mathbf{w}}_{l,k} \mathbf{e}_K^\theta}{(f_l - \alpha_N)^{\kappa-k+1}} \end{bmatrix}}_{\triangleq \boldsymbol{\sigma}^{(\kappa-1)}, \text{ known}} \end{aligned} \quad (48)$$

**Remark 5.** For any  $\kappa \in [K_c]$ , the answers at iteration  $\kappa$  specified in (48) are equal to the answers in (43) left-multiplied by the matrix  $\text{Diag}(\mathbf{u})$ . Thus, any CSA based scheme can be easily converted to an MCSA based scheme by letting server  $n$  multiply its answer generated from CSA based scheme by  $u_n$ . The generation of storage and queries remains unchanged. Therefore,  $X$ -security and  $T$ -privacy follow from the CSA code based scheme. Meanwhile, the

decodability of the desired message is guaranteed by Proposition 3, just as the decodability of CSA code based scheme is guaranteed by Proposition 2.

**Remark 6.** Compared with the generator matrix of the code defined in [26, Eq. (15)] which is a square matrix, note that the generator matrix in this paper is not square to be able to correct errors introduced by unresponsive and Byzantine servers, and it is an enhanced version of the generator matrix of CSA code in [21, Eq. (70)].

The MCSA code based scheme is specified in Protocol 2. The definition of  $\{\dot{\mathbf{w}}_{l,\kappa}\}_{l \in [L], \kappa \in [K_c]}$ ,  $z, z'$  are the same as those in (40) and (42).  $\mathbf{u} = (u_1, \dots, u_N) \in \mathbb{F}_q^N$  are  $N$  non-zero elements<sup>6</sup> in  $\mathbb{F}_q$ . Again, the storage, queries and answers generation functions are specified in Appendix B.

**Protocol 2.** E-B-MDS-X-TPIR:

MCSA  $\left( \{\dot{\mathbf{w}}_{l,\kappa}\}_{l \in [L], \kappa \in [K_c]}, z, z', \mathbf{u} \right)$  (Classical)

- 1) **Storage:**  $s_{[N]} \leftarrow \text{StoreGen} \left( \{\dot{\mathbf{w}}_{l,\kappa}\}_{l \in [L], \kappa \in [K_c]}, z \right)$
- 2) **Queries:**  $q_{[N]} \leftarrow \text{QueryGen}(\theta, z')$
- 3) **Answers:**  $\tilde{a}_{[N]} = \left\{ \tilde{a}_{[N]}^{(\kappa)} \right\}_{\kappa \in [K_c]} \leftarrow \text{AnsGen}(s_{[N]}, q_{[N]}),$   
 $a_{[N]}^{(\kappa)} \leftarrow u_n \tilde{a}_{[N]}^{(\kappa)}, \forall n \in [N], \kappa \in [K_c].$

The  $N$  answers at iteration  $\kappa \in [K_c]$  are as follows<sup>7</sup>

$$\begin{aligned} \mathbf{a}^{(\kappa)} &\stackrel{(48)}{=} \mathbf{G}_{\text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}}[w_\theta(:, \kappa); \mathbf{*}] + \sigma^{(\kappa-1)} \\ &\stackrel{(48)}{=} \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}} \mathbf{*} + \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \underline{w_\theta(:, \kappa)} + \sigma^{(\kappa-1)} \end{aligned} \quad (49)$$

4) **Corrupted Answers:** In each iteration  $\kappa \in [K_c]$ , the user receives corrupted answers  $\hat{\mathbf{a}}^{(\kappa)}$  (answers from unresponsive servers can be replaced by 0).

$$\begin{aligned} \hat{\mathbf{a}}^{(\kappa)} &= \mathbf{a}^{(\kappa)} + \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} \\ &= \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}} \mathbf{*} + \underbrace{\mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \underline{w_\theta(:, \kappa)}}_{\text{“error”}} + \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} + \sigma^{(\kappa-1)} \end{aligned} \quad (50)$$

<sup>6</sup> $\mathbf{u}$  is a constant vector included in the input to the protocol for ease of executing it twice with different parameters  $\mathbf{u}, \mathbf{v}$  in the quantum protocol.

<sup>7</sup>The notation  $\underline{w_\theta(:, \kappa)} = w_\theta(:, \kappa)$  indicates that this represents a vector.



where  $\text{supp}(\epsilon_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)}) = \mathcal{E} \cup \mathcal{B}$  denotes the errors introduced by unresponsive and Byzantine servers.

5) **Decoding:** For any  $\kappa \in [K_c]$ , user computes the syndrome

$$\begin{aligned} \mathbf{s}^{(\kappa)} &\triangleq \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \hat{\mathbf{a}}^{(\kappa)} \\ &= \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \left( \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} w_\theta(:, \kappa) + \epsilon_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} \right) \\ &\quad + \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \sigma^{(\kappa-1)}. \end{aligned} \quad (51)$$

and decodes the desired message through

$$\begin{aligned} \Phi_{\mathcal{E}}^{\text{GRS}} \left( \mathbf{s}^{(\kappa)} - \underbrace{\mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \sigma^{(\kappa-1)}}_{\text{known}} \right) &\stackrel{(51)}{=} \\ \Phi_{\mathcal{E}}^{\text{GRS}} \left( \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \left( \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} w_\theta(:, \kappa) + \epsilon_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} \right) \right) \\ &= \left( w_\theta(:, \kappa), \epsilon_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)} \right), \end{aligned} \quad (52)$$

where  $\Phi_{\mathcal{E}}^{\text{GRS}}: \mathbb{F}_q^{(N-V)} \rightarrow \mathbb{F}_q^L \times \mathbb{F}_q^N$  is the mapping from the syndrome (after subtracting  $\sigma^{(\kappa-1)}$  related terms) to the  $L$  desired message symbols and the error vector introduced by unresponsive and Byzantine server, when the unresponsive servers are those with indices in the set  $\mathcal{E}$ .

**Remark 7.** Note that besides the difference while generating the answers in step 3, compared with Protocol 1, the interpretation of the answers and user's way of decoding are all different. We will explain these in the following subsection.

### B. MCSA Classical E-B-MDS-X-TPIR—Another Interpretation

Though the MDS property of the MCSA code guarantees the decodability of message symbols when there are unresponsive and Byzantine servers, in order to make it compatible with the Q-E-B-MDS-X-TPIR scheme based on syndrome measurement of a CSS code, we interpret answers from MCSA code based classical E-B-MDS-X-TPIR scheme as the GRS code of the interfering symbols  $*$ , with CRS encoded desired message symbols added as “errors.” With this interpretation, the decoding of the classical scheme is based on the syndrome decoding of a GRS code.

Specifically, the corrupted answer (after subtracting  $\sigma$  which is known) in (50) can be interpreted as  $\text{GRS}_{N,V}^{q,(\alpha,u)}$  encoded interfering symbols, corrupted by the “errors” caused by CRS

encoded message symbols, erasures and Byzantine errors.  $\mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}} \in \mathbb{F}_q^{N \times (N-V)}$  is the parity check matrix of  $\text{GRS}_{N,V}^{q,(\alpha,u)}$ , and (51) follows from  $\mathbf{H}^\top \mathbf{G} = \mathbf{0}$ .

Next let us prove Lemma 2 which guarantees the existence of the decoding function  $\Phi_{\mathcal{E}}^{\text{GRS}}$  in (52). Essentially, Lemma 2 says that *all the correctable “errors” (including “errors” introduced by desired message symbols) have different syndromes*. The “errors” introduced by desired messages are similar to erasures in the sense that we know their error basis (columns of  $\mathbf{G}_{\text{CRS}}$ ). Thus, when  $L + E + 2B \stackrel{(28)}{=} N - V = d - 1$  where  $L$  is the dimension of the message symbols and  $d = N - V + 1$  is the minimum distance of the the GRS code, all the “errors”, including those caused by the desired message symbols, can be decoded from the syndrome.

**Lemma 2.** *Let  $L + E + 2B = N - V$ , as stated in (28). For any given unresponsive servers  $\mathcal{E} \subset [N]$ ,  $|\mathcal{E}| \leq E$  and any two sets of Byzantine servers  $\mathcal{B}, \mathcal{B}' \subset [N]$ ,  $|\mathcal{B}|, |\mathcal{B}'| \leq B$ , the syndromes will differ for any two distinct pairs  $(\mathbf{w}, \epsilon_{\mathcal{E} \cup \mathcal{B}}) \neq (\mathbf{w}', \epsilon'_{\mathcal{E} \cup \mathcal{B}'})$ , where  $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_q^L$ ,  $\epsilon_{\mathcal{E} \cup \mathcal{B}}, \epsilon'_{\mathcal{E} \cup \mathcal{B}'} \in \mathbb{F}_q^{N \times 1}$ ,  $\text{supp}(\epsilon_{\mathcal{E} \cup \mathcal{B}}) = \mathcal{E} \cup \mathcal{B}$  and  $\text{supp}(\epsilon'_{\mathcal{E} \cup \mathcal{B}'}) = \mathcal{E} \cup \mathcal{B}'$ , i.e.,*

$$\begin{aligned} & \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \left( \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \mathbf{w} + \epsilon_{\mathcal{E} \cup \mathcal{B}} \right) \\ & \neq \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \left( \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \mathbf{w}' + \epsilon'_{\mathcal{E} \cup \mathcal{B}'} \right) \end{aligned} \quad (53)$$

This implies the existence of the decoding function  $\Phi_{\mathcal{E}}^{\text{GRS}}: \mathbb{F}_q^{N \times 1} \rightarrow \mathbb{F}_q^{L \times 1} \times \mathbb{F}_q^{N \times 1}$  in (52).

*Proof.* See Appendix C. □

*C. Example 2:  $E = 0, B = 1, K_c = 1, X = 1, T = 1$  with  $N = 6$  Servers: Protocol 2*

Let  $L = N - (K_c + 2B + X + T - 1) = 2$  and  $\alpha_1, \dots, \alpha_{N=6}, f_1, f_{L=2}$  be 8 distinct elements over  $\mathbb{F}_q$  ( $q \geq 8$ ). Also, let  $u_1, u_2, \dots, u_6$  be 6 non-zero elements from  $\mathbb{F}_q$ . Let  $w_{[K]}$  be the realizations of all the  $K$  messages  $W_{[K]}$ . Each message has  $L \times K_c = 2$  symbols from  $\mathbb{F}_q$ , i.e., for any  $k \in [K]$ , message  $w_k = \{w_k(i, j)\}_{i \in [2], j=1}$  contains 2 symbols from  $\mathbb{F}_q$ . Let  $\dot{\mathbf{w}}_{1,1}, \dot{\mathbf{w}}_{2,1} \in \mathbb{F}_q^{1 \times K}$  denote the row vectors that contain the 2 symbols of the  $K$  messages, respectively, i.e.,

$$w_k = \begin{bmatrix} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^k \\ \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^k \end{bmatrix} \quad (54)$$

where  $\mathbf{e}_K^k$  is the  $k^{\text{th}}$  column vector of  $\mathbf{I}_K$ .

We skip the storage and queries. The (corrupted) answers from the servers have the following representation, where server 2 is Byzantine so that an error is added to its answer. Note that  $V = K_c + X + T - 1 = 2$ , and since  $K_c = 1$ , there is only  $\hat{\mathbf{a}}^{(1)}$  with  $\boldsymbol{\sigma}^{(0)} = \mathbf{0}$ .

$$\begin{aligned}
\hat{\mathbf{a}}^{(1)} &= \begin{bmatrix} \hat{a}_1^{(1)} & \hat{a}_2^{(1)} & \hat{a}_3^{(1)} & \hat{a}_4^{(1)} & \hat{a}_5^{(1)} & \hat{a}_6^{(1)} \end{bmatrix}^\top \\
&= \begin{bmatrix} \frac{u_1}{f_1 - \alpha_1} & \frac{u_1}{f_2 - \alpha_1} & u_1 & u_1 \alpha_1 \\ \frac{u_2}{f_1 - \alpha_2} & \frac{u_2}{f_2 - \alpha_2} & u_2 & u_2 \alpha_2 \\ \frac{u_3}{f_1 - \alpha_3} & \frac{u_3}{f_2 - \alpha_3} & u_3 & u_3 \alpha_3 \\ \frac{u_4}{f_1 - \alpha_4} & \frac{u_4}{f_2 - \alpha_4} & u_4 & u_4 \alpha_4 \\ \frac{u_5}{f_1 - \alpha_5} & \frac{u_5}{f_2 - \alpha_5} & u_5 & u_5 \alpha_5 \\ \frac{u_6}{f_1 - \alpha_6} & \frac{u_6}{f_2 - \alpha_6} & u_6 & u_6 \alpha_6 \end{bmatrix} \begin{bmatrix} \dot{\mathbf{w}}_{1,1} \mathbf{e}_K^\theta \\ \dot{\mathbf{w}}_{2,1} \mathbf{e}_K^\theta \\ * \\ * \end{bmatrix} + \begin{bmatrix} 0 \\ \epsilon \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\
&= \mathbf{G}_{\text{GRS}_{6,2}^{q,(\alpha,u)}} * + \underbrace{\mathbf{G}_{\text{CRS}_{6,2}^{q,(\alpha,f,u)}} w_\theta(:, 1)}_{\text{“error”}} + \boldsymbol{\epsilon}_{\{2\}}^{(1)} \tag{55}
\end{aligned}$$

The error correcting capability of the  $[6, 2, 5]$  GRS code will be utilized to find the two desired message symbols and the server 2 introduced error  $\epsilon$ , i.e., the syndrome  $\mathbf{H}_{\text{GRS}_{6,2}^{q,(\alpha,u)}}^\top \hat{\mathbf{a}}^{(1)}$  uniquely determines the  $w_\theta = \underline{w_\theta(:, 1)}$  and  $\boldsymbol{\epsilon}_{\{2\}}^{(1)}$ .

## VII. MCSA-CSS PROTOCOL FOR Q-E-B-MDS-X-TPIR

In this section, we propose the MCSA-CSS protocol for the Q-E-B-MDS-X-TPIR problem, based on syndrome measurement of a CSS code, that is constructed from GRS sub-codes of two MCSA codes. Exploiting the fact that the dual code of a GRS code is still a GRS code, a CSS code with  $N$  physical qudits can be constructed from two GRS codes. The  $N$  physical qudits are then delivered to  $N$  servers.<sup>8</sup> Two MCSA codes based classical PIR schemes are executed, and servers apply Pauli operators to the CSS code according to the answers from the classical scheme. The components of Pauli operators corresponding to the GRS sub-codes of interfering symbols are not detectable, because they commute with the stabilizers. This is due to the fact that the CSS code is constructed from the *same* GRS codes. However, the components associated with the Cauchy RS code encoded message symbols (regarded as “errors”), along with errors introduced by unresponsive and Byzantine servers, are identified through syndrome measurements.

<sup>8</sup>Let us clarify that the CSS code is not used to deliver logical qudits to servers. The  $N$  physical qudits are initially in a constant pure state and are shared as quantum resources for improving communication efficiency.

### A. MCSA-CSS Protocol

The MCSA-CSS scheme is presented as Protocol 3. During one execution of the quantum scheme, two independent instances of classical schemes will be executed. Thus, each message has  $2LK_c$  symbols from  $\mathbb{F}_q$ , and the randomness also has twice the size as that in classical cases.

Let  $w_{[K]}$  be the realizations of  $W_{[K]}$ , for any  $k \in [K]$ . We have  $w_k = [w_k^X \ w_k^Z] \in \mathbb{F}_q^{L \times 2K_c}$  where

$$\begin{aligned} w_k^X &= (w_k^X(l, \kappa))_{l \in [L], \kappa \in [K_c]}, \\ w_k^Z &= (w_k^Z(l, \kappa))_{l \in [L], \kappa \in [K_c]} \in \mathbb{F}_q^{L \times K_c} \end{aligned} \quad (56)$$

stand for the  $X, Z$  parts of message  $k$  respectively, so that each part has the same size to a message in the classical case. Similar to (40), define the length- $K$  vector that contains the  $(l, \kappa)^{th}$  symbol of all the  $K$  messages'  $\star$  part ( $\star \in \{X, Z\}$ ) as

$$\begin{aligned} \dot{\mathbf{w}}_{l, \kappa}^\star &\triangleq [w_1^\star(l, \kappa) \ w_2^\star(l, \kappa) \ \cdots \ w_K^\star(l, \kappa)], \\ &\forall l \in [L], \kappa \in [K_c]. \end{aligned} \quad (57)$$

Similarly,  $Z = \{Z^X, Z^Z\}, Z' = \{Z'^X, Z'^Z\}$ . Each  $Z^\star, Z'^\star, \star \in \{X, Z\}$  is specified similarly according to (42) as follows

$$\begin{aligned} Z^\star &= \{\mathbf{Z}_{l, x}^\star\}_{l \in [L], x \in [X]}, \mathbf{Z}_{l, x}^\star \in \mathbb{F}_q^{K \times 1}, \\ Z'^\star &= \{\mathbf{Z}_{l, t}'^{(\kappa)\star}\}_{l \in [L], \kappa \in [K_c], t \in [T]}, \mathbf{Z}_{l, t}'^{(\kappa)\star} \in \mathbb{F}_q^{1 \times K}. \end{aligned} \quad (58)$$

Again, let  $z, z'$  be their realizations. Let us pick some constants  $\mathbf{u} = (u_1, \dots, u_N) \in \mathbb{F}_q^N$  s.t.  $u_n \neq 0, \forall n \in [N]$ . Meanwhile, set  $\mathbf{v} = (v_1, \dots, v_N)$  as

$$v_i = u_i^{-1} \prod_{j \neq i} (\alpha_i - \alpha_j)^{-1}, \forall i \in [N]. \quad (59)$$

The protocol is specified as follows. Note that  $\mathbf{u}, \mathbf{v}$  are constants specified by the protocol.

#### Protocol 3. Q-E-B-MDS-X-TPIR:

MCSA-CSS  $\left( \{\dot{\mathbf{w}}_{l, \kappa}^X, \dot{\mathbf{w}}_{l, \kappa}^Z\}_{l \in [L], \kappa \in [K_c]}, z, z', \mathbf{u}, \mathbf{v} \right)$  (Quantum)

1) **Share Entanglement:** For all  $\kappa \in [K_c]$ ,  $N$   $q$ -dimensional qudits  $\mathcal{A}_{[N]}^{(\kappa)}$ , with initial state

$$\begin{aligned} \rho_{\mathcal{A}_{[N]}^{(\kappa)}}^0 &= |\psi\rangle \langle \psi|, \\ |\psi\rangle &\in \text{CSS} \left( \text{GRS}_{N, V}^{q, (\alpha, \mathbf{v})}, \text{GRS}_{N, V}^{q, (\alpha, \mathbf{u})} \right) \end{aligned} \quad (60)$$

are delivered to  $N$  servers so that server  $N$  gets  $\mathcal{A}_n^{(\kappa)}$ . We let

$$\rho_{\{\mathcal{A}_{[N]}^{(\kappa)}\}_{\kappa \in [K_c]}}^0 = \bigotimes_{\kappa \in [K_c]} \rho_{\mathcal{A}_{[N]}^{(\kappa)}}^0.$$

- 2) **Storage, Queries, Answers:** Two independent instances (indexed by  $X$  and  $Z$ ) of Protocol 2 will be executed to generate storage, queries and corresponding classical answers. Specifically, execute Protocol 2 with following parameters, so that the storage, queries, and classical answers can be determined by corresponding steps in Protocol 2, which are, again, generated according to the 3 functions specified in Appendix B.

E-B-MDS-X-TPIR:

$$\text{MCSA} \left( \left\{ \dot{\mathbf{w}}_{l,\kappa}^X \right\}_{l \in [L], \kappa \in [K_c]}, z^X, z'^X, \mathbf{u} \right),$$

E-B-MDS-X-TPIR:

$$\text{MCSA} \left( \left\{ \dot{\mathbf{w}}_{l,\kappa}^Z \right\}_{l \in [L], \kappa \in [K_c]}, z^Z, z'^Z, \mathbf{v} \right). \quad (61)$$

For iteration  $\kappa \in [K_c]$ , the following classical answers are generated according to (49) where  $\mathbf{a}^{(\kappa)\star} = [a_1^{(\kappa)\star} \ \dots \ a_N^{(\kappa)\star}]^\top \in \mathbb{F}_q^{N \times 1}$  such that  $a_N^{(\kappa)\star}$  is known to server  $n$  for  $\star \in \{X, Z\}$ .

$$\begin{aligned} \mathbf{a}^{(\kappa)X} &= \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}} \star^X + \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \underline{w_\theta^{(\kappa)X}(:, \kappa)} \\ &\quad + \sigma^{(\kappa-1)X}, \\ \mathbf{a}^{(\kappa)Z} &= \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{v})}} \star^Z + \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{v})}} \underline{w_\theta^{(\kappa)Z}(:, \kappa)} \\ &\quad + \sigma^{(\kappa-1)Z}. \end{aligned} \quad (62)$$

Server  $n, n \in [N]$  applies  $X^{a_n^{(\kappa)X}} Z^{a_n^{(\kappa)Z}}$  to qudit  $\mathcal{A}_n^{(\kappa)}$  so that the  $N$  answer qudits are in the following state <sup>9</sup>.

$$\rho_{\mathcal{A}_{[N]}^{(\kappa)}}^1 = \left( X^{\mathbf{a}^{(\kappa)X}} Z^{\mathbf{a}^{(\kappa)Z}} \right) \rho_{\mathcal{A}_{[N]}^{(\kappa)}}^0 \left( X^{\mathbf{a}^{(\kappa)X}} Z^{\mathbf{a}^{(\kappa)Z}} \right)^\dagger. \quad (63)$$

- 3) **Corrupted Answers:** For iteration  $\kappa \in [K_c]$ , the user replaces the unreceived qudits  $\mathcal{A}_{\mathcal{E}}^{(\kappa)}$  with  $|\mathcal{E}|$  qudits that are in completely mixed state and labels them  $\mathcal{A}_{\mathcal{E}}^{(\kappa)}$ . The received qudits

<sup>9</sup>For ease of analysis, we assume unresponsive or Byzantine servers firstly behave as reliable servers that apply correct Pauli operators to their qudits and then apply a CPTP map  $\mathcal{M}$ . There is no loss of generality since any actual CPTP map  $\mathcal{M}'$  applied by the unreliable servers can be viewed as a composition of 1) applying correct Pauli operators, 2) reverting the Pauli operators, 3) applying  $\mathcal{M}'$  where the composition of the last 2 steps is  $\mathcal{M}$ .

are in the following state due to the quantum channels applied by unresponsive and Byzantine servers.

$$\rho_{\mathcal{A}_{[N]}^{(\kappa)}}^2 = \text{id} \otimes \mathcal{M}_{\mathcal{E} \cup \mathcal{B}}(\rho_{\mathcal{A}_{[N]}^{(\kappa)}}^1) \quad (64)$$

- 4) **Decoding:** For each iteration  $\kappa \in [K_c]$ , the user performs syndrome measurement of  $\text{CSS}(\text{GRS}_{N,V}^{q,(\alpha,u)}, \text{GRS}_{N,V}^{q,(\alpha,v)})$ . The state becomes

$$\begin{aligned} \rho_{\mathcal{A}_{[N]}^{(\kappa)} | \mathbf{s}^{(\kappa)X}, \mathbf{s}^{(\kappa)Z}}^3 \\ = \mathbf{X}^{\hat{\mathbf{a}}^{(\kappa)X}} \mathbf{Z}^{\hat{\mathbf{a}}^{(\kappa)Z}} \rho_{\mathcal{A}_n^{(\kappa)}}^0 \left( \mathbf{X}^{\hat{\mathbf{a}}^{(\kappa)X}} \mathbf{Z}^{\hat{\mathbf{a}}^{(\kappa)Z}} \right)^\dagger, \end{aligned} \quad (65)$$

$$\text{where for } \star \in \{X, Z\}, \quad \hat{\mathbf{a}}^{(\kappa)\star} = \mathbf{a}^{(\kappa)\star} + \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)\star} \quad (66)$$

for some  $\boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)\star} \in \mathbb{F}_q^{N \times 1}$ . The user obtains the syndrome

$$\begin{aligned} \mathbf{s}^{(\kappa)X} &= \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \hat{\mathbf{a}}^{(\kappa)X}, \\ \mathbf{s}^{(\kappa)Z} &= \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,v)}}^\top \hat{\mathbf{a}}^{(\kappa)Z} \end{aligned} \quad (67)$$

and decodes the desired message symbols through

$$\begin{aligned} \Phi_{\mathcal{E}}^{\text{GRS}} \left( \mathbf{s}^{(\kappa)X} - \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \boldsymbol{\sigma}^{(\kappa-1)X} \right) \\ = \left( w_\theta^X(:, \kappa), \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)X} \right), \\ \Phi_{\mathcal{E}}^{\text{GRS}} \left( \mathbf{s}^{(\kappa)Z} - \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,v)}}^\top \boldsymbol{\sigma}^{(\kappa-1)Z} \right) \\ = \left( w_\theta^Z(:, \kappa), \boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}}^{(\kappa)Z} \right). \end{aligned} \quad (68)$$

**Remark 8.** We require  $V = K_c + X + T - 1 \geq N/2$ , i.e., interfering symbols occupy at least half of the answer dimensions, so that the CSS code can be constructed from the GRS codes. Consider the second regime of Theorem 1, i.e.,  $(N - E - 2B) \geq N/2 > K_c + X + T - 1$ , where  $N$  is odd. Though it is not possible to find an integer  $\bar{T} > T$  such that  $K_c + X + \bar{T} - 1 = N/2$ , one can find  $T_1 > T, T_2 \geq T, T_1 = T_2 + 1$  such that the total interfering dimensions (this idea is also used in the preliminary ArXiv version of this paper [36, Theorem 1] and in the subsequent 2<sup>nd</sup> version of [33])

$$K_c + X + T_1 - 1 + K_c + X + T_2 - 1 = N. \quad (69)$$

This means that while constructing the two instances of the classical scheme, we have  $T_1$  privacy for the  $X$  instance, and  $T_2$  privacy for the  $Z$  instance. By such choice of  $T_1, T_2$ , during each of

$K_c$  iterations, in the first instance,  $L_1 = N - E - 2B - K_c - X - T_1 + 1$  symbols of desired message are delivered, and in the second instance,  $L_2 = N - E - 2B - K_c - X - T_2 + 1$  symbols are delivered. Thus, in total  $L_1 + L_2 \stackrel{(69)}{=} N - 2E - 4B$  symbols are delivered. The rate  $R^Q = (N - 2E - 4B)/N$  is thus achieved. The key is that the CSS code will be constructed from an  $[N, \lfloor N/2 \rfloor]$  GRS code and an  $[N, \lceil N/2 \rceil]$  GRS code.

Before analyzing the protocol, let us provide an intuitive explanation. The CSS code is constructed based on the GRS sub-codes of two instances of MCSA codes designed for the PIR problem. Since the GRS sub-code corresponds to interfering symbols, the Pauli operators associated with these interfering symbols commute with the stabilizers of the CSS code and, therefore, cannot be detected through syndrome measurement. In contrast, the Pauli operators associated with message symbols, along with any erasures or Byzantine errors, shift the  $N$  qudits into an error space that can be uniquely identified through syndrome measurement. In this interpretation, the message symbols act as sources of “errors.” However, since these “errors” introduced by message symbols have a known basis, they are no more detrimental than erasures. Combined with the fact that a Pauli error corresponds to both  $X$  and  $Z$  errors, each of which can carry classical messages, the CSS code used in Protocol 3 with minimum distance  $d \geq \min(d_X, d_Z) = N - V + 1$  can transmit  $2L$  classical symbols, correct  $E$  erasures and  $B$  Byzantine errors as long as  $L + E + 2B \stackrel{(28)}{=} N - V = \min(d_X, d_Z) - 1 \leq d - 1$ .

### B. Analysis of MCSA-CSS Protocol

Let us first prove its correctness.

1) *Existence of the CSS Code:* According to [20, (5.1.6) Theorem], with the choice of  $\mathbf{v}$  in (59), we have  $\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})^\perp} = \text{GRS}_{N,N-V}^{q,(\alpha,\mathbf{v})} \subset \text{GRS}_{N,V}^{q,(\alpha,\mathbf{v})}$  when  $V \geq N/2$ . Thus the CSS  $\left(\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}, \text{GRS}_{N,V}^{q,(\alpha,\mathbf{v})}\right)$  code exists.

2) *Corrupted Answers:* Without loss of generality we assume all the unresponsive and Byzantine servers first apply the correct Pauli Gates as other (reliable) servers, and then apply an arbitrary quantum channel afterwards, as an arbitrary quantum channel can be regarded as a composition of Pauli Gates with another quantum channel.

Recall that we replaced the unreceived qudits with qudits in completely mixed state. This can be viewed as if the unresponsive servers’ answer qudits were received but went through a quantum depolarizing channel (Qudit Twirl, [41, Exercise 4.7.6]). Thus the state derived in (64) is correct.

3) *State after Syndrome Measurement*: The two underlying GRS codes of the CSS code have distance  $d_X = d_Z = N - V + 1 \geq N - (L + V) + 1 \stackrel{(28)}{=} E + 2B + 1$ , thus  $\min(d_X, d_Z) \geq E + 2B + 1$ . Thus  $|\mathcal{E} \cup \mathcal{B}| \leq E + B \leq \min(d_X, d_Z) - 1$ , and according to Lemma 1, the error reduces to Pauli Operators and (65) is correct.

4) *Syndrome and Decoding*: Again, according to Lemma 1, (67) is correct and the decoding reduces to classical case by identifying (62), (66), (67) with (49), (50), (51). Thus the decodability is guaranteed by the decoder in Protocol 2.

5) *MDS, Security and Privacy*: The satisfaction of these constraints is ensured by Protocol 2, which, in turn, is guaranteed by Protocol 1, as demonstrated in [21]. Note that the pre-shared entangled systems do not break the privacy or security since they are completely independent of the messages, randomness, and the index of the desired message.

Finally, consider the rate of the Q-E-B-MDS-X-TPIR scheme in Protocol 3. In each iteration  $\kappa \in [K_c]$ ,  $N$  qudits are downloaded, and  $2L$  desired message symbols  $w^{(\kappa)X}(:, \kappa), w^{(\kappa)Z}(:, \kappa)$  are retrieved. Therefore, the overall rate is

$$R^Q = \frac{2K_c L}{K_c N} = \frac{2(N - E - 2B - K_c - X - T + 1)}{N}. \quad (70)$$

## VIII. CONCLUSION

The Q-E-B-MDS-X-TPIR problem is studied where the main challenge is to find a coding structure that is compatible with  $X$ -secure, MDS storage,  $T$ -privacy and the construction of quantum CSS code (MCSA codes), while satisfying erasure and Byzantine error-resilience. The new scheme, MCSA-CSS, leverages the error-correcting capabilities of CSS code to efficiently encode desired computation results (desired message symbols in the PIR case) into the error space, while correcting quantum erasure and errors. The optimality of the proposed scheme remains a challenging open question. Application of MCSA-CSS to quantum coded distributed computation is a promising direction for future work.

## APPENDIX

### A. Proof of Lemma 1

While the distance of CSS code can be greater than  $\min(d_X, d_Z)$ , let us define  $d \triangleq \min(d_X, d_Z)$  in this proof for ease of notation. Let us prove Lemma 1 for  $\mathcal{S} = [d - 1]$ . The proof for other realizations of  $\mathcal{S}$  follows similarly.



The initial state is  $\rho^0 = X^x Z^z |\psi\rangle \langle \psi| (X^x Z^z)^\dagger$ . After applying the quantum channel, using the Kraus representation of the channel, we have

$$\begin{aligned} \rho^1 = \sum_i (K_i \otimes X^0 Z^0) X^x Z^z |\psi\rangle \\ \cdot \langle \psi| (X^x Z^z)^\dagger (K_i \otimes X^0 Z^0)^\dagger \end{aligned} \quad (71)$$

where  $K_i \in \mathbb{C}^{q^{(d-1)} \times q^{(d-1)}}$  and  $\mathbf{0}$  has length  $(n - d + 1)$ .

Since the  $\{X^\alpha Z^\beta\}_{\alpha, \beta \in \mathbb{F}_q^{(d-1)} \times 1}$  form a basis for the linear space of all  $q^{(d-1)} \times q^{(d-1)}$  complex matrices [37], by representing  $K_i$  as linear combinations of Pauli operators,  $\rho^1$  can be further written as

$$\begin{aligned} \rho^1 = \sum_{\alpha, \beta, \alpha', \beta' \in \mathbb{F}_q^{(d-1)}} c_{\alpha, \beta}^{\alpha', \beta'} (X^\alpha Z^\beta \otimes X^0 Z^0) X^x Z^z |\psi\rangle \\ \cdot \langle \psi| (X^x Z^z)^\dagger (X^{\alpha'} Z^{\beta'} \otimes X^0 Z^0)^\dagger \\ \stackrel{(3)}{=} \sum_{\mu, \tau, \mu', \tau' \in \mathcal{F}} \tilde{c}_{\mu, \tau}^{\mu', \tau'} X^{x+\mu} Z^{z+\tau} |\psi\rangle \langle \psi| (X^{x+\mu'} Z^{z+\tau'})^\dagger \end{aligned} \quad (72)$$

where  $c, \tilde{c}$  are some coefficients that depend only on the Kraus Operators, and  $\mu, \tau, \mu', \tau'$  are chosen from

$$\mathcal{F} \triangleq \{\mathbf{v} \in \mathbb{F}_q^{n \times 1} \mid \text{supp}(\mathbf{v}) = [d - 1]\}. \quad (73)$$

After the PVM with orthogonal projections  $\{\mathbf{P}_i^{\mathbf{a}, \mathbf{b}}\}_{i \in \mathbb{F}_p}$  corresponding to stabilizers  $X^{\mathbf{a}} Z^{\mathbf{b}}$ , in (72) we have

$$\begin{aligned} X^{x+\mu} Z^{z+\tau} |\psi\rangle \langle \psi| (X^{x+\mu'} Z^{z+\tau'})^\dagger \longrightarrow \\ \sum_{i \in \mathbb{F}_p} \mathbf{P}_i^{\mathbf{a}, \mathbf{b}} X^{x+\mu} Z^{z+\tau} |\psi\rangle \langle \psi| (X^{x+\mu'} Z^{z+\tau'})^\dagger \mathbf{P}_i^{\mathbf{a}, \mathbf{b}^\dagger}. \end{aligned} \quad (74)$$

Note that  $X^{x+\mu} Z^{z+\tau} |\psi\rangle$  and  $X^{x+\mu'} Z^{z+\tau'} |\psi\rangle$  are eigenvectors of all stabilizers, and we have (75), i.e., after measuring with stabilizer  $X^{\mathbf{a}} Z^{\mathbf{b}}$ ,  $X^{x+\mu} Z^{z+\tau} |\psi\rangle \langle \psi| (X^{x+\mu'} Z^{z+\tau'})^\dagger$  does not disappear if and only if  $X^{x+\mu} Z^{z+\tau} |\psi\rangle$  and  $X^{x+\mu'} Z^{z+\tau'} |\psi\rangle$  lie in the same eigen space of the stabilizer.

$$\begin{aligned}
& \mathbf{P}_i^{\mathbf{a},\mathbf{b}} \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \langle\psi| \left( \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} \right)^\dagger \mathbf{P}_i^{\mathbf{a},\mathbf{b}\dagger} = \\
& \begin{cases} \mathbf{P}_i^{\mathbf{a},\mathbf{b}} \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \mathbf{0}_{1 \times q^n} = \mathbf{0} & \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \in \text{Im}(\mathbf{P}_i^{\mathbf{a},\mathbf{b}}), \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} |\psi\rangle \notin \text{Im}(\mathbf{P}_i^{\mathbf{a},\mathbf{b}}) \\ \mathbf{0}_{q^n \times 1} \langle\psi| \left( \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} \right)^\dagger \mathbf{P}_i^{\mathbf{a},\mathbf{b}\dagger} = \mathbf{0} & \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \notin \text{Im}(\mathbf{P}_i^{\mathbf{a},\mathbf{b}}), \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} |\psi\rangle \in \text{Im}(\mathbf{P}_i^{\mathbf{a},\mathbf{b}}) \\ \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \langle\psi| \left( \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} \right)^\dagger & \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle, \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} |\psi\rangle \in \text{Im}(\mathbf{P}_i^{\mathbf{a},\mathbf{b}}) \end{cases}
\end{aligned} \tag{75}$$


---

Thus, after the syndrome measurement,  $\mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \langle\psi| \left( \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} \right)^\dagger$  exists if and only if for every stabilizer,  $\mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle$  and  $\mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}'} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}'} |\psi\rangle$  lie in the same eigen space, or equivalently, they correspond to the same syndrome (similar to Proposition 1)

$$\begin{aligned}
& \mathbf{H}_{\mathcal{C}_Z}^\top (\mathbf{x} + \boldsymbol{\mu}) = \mathbf{H}_{\mathcal{C}_Z}^\top (\mathbf{x} + \boldsymbol{\mu}') \\
& \rightarrow \mathbf{H}_{\mathcal{C}_Z}^\top (\boldsymbol{\mu} - \boldsymbol{\mu}') = \mathbf{0} \rightarrow \boldsymbol{\mu} = \boldsymbol{\mu}',
\end{aligned} \tag{76}$$

$$\begin{aligned}
& \mathbf{H}_{\mathcal{C}_X}^\top (\mathbf{z} + \boldsymbol{\tau}) = \mathbf{H}_{\mathcal{C}_X}^\top (\mathbf{z} + \boldsymbol{\tau}') \\
& \rightarrow \mathbf{H}_{\mathcal{C}_X}^\top (\boldsymbol{\tau} - \boldsymbol{\tau}') = \mathbf{0} \rightarrow \boldsymbol{\tau} = \boldsymbol{\tau}',
\end{aligned} \tag{77}$$

where last the step of (76) follows from the fact that  $\text{wt}(\boldsymbol{\mu} - \boldsymbol{\mu}') \leq \min(d_X, d_Z) - 1 \leq d_Z - 1$ , i.e.,  $\boldsymbol{\mu} - \boldsymbol{\mu}' \notin \mathcal{C}_Z = \ker(\mathbf{H}_{\mathcal{C}_Z})$  if  $\boldsymbol{\mu} - \boldsymbol{\mu}' \neq \mathbf{0}$  (the last step of (77) follows similarly). After syndrome measurement, the  $n$  qudits are in the state,

$$\rho^2 = \sum_{\boldsymbol{\mu}, \boldsymbol{\tau} \in \mathcal{F}} c'_{\boldsymbol{\mu}, \boldsymbol{\tau}} \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \langle\psi| \left( \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} \right)^\dagger. \tag{78}$$

Suppose the outcome of syndrome measurement is  $\mathbf{s}_X = \mathbf{H}_{\mathcal{C}_Z}^\top (\mathbf{x} + \boldsymbol{\epsilon}_{[d-1]}^X)$ ,  $\mathbf{s}_Z = \mathbf{H}_{\mathcal{C}_X}^\top (\mathbf{z} + \boldsymbol{\epsilon}_{[d-1]}^Z)$  with  $\boldsymbol{\epsilon}_{[d-1]}^X, \boldsymbol{\epsilon}_{[d-1]}^Z \in \mathcal{F}$ . Then  $\forall \boldsymbol{\mu}, \boldsymbol{\tau} \in \mathcal{F}$ , the term  $\mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} |\psi\rangle \langle\psi| \left( \mathbf{X}^{\mathbf{x}+\boldsymbol{\mu}} \mathbf{Z}^{\mathbf{z}+\boldsymbol{\tau}} \right)^\dagger$  does not disappear if and only if,

$$\mathbf{H}_{\mathcal{C}_Z}^\top (\mathbf{x} + \boldsymbol{\mu}) = \mathbf{H}_{\mathcal{C}_Z}^\top (\mathbf{x} + \boldsymbol{\epsilon}_{[d-1]}^X) \rightarrow \boldsymbol{\mu} = \boldsymbol{\epsilon}_{[d-1]}^X, \tag{79}$$

$$\mathbf{H}_{\mathcal{C}_X}^\top (\mathbf{z} + \boldsymbol{\tau}) = \mathbf{H}_{\mathcal{C}_X}^\top (\mathbf{z} + \boldsymbol{\epsilon}_{[d-1]}^Z) \rightarrow \boldsymbol{\tau} = \boldsymbol{\epsilon}_{[d-1]}^Z, \tag{80}$$

where the correctness of the last steps follows by the same reasoning as that for (76) and (77).

Thus, the state becomes

$$\rho_{|s_X, s_Z}^3 = \mathbf{X}^{\mathbf{x} + \epsilon_{[d-1]}^X} \mathbf{Z}^{\mathbf{z} + \epsilon_{[d-1]}^Z} |\psi\rangle \langle \psi| \left( \mathbf{X}^{\mathbf{x} + \epsilon_{[d-1]}^X} \mathbf{Z}^{\mathbf{z} + \epsilon_{[d-1]}^Z} \right)^\dagger. \quad (81)$$

### B. Storage, Queries, Answers Generation in [21]

<p>StoreGen <math>\left( \{\dot{\mathbf{w}}_{l,\kappa}\}_{l \in [L], \kappa \in [K_c]}, z = \{\mathbf{z}_{l,x}\}_{l \in [L], x \in [X]} \right)</math></p> <p>For all <math>n \in [N], l \in [L]</math></p> $s_n = [s_n(1) \ s_n(2) \ \cdots \ s_n(L)]$ $s_n(l) = \sum_{l \in [L], \kappa \in [K_c]} \frac{1}{(f_l - \alpha_n)^{K_c - \kappa + 1}} \dot{\mathbf{w}}_{l,\kappa}$ $+ \sum_{x \in [X]} (f_l - \alpha_n)^{x-1} \mathbf{z}_{l,x} \in \mathbb{F}_q^{1 \times K} \quad (82)$ <p>Return <math>s_{[N]}</math></p>
<p>QueryGen <math>\left( \theta, z' = \{\mathbf{z}'_{l,t}^{(\kappa)}\}_{l \in [L], t \in [T], \kappa \in [K_c]} \right)</math></p> <p>For all <math>n \in [N], l \in [L]</math></p> $q_n = \{q_n^{(1)}, q_n^{(2)}, \dots, q_n^{(K_c)}\}$ $q_n^{(\kappa)} = [q_n^{(\kappa)}(1); \ q_n^{(\kappa)}(2); \ \dots; \ q_n^{(\kappa)}(L)]$ $q_n^{(\kappa)}(l) = \sum_{l \in [L], \kappa \in [K_c]} (f_l - \alpha_n)^{K_c - \kappa} \mathbf{e}_K^\theta$ $+ \sum_{t \in [T]} (f_l - \alpha_n)^{K_c + t - 1} \mathbf{z}'_{l,t}^{(\kappa)} \in \mathbb{F}_q^{K \times 1} \quad (83)$ <p>Return <math>q_{[N]}</math></p>
<p>AnsGen <math>\left( s_{[N]}, \{q_{[N]}^{(\kappa)}\}_{\kappa \in [K_c]} \right)</math></p> <p>For all <math>n \in [N], \kappa \in [K_c]</math></p> $a_n = \{a_n^{(1)}, a_n^{(2)}, \dots, a_n^{(K_c)}\}$ $a_n^{(\kappa)} = s_n q_n^{(\kappa)} \in \mathbb{F}_q \quad (84)$ <p>Return <math>a_{[N]} = \{a_{[N]}^{(\kappa)}\}_{\kappa \in [K_c]}</math></p>

### C. Proof of Lemma 2

We only need to prove

$$\begin{aligned} & \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}}^\top \left( \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \underbrace{(\mathbf{w} - \mathbf{w}')}_{\triangleq \mathbf{w}''} + \underbrace{(\boldsymbol{\epsilon}_{\mathcal{E} \cup \mathcal{B}} - \boldsymbol{\epsilon}'_{\mathcal{E} \cup \mathcal{B}'})}_{\triangleq \boldsymbol{\epsilon}''_{\mathcal{E} \cup \mathcal{B} \cup \mathcal{B}'}} \right) \\ & \neq \mathbf{0}, \quad \forall (\mathbf{w}'', \boldsymbol{\epsilon}''_{\mathcal{E} \cup \mathcal{B} \cup \mathcal{B}'}) \neq (\mathbf{0}, \mathbf{0}). \end{aligned} \quad (85)$$

Note that since  $|\mathcal{E} \cup \mathcal{B} \cup \mathcal{B}'| \leq E + 2B$ , we can find a set  $\mathcal{S} \subset [N]$  where  $|\mathcal{S}| = E + 2B$  and  $\mathcal{E} \cup \mathcal{B} \cup \mathcal{B}' \subset \mathcal{S}$  so that

$$\boldsymbol{\epsilon}''_{\mathcal{E} \cup \mathcal{B} \cup \mathcal{B}'} = \mathbf{I}_N(:, \mathcal{S}) \boldsymbol{\epsilon}'', \boldsymbol{\epsilon}'' \in \mathbb{F}_q^{(E+2B) \times 1}. \quad (86)$$

Thus, we only need to prove for all length- $(L+E+2B \stackrel{(28)}{=} N-V)$  column vectors  $[\mathbf{w}''; \boldsymbol{\epsilon}''] \neq \mathbf{0}$

$$\begin{aligned} & \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}}^\top \left( \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \mathbf{w}'' + \mathbf{I}_N(:, \mathcal{S}) \boldsymbol{\epsilon}'' \right) \\ & = \mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}}^\top \begin{bmatrix} \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} & \mathbf{I}_N(:, \mathcal{S}) \end{bmatrix} \begin{bmatrix} \mathbf{w}'' \\ \boldsymbol{\epsilon}'' \end{bmatrix} \neq \mathbf{0}. \end{aligned} \quad (87)$$

As a consequence, we only need to prove the following  $(N-V) \times (N-V)$  matrix is invertible.

$$\mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}}^\top \begin{bmatrix} \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} & \mathbf{I}_N(:, \mathcal{S}) \end{bmatrix} \quad (88)$$

For invertibility of (88), we first prove the following lemma.

**Lemma 3.** *The following  $N \times N$  matrix is invertible.*

$$\begin{bmatrix} \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}} & \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} & \mathbf{I}_N(:, \mathcal{S}) \end{bmatrix} \quad (89)$$

*Proof.* On one hand,

$$\begin{aligned} & \forall \mathbf{c} \neq \mathbf{0} \in \text{colspan} \left( \begin{bmatrix} \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,\mathbf{u})}} & \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,\mathbf{f},\mathbf{u})}} \end{bmatrix} \right) \\ & \stackrel{(48)}{=} \text{MCSA}_{N,L,V}^{q,(\alpha,\mathbf{f},\mathbf{u})}, \\ & \text{wt}(\mathbf{c}) \geq N - (L + V) + 1, \end{aligned} \quad (90)$$

since  $\text{MCSA}_{N,L,V}^{q,(\alpha,f,u)}$  is an  $[N, L + V]$  MDS code according to Proposition 3. On the other hand,

$$\begin{aligned} \forall \mathbf{c}' \neq \mathbf{0} &\in \text{colspan}(\mathbf{I}_N(:, \mathcal{S})), \\ \text{wt}(\mathbf{c}') &\leq |\mathcal{S}| = \text{rank}(\mathbf{I}_N(:, \mathcal{S})) \\ &= E + 2B \stackrel{(28)}{=} N - (L + V). \end{aligned} \quad (91)$$

Thus,

$$\begin{aligned} &\text{colspan} \left( \begin{bmatrix} \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,u)}} & \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \end{bmatrix} \right) \\ &\cap \text{colspan}(\mathbf{I}_N(:, \mathcal{S})) = \text{colspan}(\mathbf{0}). \end{aligned} \quad (92)$$

Combined with the following equation

$$\begin{aligned} &\text{rank} \left( \begin{bmatrix} \mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,u)}} & \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \end{bmatrix} \right) \\ &= \text{rank} \left( \mathbf{G}_{\text{MCSA}_{N,L,V}^{q,(\alpha,f,u)}} \right) = L + V, \\ &\text{rank}(\mathbf{I}_N(:, \mathcal{S})) = E + 2B \stackrel{(28)}{=} N - (L + V) \end{aligned} \quad (93)$$

the proof is complete.  $\square$

Now let us prove the invertibility of (88) through a contradiction. Suppose to the contrary, the matrix in (88) is not invertible, then there exists  $\mathbf{v} \in \mathbb{F}_q^{(N-V) \times 1}$ ,  $\mathbf{v} \neq \mathbf{0}$  such that

$$\mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top \underbrace{\begin{bmatrix} \mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} & \mathbf{I}_N(:, \mathcal{S}) \end{bmatrix}}_{\triangleq \mathbf{v}' \in \mathbb{F}_q^{N \times 1}} \mathbf{v} = \mathbf{0}. \quad (94)$$

On the one hand, by definition  $\mathbf{v}' \in \text{colspan}([\mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \quad \mathbf{I}_N(:, \mathcal{S})])$ . Additionally,  $\mathbf{v}' \neq \mathbf{0}$  since  $[\mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \quad \mathbf{I}_N(:, \mathcal{S})]$  has rank  $N - V$  according to Lemma 3 and because  $\mathbf{v} \neq \mathbf{0}$ . On the other hand,  $\mathbf{v}' \in \ker(\mathbf{H}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}^\top) = \text{colspan}(\mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,u)}})$ .

A contradiction occurs since  $\text{colspan}([\mathbf{G}_{\text{CRS}_{N,L}^{q,(\alpha,f,u)}} \quad \mathbf{I}_N(:, \mathcal{S})]) \cap \text{colspan}(\mathbf{G}_{\text{GRS}_{N,V}^{q,(\alpha,u)}}) = \text{colspan}(\mathbf{0}) \not\ni \mathbf{v}'$  according to Lemma 3. Therefore, (88) is invertible.

## REFERENCES

- [1] A. Shamir, “How to share a secret,” *Commun. of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [2] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” *Physical review letters*, vol. 83, no. 3, p. 648, 1999.
- [3] K. Senthoor and P. K. Sarvepalli, “Theory of communication efficient quantum secret sharing,” *IEEE Trans. on Inform. Theory*, vol. 68, no. 5, pp. 3164–3186, 2022.
- [4] M. Hayashi and S. Song, “Unified approach to secret sharing and symmetric private information retrieval with colluding servers in quantum systems,” *IEEE Trans. on Inform. Theory*, vol. 69, no. 10, pp. 6537–6563, 2023.

- [5] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Journal of the ACM*, vol. 45, no. 6, pp. 965–981, 1998.
- [6] H. Sun and S. A. Jafar, "The capacity of robust private information retrieval with colluding databases," *IEEE Trans. on Inform. Theory*, vol. 64, no. 4, pp. 2361–2370, 2017.
- [7] R. Freij-Hollanti, O. W. Gnilke, C. Hollanti, and D. A. Karpuk, "Private information retrieval from coded databases with colluding servers," *SIAM J. on Appl. Algebra and Geometry*, vol. 1, no. 1, pp. 647–664, 2017.
- [8] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, and C. Hollanti, "Private information retrieval from coded storage systems with colluding, Byzantine, and unresponsive servers," *IEEE Trans. on Inform. Theory*, vol. 65, no. 6, pp. 3898–3906, June 2019.
- [9] S. Song and M. Hayashi, "Capacity of quantum private information retrieval with colluding servers," *IEEE Trans. on Inform. Theory*, vol. 67, no. 8, pp. 5491–5508, 2021.
- [10] M. Allaix, S. Song, L. Holzbaier, T. Pillaha, M. Hayashi, and C. Hollanti, "On the capacity of quantum private information retrieval from MDS-coded and colluding servers," *IEEE J. on Sel. Areas in Commun.*, vol. 40, no. 3, pp. 885–898, 2022.
- [11] A. Aytekin, M. Nomeir, S. Vithana, and S. Ulukus, "Quantum symmetric private information retrieval with secure storage and eavesdroppers," in *2023 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2023, pp. 1057–1062.
- [12] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and S. A. Avestimehr, "Lagrange coded computing: Optimal design for resiliency, security, and privacy," in *The 22nd International Conf. on Artificial Intelligence and Statistics*. PMLR, 2019, pp. 1215–1225.
- [13] S. Song and M. Hayashi, "Secure quantum network code without classical communication," *IEEE Trans. on Inform. Theory*, vol. 66, no. 2, pp. 1178–1192, 2019.
- [14] Y. Yao and S. A. Jafar, "The capacity of classical summation over a quantum MAC with arbitrarily distributed inputs and entanglements," *IEEE Trans. on Inform. Theory*, vol. 70, no. 9, pp. 6350–6370, 2024.
- [15] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.
- [16] A. Kawachi and H. Nishimura, "Communication complexity of private simultaneous quantum messages protocols," in *Proc. Conf. on Inform. Theoretic Cryptography (ITC 2021)*, vol. 199, 2021, pp. 20:1–20:19.
- [17] R. Christensen and P. Popovski, "Private product computation using quantum entanglement," *IEEE Trans. on Quantum Eng.*, vol. 4, 2023.
- [18] Y. Lu, Y. Yao, and S. A. Jafar, "On the capacity of secure  $K$ -user product computation over a quantum MAC," *IEEE Commun. Letters*, vol. 27, no. 10, pp. 2598–2602, 2023.
- [19] A. Aytekin, M. Nomeir, and S. Ulukus, "Quantum private membership aggregation," in *2024 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2024, pp. 3314–3319.
- [20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, 1977, vol. 1.
- [21] Z. Jia and S. A. Jafar, " $X$ -secure  $T$ -private information retrieval from MDS coded storage with Byzantine and unresponsive servers," *IEEE Trans. on Inform. Theory*, vol. 66, no. 12, pp. 7427–7438, 2020.
- [22] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, p. 1098, 1996.
- [23] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. the Royal Society of London. Series A: Mathematical, Physical and Eng. Sciences*, vol. 452, no. 1954, pp. 2551–2577, 1996.
- [24] Z. Jia, H. Sun, and S. A. Jafar, "Cross subspace alignment and the asymptotic capacity of  $X$ -secure  $T$ -private information retrieval," *IEEE Trans. on Inform. Theory*, vol. 65, no. 9, pp. 5783–5798, Sep. 2019.

- [25] S. Ulukus, S. Avestimehr, M. Gastpar, S. A. Jafar, R. Tandon, and C. Tian, "Private retrieval, computing, and learning: Recent progress and future challenges," *IEEE J. on Sel. Areas in Commun.*, vol. 40, no. 3, pp. 729–748, 2022.
- [26] M. Allaix, Y. Lu, Y. Yao, T. Pillaha, C. Hollanti, and S. A. Jafar, " $N$ -sum box: An abstraction for linear computation over many-to-one quantum networks," *IEEE Trans. on Inform. Theory*, vol. 71, no. 2, pp. 1121–1139, 2025.
- [27] Y. Lu and S. A. Jafar, "Quantum cross subspace alignment codes via the  $N$ -sum box abstraction," in *2023 57th Asilomar Conf. on Signals, Systems, and Computers*. IEEE, 2023, pp. 670–674.
- [28] N. Raviv and D. A. Karpuk, "Private polynomial computation from Lagrange encoding," *IEEE Trans. on Inform. Forensics and Security*, vol. 15, pp. 553–563, 2019.
- [29] W.-T. Chang and R. Tandon, "On the upload versus download cost for secure and private matrix multiplication," in *2019 IEEE Inform. Theory Workshop (ITW)*. IEEE, 2019, pp. 1–5.
- [30] Z. Jia and S. A. Jafar, "Cross subspace alignment codes for coded distributed batch computation," *IEEE Trans. on Inform. Theory*, vol. 67, no. 5, pp. 2821–2846, 2021.
- [31] T. A. Brun, "Quantum error correction," *arXiv preprint arXiv:1910.03672*, 2019.
- [32] H. Yang, W. Shin, and J. Lee, "Private information retrieval for secure distributed storage systems," *IEEE Trans. on Inform. Forensics and Security*, vol. 13, no. 12, pp. 2953–2964, 2018.
- [33] M. Nomeir, A. Aytakin, and S. Ulukus, "Quantum  $X$ -secure  $B$ -Byzantine  $T$ -colluding private information retrieval," *arXiv preprint arXiv:2401.17252v2*, 2024.
- [34] Y. Lu and S. A. Jafar, "A coding scheme for straggler resilient quantum  $X$ -secure  $T$ -private information retrieval," in *2024 IEEE International Conf. on Commun. (ICC)*. IEEE, 2024, pp. 2803–2808.
- [35] —, "A coding scheme for straggler resilient quantum  $X$ -secure  $T$ -private information retrieval," *arXiv preprint arXiv:2311.07829v1*, 2023.
- [36] —, "A coding scheme for unresponsive and Byzantine server resilient quantum  $X$ -secure  $T$ -private information retrieval," *arXiv preprint arXiv:2311.07829v2*, 2024.
- [37] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. on Inform. Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.
- [38] L. Golowich and V. Guruswami, "Quantum locally recoverable codes," *arXiv preprint arXiv:2311.08653*, 2023.
- [39] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum Inform.* Cambridge university press, 2010.
- [40] H. Yamamoto, "Secret sharing system using  $(k, L, n)$  threshold scheme," *Electronics and Commun. in Japan (Part I: Commun.)*, vol. 69, no. 9, pp. 46–54, 1986.
- [41] M. M. Wilde, *Quantum Information theory*, 2nd ed. Cambridge university press, 2017.