On the Capacity of Erasure-prone Quantum Storage with Erasure-prone Entanglement Assistance

Hua Sun, Syed A. Jafar

Abstract

A quantum message is encoded into N quantum storage systems $(Q_1 \ldots Q_N)$ with assistance from N_B maximally entangled bi-partite quantum systems $A_1 B_1, \ldots, A_{N_B} B_{N_B}$, that are prepared in advance such that $B_1 \ldots B_{N_B}$ are stored separately as entanglement assistance (EA) systems, while $A_1 \ldots A_{N_B}$ are made available to the encoder. Both the storage systems and EA systems are erasure-prone. The quantum message must be recoverable given any K of the N storage systems along with any K_B of the N_B EA systems. The capacity for this setting is the maximum size of the quantum message, given that the size of each EA system is λ_B. All system sizes are relative to the size of a storage system, which is normalized to unity. The exact capacity is characterized as a function of $N, K, N_B, K_B, \lambda_B$ in all cases, with one exception. The capacity remains open for an intermediate range of λ_B values when a strict majority of the N storage systems, and a strict non-zero minority of the N_B EA systems, are erased. As a key stepping stone, an analogous classical storage (with shared-randomness assistance) problem is introduced. A set of constraints is identified for the classical problem, such that classical linear code constructions translate to quantum storage codes, and the converse bounds for the two settings utilize similar insights. In particular, the capacity characterizations for the classical and quantum settings are shown to be identical in all cases where the capacity is settled.

Hua Sun (email: hua.sun@unt.edu) is with the Department of Electrical Engineering at the University of North Texas. Syed A. Jafar (email: syed@uci.edu) is with the Department of Electrical Engineering and Computer Science (EECS) at the University of California Irvine.

I. INTRODUCTION

As a cornerstone of the theory of error-correcting codes, coding for *erasures* plays a critical role in ensuring the reliable storage of information. In quantum systems, where both the information and the storage medium are quantum in nature, even the act of error detection can introduce additional errors. Erasures — errors at *known* locations — are less susceptible to this vulnerability and are consequently easier to correct. This underpins the concept of erasure conversion [1], [2], which utilizes physical principles to transform other types of quantum errors into erasures. Erasures may also emerge as the predominant error mode in future quantum distributed storage systems, particularly if such systems can be scaled to the size of modern classical data centers, where each storage system functions as a fault-tolerant memory unit [3], [4]. Furthermore, from an information theoretic perspective, erasures are among the most tractable of all quantum error paradigms [4], [5], creating opportunities for synergies between the studies of fundamental limits on one hand and practical code designs on the other [6]. Let us denote '*erasure-prone quantum storage*' as $\widetilde{\text{QS}}$, with the $\sim$ indicating susceptibility to erasures.

The capabilities of $\widetilde{\text{QS}}$ are significantly enhanced by *entanglement assistance* (EA), i.e., when quantum entanglement is available in advance as an additional shared resource between the encoder and decoder. For example, it is known that quantum erasure codes do not exist in the parameter regime where the locality is less than the code distance [3]. This limitation arises primarily due to the *no-cloning theorem* [7], which prohibits the recovery of quantum information from a set of storage systems whose erasure (i.e., absence) must be tolerated. Otherwise, *two* copies of the stored quantum information could be reconstructed – one by a legitimate receiver without access to the erased/missing systems, and another by a hypothetical party with access only to the 'missing' systems. However, such limitations can be circumvented by utilizing EA. Remarkably, EA is also associated with improved analytical tractability from an information theoretic standpoint. A textbook example is the capacity of a quantum channel, which remains unresolved in general but is settled if EA is available [8].

Aside from a few notable exceptions [9], [10], $\widetilde{\text{QS}}$ with EA has been studied primarily under the assumption that the EA is perfect, a paradigm that we may refer to as $\widetilde{\text{QS}}$EA [5], [11], [12], [13], [14], [15], [16]. Such a setting is illustrated in Figure 1. While entanglement distribution is seldom perfect, the assumption of perfect EA may be justified if the encoder and decoder can perform entanglement distillation [17], [18], [19] prior to the encoding of the quantum information, and the coded systems are immediately sent to the receiver so the decoding can take place prior to any new corruption in the EA resource. This may not be possible in some settings, e.g., distributed storage over an extended period. The classical communication required in advance for entanglement distillation may not be feasible, or there may be significant risk of corruption of the EA resource after the quantum information is encoded and before it can be decoded. It is therefore important to study settings with imperfect EA. References [9], [10] have found various coding schemes for error-prone quantum storage with error prone EA, to show that even imperfect EA can be quite useful. Motivated by these observations, in this work we explore the information theoretic capacity of $\widetilde{\text{QSEA}}$, i.e., erasure-prone quantum storage with erasure-prone entanglement assistance.
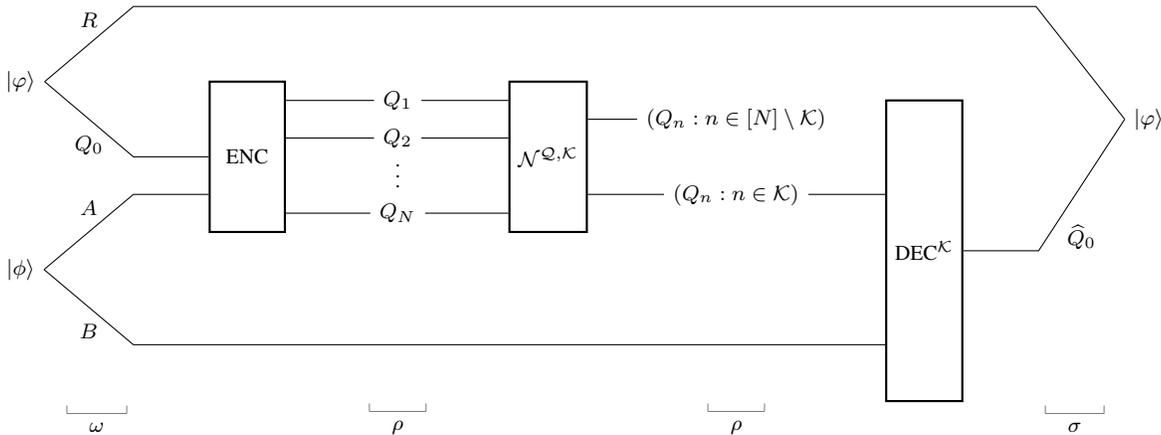

Fig. 1. A $\widetilde{\text{QS}}$EA setting studied in [5] is illustrated. A quantum message Q_0 (possibly entangled with a purifying reference system R) is encoded into N quantum storage systems $(Q_1 \ldots Q_N)$ by an encoder with entanglement assistance A. Any $N - K$ of these N systems are erased by a channel. A decoder must recover the quantum information from the remaining (unerased) systems and the entanglement assistance B. Note that the entanglement assistance is perfect (not prone to erasures). A feasible coding scheme specifies an encoder ENC, and an array of decoders DEC$^{\mathcal{K}}$, guaranteeing recovery for every $\mathcal{K} \in \binom{[N]}{K}$.

Building upon the foundation laid in [5] for a Shannon theoretic study of $\widetilde{\text{QS}}$EA, we incorporate EA erasures and define a $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$ problem. The schematic for $\widetilde{\text{QSEA}}$ appears in Figure 2. The formal problem description appears in Section II-B. An informal description is provided here. In the $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$ problem, a quantum message is encoded into N storage systems (quantum systems $Q_1 \ldots Q_N$) with assistance from N_B maximally entangled bi-partite quantum systems $A_1 B_1, \ldots, A_{N_B} B_{N_B}$, that are prepared in advance such that $B_1 \ldots B_{N_B}$ are stored separately as EA systems, while $A_1 \ldots A_{N_B}$ are made available to the encoder. Both the storage systems and EA systems are erasure-prone. The quantum message must

be recoverable given any K of the N storage systems along with any K_B of the N_B EA systems. The information theoretic capacity for this setting is the maximum size of the quantum message, given that the size of each EA system is λ_B. All system sizes are relative to the size of a storage system, which is normalized to unity. The goal of this work is to characterize the information theoretic capacity of $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$. Note that setting $N_B = K_B$ would mean no EA systems are erased, reducing our $\widetilde{\text{QSEA}}$ setting to the QSEA setting. It is noteworthy that there are certain cases identified in [5] for which the capacity of QSEA is open, which will be resolved (see Observation 6 following Theorem 1) as a byproduct of our capacity results for $\widetilde{\text{QSEA}}$. A brief summary of our results is presented next.
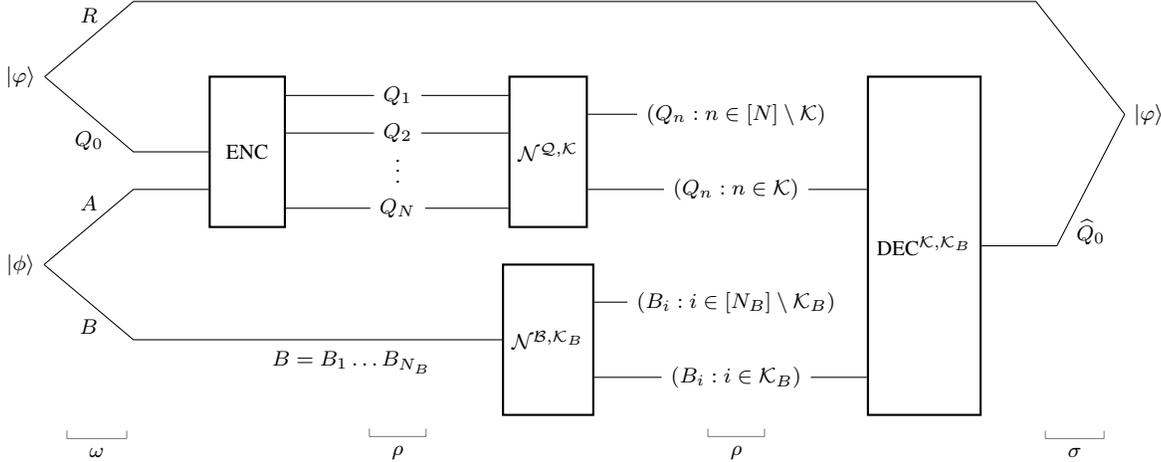

Fig. 2. The $\widetilde{\text{QSEA}}$ setting studied in this work. Note that the entanglement assistance systems B are also subject to erasures.

As the main result of this work, the exact capacity of $\widetilde{\text{QSEA}}$ is characterized as a function of $N, K, N_B, K_B, \lambda_B$ in all cases, with one exception. The capacity remains open for an intermediate range of λ_B values, specifically $K/(2K_B) < \lambda_B < (N - 2K)/N_B + K/K_B$, when a strict majority of the N storage systems, and a strict non-zero minority of the N_B EA systems, are erased, i.e., $K < N/2$ and $N_B > K_B > N_B/2$. For the setting that remains open, we present a lower bound (a feasible coding scheme) that we conjecture (Observation 1 following Theorem 1) to be information theoretically optimal. As a key stepping stone for $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$, an analogous classical storage (with shared-randomness assistance (SRA)) problem, called $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$, is introduced, where both the classical storage and the SRA are erasure-prone. A set of constraints is identified for the classical problem, such that classical linear code constructions translate to quantum storage codes via a CSS construction. It is worth noting that even after the corresponding classical problem $\widetilde{\text{CSSRA}}$ is identified, challenges remain on both achievability and converse fronts. On the achievability side, since $\widetilde{\text{CSSRA}}$ has not been previously studied, new optimal codes have to be designed for this problem. As it turns out these optimal codes involve rather non-trivial alignment structures. On the converse side, first a classical converse is needed to test the optimality of the codes for $\widetilde{\text{CSSRA}}$, and then after the codes are translated into quantum codes via the CSS construction, a tight quantum information-theoretic converse is still needed to establish the information-theoretic optimality of the corresponding quantum code. Yet, it is remarkable that the capacity characterizations for the classical and quantum settings are found to be identical in all cases where the capacity is settled.

Figure 3 previews briefly via an example how a classical code for $\widetilde{\text{CSSRA}}$ is translated into a quantum code for $\widetilde{\text{QSEA}}$. The setting illustrated in the figure is $\widetilde{\text{QSEA}}(3, 1, 3, 2)$, where any $N - K = 2$ out of $N = 3$ storage systems and any $N_B - K_B = 1$ out of $N_B = 3$ EA systems can be erased. A decoder is specified for each possible erasure scenario, and the goal is to find the maximum size λ_0 of the quantum message that can be stored and perfectly recovered in every allowed erasure scenario, when all storage systems have size normalized to unity and all EA systems $(A_1, A_2, A_3, B_1, B_2, B_3)$ have size λ_B. When the $\widetilde{\text{QSEA}}$ setting is mapped to a $\widetilde{\text{CSSRA}}$ setting, all quantum systems become classical systems, and we are left with a classical problem to solve, subject to certain entropic constraints. The constraints are listed in the figure. Detailed explanations are relegated to subsequent sections. The optimal classical code (construction of Y_1, Y_2, Y_3) is also shown in the figure, and it is not difficult to verify that the construction satisfies all entropic constraints, mainly because of the careful alignments of message and SR terms. The $\widetilde{\text{CSSRA}}$ code is then mapped to a $\widetilde{\text{QSEA}}$ code via the CSS construction [20], [21]. The alignments reflect the non-trivial nature of code design for $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$, which is inherited by the optimal quantum codes for $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$.

The construction shown in Figure 3 achieves storage size $\lambda_0 = 1/2$ with $\lambda_B = 5/6$. Information theoretic converse arguments, not represented in Figure 3, but established later in the paper (Theorem 1 in Section III-A), imply that the message size $\lambda_0 = 1/2$ is optimal not only for $\lambda_B = 5/6$ but also for any value of $\lambda_B \geq 5/6$, i.e., larger sizes of EA systems do not increase the storage capacity for this setting. The open problem in the context of Figure 3 corresponds to the question: is the

message size $\lambda_0 = 1/2$ also achievable with λ_B strictly smaller than $5/6$? If our conjecture holds, then applied to this example it would imply that $\lambda_0 = 1/2$ cannot be achieved by any coding scheme with EA system sizes strictly smaller than $5/6$.

Lastly, note that the coding scheme shown in Figure 3 does not require particularly large alphabet. Indeed, it works over any finite field $\mathbb{F}_q$, including the binary field $\mathbb{F}_2$. Over $\mathbb{F}_2$ it corresponds to the setting where each quantum storage system has size 6 qubits, each EA system has size 5 qubits, and the quantum message has size 3 qubits. Generally in this work, since we pursue a Shannon theoretic formulation of storage capacity, which is not sensitive to field size, we will not attempt to minimize the field size for our coding schemes. Indeed, in Section IV-C we present the same example from a slightly different perspective that is easier to generalize, but requires a larger field size.
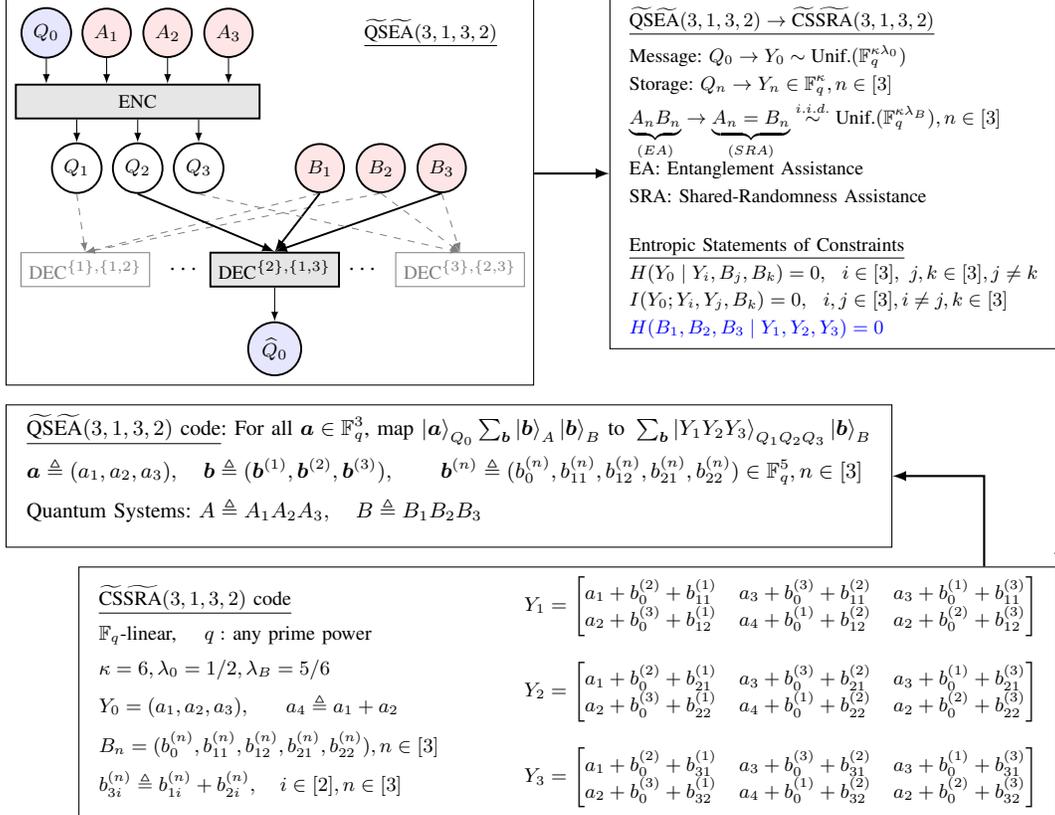

Fig. 3. Constructing a $\widetilde{\text{QSEA}}$ code from a $\widetilde{\text{CSSRA}}$ code for $(N, K, N_B, K_B) = (3, 1, 3, 2)$ and $(\lambda_0, \lambda_B) = (1/2, 5/6)$. First, quantum systems are mapped to classical systems. In addition to the decodability and security constraints identified in prior works [4], [22], [23], here the constraints for the classical setting also include (shown in blue) recovery of the shared-randomness from the storage systems. Next, a classical code is constructed by optimally aligning shared-randomness, local randomness (not needed in this example) and message terms to satisfy all constraints. Finally, the classical code is mapped to a quantum code via the CSS construction [20], [21].

A. Notation

$\mathbb{Z}, \mathbb{R}, \mathbb{C}$ are the sets of integers, reals, and complex numbers respectively. The notations $\mathbb{Z}_{\geq a}$ ($\mathbb{R}_{\geq a}$) represent the sets of integers (reals) greater than or equal to a, respectively. $[N]$ denotes the set $\{1, 2, \cdots, N\}, N \in \mathbb{Z}_{\geq 1}$. For $i, j \in \mathbb{Z}$, the notation $[i : j]$ denotes the set $\{i, i+1, \cdots, j\}$ when $i \leq j$ and the empty set otherwise. $|X|$ denotes the cardinality of X if X is a set, the support of X if X is a classical random variable, and the dimension of the Hilbert space associated with X if X is a quantum system. For a set $\mathcal{X}$, the set of its cardinality-k subsets is denoted as $\binom{\mathcal{X}}{k} \triangleq \{\mathcal{Y} : \mathcal{Y} \subset \mathcal{X}, |\mathcal{Y}| = k\}$, and the notation $Q_{\mathcal{X}}$ denotes $(Q_i : i \in \mathcal{X})$. For two sets $\mathcal{X}, \mathcal{Y}$, the notation $\mathcal{X} \setminus \mathcal{Y}$ denotes the set of elements that are in $\mathcal{X}$ but not in $\mathcal{Y}$. We will frequently use the notation $\mathcal{K} \in \binom{[N]}{K}$ and $\mathcal{K}_B \in \binom{[N_B]}{K_B}$ to represent subsets of $[N]$ and $[N_B]$ of size K and K_B, respectively. It will be convenient to denote their complements as $\mathcal{K}^c = [N] \setminus \mathcal{K}$ and $\mathcal{K}_B^c = [N_B] \setminus \mathcal{K}_B$, respectively. For matrices $\mathbf{M}_1, \mathbf{M}_2$ of compatible dimensions, $(\mathbf{M}_1, \mathbf{M}_2)$ and $(\mathbf{M}_1; \mathbf{M}_2)$ represent their horizontal and vertical concatenations, respectively. $\mathbf{M}^T$ represents the transpose of the matrix $\mathbf{M}$. The notation $\mathbf{M}(\mathcal{I}, \mathcal{J})$ represents the sub-matrix of $\mathbf{M}$ formed by retaining only the rows from the index tuple $\mathcal{I}$ and the columns from the index tuple $\mathcal{J}$. For example, $\mathbf{M}((1, 2), (3, 4))$ represents the 2×2 sub-matrix comprising rows $1, 2$ and columns $3, 4$ of $\mathbf{M}$. For quantum systems X, Y, the notation $X \rightsquigarrow Y$ denotes that a unitary (isometric) map is applied to X so that it is transformed to Y. When X is a set of classical random variables or quantum systems, $H(X)$ denotes the joint Shannon or von Neumann (quantum) entropy of the elements in X.

$\mathbb{F}_q$ denotes the finite field with q elements where q is a power of a prime. For non-zero vectors u, v, we write $u \equiv v$ to mean $u = v/||v||$, i.e., u is the unit vector obtained by normalizing v.

II. PROBLEM STATEMENT

A. Preliminaries

The dimension $|Q|$ of a quantum system Q corresponds to the dimension of its associated Hilbert space $\mathcal{H}_Q$. Only finite dimensional Hilbert spaces are considered in this work. Define $S(\mathcal{H}_Q)$ as the set of all states of Q, represented as density matrices (unit-trace positive semidefinite matrices) over $\mathcal{H}_Q$. The set of unit rank density matrices, $S_1(\mathcal{H}_Q) \triangleq \{|x\rangle \langle x| : |x\rangle \in \mathcal{H}_Q, \langle x|x\rangle = 1\}$ corresponds to pure states. Pure states can also be represented as unit vectors $|x\rangle \in \mathcal{H}_Q, \langle x|x\rangle = 1$. A composite system $Q_1 Q_2 \ldots Q_N$ is associated with the Hilbert space $\mathcal{H}_{Q_1} \otimes \mathcal{H}_{Q_2} \otimes \cdots \otimes \mathcal{H}_{Q_N}$, where each Q_n is associated with the Hilbert space $\mathcal{H}_{Q_n}$, $n \in [N]$. A *qudit*, representing a q-dimensional quantum system, is a unit for expressing the size of a quantum system. The size of a quantum system Q is $\log_q |Q|$ qudits. The composite system $Q_1 Q_2 \ldots Q_N$ has size $\log_q |Q_1 Q_2 \ldots Q_N| = \log_q |Q_1| + \log_q |Q_2| + \cdots + \log_q |Q_N|$ qudits.

B. Problem Formulation: $\widetilde{QSEA}(N, K, N_B, K_B)$

The goal of $\widetilde{QSEA}$ is to encode an arbitrary quantum message Q_0, into N storage systems (quantum systems), $Q_1 Q_2 \ldots Q_N$, with assistance from a quantum-entanglement resource AB, $A = A_1 \ldots A_{N_B}$, $B = B_1 \ldots B_{N_B}$ where all of A is available to the encoder, such that given any K of the N storage systems $Q_1 Q_2 \ldots Q_N$ and any K_B of the N_B EA systems $B = B_1 \ldots B_{N_B}$, there exists a decoder that can recover Q_0. Note that $N, K, N_B, K_B \in \mathbb{Z}_{\geq 0}$ and $K \leq N$, $K_B \leq N_B$. To highlight key parameters we refer to an instance of $\widetilde{QSEA}$ as $\widetilde{QSEA}(N, K, N_B, K_B)$. The problem is formalized by the following description of a coding scheme.

1) Encoding and Decoding for $\widetilde{QSEA}$: A diagram of the encoding and decoding procedure is shown in Figure 2.

A coding scheme for $\widetilde{QSEA}(N, K, N_B, K_B)$ is specified by the parameters

$$\left(\lambda_0, \lambda_B, \kappa, q, \text{ENC}, \left(\text{DEC}^{\mathcal{K}, \mathcal{K}_B} : \mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B} \right) \right), \tag{1}$$

where $\kappa \in \mathbb{Z}_{\geq 1}$, $q \in \mathbb{Z}_{\geq 2}$, and $q^{\kappa \lambda_0}, q^{\kappa \lambda_B} \in \mathbb{Z}_{\geq 1}$. In order to emphasize the dependence of parameters on the coding scheme, given a coding scheme identified by a label $\mathfrak{S}$, we may refer to its parameters as $\lambda_0(\mathfrak{S}), \lambda_B(\mathfrak{S}), \kappa(\mathfrak{S}), q(\mathfrak{S}), \text{ENC}(\mathfrak{S}), \text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S})$. Usually however, as in the following discussion, the label for the coding scheme will be suppressed in order to simplify the notation if there is no potential for ambiguity.

The scheme encodes an arbitrary quantum *message*, Q_0, of size $\log_q |Q_0| = \kappa \lambda_0$ qudits. Associated with Q_0, define R, without loss of generality also of the same size $\log_q |R| = \kappa \lambda_0$ qudits, as a *reference* quantum system such that RQ_0 is an arbitrary pure state $|\varphi\rangle \langle\varphi|_{RQ_0} \in S_1(\mathcal{H}_R \otimes \mathcal{H}_{Q_0})$.

The scheme utilizes EA, represented by a maximally entangled quantum system AB, where $A = A_1 \ldots A_{N_B}$, and $B = B_1 \ldots B_{N_B}$ are N_B-partite systems, with sizes $\log_q |A_n| = \log_q |B_n| = \kappa \lambda_B$ qudits, $\forall n \in [N_B]$. The system AB is in a pure state,

$$|\phi\rangle_{AB} = |\psi\rangle_{A_1 B_1} \otimes \cdots \otimes |\psi\rangle_{A_{N_B} B_{N_B}},$$
$$|\psi\rangle_{A_n B_n} \equiv \sum_{\boldsymbol{j} \in q^{\kappa \lambda_B}} |\boldsymbol{j}, \boldsymbol{j}\rangle_{A_n B_n}, \qquad n \in [N_B]. \tag{2}$$

RQ_0 and AB are in a product state.

$$\omega_{RQ_0 AB} = |\varphi\rangle \langle\varphi|_{RQ_0} \otimes |\phi\rangle \langle\phi|_{AB}. \tag{3}$$

The encoding operation applies the CPTP (completely positive trace preserving) map 'ENC',

$$\text{ENC} : S(\mathcal{H}_{Q_0} \otimes \mathcal{H}_A) \to S(\mathcal{H}_{Q_1} \otimes \cdots \otimes \mathcal{H}_{Q_N}), \tag{4}$$

to the collective input comprised of the quantum message Q_0 and the entanglement resource A, and produces the quantum storage systems $Q_1 Q_2 \ldots Q_N$. The size of each storage system, $\log_q |Q_n| = \kappa$ qudits, for all $n \in [N]$. Following the encoding, the resulting state of $RQ_1 Q_2 \ldots Q_N B$,

$$\rho_{RQ_1 \ldots Q_N B} = I_{RB} \otimes \text{ENC}_{Q_0 A \to Q_1 \ldots Q_N}(\omega_{RQ_0 AB}). \tag{5}$$

Next we describe the decoding operation. Let $\mathcal{K}, \mathcal{K}_B$ denote the sets of indices of storage and EA systems that remain available to the decoder, respectively, after the rest of the storage and EA systems are erased (see Figure 2). For each $\mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}$, the coding scheme specifies a CPTP decoding map,

$$\text{DEC}^{\mathcal{K}, \mathcal{K}_B} : S(\otimes_{i \in \mathcal{K}} \mathcal{H}_{Q_i} \otimes_{j \in \mathcal{K}_B} \mathcal{H}_{B_j}) \to S(\mathcal{H}_{Q_0}), \tag{6}$$

which acts on the 'unerased systems' to output a quantum system $\widehat{Q}_0$. The resulting state σ following the decoding operation is expressed as follows.

$$\sigma_{R\widehat{Q}_0 Q_{\mathcal{K}^c} B_{\mathcal{K}_B^c}} = I_{RQ_{\mathcal{K}^c} B_{\mathcal{K}_B^c}} \otimes \text{DEC}^{\mathcal{K},\mathcal{K}_B}_{Q_{\mathcal{K}} B_{\mathcal{K}_B} \to \widehat{Q}_0} (\rho_{RQ_1 \ldots Q_N B_1 \ldots B_{N_B}}). \tag{7}$$

Recall from Section I-A that $\mathcal{K}^c \triangleq [N] \setminus \mathcal{K}$ and $\mathcal{K}_B^c \triangleq [N_B] \setminus \mathcal{K}_B$. A coding scheme is feasible if it satisfies the recovery condition,

$$\sigma_{R\widehat{Q}_0} = |\varphi\rangle \langle\varphi|_{RQ_0}, \tag{8}$$

for all $|\varphi\rangle \langle\varphi| \in S_1(\mathcal{H}_R \otimes \mathcal{H}_{Q_0}) = S_1(\mathbb{C}^{q^{\kappa\lambda_0}} \otimes \mathbb{C}^{q^{\kappa\lambda_0}})$ and for all $\mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}$.

2) Storage Capacity Region and Storage Capacity for $\widetilde{QSEA}(N, K, N_B, K_B)$: Taking a Shannon theoretic perspective as in [4], the dependence on κ, q is relaxed by allowing coding schemes to freely optimize over these parameters. Accordingly, a tuple $(\lambda_0, \lambda_B) \in \mathbb{R}^2_{\geq 0}$ is said to be *achievable* for $\widetilde{QSEA}(N, K, N_B, K_B)$ if there exists a feasible coding scheme $\mathfrak{S}$ with $\lambda_0(\mathfrak{S}) \geq \lambda_0$ and $\lambda_B(\mathfrak{S}) \leq \lambda_B$. The closure of the set of achievable (λ_0, λ_B) tuples is defined to be the storage capacity region $\mathcal{C}_Q(N, K, N_B, K_B)$. For each $\lambda_B \in \mathbb{R}_{\geq 0}$, the storage capacity of $\widetilde{QSEA}(N, K, N_B, K_B)$ is defined as

$$C_Q(N, K, N_B, K_B, \lambda_B) \triangleq \max\{\lambda_0 : (\lambda_0, \lambda_B) \in \mathcal{C}_Q(N, K, N_B, K_B)\}. \tag{9}$$

The storage capacity region and the storage capacity may be abbreviated as $\mathcal{C}_Q, C_Q(\lambda_B)$, respectively, when the values of the remaining parameters are obvious from the context.

C. Problem Formulation: $\widetilde{CSSRA}(N, K, N_B, K_B)$

Closely related to $\widetilde{QSEA}(N, K, N_B, K_B)$, here we introduce the problem of *classical storage with shared-randomness assistance*, i.e., $\widetilde{CSSRA}(N, K, N_B, K_B)$. The latter is a conceptually simpler setting that will turn out to be quite insightful for exploring $\widetilde{QSEA}(N, K, N_B, K_B)$. To emphasize the relationship between the two problems, we use similar notation for corresponding quantities.

The goal of $\widetilde{CSSRA}$ is to encode an arbitrary classical message Y_0, into N classical storage systems, $Y_1, Y_2, \ldots, Y_N$, with assistance from shared-randomness (SR) resource AB, $A = A_1 \ldots A_{N_B}$, $B = B_1 \ldots B_{N_B}$ where all of A is available to the encoder, such that given any K of the N storage systems $Y_1, Y_2, \ldots, Y_N$ and any K_B of the N_B SRA systems $B_1, \ldots, B_{N_B}$, there exists a decoder that can recover Y_0. Since classical information can be copied, in this case it suffices to set $A_n = B_n$ for all $n \in [N_B]$. Note that $N, K, N_B, K_B \in \mathbb{Z}_{\geq 0}$ and $K \leq N$, $K_B \leq N_B$. The problem is formalized by the following description of a coding scheme.

1) Encoding and Decoding for $\widetilde{CSSRA}$: A coding scheme for $\widetilde{CSSRA}(N, K, N_B, K_B)$ is specified by the parameters

$$\left(\lambda_0, \lambda_B, \kappa, q, \text{ENC}, \left(\text{DEC}^{\mathcal{K},\mathcal{K}_B} : \mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B} \right) \right), \tag{10}$$

where $\kappa \in \mathbb{Z}_{\geq 1}$, $q \in \mathbb{Z}_{\geq 2}$, and $q^{\kappa\lambda_0}, q^{\kappa\lambda_B} \in \mathbb{Z}_{\geq 1}$. For a coding scheme labeled $\mathfrak{S}$, we may refer to its parameters as $\lambda_0(\mathfrak{S}), \lambda_B(\mathfrak{S}), \kappa(\mathfrak{S}), q(\mathfrak{S}), \text{ENC}(\mathfrak{S}), \text{DEC}^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S})$. The label identifying the coding scheme will be suppressed if there is no potential for ambiguity.

The scheme encodes a classical message, Y_0, drawn uniformly from its alphabet $\mathcal{Y}_0$, of size $\log_q |\mathcal{Y}_0| = \kappa\lambda_0$ *dits*, where we define the term *dit* to mean a q-ary classical symbol.

$$\Pr(Y_0 = y_0) = \frac{1}{q^{\kappa\lambda_0}}, \qquad\qquad \forall y_0 \in \mathcal{Y}_0. \tag{11}$$

The scheme utilizes SRA, represented by B, where $B = (B_1, \ldots, B_{N_B}) \in \mathcal{B}^{N_B}$, with size $\log_q |\mathcal{B}| = \kappa\lambda_B$ dits. We refer to each B_i as an SR-system. The SR is uniformly distributed.

$$\Pr(B = \boldsymbol{b}) = \frac{1}{q^{\kappa\lambda_B}}, \qquad\qquad \forall \boldsymbol{b} \in \mathcal{B}^{N_B}. \tag{12}$$

The scheme also utilizes local randomness, represented by $Z \in \mathcal{Z}$, generated locally by the encoder. The message, SR and local randomness are independent.

$$\Pr(B = \boldsymbol{b}, Z = \boldsymbol{z}, Y_0 = y_0) = \Pr(B = \boldsymbol{b}) \Pr(Z = \boldsymbol{z}) \Pr(Y_0 = y_0), \qquad \forall \boldsymbol{b} \in \mathcal{B}^{N_B}, \boldsymbol{z} \in \mathcal{Z}, y_0 \in \mathcal{Y}_0. \tag{13}$$

The encoding operation applies the map

$$\text{ENC} : \mathcal{Y}_0 \times \mathcal{B}^{N_B} \times \mathcal{Z} \to \mathcal{Y}^N,$$

to the collective input comprised of the classical message Y_0, the SR-resource B, and the local randomness-resource Z, and produces the storage systems $Y_1, Y_2, \ldots, Y_N \in \mathcal{Y}$.

$$(Y_1, \ldots, Y_N) = \text{ENC}(Y_0, B, Z). \tag{14}$$

The size of each storage system, $\log_q |\mathcal{Y}| = \kappa$ dits.

Next consider the decoding operation. Let $\mathcal{K}, \mathcal{K}_B$ denote the sets of indices of storage and SR systems available to the decoder, respectively, after the remaining systems are erased. For each $\mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}$, the coding scheme specifies a decoder

$$\text{DEC}^{\mathcal{K}, \mathcal{K}_B} : \mathcal{Y}^K \times \mathcal{B}^{K_B} \to \mathcal{Y}_0,$$

which maps the unerased systems to a decoded message,

$$\widehat{Y}_0 = \text{DEC}^{\mathcal{K}, \mathcal{K}_B}(Y_{\mathcal{K}}, B_{\mathcal{K}_B}), \tag{15}$$

where we define $Y_{\mathcal{K}} = (Y_n, n \in \mathcal{K})$ and $B_{\mathcal{K}_B} = (B_i, i \in \mathcal{K}_B)$. The coding scheme is feasible if it guarantees perfect decodability, i.e.,

$$\Pr(\widehat{Y}_0 = Y_0) = 1, \qquad\qquad \forall \mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}. \tag{16}$$

The decodability constraint can be expressed equivalently as the following entropic condition,

$$H(Y_0 \mid Y_{\mathcal{K}}, B_{\mathcal{K}_B}) = 0, \qquad\qquad \forall \mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}. \tag{17}$$

As a key distinctive feature, the $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ problem contains two additional constraints, stated in entropic terms in (18) and (19) as follows.

1) Security Constraint: The erased systems must not contain any information about the classical message.

$$I(Y_0; Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}) = 0, \qquad\qquad \forall \mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}. \tag{18}$$

2) SR Recovery Constraint: Collectively the storage systems $Y_1, \ldots, Y_N$ must fully determine the SR B.

$$H(B \mid Y_1, \ldots, Y_N) = 0. \tag{19}$$

These constraints are imposed to strengthen the connection between $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ and $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$, so that insights from the former may transfer to the latter. The motivation for the security constraint (18) is apparent as it corresponds to the no-cloning condition inherent in $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$. The motivation for the SR recovery constraint (19) is perhaps less obvious. As it turns out (Theorem 1 in Section III), imposing these constraints allows the capacity results for $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ to parallel those for $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$.

2) Storage Capacity Region and Storage Capacity for $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$: A tuple $(\lambda_0, \lambda_B) \in \mathbb{R}_{\geq 0}^2$ is said to be *achievable* for $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ if there exists a feasible coding scheme $\mathfrak{S}$ with $\lambda_0(\mathfrak{S}) \geq \lambda_0$ and $\lambda_B(\mathfrak{S}) \leq \lambda_B$. The closure of the set of achievable (λ_0, λ_B) tuples is defined to be the storage capacity region $\mathcal{C}(N, K, N_B, K_B)$. For each $\lambda_B \in \mathbb{R}_{\geq 0}$, the storage capacity of $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ is defined as

$$C(N, K, N_B, K_B, \lambda_B) \triangleq \max\{\lambda_0 : (\lambda_0, \lambda_B) \in \mathcal{C}(N, K, N_B, K_B)\}. \tag{20}$$

The storage capacity region and the storage capacity may be abbreviated as $\mathcal{C}, C(\lambda_B)$, respectively, when the values of the remaining parameters are obvious from the context.

III. RESULTS

A. Capacity Characterizations for $\widetilde{\text{QSEA}}$ and $\widetilde{\text{CSSRA}}$

Define the following sets.

$$\mathcal{R}_{cut} \triangleq \left\{ (\lambda_0, \lambda_B) \in \mathbb{R}_{\geq 0}^2 : \lambda_0 \leq \max(2K - N, 0) + \lambda_B \cdot \max(2K_B - N_B, 0) \right\}, \tag{21}$$

$$\mathcal{R}_{\infty} \triangleq \left\{ (\lambda_0, \lambda_B) \in \mathbb{R}_{\geq 0}^2 : \lambda_0 \leq \min(N, 2K) - \min(N - K, K)\frac{N_B}{K_B} \right\}, \tag{22}$$

$$\mathcal{R}_1 \triangleq \left\{ (\lambda_0, \lambda_B) \in \mathbb{R}_{\geq 0}^2 : \lambda_0 \leq K(2K_B - N_B)\frac{(N - 2K) + N_B \lambda_B}{(N - 2K)2K_B + KN_B} \right\}. \tag{23}$$

Our main result appears in the following theorem.

Theorem 1. *For the* $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$ *and* $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ *problems defined in Sections II-B and II-C, the capacity regions* $\mathcal{C}_Q$ *and* $\mathcal{C}$, *respectively, are characterized as follows.*

    Case 1: $K_B/N_B \leq 1/2$,

$$\forall X \in \{\mathcal{C}_Q, \mathcal{C}\}, \qquad\qquad X = \mathcal{R}_{cut}. \tag{24}$$

    Case 2: $K_B/N_B > 1/2, K/N \geq 1/2$,

$$\forall X \in \{\mathcal{C}_Q, \mathcal{C}\}, \qquad\qquad X = \mathcal{R}_{cut} \cap \mathcal{R}_{\infty}. \tag{25}$$

Case 3: $K_B/N_B > 1/2, K/N < 1/2,$

$$\forall X \in \{\mathcal{C}_Q, \mathcal{C}\}, \qquad\qquad\qquad X \subset \mathcal{R}_{cut} \cap \mathcal{R}_\infty, \qquad\qquad (26)$$

$$X \supset \mathcal{R}_{cut} \cap \mathcal{R}_\infty \cap \mathcal{R}_1. \qquad\qquad (27)$$

The proof of Theorem 1 is presented in Section VI. In particular, Section VI-C considers the quantum case and Sections VI-A and VI-B consider the converse and achievability of the classical case, respectively.

Theorem 1 implies that in Case 1, the capacity is simply $C_Q(\lambda_B) = C(\lambda_B) = \max(2K - N, 0)$, same as the capacity without assistance from entanglement or SR. Figure 4 illustrates the capacity regions for Case 2 and Case 3.
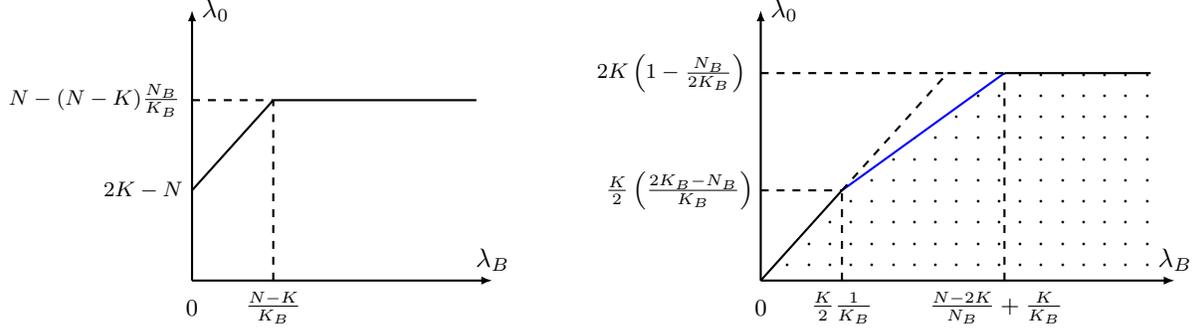

Fig. 4. Left: Capacity region for Case 2, i.e., when $K_B/N_B > 1/2, K/N \geq 1/2$. Note that the upper boundary of the capacity region represents the capacity $C_Q(\lambda_B) = C(\lambda_B)$. Right: Inner and outer bounds for capacity region in Case 3, i.e., when $K/N < 1/2, K_B/N_B > 1/2$. Note that the bounds match if $\lambda_B \leq K/(2K_B)$ or if $\lambda_B \geq (N - 2K)/N_B + K/K_B$, providing an exact capacity characterization in both cases.

The following observations are in order.

1) $\mathcal{C}_Q$ vs $\mathcal{C}$: Our results on $\mathcal{C}_Q$ and $\mathcal{C}$ are identical in all cases, highlighting the relationship between the two problems. The exact capacities C_Q and C are characterized in all cases except if $K/N < 1/2, K_B/N_B > 1/2$ and $K/(2K_B) < \lambda_B < (N - 2K)/N_B + K/K_B$. We conjecture that even in the case which remains open, the capacity regions are identical, so that $\mathcal{C}_Q = \mathcal{C}$ in all cases. Furthermore, we conjecture that in the case that remains open, it is our *inner bound* that is tight, i.e., $\mathcal{C}_Q = \mathcal{C} = \mathcal{R}_{cut} \cap \mathcal{R}_\infty \cap \mathcal{R}_1$ in Case 3.

2) Achievability: Our coding schemes for $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$ are obtained by first designing coding schemes for classical setting of $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$, and then translating them to the quantum setting via CSS codes to achieve the same rate tuple. The connection is developed in Section III-B and formalized in Theorem 2. Remarkably, all the extreme points (see Figure 4) of our inner bound for $\mathcal{C}_Q$ are achieved by *pure* coded states $\rho_{RQ_1...Q_N B_1...B_{N_B}}$ (see Figure 2).

3) Converse: Theorem 1 contains two converse bounds, i.e., the two hyperplanes in $\mathcal{R}_{cut}$ and $\mathcal{R}_\infty$. The converse bound in $\mathcal{R}_{cut}$ is

$$\lambda_0 \leq \max(2K - N, 0) + \lambda_B \cdot \max(2K_B - N_B, 0). \qquad\qquad (28)$$

This bound has a cut-set interpretation via the classical storage problem $\widetilde{\text{CSSRA}}$ as follows. In (28), the LHS corresponds to the message size $H(Y_0)$. The first term on the RHS corresponds to the total storage size of the K unerased storage systems after subtracting from those K systems another $N - K$ systems which need to be kept secure, and therefore cannot provide information about the message. Intuitively, the first term on the RHS corresponds to $H(Y_{[K] \setminus [N-K]})$. Similarly, the second term on the RHS is the total storage size available in the K_B unerased SR-systems, after removing $N_B - K_B$ of those systems, which need to be kept secure, i.e., $H(B_{[K_B] \setminus [N_B - K_B]})$. The insight extends to the quantum storage problem $\widetilde{\text{QSEA}}$ by the connection between the two problems.

The converse bound in $\mathcal{R}_\infty$ is

$$\lambda_0 \leq \min(N, 2K) - \min(N - K, K)\frac{N_B}{K_B}. \qquad\qquad (29)$$

This can be interpreted as the unlimited EA (or unlimited SR) bound, corresponding to $\lambda_B \to \infty$. Note that the RHS of (29) is equal to K, the number of surviving storage systems out of $Q_1 ... Q_N$, if $N_B = K_B$, i.e., EA is *not* erasure-prone. On the other hand, if $K_B < N_B$, i.e., entanglement *is* erasure-prone, then the RHS is strictly smaller than K. Thus, erasure-prone EA imposes a non-zero penalty, even if the size λ_B of the entanglement systems is arbitrarily large, which limits the storage capacity to a value strictly less than K. The exact magnitude of the penalty, which can be deduced from (29), is perhaps not intuitively obvious, and depends on the ratio N_B/K_B. An example of (29) when $(N, K, N_B, K_B) = (3, 2, 4, 3)$ is given in Section IV-D for the classical problem; the proof also generalizes to the quantum setting.

4) In Case 1, i.e., when $K_B/N_B \leq 1/2$, evidently EA is useless.

5) In Case 2, i.e., when $K/N \geq 1/2$ and $K_B/N_B > 1/2$, we have only one non-trivial extreme point (see Figure 4). In the classical problem $\widetilde{\text{CSSRA}}$, the SR B is sufficient for the coding scheme and no local randomness Z is used; correspondingly, for the quantum problem $\widetilde{\text{QSEA}}$, no ancilla qudits are needed for the encoding map ENC, i.e., ENC is unitary. An example of $(N, K, N_B, K_B) = (2, 1, 3, 2)$ is given in Section IV-A for the classical problem.

6) Case 3, where $K/N < 1/2, K_B/N_B > 1/2$, turns out to be the most challenging, and also the most interesting regime. Here more storage systems are erased than unerased $(N - K > K)$, so if there is no EA, then no message can be stored, i.e., capacity is zero. EA, even though it is itself erasure-prone, still improves the capacity (see Figure 4). Remarkably, our inner bound (conjectured optimal) contains two non-trivial extreme points. Highlights of the codes are discussed below from the $\widetilde{\text{CSSRA}}$ perspective.

   a) Extreme point $(\lambda_0, \lambda_B) = \left(\frac{K}{2K_B}, \frac{K(2K_B - N_B)}{2K_B} \right)$: In addition to SR B, local randomness Z is used by the encoder; correspondingly, the quantum scheme has to carefully design ancilla qudits for the encoding. The classical (and quantum) codes involve rather delicate structures. An example is given in Section IV-B for the classical problem. For example, in (42), each storage system Y_n contains two parts f, h, where f is some generic combination of (Y_0, B), while h is some generic combination of (Y_0, Z, f_0), where f_0 is a part of f. Thus h contains a mixture of the message Y_0, the same f_0 (across all $Y_1, \ldots, Y_N$) which already contains the SR B, and the local randomness Z. Further, f is repetition coded (MDS coded in general) across $Y_1 \ldots Y_N$ (see (42)).

   b) Extreme point $(\lambda_0, \lambda_B) = \left(2K \left(1 - \frac{N_B}{2K_B} \right), \frac{N-2K}{N_B} + \frac{K}{K_B} \right)$: The classical and quantum codes in this case again involve rather interesting alignment structure. Figure 3 illustrates the structure via a small example, which is presented again in Section IV-C from a more conceptual, and therefore more generalizable perspective, albeit for larger field sizes.

   c) Consider $N_B = K_B = 1$, so EA is not erasure-prone. The above two extreme points reduce to $(\lambda_0, \lambda_B) = (K/2, K/2)$ and $(\lambda_0, \lambda_B) = (K, N - K)$; space sharing of these two rate tuples achieves the blue line in Figure 4 (see Appendix A). This resolves an open problem[1] in [5], which left the achievability of the blue line segment open, while providing a proof that it represents a valid converse bound. Evidently, our inner bound for $\mathcal{C}_Q$ is indeed optimal when $N_B = K_B = 1$, lending support to our conjecture that our inner bound is *always* optimal in Case 3.

B. Translating a Linear Coding Scheme from $\widetilde{\text{CSSRA}}$ to $\widetilde{\text{QSEA}}$

Recall from Section II-C1 that a $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ coding scheme is specified by the parameters $\left(\lambda_0, \lambda_B, \kappa, q, \text{ENC}, \left(\text{DEC}^{\mathcal{K}, \mathcal{K}_B} : \mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B} \right) \right)$.

Definition 1 (Linear Scheme). A $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ coding scheme is *linear* if,
   1) the parameter q is a power of a prime, so that the finite field $\mathbb{F}_q$ exists, and
   2) the encoding map ENC is $\mathbb{F}_q$-linear, with the message, storage, SR and local randomness represented as vectors over $\mathbb{F}_q$, i.e., message $Y_0 \in \mathbb{F}_q^{1 \times \kappa \lambda_0}$, storage $Y_n \in \mathbb{F}_q^{1 \times \kappa}$ for all $n \in [N]$, i.i.d. uniform SR $B_i \in \mathbb{F}_q^{1 \times \kappa \lambda_B}$ for all $i \in [N_B]$, and local randomness $Z = (Z_1, \ldots, Z_L)$ with i.i.d. uniform $Z_l \in \mathbb{F}_q$ for all $l \in [L]$.

Since the encoder for a linear scheme is $\mathbb{F}_q$-linear, it follows that it can be specified by matrices $\mathbf{A}_n \in \mathbb{F}_q^{\kappa \lambda_0 \times \kappa}$, $\mathbf{B}_n \in \mathbb{F}_q^{N_B \kappa \lambda_B \times \kappa}$ and $\mathbf{Z}_n \in \mathbb{F}_q^{L \times \kappa}$ for all $n \in [N]$, such that

$$(Y_1, \ldots, Y_N) = \text{ENC}(Y_0, B, Z) \tag{30}$$
$$= Y_0 \begin{bmatrix} \mathbf{A}_1 & \ldots & \mathbf{A}_N \end{bmatrix} + B \begin{bmatrix} \mathbf{B}_1 & \ldots & \mathbf{B}_N \end{bmatrix} + Z \begin{bmatrix} \mathbf{Z}_1 & \ldots & \mathbf{Z}_N \end{bmatrix}. \tag{31}$$

Given the parameters $\lambda_0, \lambda_B, \kappa, q$ and matrices $\mathbf{A}_n, \mathbf{B}_n, \mathbf{Z}_n, n \in [N]$ that specify the encoder ENC as in (31), note that the feasibility of the scheme is guaranteed (and the existence of suitable linear decoders is implied) if the constraints (17), (18), (19) are satisfied.

A rate tuple (λ_0, λ_B) is said to be linearly achievable if there exists a feasible linear scheme $\mathfrak{S}$ such that $\lambda_0(\mathfrak{S}) \geq \lambda_0$ and $\lambda_B(\mathfrak{S}) \leq \lambda_B$. The following theorem formalizes the relationship between $\widetilde{\text{CSSRA}}$ and $\widetilde{\text{QSEA}}$ via linear achievability.

Theorem 2. *If a rate tuple (λ_0, λ_B) is linearly achievable for $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$, then the same rate tuple is achievable for $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$.*

The proof of Theorem 2 is presented in Section V. The proof is a generalization of the corresponding proof of [4, Theorem 2]. The latter setting assumes no entanglement (or SR) assistance, and the classical-quantum connection in such cases has been noted in the prior literature [4], [22], [23]. To the best of our knowledge, the generalization in Theorem 2 to include EA (and the corresponding SRA in the classical setting) is new, i.e., (erasure-prone) entanglement-assisted quantum storage codes have

---

[1]Remarkably, the same space-sharing argument also proves the tightness of the entropic quantum Singleton bounds, which was left open in [24] and [25], for settings that include both classical and quantum messages [24] or only classical messages [25], respectively.

not been previously connected to (erasure-prone) SR-assisted classical storage codes. Apparently, the main difference due to EA is that in order to ensure that the classical code can be translated to a quantum code where the quantum encoding map is unitary (or an isometry), we end up including the additional constraint (19) to the classical problem (i.e., we require recovery of B from $Y_{[N]}$).

IV. EXAMPLES

In this section, we provide some examples that illustrate the key ideas in settings with smaller values of the parameters N, K, N_B, K_B, so that the notation is simpler. Sections IV-A, IV-B, and IV-C present the achievable schemes for various extreme points of $\mathcal{C}$, and Section IV-D presents the proof of the $\mathcal{R}_\infty$ (unlimited SR) bound.

A. $(N, K, N_B, K_B) = (2, 1, 3, 2)$: Achievability of $(\lambda_0, \lambda_B) = (1/2, 1/2)$

Consider the $\widetilde{\text{CSSRA}}(2, 1, 3, 2)$ setting as our next example. We present a linear scheme that achieves the rate tuple $(\lambda_0, \lambda_B) = (1/2, 1/2)$. The parameters of the linear scheme are as follows.

1) Field size $q \geq 8$ is a prime power.
2) Scaling factor $\kappa = 2$.
3) Precoding matrices are chosen such that

$$\begin{bmatrix} \mathbf{A}_1^{1\times 2} & \mathbf{A}_2^{1\times 2} \\ \mathbf{B}_1^{3\times 2} & \mathbf{B}_2^{3\times 2} \end{bmatrix} = \mathbf{H}_{4\times 4} = \left[\frac{1}{\alpha_i - \beta_j} \right]_{ij}. \tag{32}$$

$\alpha_i, \beta_j, i, j \in [4]$ are distinct elements in $\mathbb{F}_q$. Since $q \geq 8$, these distinct elements exist. Note that by construction $\mathbf{H}$ is a 4×4 Cauchy matrix with $\frac{1}{\alpha_i - \beta_j}$ being its element in the ith row and j^{th} column.

Local randomness Z is not needed for this scheme. The storage systems are set as

$$(Y_1, Y_2)_{1\times 4} = (Y_0, B_1, B_2, B_3)_{1\times 4} \times \mathbf{H}, \tag{33}$$

where $Y_0 \in \mathbb{F}_q^{1\times \kappa\lambda_0} = \mathbb{F}_q$, the SR $B_1, B_2, B_3 \in \mathbb{F}_q^{1\times \kappa\lambda_B} = \mathbb{F}_q$, and the storage systems $Y_1, Y_2 \in \mathbb{F}_q^{1\times \kappa} = \mathbb{F}_q^{1\times 2}$.

To show that the scheme works it suffices to verify that the constraints (17), (18), (19) are satisfied. Let us consider the case $\mathcal{K} = \{1\}, \mathcal{K}_B = \{1, 3\}$. Other cases follow similarly.

1) (17): We need to show that Y_0 can be recovered from the unerased systems Y_1, B_1, B_3. Proceed as follows. Subtract the contributions of B_1, B_3 from Y_1 to obtain $(Y_0, B_2) \times \mathbf{H}_{sub}$ where $\mathbf{H}_{sub} = \mathbf{H}((1, 3), (1, 2))$ is the 2×2 sub-matrix of $\mathbf{H}$ corresponding to row-indices $1, 3$, and column-indices $1, 2$, according to (33). As a square sub-matrix of a Cauchy matrix, $\mathbf{H}_{sub}$ is an invertible matrix. Invert $\mathbf{H}_{sub}$ to recover Y_0.

2) (18): We need to show that Y_0 is independent of (Y_2, B_2). Proceed as follows.

$$\begin{align}
I(Y_0; Y_2, B_2) &= I(Y_0; Y_2 \mid B_2) \tag{34} \\
&\leq H(Y_2) - H(Y_2 \mid Y_0, B_2) \tag{35} \\
&\leq 2 - H\left((B_1, B_3)\mathbf{H}_{sub}^{2\times 2} \mid Y_0, B_2\right) \tag{36} \\
&= 2 - H\left((B_1, B_3)\mathbf{H}_{sub}^{2\times 2}\right) \tag{37} \\
&= 2 - H(B_1, B_3) \tag{38} \\
&= 2 - 2 = 0. \tag{39}
\end{align}$$

(34) follows from the independence of Y_0 and B_2 (refer to (13)). (35) follows from the fact that $H(Y_2|B_2) \leq H(Y_2)$ (conditioning reduces entropy). In (36), the first term (expressed in q-ary units) follows from the facts that Y_2 contains 2 symbols from $\mathbb{F}_q$, and the uniform distribution maximizes Shannon entropy; the second term follows from subtracting the contribution of Y_0, B_2 from Y_2, to obtain $(B_1, B_3)\mathbf{H}_{sub}$ where $\mathbf{H}_{sub} = \mathbf{H}((2, 4), (3, 4))$. Step (37) uses the fact that Y_0, B_1, B_2, B_3 are independent. Step (38) uses the fact that as a 2×2 sub-matrix of a Cauchy matrix, $\mathbf{H}_{sub}$ is invertible. The last step uses the fact that B_1, B_3 are i.i.d. uniform symbols from $\mathbb{F}_q$, so that $H(B_1, B_3) = 2$ in q-ary units.

3) (19): We need to show that $B = (B_1, B_2, B_3)$ can be recovered from (Y_1, Y_2). This follows immediately from (33), because as a Cauchy matrix by construction, $\mathbf{H}$ is invertible.

B. $(N, K, N_B, K_B) = (3, 1, 3, 2)$: Achievability of $(\lambda_0, \lambda_B) = (1/4, 1/4)$

For this example, we present a linear scheme for $\widetilde{\text{CSSRA}}(3, 1, 3, 2)$ that achieves the rate tuple $(\lambda_0, \lambda_B) = (1/4, 1/4)$. Local randomness Z will be useful in this example. The parameters of the linear scheme are as follows.

1) Field size $q \geq 13$ is a prime power.
2) Scaling factor $\kappa = 4$.
3) Local randomness $Z = (Z_1, Z_2, Z_3, Z_4) \in \mathbb{F}_q^{1\times 4}$ is uniformly distributed.

4) Precoding matrices are specified through the following steps. Note that Y_0 contains $\kappa\lambda_0 = 1$ element in $\mathbb{F}_q$ and B_1, B_2, B_3 each contains $\kappa\lambda_B = 1$ element in $\mathbb{F}_q$. First, choose a 4×3 Cauchy matrix $\mathbf{F} = \left[\frac{1}{\alpha_i - \beta_j}\right]_{ij}$ where the element in the ith row and j^{th} column is $\frac{1}{\alpha_i - \beta_j}$ and $\alpha_i, \beta_j, i \in [4], j \in [3]$ are distinct elements in $\mathbb{F}_q$. Define

$$(f_0, f_1, f_2)_{1\times 3} \triangleq (Y_0, B_1, B_2, B_3)_{1\times 4} \times \mathbf{F}_{4\times 3}. \tag{40}$$

Second, choose a 6×6 Cauchy matrix $\mathbf{H} = \left[\frac{1}{\gamma_i - \delta_j}\right]_{ij}$ where the element in the ith row and j^{th} column is $\frac{1}{\gamma_i - \delta_j}$ and $\gamma_i, \delta_j, i, j \in [6]$ are distinct elements in $\mathbb{F}_q$. Define

$$(h_1, h_2, h_3, h_4, h_5, h_6)_{1\times 6} \triangleq (f_0, Y_0, Z_1, Z_2, Z_3, Z_4)_{1\times 6} \times \mathbf{H}_{6\times 6}. \tag{41}$$

We are now ready to specify the storage systems. Note that Y_1, Y_2, Y_3 each contains $\kappa = 4$ elements in $\mathbb{F}_q$.

$$
\begin{aligned}
Y_1 &= (f_1, f_2, h_1, h_2), \\
Y_2 &= (f_1, f_2, h_3, h_4), \\
Y_3 &= (f_1, f_2, h_5, h_6).
\end{aligned} \tag{42}
$$

Note that the first two elements in Y_1, Y_2, Y_3 are identical, i.e., f_1, f_2. The above encoding procedure is linear and thus the precoding matrices $\mathbf{A}_n, \mathbf{B}_n, \mathbf{Z}_n, n \in [3]$ are implied.

To show that the scheme works we need to verify the constraints (17), (18), (19). Consider the case $\mathcal{K} = \{1\}, \mathcal{K}_B = \{1, 3\}$. Other cases follow similarly.

1) (17): We need to show that Y_0 is determined by (Y_1, B_1, B_3). Proceed as follows. Subtracting the contribution of B_1, B_3 from f_1, f_2 (the first two elements of Y_1) in (40), we obtain $(Y_0, B_2)_{1\times 2} \times \mathbf{F}_{sub}$. As a 2×2 sub-matrix of a Cauchy matrix, $\mathbf{F}_{sub} = \mathbf{F}((1, 3), (2, 3))_{2\times 2}$ is invertible. Invert $\mathbf{F}_{sub}$ to obtain Y_0.

2) (18): We need to show that Y_0 is independent of Y_2, Y_3, B_2. Proceed as follows.

$$
\begin{aligned}
&I(Y_0; Y_2, Y_3, B_2) \\
&= I(Y_0; f_1, f_2, h_3, h_4, h_5, h_6 \mid B_2) \tag{43} \\
&\leq H(f_1, f_2, h_3, h_4, h_5, h_6) - H(f_1, f_2, h_3, h_4, h_5, h_6 \mid Y_0, B_2) \tag{44} \\
&\leq 6 - H(f_1, f_2 \mid Y_0, B_2) - H(h_3, h_4, h_5, h_6 \mid f_1, f_2, Y_0, B_1, B_2, B_3) \tag{45} \\
&\leq 6 - H((B_1, B_3)\mathbf{F}((2, 4), (2, 3)) \mid Y_0, B_2) \\
&\quad\quad - H((Z_1, Z_2, Z_3, Z_4)\mathbf{H}((3, 4, 5, 6), (3, 4, 5, 6)) \mid Y_0, B_1, B_2, B_3) \tag{46} \\
&= 6 - H(B_1, B_3 \mid Y_0, B_2) - H(Z_1, Z_2, Z_3, Z_4 \mid Y_0, B_1, B_2, B_3) \tag{47} \\
&= 6 - 2 - 4 = 0. \tag{48}
\end{aligned}
$$

In (43), we plug in the design of Y_2, Y_3 and use the fact that message Y_0 is independent of SR B_2 (refer to (13)). Step (44) follows because dropping conditioning cannot reduce entropy. In (45), the first term follows from the fact that $f_1, f_2, h_3, h_4, h_5, h_6$ are 6 symbols in $\mathbb{F}_q$ and the uniform distribution maximizes entropy; the third term follows from the property that adding conditioning (on B_1, B_3) cannot increase entropy. In (46), the second term is obtained by subtracting the contribution of Y_0, B_2 from f_1, f_2 and we are left with 2 linear combinations in B_1, B_3; to obtain the third term, we note that f_1, f_2 are deterministic functions of Y_0, B_1, B_2, B_3 so that they can be dropped from the conditioning term, and subtracting the contribution of Y_0, B_1, B_2, B_3 from h_3, h_4, h_5, h_6 we are left with 4 linear combinations in Z_1, Z_2, Z_3, Z_4. (47) follows because $\mathbf{F}$ and $\mathbf{H}$ are Cauchy matrices by construction, so their sub-matrices have full rank. The last step (48) is due to the fact that $Z_1, Z_2, Z_3, Z_4, B_1, B_2, B_3$ comprise i.i.d. uniform symbols in $\mathbb{F}_q$ and are independent of the message Y_0.

3) (19): We need to show that (B_1, B_2, B_3) is determined by (Y_1, Y_2, Y_3). Proceed as follows. First, as Cauchy $\mathbf{H}_{6\times 6}$ is invertible, from $h_1, h_2, h_3, h_4, h_5, h_6$ (the last two elements of Y_1, Y_2, Y_3) we obtain $f_0, Y_0, Z_1, Z_2, Z_3, Z_4$. Second, we subtract the contribution of Y_0 from f_0, f_1, f_2 (f_0, Y_0 have been recovered and f_1, f_2 are the first two elements of Y_1, Y_2, Y_3) and obtain $(B_1, B_2, B_3) \times \mathbf{F}((2, 3, 4), (1, 2, 3))$, from which B_1, B_2, B_3 is recovered as $\mathbf{F}$ is Cauchy. Thus (B_1, B_2, B_3) is determined by (Y_1, Y_2, Y_3).

C. $(N, K, N_B, K_B) = (3, 1, 3, 2)$: Achievability of $(\lambda_0, \lambda_B) = (1/2, 5/6)$

Continuing with the same setting of $\widetilde{\mathrm{CSSRA}}(3, 1, 3, 2)$, here we present the linear scheme for a different rate tuple $(\lambda_0, \lambda_B) = (1/2, 5/6)$. Local randomness Z will not be used in this scheme. The parameters of the linear scheme are as follows.

1) Field size q is any prime power such that $q \geq 13$.
2) Scaling factor $\kappa = 6$.

3) Precoding matrices are specified through the following steps. Note that Y_0 contains $\kappa\lambda_0 = 3$ elements in $\mathbb{F}_q$, denoted as $Y_0 = (a_1, a_2, a_3)$ and B_1, B_2, B_3 each contains $\kappa\lambda_B = 5$ elements in $\mathbb{F}_q$. We divide the 5 elements into 2 parts, labelled by the superscript x, y.

$$B_1 = \left(\underbrace{\boldsymbol{b}_1^{1,x}}_{1\times 2}, \underbrace{\boldsymbol{b}_1^{2,x}}_{1\times 2}, \underbrace{b_1^y}_{1\times 1}\right), B_2 = \left(\underbrace{\boldsymbol{b}_2^{1,x}}_{1\times 2}, \underbrace{\boldsymbol{b}_2^{2,x}}_{1\times 2}, \underbrace{b_2^y}_{1\times 1}\right), B_3 = \left(\underbrace{\boldsymbol{b}_3^{1,x}}_{1\times 2}, \underbrace{\boldsymbol{b}_3^{2,x}}_{1\times 2}, \underbrace{b_3^y}_{1\times 1}\right). \tag{49}$$

Choose a 6×6 Cauchy matrix $\mathbf{H} = \left[\frac{1}{\alpha_i - \beta_j}\right]_{ij}$ where the element in the ith row and j^{th} column is $\frac{1}{\alpha_i - \beta_j}$ and $\alpha_i, \beta_j, i \in [6], j \in [6]$ are distinct elements in $\mathbb{F}_q$. Then define

$$\left(\underbrace{\boldsymbol{h}_1}_{1\times 2}, \underbrace{\boldsymbol{h}_2}_{1\times 2}, \underbrace{\boldsymbol{h}_3}_{1\times 2}\right)_{1\times 6} \triangleq (a_1, a_2, a_3, b_1^y, b_2^y, b_3^y)_{1\times 6} \times \mathbf{H}_{6\times 6}. \tag{50}$$

We are now ready to specify the storage systems. Note that Y_1, Y_2, Y_3 each contains $\kappa = 6$ elements in $\mathbb{F}_q$.

$$\begin{aligned}
Y_1 &= \left(\boldsymbol{h}_1 + \boldsymbol{b}_1^{1,x}, \boldsymbol{h}_2 + \boldsymbol{b}_2^{1,x}, \boldsymbol{h}_3 + \boldsymbol{b}_3^{1,x}\right)_{1\times 6}, \\
Y_2 &= \left(\boldsymbol{h}_1 + \boldsymbol{b}_1^{2,x}, \boldsymbol{h}_2 + \boldsymbol{b}_2^{2,x}, \boldsymbol{h}_3 + \boldsymbol{b}_3^{2,x}\right)_{1\times 6}, \\
Y_3 &= \left(\boldsymbol{h}_1 + \boldsymbol{b}_1^{1,x} + \boldsymbol{b}_1^{2,x}, \boldsymbol{h}_2 + \boldsymbol{b}_2^{1,x} + \boldsymbol{b}_2^{2,x}, \boldsymbol{h}_3 + \boldsymbol{b}_3^{1,x} + \boldsymbol{b}_3^{2,x}\right)_{1\times 6}.
\end{aligned} \tag{51}$$

Observe that across Y_1, Y_2, Y_3, the pattern of $\boldsymbol{h}$ terms is repeated, whereas $\boldsymbol{b}^{1,x}, \boldsymbol{b}^{2,x}$ go through a $(3,2)$ MDS code $(x, y) \to (x, y, x+y)$.

To show that the scheme works we verify the constraints (17), (18), (19). Consider the case $\mathcal{K} = \{1\}, \mathcal{K}_B = \{1,3\}$. Other cases follow similarly.

1) (17): We need to show that Y_0 is determined by (Y_1, B_1, B_3). Let us proceed as follows. $\boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x}$ are known from B_1, B_3. Subtract the contributions of $\boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x}$ from Y_1 (consider the first and third terms) and obtain

$$(\boldsymbol{h}_1, \boldsymbol{h}_3)_{1\times 4} = (a_1, a_2, a_3, b_1^y, b_2^y, b_3^y)_{1\times 6} \times \mathbf{H}(:, (1,2,5,6))_{6\times 4}. \tag{52}$$

Observe that b_1^y, b_3^y are known from B_1, B_3. Subtract the contribution of b_1^y, b_3^y from $\boldsymbol{h}_1, \boldsymbol{h}_3$ and obtain

$$(a_1, a_2, a_3, b_2^y)_{1\times 4} \times \mathbf{H}((1,2,3,5), (1,2,5,6))_{4\times 4}. \tag{53}$$

As a sub-matrix of the Cauchy matrix $\mathbf{H}$, the 4×4 matrix $\mathbf{H}((1,2,3,5), (1,2,5,6))$ is invertible. Invert to recover $Y_0 = (a_1, a_2, a_3)$.

2) (18): We need to show that Y_0 is independent of (Y_2, Y_3, B_2). Proceed as follows.

$$\begin{aligned}
&I(Y_0; Y_2, Y_3, B_2) \\
&\overset{(13),(51)}{=} I\left(Y_0; \boldsymbol{h}_1 + \boldsymbol{b}_1^{2,x}, \boldsymbol{h}_2, \boldsymbol{h}_3 + \boldsymbol{b}_3^{2,x}, \boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x} \mid B_2\right) \tag{54} \\
&= H\left(\underbrace{\boldsymbol{h}_1 + \boldsymbol{b}_1^{2,x}, \boldsymbol{h}_2, \boldsymbol{h}_3 + \boldsymbol{b}_3^{2,x}, \boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x}}_{1\times 10} \mid B_2\right) \\
&\quad - H\left(\boldsymbol{h}_1 + \boldsymbol{b}_1^{2,x}, \boldsymbol{h}_2, \boldsymbol{h}_3 + \boldsymbol{b}_3^{2,x}, \boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x} \mid Y_0, B_2\right) \tag{55} \\
&\leq 10 - H(\boldsymbol{h}_2 \mid Y_0, B_2) - H\left(\boldsymbol{h}_1 + \boldsymbol{b}_1^{2,x}, \boldsymbol{h}_3 + \boldsymbol{b}_3^{2,x}, \boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x} \mid Y_0, B_2, \boldsymbol{h}_2, b_1^y, b_2^y, b_3^y\right) \tag{56} \\
&\overset{(50)}{\leq} 10 - H\left((b_1^y, b_3^y) \times \mathbf{H}((4,6), (3,4)) \mid Y_0, B_2\right) \\
&\quad - H\left(\boldsymbol{b}_1^{2,x}, \boldsymbol{b}_3^{2,x}, \boldsymbol{b}_1^{1,x}, \boldsymbol{b}_3^{1,x} \mid Y_0, B_2, b_1^y, b_2^y, b_3^y\right) \tag{57} \\
&= 10 - 2 - 8 = 0. \tag{58}
\end{aligned}$$

In (54), we plug in the design of Y_2, Y_3, subtract the contribution of B_2, i.e., $\boldsymbol{b}_2^x$, and perform invertible transformations to simplify the terms. In (57), the third term follows from the fact that $\boldsymbol{h}$ are known given Y_0, b^y. (58) follows from the fact that $\mathbf{H}$ is Cauchy and the SR B is i.i.d. uniform and independent of Y_0.

3) (19): We need to show that $B = (B_1, B_2, B_3)$ is determined by (Y_1, Y_2, Y_3). Proceed as follows.

$$Y_3 - Y_1 = \left(\boldsymbol{b}_1^{2,x}, \boldsymbol{b}_2^{2,x}, \boldsymbol{b}_3^{2,x} \right)_{1 \times 6}, \tag{59}$$

$$Y_3 - Y_2 = \left(\boldsymbol{b}_1^{1,x}, \boldsymbol{b}_2^{1,x}, \boldsymbol{b}_3^{1,x} \right)_{1 \times 6}. \tag{60}$$

Subtract the contribution of $\boldsymbol{b}^x$ terms from Y_1, Y_2, Y_3 and obtain $\boldsymbol{h}_1, \boldsymbol{h}_2, \boldsymbol{h}_3$, from which a_1, a_2, a_3, b_1^y, b_2^y, b_3^y are determined because $\mathbf{H}$ is invertible (refer to (50)). Thus B ($\boldsymbol{b}^x, b^y$ terms) is recovered.

D. $(N, K, N_B, K_B) = (3, 2, 4, 3)$: *Proof of Converse* $\lambda_0 \leq 5/3$

For the setting of $\widetilde{\text{CSSRA}}(3, 2, 4, 3)$, here we present an information theoretic proof that the bound $\lambda_0 \leq 5/3$ applies to *all* (not limited to linear) feasible coding schemes. Consider any feasible coding scheme $\mathfrak{S}$. Suppose $\mathcal{K} = \{1, 2\}, \mathcal{K}_B = \{1, 2, 4\}$, and Y_0 is uniformly distributed. A feasible scheme must be able to recover Y_0 from $Y_{\mathcal{K}}, B_{\mathcal{K}_B}$. From the decodability constraint (17), we have

$$
\begin{aligned}
\kappa\lambda_0 \leq \kappa\lambda_0(\mathfrak{S}) \quad &= \quad H(Y_0) \overset{(17)}{=} I(Y_0; Y_1, Y_2, B_1, B_2, B_4) &&(61) \\
&= \quad I(Y_0; Y_1, B_1, B_2, B_4) + I(Y_0; Y_2 \mid Y_1, B_1, B_2, B_4) &&(62) \\
&\overset{(13)}{=} \quad I(Y_0; Y_1 \mid B_1, B_2, B_4) + I(Y_0; Y_2 \mid Y_1, B_1, B_2, B_4) &&(63) \\
&\leq \quad I(Y_0, B_1, B_2; Y_1 \mid B_4) + H(Y_2) &&(64) \\
&\leq \quad \underbrace{I(Y_0; Y_1 \mid B_4)}_{\overset{(18)}{\leq} 0} + I(B_1, B_2; Y_1 \mid Y_0, B_4) + \kappa &&(65) \\
\implies \quad \kappa\lambda_0 - \kappa \quad &\leq \quad I(B_1, B_2; Y_1 \mid Y_0, B_4). &&(66)
\end{aligned}
$$

(63) follows from the fact that Y_0 is independent of B. In (65), the first term is zero due to the security constraint (18), where $\mathcal{K}^c = \{1\}$ and $\mathcal{K}_B^c = \{4\}$.

Following the same procedure as above, and setting $\mathcal{K}_B$ as $\{1, 3, 4\}$ and $\{2, 3, 4\}$, respectively, we obtain

$$
\begin{aligned}
\kappa\lambda_0 - \kappa \quad &\leq \quad I(B_1, B_3; Y_1 \mid Y_0, B_4), &&(67) \\
\kappa\lambda_0 - \kappa \quad &\leq \quad I(B_2, B_3; Y_1 \mid Y_0, B_4). &&(68)
\end{aligned}
$$

Adding (66), (67), and (68), we have

$$
\begin{aligned}
&3\kappa\lambda_0 - 3\kappa \\
&\leq \quad I(B_1, B_2; Y_1 \mid Y_0, B_4) + I(B_1, B_3; Y_1 \mid Y_0, B_4) + I(B_2, B_3; Y_1 \mid Y_0, B_4) &&(69) \\
&\overset{(13)}{=} \quad I(B_1, B_2; Y_1 \mid Y_0, B_4) + I(B_1, B_3; Y_1, Y_0, B_4) + I(B_2, B_3; Y_1 \mid Y_0, B_4) &&(70) \\
&\overset{(13)}{\leq} \quad I(B_1, B_2; Y_1 \mid Y_0, B_4) + I(B_1, B_3; Y_1 \mid Y_0, B_2, B_4) + I(B_2, B_3; Y_1 \mid Y_0, B_4) &&(71) \\
&= \quad I(B_1, B_2; Y_1 \mid Y_0, B_4) + I(B_3; Y_1 \mid Y_0, B_1, B_2, B_4) \\
&\quad + I(B_1; Y_1 \mid Y_0, B_2, B_4) + I(B_2, B_3; Y_1 \mid Y_0, B_4) &&(72) \\
&\overset{(13)}{\leq} \quad I(B_1, B_2, B_3; Y_1 \mid Y_0, B_4) + I(B_1; Y_1 \mid Y_0, B_2, B_3, B_4) + I(B_2, B_3; Y_1 \mid Y_0, B_4) &&(73) \\
&= \quad 2I(B_1, B_2, B_3; Y_1 \mid Y_0, B_4) &&(74) \\
&\leq \quad 2H(Y_1) \leq 2\kappa &&(75) \\
\implies \quad &3\lambda_0 \leq 5, &&(76)
\end{aligned}
$$

thus producing the desired bound. Note that we repeatedly use the independence of Y_0 and B and the uniformity of B (so that B_i are independent) to add conditioning terms and to combine the mutual information terms.

V. PROOF OF THEOREM 2

Consider any classical linear scheme for $\widetilde{\text{CSSRA}}(N, K, N_B, K_B)$ as defined in Definition 1, i.e., we are given λ_0, λ_B, κ, q, $\mathbf{A}_n$, $\mathbf{B}_n$, $\mathbf{Z}_n$, $\forall n \in [N]$ such that (17), (18), (19) are satisfied. We show how this allows us to design a quantum coding scheme for $\widetilde{\text{QSEA}}(N, K, N_B, K_B)$ as follows.

Consider the quantum encoding procedure first. Suppose the quantum message Q_0 has $\kappa\lambda_0$ qudits where each qudit is q-dimensional. Suppose Q_0 is in an arbitrary state with density matrix ω_{Q_0}. Without loss of generality, suppose ω_{Q_0} has a spectral decomposition $\omega_{Q_0} = \sum_{\boldsymbol{a}} p_{\boldsymbol{a}} |\boldsymbol{a}\rangle \langle \boldsymbol{a}|$ and a purification $|\varphi\rangle_{RQ_0} = \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle |\boldsymbol{a}\rangle$. The encoding proceeds as follows.

$$|\varphi\rangle_{RQ_0} |\phi\rangle_{AB} \tag{77}$$

$$= \sum_{\boldsymbol{a} \in \mathbb{F}_q^{1 \times \kappa \lambda_0}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \, |\boldsymbol{a}\rangle_{Q_0} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{1 \times N_B \kappa \lambda_B}} \frac{1}{\sqrt{q^{N_B \kappa \lambda_B}}} \, |\boldsymbol{b}\rangle_A \, |\boldsymbol{b}\rangle_B \tag{78}$$

$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b}, \boldsymbol{z} \in \mathbb{F}_q^{1 \times L}} \frac{1}{\sqrt{q^{N_B \kappa \lambda_B + L}}} \, |Y_1, Y_2, \dots, Y_N\rangle_{Q_1 \dots Q_N} \, |\boldsymbol{b}\rangle_B \,, \tag{79}$$

where (79) is an isometric map from $Q_0 A$ to $Q_1 \dots Q_N$, because (17) and (19) guarantee that from $(Y_n, n \in [N]) = (\boldsymbol{a}\mathbf{A}_n + \boldsymbol{b}\mathbf{B}_n + \boldsymbol{z}\mathbf{Z}_n, n \in [N])$, one can recover $\boldsymbol{a}, \boldsymbol{b}$. Observe that R and B go through an identity map and $RQ_1 \dots Q_N B$ ends up in a pure state. Compared to Theorem 2 in [4] the main difference in the above encoding procedure is that here we have EA AB and need to ensure that the encoding does not require access to B.

Remark 1. *Note that the additional constraint (19) that we impose for $\widetilde{\mathrm{CSSRA}}$, guarantees that the above quantum encoding procedure is feasible for $\widetilde{\mathrm{QSEA}}$, i.e., the map to produce (79) from $Q_0 A$ to $Q_1 \dots Q_N$ is isometric. Recall that according to the problem formulation the encoding needs not be restricted to isometric maps. Restricted as it might seem, our approach (combined with space-sharing) provides optimal quantum schemes for all regimes where capacity is known (Case 1 and Case 2 in Theorem 1) and is conjectured to be optimal in the remaining regime (Case 3) as well.*

The quantum decoding process follows from [4, Theorem 2]. Note that the same classical constraints are satisfied, i.e., (17) for the decoding of Y_0 from each decoding set (i.e., any K storage systems and any K_B SR-systems) and (18) for the security of Y_0 from the complement of each decoding set (i.e., any $N - K$ storage systems and any $N_B - K_B$ SR-systems). Thus, [4, Theorem 2] guarantees perfect recovery for any decoding set (the decoding sets are identical for $\widetilde{\mathrm{CSSRA}}(N, K, N_B, K_B)$ and $\widetilde{\mathrm{QSEA}}(N, K, N_B, K_B)$). For the sake of completeness let us briefly sketch the decoding procedure of [4, Theorem 2] here.

Fix any $\mathcal{K}, \mathcal{K}_B$. Consider the state for $RQ_1 \dots Q_N B = RQ_{\mathcal{K}} B_{\mathcal{K}_B} Q_{\mathcal{K}^c} B_{\mathcal{K}_B^c}$, expressed as follows.

$$\sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b}, \boldsymbol{z}} \frac{1}{\sqrt{q^{N_B \kappa \lambda_B + L}}} \, |\boldsymbol{a}\mathbf{A}_{[N]} + \boldsymbol{b}\mathbf{B}_{[N]} + \boldsymbol{z}\mathbf{Z}_{[N]}\rangle_{Q_1 \dots Q_N} \, |\boldsymbol{b}\rangle_B$$

$$\equiv \sum_{\boldsymbol{a}} |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b}, \boldsymbol{z}} |\boldsymbol{a}\mathbf{A}_{\mathcal{K}} + \boldsymbol{b}\mathbf{B}_{\mathcal{K}} + \boldsymbol{z}\mathbf{Z}_{\mathcal{K}}\rangle_{Q_{\mathcal{K}}} \, |\boldsymbol{b}_{\mathcal{K}_B}\rangle_{B_{\mathcal{K}_B}} \, |\boldsymbol{a}\mathbf{A}_{\mathcal{K}^c} + \boldsymbol{b}\mathbf{B}_{\mathcal{K}^c} + \boldsymbol{z}\mathbf{Z}_{\mathcal{K}^c}\rangle_{Q_{\mathcal{K}^c}} \, |\boldsymbol{b}_{\mathcal{K}_B^c}\rangle_{B_{\mathcal{K}_B^c}} \,, \tag{80}$$

where for any matrix $\mathbf{A}$ and any set $\mathcal{K}$, $\mathbf{A}_{\mathcal{K}}$ denotes the sub-matrix of $\mathbf{A}$ with all columns whose indices are in $\mathcal{K} = \{k_1, \cdots, k_{|\mathcal{K}|}\}$,

$$\mathbf{A}_{\mathcal{K}} \triangleq \left(\mathbf{A}(:, k_1), \dots, \mathbf{A}(:, k_{|\mathcal{K}|}) \right). \tag{81}$$

The next key step is to perform a change of basis operation. Note that the decodability constraint (17) holds, i.e., from $(\boldsymbol{a}\mathbf{A}_{\mathcal{K}} + \boldsymbol{b}\mathbf{B}_{\mathcal{K}} + \boldsymbol{z}\mathbf{Z}_{\mathcal{K}}, \boldsymbol{b}_{\mathcal{K}_B}) \triangleq \boldsymbol{s}$, we may recover $\boldsymbol{a}$; the security constraint (18) holds, i.e., $(\boldsymbol{a}\mathbf{A}_{\mathcal{K}^c} + \boldsymbol{b}\mathbf{B}_{\mathcal{K}^c} + \boldsymbol{z}\mathbf{Z}_{\mathcal{K}^c}, \boldsymbol{b}_{\mathcal{K}_B^c}) \triangleq \boldsymbol{n}$ is independent of $\boldsymbol{a}$. Then denoting $\boldsymbol{z}_1'$ as the common part of $\boldsymbol{s}$ and $\boldsymbol{n}$ (identified through the intersection of linear subspaces), $\boldsymbol{z}_2'$ as the part that is in $\boldsymbol{s}$ (a linear function of $\boldsymbol{s}$) but not in $\boldsymbol{n}$ (identified through the linear space that lies in $\boldsymbol{s}$, but has no overlap with $\boldsymbol{n}$), $\boldsymbol{z}_3'$ as the part that is in $\boldsymbol{n}$ but not in $\boldsymbol{s}$, we have

$$(\boldsymbol{a}\mathbf{A}_{\mathcal{K}} + \boldsymbol{b}\mathbf{B}_{\mathcal{K}} + \boldsymbol{z}\mathbf{Z}_{\mathcal{K}}, \boldsymbol{b}_{\mathcal{K}_B}) \stackrel{\text{invertible}}{\longleftrightarrow} (\boldsymbol{a}, \boldsymbol{z}_1', \boldsymbol{z}_2', l(\boldsymbol{z}_1', \boldsymbol{z}_2')) \,, \tag{82}$$

$$\left(\boldsymbol{a}\mathbf{A}_{\mathcal{K}^c} + \boldsymbol{b}\mathbf{B}_{\mathcal{K}^c} + \boldsymbol{z}\mathbf{Z}_{\mathcal{K}^c}, \boldsymbol{b}_{\mathcal{K}_B^c} \right) = (l(\boldsymbol{z}_1', \boldsymbol{z}_3')) \,, \tag{83}$$

where l denotes some linear combinations and the crucial observation is that $\boldsymbol{a}$ can be separated out from $\boldsymbol{s}$ while $\boldsymbol{a}$ cannot be obtained at all from $\boldsymbol{n}$. Furthermore, for any fixed $\boldsymbol{a}$, we have $(\boldsymbol{z}_1', \boldsymbol{z}_2', \boldsymbol{z}_3')$, which contains all $\boldsymbol{b}$ and $\boldsymbol{z}$ that appear in $Q_1 \dots Q_N B$, is invertible to $(\boldsymbol{b}, \boldsymbol{z}\mathbf{Z}_{[N]})$. A detailed treatment of the above change of basis operation can be found in [4, Theorem 2].

We now proceed with the decoding procedure, continuing from (80).

$$\stackrel{(80)}{\rightsquigarrow} \sum_{\boldsymbol{a}} |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b}, \boldsymbol{z}} |\boldsymbol{a}, \boldsymbol{z}_1', \boldsymbol{z}_2', l(\boldsymbol{z}_1', \boldsymbol{z}_2')\rangle \, |l(\boldsymbol{z}_1', \boldsymbol{z}_3')\rangle_{Q_{\mathcal{K}^c} B_{\mathcal{K}_B^c}} \tag{84}$$

$$\equiv \sum_{\boldsymbol{a}} |\boldsymbol{a}\rangle_R \, |\boldsymbol{a}\rangle_{\widehat{Q}_0} \sum_{\boldsymbol{z}_1', \boldsymbol{z}_2', \boldsymbol{z}_3'} |\boldsymbol{z}_1', \boldsymbol{z}_2', l(\boldsymbol{z}_1', \boldsymbol{z}_2')\rangle \, |l(\boldsymbol{z}_1', \boldsymbol{z}_3')\rangle_{Q_{\mathcal{K}^c} B_{\mathcal{K}_B^c}} \tag{85}$$

$$= \left(\sum_{\boldsymbol{a}} |\boldsymbol{a}\rangle_R \, |\boldsymbol{a}\rangle_{\widehat{Q}_0} \right) \otimes \cdots . \tag{86}$$

Therefore, the decodability constraint (17) and the security constraint (18) together guarantee that we can unentangle $R\widehat{Q}_0$ from the rest of the codeword and the state of $R\widehat{Q}_0$ is identical to that of RQ_0. The rate tuple achieved for $\widetilde{\mathrm{QSEA}}(N, K, N_B, K_B)$ is (λ_0, λ_B), same as that for $\widetilde{\mathrm{CSSRA}}(N, K, N_B, K_B)$.

Remark 2. *Recall that according to (19), the code for $\widetilde{CSSRA}$ requires the full recovery of B from $Y_1, \ldots, Y_N$. It is not difficult to see that such a constraint can sometimes exclude optimal schemes, e.g., in the regime where λ_B is large. However, as we show in the following sections, this code achieves all (including conjectured) extreme points of the capacity region $\mathcal{C}$. The corresponding insight for $\widetilde{QSEA}$ is that while a pure ρ might not always be optimal (e.g., for large λ_B) but a pure ρ may still achieve all extreme points of the capacity region. The achievability of the remaining points is then implied by convexity of the capacity region, e.g., via space-sharing (see Appendix A).*

VI. PROOF OF THEOREM 1

A. Converse Proof of $\mathcal{C}$: Classical Storage

Our problem formulation requires perfect recovery for an arbitrarily distributed Y_0, so in particular perfect recovery is required for a uniform Y_0, i.e., $H(Y_0) = \log_q |Y_0| = \kappa \lambda_0$. In the following, we assume Y_0 is uniform over $\mathcal{Y}_0$, a set of cardinality $q^{\kappa \lambda_0}$.

1) Proof of $\mathcal{R}_{cut}$ Bound: We prove that $\lambda_0 \leq \max(2K - N, 0) + \lambda_B \cdot \max(2K_B - N_B, 0)$ for any feasible coding scheme $\mathfrak{S}$. Start from the entropic decodability condition (17) and set $\mathcal{K} = [K], \mathcal{K}_B = [N_B]$.

$$
\begin{align}
\kappa \lambda_0 \quad &\leq \quad \kappa \lambda_0(\mathfrak{S}) = H(Y_0) \overset{(17)}{=} I\left(Y_0; Y_{[K]}, B_{[K_B]}\right) \tag{87}\\
&\leq \quad I\left(Y_0; Y_{[N-K]}, Y_{[N-K+1:K]}, B_{[N_B-K_B]}, B_{[N_B-K_B+1:K_B]}\right) \tag{88}\\
&\overset{(18)}{=} \quad I\left(Y_0; Y_{[N-K+1:K]}, B_{[N_B-K_B+1:K_B]} \mid Y_{[N-K]}, B_{[N_B-K_B]}\right) \tag{89}\\
&\leq \quad H\left(Y_{[N-K+1:K]}\right) + H\left(B_{[N_B-K_B+1:K_B]}\right) \tag{90}\\
&\leq \quad \log_q \prod_{n \in [N-K+1:K]} |Y_n| + \log_q \prod_{i \in [N_B-K_B+1:K_B]} |B_i| \tag{91}\\
&\leq \quad \kappa \cdot \max(2K - N, 0) + \kappa \lambda_B(\mathfrak{S}) \cdot \max(2K_B - N_B, 0) \tag{92}\\
\implies \lambda_0 \quad &\leq \quad \max(2K - N, 0) + \lambda_B \cdot \max(2K_B - N_B, 0). \tag{93}
\end{align}
$$

Step (89) uses the security constraint (18) when $\mathcal{K}^c = [N - K], \mathcal{K}_B^c = [N_B - K_B]$.

2) Proof of $\mathcal{R}_\infty$ Bound: We prove that for any feasible coding scheme $\mathfrak{S}$, $\lambda_0 \leq \min(N, 2K) - \min(N - K, K)\frac{N_B}{K_B}$, which becomes

$$
\lambda_0 \leq N - (N - K)\frac{N_B}{K_B} \text{ when } K/N \geq 1/2, \tag{94}
$$

and becomes

$$
\lambda_0 \leq K - 2K\frac{N_B}{K_B} \text{ when } K/N < 1/2. \tag{95}
$$

(94) implies (95) because we may set $N = 2K$ in (94) so that it becomes (95). Reducing N to $2K$ means that we only consider $2K$ out of the N storage systems, which does not violate a converse argument. Therefore, it suffices to prove (94) only, considered next. The proof is a generalization of the example in Section IV-D, where the summation of the mutual information terms in (69) needs to be generalized (see Lemma 1).

Consider $\mathcal{K} = [K] = [N-K] \cup [N-K+1:K], \mathcal{K}_B = \mathcal{I} \cup [K_B+1:N_B]$ where $\mathcal{I} \subset [K_B], |\mathcal{I}| = 2K_B - N_B$. Note that $2K_B - N_B \leq K_B$ and $K/N \geq 1/2$. From the decodability constraint (17), we have

$$
\begin{align}
\kappa \lambda_0 \quad &\leq \quad \kappa \lambda_0(\mathfrak{S}) = H(Y_0) \overset{(17)}{=} I\left(Y_0; Y_{\mathcal{K}}, B_{\mathcal{K}_B}\right) \tag{96}\\
&= \quad I\left(Y_0; Y_{[N-K]}, Y_{[N-K+1:K]}, B_{\mathcal{K}_B}\right) \tag{97}\\
&\leq \quad I\left(Y_0; Y_{[N-K]}, B_{\mathcal{K}_B}\right) + H\left(Y_{[N-K+1:K]}\right) \tag{98}\\
&\overset{(13)}{=} \quad I\left(Y_0; Y_{[N-K]} \mid B_{\mathcal{I}}, B_{[K_B+1:N_B]}\right) + \kappa(2K - N) \tag{99}\\
&\leq \quad I\left(Y_0, B_{\mathcal{I}}; Y_{[N-K]} \mid B_{[K_B+1:N_B]}\right) + \kappa(2K - N) \tag{100}\\
&= \quad \underbrace{I\left(Y_0; Y_{[N-K]} \mid B_{[K_B+1:N_B]}\right)}_{\overset{(18)}{\leq} 0} + I\left(B_{\mathcal{I}}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)\\
&\quad + \kappa(2K - N) \tag{101}\\
\implies \quad &\kappa \lambda_0 - \kappa(2K - N) \leq I\left(B_{\mathcal{I}}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right). \tag{102}
\end{align}
$$

Next we focus on the RHS of (102). Consider the following K_B choices of $\mathcal{I}$.

$$
\begin{align}
&\mathcal{I}_1 = \{1, 2, \cdots, 2K_B - N_B\}, \mathcal{I}_2 = \{2K_B - N_B + 1, \cdots, 2(2K_B - N_B)\}_{mod}, \cdots,\\
&\mathcal{I}_{K_B} = \{(K_B - 1)(2K_B - N_B) + 1, \cdots, K_B(2K_B - N_B)\}_{mod}. \tag{103}
\end{align}
$$

The subscript mod means that each element i in the set is defined as $i \mod K_B$. That is, each $\mathcal{I}_j, j \in [K_B]$ has K_B elements in the set $[K_B]$ and the elements are taken consecutively (in a cyclic manner). In total, $\sum_{j \in [K_B]} |\mathcal{I}_j| = K_B(2K_B - N_B)$ so that overall the union of all $\mathcal{I}_j$ covers the set $[K_B]$ for a total of $2K_B - N_B$ times. For example, consider $K_B = 5$, $2K_B - N_B = 3$.

$$\mathcal{I}_1 = \{1,2,3\}, \mathcal{I}_2 = \{4,5,1\}, \mathcal{I}_3 = \{2,3,4\}, \mathcal{I}_4 = \{5,1,2\}, \mathcal{I}_5 = \{3,4,5\}. \tag{104}$$

To proceed with the derivation of the converse, our goal is to treat the sum of the RHS of (102) for all $\mathcal{I}_1, \ldots, \mathcal{I}_{K_B}$. This result is stated in the following lemma.

Lemma 1. *For the sets $\mathcal{I}_1, \ldots, \mathcal{I}_{K_B}$ defined in (103) and any disjoint sets $\mathcal{J}_1, \mathcal{J}_2 \subset [K_B]$, i.e., $\mathcal{J}_1 \cap \mathcal{J}_2 = \emptyset$, we have*

$$I\left(B_{\mathcal{J}_1}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \leq I\left(B_{\mathcal{J}_1}; Y_{[N-K]} \mid B_{\mathcal{J}_2}, Y_0, B_{[K_B+1:N_B]}\right), \tag{105}$$

$$\sum_{j \in [K_B]} I\left(B_{\mathcal{I}_j}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \leq (2K_B - N_B) I\left(B_{[K_B]}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right). \tag{106}$$

Proof: (105) states that we can add arbitrary conditional terms $B_{\mathcal{J}}$. It is a simple consequence of the independence of Y_0 and B and the uniformity of B, proved as follows.

$$I\left(B_{\mathcal{J}_1}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \overset{(13)}{=} I\left(B_{\mathcal{J}_1}; Y_{[N-K]}, Y_0, B_{[K_B+1:N_B]}\right) \tag{107}$$

$$\leq I\left(B_{\mathcal{J}_1}; Y_{[N-K]}, B_{\mathcal{J}_2}, Y_0, B_{[K_B+1:N_B]}\right) \tag{108}$$

$$\overset{(13)}{=} I\left(B_{\mathcal{J}_1}; Y_{[N-K]} \mid B_{\mathcal{J}_2}, Y_0, B_{[K_B+1:N_B]}\right). \tag{109}$$

We are now ready to prove (106) by combining the mutual information terms with the chain rule and repeatedly using (105).

$$\sum_{j \in [K_B]} I\left(B_{\mathcal{I}_j}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{110}$$

$$= I\left(B_{\mathcal{I}_1}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_{\mathcal{I}_2}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + \cdots \tag{111}$$

$$\overset{(105)}{\leq} I\left(B_{\mathcal{I}_1 \cup \mathcal{I}_2}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + \cdots \quad \text{if } \mathcal{I}_1 \cup \mathcal{I}_2 \subset [K_B] \tag{112}$$

$$\overset{(105)}{\leq} I\left(B_{[K_B]}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_{\mathcal{I}_1 \cap \mathcal{I}_2}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + \cdots$$
$$\text{else if } [K_B] \subset \mathcal{I}_1 \cup \mathcal{I}_2 \tag{113}$$

$$\overset{(105)}{\leq} \cdots \tag{114}$$

$$\overset{(105)}{\leq} (2K_B - N_B) I\left(B_{[K_B]}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right). \tag{115}$$

In the above proof, as adding conditioning preserves the direction of inequality (proved in (105)), we keep taking union of the $\mathcal{I}_1, \mathcal{I}_2, \ldots$ sets and split out a copy of $I\left(B_{[K_B]}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$ when the union covers $[K_B]$; and keep going until we have collected $2K_B - N_B$ copies. This process is easily explained by an example. Consider the sets in (104).

$$I\left(B_1, B_2, B_3; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_4, B_5, B_1; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$$
$$+ I\left(B_2, B_3, B_4; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_5, B_1, B_2; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$$
$$+ I\left(B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{116}$$

$$\leq I\left(B_1, B_2, B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_1; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$$
$$+ I\left(B_2, B_3, B_4; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_5, B_1, B_2; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$$
$$+ I\left(B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{117}$$

$$\leq I\left(B_1, B_2, B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_1, B_2, B_3, B_4; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$$
$$+ I\left(B_5, B_1, B_2; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{118}$$

$$\leq 2I\left(B_1, B_2, B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right)$$
$$+ I\left(B_1, B_2; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) + I\left(B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{119}$$

$$\leq 3I\left(B_1, B_2, B_3, B_4, B_5; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right). \tag{120}$$

$$\square$$

To complete the overall proof, we add (102) for all $\mathcal{I} = \mathcal{I}_j, j \in [K_B]$.

$$(\kappa\lambda_0 - \kappa(2K - N)) K_B \quad \leq \quad \sum_{j \in [K_B]} I\left(B_{\mathcal{I}_j}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{121}$$

$$\overset{(106)}{\leq} \quad (2K_B - N_B)\, I\left(B_{[K_B]}; Y_{[N-K]} \mid Y_0, B_{[K_B+1:N_B]}\right) \tag{122}$$

$$\leq \quad (2K_B - N_B)H(Y_{[N-K]}) \leq \kappa(N-K)(2K_B - N_B) \tag{123}$$

$$\implies \lambda_0 \quad \leq \quad \frac{(2K-N)K_B + (N-K)(2K_B - N_B)}{K_B} \tag{124}$$

$$= \quad N - (N-K)\frac{N_B}{K_B}. \tag{125}$$

B. Achievability Proof of $\mathcal{C}$: Classical Storage

Recall that the achievable rate region is convex (i.e., any convex combination of rate tuples can be achieved through space sharing, refer to Appendix A). Also recall the fact that if a rate tuple (λ_0, λ_B) is achievable, then $(\lambda_0 - \alpha, \lambda_B + \beta)$ is achievable for any $\lambda_0 \geq \alpha \geq 0$, $\beta \geq 0$. Thus, it suffices to consider only the extreme points.

First consider the extreme point $(\lambda_0, \lambda_B) = (\max(2K-N, 0), 0)$ that appears in all three regimes. To see that $\lambda_0 = \max(2K-N, 0)$ is achievable when $\lambda_B = 0$, i.e., SR-systems are empty and will not be used, we note that the problem is reduced to the uniform capacity of MDS storage graphs [4]; according to Theorem 3 of [4], $\lambda_0 = \max(2K-N, 0)$ is *linearly* achievable.

Next consider the remaining extreme points that are unique to the considered regime.

1) $K/N \geq 1/2, K_B/N_B > 1/2$: Achievability of $(\lambda_0, \lambda_B) = \left(N - \frac{(N-K)N_B}{K_B}, \frac{N-K}{K_B}\right)$: This proof is a straightforward generalization of the example in Section IV-A. We give a linear scheme that achieves the desired rate tuple. The parameters of the linear scheme are given as follows.

1) Field size q is any prime power such that $q \geq 2NK_B$.
2) Scaling factor $\kappa = K_B$.
3) Precoding matrices are chosen such that

$$\left(\mathbf{A}_1^{K_B\lambda_0 \times K_B}, \ldots, \mathbf{A}_N^{K_B\lambda_0 \times K_B}; \mathbf{B}_1^{N_B K_B \lambda_B \times K_B}, \ldots, \mathbf{B}_N^{N_B K_B \lambda_B \times K_B}\right) = \mathbf{H}_{NK_B \times NK_B}, \tag{126}$$

where $K_B\lambda_0 + N_B K_B \lambda_B = NK_B$, and $\mathbf{H}$ is a Cauchy matrix with $\frac{1}{\alpha_i - \beta_j}$ being the element in the ith row and j^{th} column; $\alpha_i, \beta_j, i, j \in [NK_B]$ are distinct elements in $\mathbb{F}_q$ (note that the field size q is large enough for such distinct elements to exist).

Local noise Z is not used. The storage systems are set as

$$(Y_1, \ldots, Y_N)_{1 \times NK_B} = (Y_0, B_1, \ldots, B_{N_B})_{1 \times NK_B} \times \mathbf{H}, \tag{127}$$

where Y_0 contains $\kappa\lambda_0 = NK_B - (N-K)N_B$ elements in $\mathbb{F}_q$. The SR-system $B_i, i \in [N_B]$ contains $\kappa\lambda_B = (N-K)$ elements in $\mathbb{F}_q$, and $Y_n, n \in [N]$ contains $\kappa = K_B$ elements in $\mathbb{F}_q$.

We show that the above linear scheme works by verifying the constraints (17), (18), (19) sequentially. Consider any $\mathcal{K} \in \binom{[N]}{K}$ and any $\mathcal{K}_B \in \binom{[N_B]}{K_B}$.

1) (17): We need to show that Y_0 is determined by $Y_{\mathcal{K}}, B_{\mathcal{K}_B}$. To see this, subtracting the contribution of $B_{\mathcal{K}_B}$ from $Y_{\mathcal{K}}$ gives us $(Y_0, B_{\mathcal{K}_B^c}) \times \mathbf{H}_{sub}^{KK_B \times KK_B}$ where $\mathbf{H}_{sub}$ is square because

$$K_B\lambda_0 + (N_B - K_B)K_B\lambda_B = KK_B.$$

As $\mathbf{H}$ is Cauchy, Y_0 is obtained.

2) (18): We need to show that Y_0 is independent of $Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}$. Proceed as follows.

$$I\left(Y_0; Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}\right) \overset{(13)}{=} I\left(Y_0; Y_{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c}\right) \tag{128}$$

$$= H\left(Y_{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c}\right) - H\left(Y_{\mathcal{K}^c} \mid Y_0, B_{\mathcal{K}_B^c}\right) \tag{129}$$

$$\leq (N-K)K_B - H\left(B_{\mathcal{K}_B}\mathbf{H}_{sub}^{K_B^2\lambda_B \times (N-K)K_B}\right) \tag{130}$$

$$= 0, \tag{131}$$

where the last step follows from the fact that

$$K_B^2\lambda_B = (N-K)K_B.$$

3) (19): $\mathbf{H}$ has full rank, so B is determined by $Y_1, \ldots, Y_N$ (see (127)).

2) $K/N < 1/2, K_B/N_B > 1/2$: *Achievability of* $(\lambda_0, \lambda_B) = \left(\frac{K(2K_B - N_B)}{2K_B}, \frac{K}{2K_B} \right)$: The linear scheme of this section generalizes that of the example in Section IV-B. Specifically, the repetition code (f_1, f_2 is repeated in Y_1, Y_2, Y_3) in the example is generalized to an (N, K) MDS code which reduces to the $(N, 1)$ repetition code when $K = 1$. The parameters of the linear scheme that achieves the desired rate tuple are given as follows.

1) Field size q is any prime power such that $q \geq 2NK_B > 2KK_B + KN_B$.
2) Scaling factor $\kappa = 2K_B$.
3) Uniform local randomness $Z = (Z_1, \ldots, Z_{(N-K)K_B}) \in \mathbb{F}_q^{1 \times (N-K)K_B}$.
4) Precoding matrices are specified through the following steps. Note that Y_0 contains $\kappa \lambda_0 = K(2K_B - N_B)$ elements in $\mathbb{F}_q$ and $B_i, i \in [N_B]$ contains $\kappa \lambda_B = K$ elements in $\mathbb{F}_q$. First, choose a $2KK_B \times KN_B$ Cauchy matrix $\mathbf{F} = \left[\frac{1}{\alpha_i - \beta_j} \right]_{ij}$ where the element in the ith row and j^{th} column is $\frac{1}{\alpha_i - \beta_j}$ and $\alpha_i, \beta_j, i \in [2KK_B], j \in [KN_B]$ are distinct elements in $\mathbb{F}_q$. Then define

$$\left(\underbrace{\boldsymbol{f}_0}_{1 \times K(N_B - K_B)}, \underbrace{\boldsymbol{f}_1}_{1 \times K_B}, \ldots, \underbrace{\boldsymbol{f}_K}_{1 \times K_B} \right)_{1 \times KN_B} \triangleq (Y_0, B_1, \ldots, B_{N_B})_{1 \times 2KK_B} \times \mathbf{F}_{2KK_B \times KN_B}. \tag{132}$$

Second, pass $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_K$ through an (N, K) MDS code to generate $\overline{\boldsymbol{f}}_1, \ldots, \overline{\boldsymbol{f}}_N$ such that any K distinct $\overline{\boldsymbol{f}}_i$ may recover $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_K$. To this end, choose a $K \times N$ Vandermonde matrix $\mathbf{V} = [\zeta_j^{i-1}]_{ij}$ where the element in the ith row and j^{th} column is $\zeta_j^{i-1}, \forall i \in [K], j \in [N]$ and ζ_j are distinct elements in $\mathbb{F}_q$. Then define

$$\left(\underbrace{\overline{\boldsymbol{f}}_1^T}_{K_B \times 1}, \ldots, \underbrace{\overline{\boldsymbol{f}}_N^T}_{K_B \times 1} \right)_{K_B \times N} \triangleq \left(\boldsymbol{f}_1^T, \ldots, \boldsymbol{f}_K^T \right)_{K_B \times K} \times \mathbf{V}_{K \times N}. \tag{133}$$

Third, choose an $NK_B \times NK_B$ Cauchy matrix $\mathbf{H} = \left[\frac{1}{\gamma_i - \delta_j} \right]_{ij}$ where the element in the ith row and j^{th} column is $\frac{1}{\gamma_i - \delta_j}$ and $\gamma_i, \delta_j, i, j \in [NK_B]$ are distinct elements in $\mathbb{F}_q$. Then define

$$\left(\underbrace{\boldsymbol{h}_1}_{1 \times K_B}, \ldots, \underbrace{\boldsymbol{h}_N}_{1 \times K_B} \right)_{1 \times NK_B} \triangleq \left(\underbrace{\boldsymbol{f}_0}_{1 \times K(N_B - K_B)}, \underbrace{Y_0}_{1 \times K(2K_B - N_B)}, \underbrace{Z}_{1 \times (N-K)K_B} \right)_{1 \times NK_B} \times \mathbf{H}_{NK_B \times NK_B}. \tag{134}$$

We are now ready to specify the storage systems. Note that $Y_n, n \in [N]$ contains $\kappa = 2K_B$ elements in $\mathbb{F}_q$.

$$Y_n = \left(\underbrace{\overline{\boldsymbol{f}}_n}_{1 \times K_B}, \underbrace{\boldsymbol{h}_n}_{1 \times K_B} \right)_{1 \times 2K_B}, \forall n \in [N]. \tag{135}$$

The above encoding procedure is linear, thus the existence of precoding matrices $\mathbf{A}_n, \mathbf{B}_n, \mathbf{Z}_n$ is implied.

We show that the above linear scheme works by verifying the constraints (17), (18), (19) sequentially. Consider any $\mathcal{K} = \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}$.

1) (17): We need to show that Y_0 is determined by $Y_\mathcal{K}, B_{\mathcal{K}_B}$. Proceed as follows. First, $Y_\mathcal{K}$ contains $\overline{\boldsymbol{f}}_\mathcal{K}$, which is invertible to $\boldsymbol{f}_{[K]}$ as $\mathbf{V}$ is a Vandermonde matrix. Second, we may subtract the contribution of $B_{\mathcal{K}_B}$ from $\boldsymbol{f}_{[K]}$ and obtain

$$\left(\underbrace{Y_0}_{1 \times K(2K_B - N_B)}, \underbrace{B_{\mathcal{K}_B^c}}_{1 \times K(N_B - K_B)} \right)_{1 \times KK_B} \times \mathbf{F}_{sub}^{KK_B \times KK_B}. \tag{136}$$

$\mathbf{F}_{sub}$ has full rank as it is a sub-matrix of the Cauchy matrix $\mathbf{F}$, then Y_0 is obtained with no error.

2) (18): We need to show that Y_0 is independent of $Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}$. To this end, we prove the following mutual information is zero.

$$I\left(Y_0; Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c} \right)$$

$$\overset{(13),(135)}{=} I\left(Y_0; \overline{\boldsymbol{f}}_{\mathcal{K}^c}, \boldsymbol{h}_{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c} \right) \tag{137}$$

$$\leq I\left(Y_0; \overline{\boldsymbol{f}}_{\mathcal{K}^c}, \boldsymbol{f}_{[K]}, \boldsymbol{h}_{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c} \right) \tag{138}$$

$$\overset{(133)}{\leq} I\left(Y_0; \boldsymbol{f}_{[K]}, \boldsymbol{h}_{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c} \right) \tag{139}$$

$$= \quad H\left(\boldsymbol{f}_{[K]}, \boldsymbol{h}_{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c}\right) - H\left(\boldsymbol{f}_{[K]}, \boldsymbol{h}_{\mathcal{K}^c} \mid Y_0, B_{\mathcal{K}_B^c}\right) \tag{140}$$

$$\leq \quad NK_B - H\left(\boldsymbol{f}_{[K]} \mid Y_0, B_{\mathcal{K}_B^c}\right) - H\left(\boldsymbol{h}_{\mathcal{K}^c} \mid \boldsymbol{f}_{[K]}, Y_0, B\right) \tag{141}$$

$$\overset{(132),(134)}{=} \quad NK_B - H\left(B_{\mathcal{K}} \times \mathbf{F}_{sub}^{KK_B \times KK_B} \mid Y_0, B_{\mathcal{K}_B^c}\right)$$

$$\qquad\qquad - H\left(Z \times \mathbf{H}_{sub}^{(N-K)K_B \times (N-K)K_B} \mid Y_0, B\right) \tag{142}$$

$$= \quad NK_B - KK_B - (N-K)K_B = 0. \tag{143}$$

(139) follows from the fact that $\overline{\boldsymbol{f}}_{\mathcal{K}^c}$ is a deterministic function of $\boldsymbol{f}_{[K]}$ (refer to (133)). To obtain the first term of (141), note that $\boldsymbol{f}_{[K]}, \boldsymbol{h}_{\mathcal{K}^c}$ contains $KK_B + (N-K)K_B = NK_B$ elements.

3) (19): We need to show that B is determined by $Y_{[N]}$. Proceed as follows. First, as Cauchy $\mathbf{H}_{NK_B \times NK_B}$ has full rank, we may from $\boldsymbol{h}_{[N]}$ (the last K_B elements of $Y_{[N]}$), recover $\boldsymbol{f}_0, Y_0, Z$ with no error. Second, $Y_{[N]}$ contains $\overline{\boldsymbol{f}}_{[N]}$, from which we may obtain $\boldsymbol{f}_{[K]}$ as $\mathbf{V}$ is Vandermonde. Third, we may eliminate the contribution of Y_0 from $\boldsymbol{f}_{[K]}$ and combine with $\boldsymbol{f}_0$ to obtain $(B_{[N_B]})_{1 \times KN_B} \times \mathbf{F}_{sub}^{KN_B \times KN_B}$, from which $B_{[N_B]}$ can be recovered with no error as $\mathbf{F}$ is Cauchy. Thus SR $B = B_{[N_B]}$ is obtained.

3) $K/N < 1/2, K_B/N_B > 1/2$: Achievability of $(\lambda_0, \lambda_B) = \left(2K\left(1 - \frac{N_B}{2K_B}\right), \frac{N-2K}{N_B} + \frac{K}{K_B}\right)$: The linear scheme of this section generalizes that of the example in Section IV-C. Specifically, the repetition code (of $\boldsymbol{h}$ in Y) and the $(3,2)$ MDS code (of $\boldsymbol{b}^x$ in Y) in the example are generalized to a tuple of (N, K) and $(N, N-K)$ MDS codes respectively that satisfy the property that the product of the parity check matrix of the (N, K) MDS code and the generator matrix of the $(N, N-K)$ MDS code has full rank (set as generalized Reed-Solomon codes, see Lemma 2). The parameters of the linear scheme that achieves the desired rate tuple are given as follows. Local randomness Z is not used.

1) Field size q is any prime power such that $q \geq \max(2KN_BK_B, N)$.
2) Scaling factor $\kappa = N_BK_B$.
3) Precoding matrices are specified through the following steps. Y_0 contains $\kappa\lambda_0 = KN_B(2K_B - N_B)$ elements in $\mathbb{F}_q$ and $B_t, t \in [N_B]$ contains $\kappa\lambda_B = (N-K)K_B + K(N_B - K_B)$ elements in $\mathbb{F}_q$. First, we divide B_t into 2 parts, labelled by the superscript x, y.

$$B_t = \left(\underbrace{\boldsymbol{b}_t^{1,x}}_{1 \times K_B}, \ldots, \underbrace{\boldsymbol{b}_t^{N-K,x}}_{1 \times K_B}, \underbrace{\boldsymbol{b}_t^{y}}_{1 \times K(N_B - K_B)}\right), t \in [N_B]. \tag{144}$$

Second, define $\boldsymbol{\alpha} \triangleq (\alpha_1, \ldots, \alpha_N) \in \mathbb{F}_q^{1 \times N}$, $\boldsymbol{v} \triangleq (v_1, \ldots, v_N) \in \mathbb{F}_q^{1 \times N}$ where $\forall n \in [N], \alpha_n$ are distinct elements in $\mathbb{F}_q$ and $v_n \neq 0$; choose an $N \times N$ matrix $\mathrm{GRS}_{N \times N}(\boldsymbol{v}, \boldsymbol{\alpha}) = \left[v_j \alpha_j^{i-1}\right]_{ij}$ where the element in the ith row and j^{th} column is $v_j \alpha_j^{i-1}, i, j \in [N]$. Note that GRS is the generator matrix of a generalized Reed-Solomon code. Define $\mathrm{GRS}_{N \times N}(\boldsymbol{v}, \boldsymbol{\alpha}) \triangleq \left(\mathbf{G}_{K \times N}; \mathbf{F}_{(N-K) \times N}\right)$, i.e., the first K rows are defined as $\mathbf{G}$ and the last $N-K$ rows are defined as $\mathbf{F}$ and note that both $\mathbf{G}, \mathbf{F}$ are MDS, i.e., any maximal square sub-matrix has full rank.

Third, pass $\boldsymbol{b}_t^{1,x}, \ldots, \boldsymbol{b}_t^{N-K,x}$ through an $(N, N-K)$ MDS code (with generator matrix $\mathbf{F}$) to generate $\overline{\boldsymbol{b}}_t^{1,x}, \ldots, \overline{\boldsymbol{b}}_t^{N,x}$ such that any $(N-K)$ distinct $\overline{\boldsymbol{b}}_t^x$ may recover $\boldsymbol{b}_t^{1,x}, \ldots, \boldsymbol{b}_t^{N-K,x}$, i.e., $\forall t \in [N_B]$,

$$\left(\underbrace{\left(\overline{\boldsymbol{b}}_t^{1,x}\right)^T}_{K_B \times 1}, \ldots, \underbrace{\left(\overline{\boldsymbol{b}}_t^{N,x}\right)^T}_{K_B \times 1}\right)_{K_B \times N} \triangleq \left(\left(\boldsymbol{b}_t^{1,x}\right)^T, \ldots, \left(\boldsymbol{b}_t^{N-K,x}\right)^T\right)_{K_B \times (N-K)} \times \mathbf{F}_{(N-K) \times N}. \tag{145}$$

Fourth, choose a $KN_BK_B \times KN_BK_B$ Cauchy matrix $\mathbf{H} = \left[\frac{1}{\beta_i - \gamma_j}\right]_{ij}$ where the element in the ith row and j^{th} column is $\frac{1}{\beta_i - \gamma_j}$ and $\beta_i, \gamma_j, i, j \in [KN_BK_B]$ are distinct elements in $\mathbb{F}_q$. Then define

$$\left(\underbrace{\boldsymbol{h}_1^1}_{1 \times K_B}, \ldots, \underbrace{\boldsymbol{h}_1^K}_{1 \times K_B}, \ldots, \underbrace{\boldsymbol{h}_{N_B}^1}_{1 \times K_B}, \ldots, \underbrace{\boldsymbol{h}_{N_B}^K}_{1 \times K_B}\right)_{1 \times KN_BK_B} \triangleq \left(Y_0, \boldsymbol{b}_1^y, \ldots, \boldsymbol{b}_{N_B}^y\right)_{1 \times KN_BK_B}$$

$$\times \mathbf{H}_{KN_BK_B \times KN_BK_B}. \tag{146}$$

Fifth, pass $h_t^1, \ldots, h_t^K, t \in [N_B]$ through an (N, K) MDS code (with generator matrix $\mathbf{G}$) to generate $\overline{h}_t^1, \ldots, \overline{h}_t^N$ such that any K distinct $\overline{h}_t$ may recover $h_t^1, \ldots, h_t^K$, i.e., $\forall t \in [N_B]$,

$$\left(\underbrace{\left(\overline{h}_t^1\right)^T}_{K_B \times 1}, \ldots, \underbrace{\left(\overline{h}_t^N\right)^T}_{K_B \times 1} \right)_{K_B \times N} \triangleq \left(\left(h_t^1\right)^T, \ldots, \left(h_t^K\right)^T \right)_{K_B \times K} \times \mathbf{G}_{K \times N}. \tag{147}$$

We are now ready to specify the storage systems. Note that $Y_n, n \in [N]$ contains $\kappa = N_B K_B$ elements in $\mathbb{F}_q$.

$$Y_n = \left(\overline{h}_1^n + \overline{b}_1^{n,x}, \ldots, \overline{h}_{N_B}^n + \overline{b}_{N_B}^{n,x} \right)_{1 \times N_B K_B}, \forall n \in [N]. \tag{148}$$

We show that the above linear scheme works by verifying the constraints (17), (18), (19) sequentially. Consider any $\mathcal{K} \in \binom{[N]}{K}, \mathcal{K}_B \in \binom{[N_B]}{K_B}$.

1) (17): We need to show that Y_0 is determined by $Y_{\mathcal{K}}, B_{\mathcal{K}_B}$. Proceed as follows.
   $b_{\mathcal{K}_B}^{1,x}, \ldots, b_{\mathcal{K}_B}^{N-K,x}$ are known from $B_{\mathcal{K}_B}$ and thus $\overline{b}_{\mathcal{K}_B}^{1,x}, \ldots, \overline{b}_{\mathcal{K}_B}^{N,x}$ are known from $B_{\mathcal{K}_B}$ due to the $(N, N-K)$ MDS precoding in (145). Then subtract the contribution of $\overline{b}_{\mathcal{K}_B}^{\mathcal{K},x}$ from $Y_{\mathcal{K}}$ and obtain $\overline{h}_{\mathcal{K}_B}^{\mathcal{K}}$, from which we can then obtain $h_{\mathcal{K}_B}^1, \ldots, h_{\mathcal{K}_B}^K$ due to the (N, K) MDS precoding in (147). Note that

$$\left(h_{\mathcal{K}_B}^1, \ldots, h_{\mathcal{K}_B}^K \right)_{1 \times KK_B^2} = \left(Y_0, b_1^y, \ldots, b_{N_B}^y \right)_{1 \times KN_B K_B} \times \mathbf{H}_{sub}^{KN_B K_B \times KK_B^2}. \tag{149}$$

$\mathbf{H}_{sub}$ denotes a sub-matrix of $\mathbf{H}$ where the superscript shows the dimension. Note that $b_{\mathcal{K}_B}^y$ are known from $B_{\mathcal{K}_B}$ and we may further subtract their contribution from $h_{\mathcal{K}_B}^1, \ldots, h_{\mathcal{K}_B}^K$ and obtain

$$\left(Y_0, b_{\mathcal{K}_B^c}^y \right)_{1 \times KK_B^2} \times \mathbf{H}_{sub}^{KK_B^2 \times KK_B^2}. \tag{150}$$

$\mathbf{H}_{sub}$ has full rank as it is a sub-matrix of the Cauchy matrix $\mathbf{H}$. Thus Y_0 is perfectly recovered.

2) (18): We need to show that Y_0 is independent of $Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}$. Proceed as follows.

$$I\left(Y_0; Y_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}\right)$$

$$\overset{(13),(148)}{=} I\left(Y_0; \overline{h}_{\mathcal{K}_B}^{\mathcal{K}^c} + \overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x}, \overline{h}_{\mathcal{K}_B}^{\mathcal{K}^c} \mid B_{\mathcal{K}_B^c}\right) \tag{151}$$

$$\leq I\left(Y_0; \overline{h}_{\mathcal{K}_B}^{\mathcal{K}^c} + \overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x}, h_{\mathcal{K}_B^c}^{[K]} \mid B_{\mathcal{K}_B^c}\right) \tag{152}$$

$$= H\left(\underbrace{\overline{h}_{\mathcal{K}_B}^{\mathcal{K}^c} + \overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x}, h_{\mathcal{K}_B^c}^{[K]}}_{1 \times \Delta} \middle| B_{\mathcal{K}_B^c} \right) - H\left(\overline{h}_{\mathcal{K}_B}^{\mathcal{K}^c} + \overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x}, h_{\mathcal{K}_B^c}^{[K]} \mid Y_0, B_{\mathcal{K}_B^c} \right) \tag{153}$$

$$\leq \Delta - H\left(h_{\mathcal{K}_B^c}^{[K]} \mid Y_0, B_{\mathcal{K}_B^c} \right) - H\left(\overline{h}_{\mathcal{K}_B}^{\mathcal{K}^c} + \overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x} \mid h_{\mathcal{K}_B^c}^{[K]}, Y_0, B_{\mathcal{K}_B^c}, b_{[N_B]}^y \right) \tag{154}$$

$$\leq \Delta - H\left(b_{\mathcal{K}_B}^y \times \mathbf{H}_{sub}^{K(N_B-K_B)K_B \times K(N_B-K_B)K_B} \mid Y_0, B_{\mathcal{K}_B^c} \right)$$
$$- H\left(\overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x} \mid Y_0, B_{\mathcal{K}_B^c}, b_{[N_B]}^y \right) \tag{155}$$

$$= \Delta - K(N_B - K_B)K_B - H\left(b_{\mathcal{K}_B}^{[N-K],x} \mid Y_0, B_{\mathcal{K}_B^c}, b_{[N_B]}^y \right) \tag{156}$$

$$= \Delta - K(N_B - K_B)K_B - (N - K)K_B^2 \tag{157}$$

$$= 0. \tag{158}$$

Note that the notation $h_{\mathcal{X}}^{\mathcal{Y}} = \left\{ h_i^j, i \in \mathcal{X}, j \in \mathcal{Y} \right\}$ and $\Delta = (N - K)K_B^2 + K(N_B - K_B)K_B$. (152) follows from the MDS encoding (147) so that $\overline{h}_{\mathcal{K}_B^c}^{\mathcal{K}^c}$ is a function of $h_{\mathcal{K}_B^c}^{[K]}$ and $N - K > K$. In (156), the third term follows from the MDS encoding (145) so that $\overline{b}_{\mathcal{K}_B}^{\mathcal{K}^c,x}$ is invertible to $b_{\mathcal{K}_B}^{[N-K],x}$.

3) (19): We need to show that B is determined by $Y_{[N]}$.
   First, it is well known that the dual of a generalized Reed-Solomon code is another generalized Reed-Solomon code [26]. Then the null space of the row space of $\mathbf{G}_{K \times N}$ is the row space of an $(N - K) \times N$ matrix $\mathbf{G}_{(N-K) \times N}^{\perp}$ where

$$\mathbf{G}^{\perp} = \mathrm{GRS}_{(N-K) \times N}(\boldsymbol{u}, \boldsymbol{\alpha}), \ \boldsymbol{u} = (u_1, \ldots, u_N), \text{ and } u_n = \left(v_n \prod_{i \neq n} (\alpha_n - \alpha_i) \right)^{-1}, n \in [N], \text{ i.e.,}$$

$$\mathbf{G}_{(N-K) \times N}^{\perp} \times \mathbf{G}_{N \times K}^T = \mathbf{0}_{(N-K) \times K}. \tag{159}$$

Then we use $\mathbf{G}^{\perp}_{(N-K)\times N}$ to zero-force the $\boldsymbol{h}_t, t \in [N_B]$ terms in Y_n.

$$\mathbf{G}^{\perp}_{(N-K)\times N} \underbrace{\begin{bmatrix} Y_1 \\ \vdots \\ Y_N \end{bmatrix}}_{N \times N_B K_B} = \mathbf{G}^{\perp}_{(N-K)\times N} \mathbf{F}^{T}_{N\times(N-K)} \underbrace{\begin{bmatrix} \boldsymbol{b}_1^{1,x} & \cdots & \boldsymbol{b}_{N_B}^{1,x} \\ \vdots & \ddots & \vdots \\ \boldsymbol{b}_1^{N-K,x} & \cdots & \boldsymbol{b}_{N_B}^{N-K,x} \end{bmatrix}}_{(N-K)\times N_B K_B}, \tag{160}$$

which from Lemma 2 (i.e., $\mathbf{G}^{\perp}\mathbf{F}^T$ has full rank), is invertible to $\boldsymbol{b}_{[N_B]}^{[N-K],x}$, i.e., we recover all $\boldsymbol{b}^x$.

Second, given all $\boldsymbol{b}^x$, we subtract their contribution from $Y_n, n \in [N]$ and obtain $\overline{\boldsymbol{h}}_{[N_B]}^{[N]}$, from which we further obtain $\boldsymbol{h}_{[N_B]}^{[K]}$.

Finally, from $\boldsymbol{h}_{[N_B]}^{[K]}$, we obtain B (i.e., all $\boldsymbol{b}^x, \boldsymbol{b}^y$).

Lemma 2.

$$rank\left(\mathbf{G}^{\perp}_{(N-K)\times N}\mathbf{F}^{T}_{N\times(N-K)}\right) = N - K. \tag{161}$$

Proof: To set up the proof by contradiction, let us assume $\left(\mathbf{G}^{\perp}\mathbf{F}^{T}\right)_{(N-K)\times(N-K)}$ does not have full rank, i.e., there exists a vector $\boldsymbol{\gamma} \in \mathbb{F}_q^{(N-K)\times 1}$ such that $\mathbf{G}^{\perp}\mathbf{F}^T\boldsymbol{\gamma} = \mathbf{0}_{(N-K)\times 1}$. Then defining $\boldsymbol{\delta} \triangleq \mathbf{F}^T\boldsymbol{\gamma}$, we have $\mathbf{G}^{\perp}\boldsymbol{\delta} = \mathbf{0}$, i.e., $\boldsymbol{\delta}$ lies in the null space of the row space of $\mathbf{G}^{\perp}$, which is the row space of $\mathbf{G}$ as $\mathbf{G}^{\perp}\mathbf{G}^T = \mathbf{0}$. Now we arrive at the property that $\boldsymbol{\delta}$ lies in the row space of $\mathbf{G}$. However, $\boldsymbol{\delta} = \mathbf{F}^T\boldsymbol{\gamma}$ also lies in the row space of $\mathbf{F}$, i.e., $\boldsymbol{\delta}$ lies in the row space of both $\mathbf{F}$ and $\mathbf{G}$, which leads to the conclusion that $\boldsymbol{\delta} = \mathbf{0}$ because the row spaces of $\mathbf{F}$ and $\mathbf{G}$ intersect only at the trivial zero vector as matrix $(\mathbf{G};\mathbf{F}) = \mathrm{GRS}_{N\times N}(\boldsymbol{v},\boldsymbol{\alpha})$ has full rank. Finally, $\boldsymbol{\delta}$ being the zero vector indicates that $\boldsymbol{\gamma}$ must also be the zero vector as $\mathbf{F}^T$ has independent columns and $\boldsymbol{\delta} = \mathbf{F}^T\boldsymbol{\gamma}$. Finally, $\boldsymbol{\gamma}$ being the zero vector shows that $\mathbf{G}^{\perp}\mathbf{F}^T$ has full rank. $\square$

C. $\mathcal{C}_Q$: Capacity region for $\widetilde{QSEA}$

Based on Theorem 2 and the convexity of $\mathcal{C}_Q$ proved in Appendix A, the inner bound (achievable rate region) for $\mathcal{C}_Q$ is implied by the inner bound for the capacity region $\mathcal{C}$ of $\widetilde{CSSRA}$, which is presented in Section VI-B. Thus, here it suffices to prove only the outer bound (converse) for $\mathcal{C}_Q$.

We have two bounds to prove, i.e., $\mathcal{R}_{cut}$ and $\mathcal{R}_{\infty}$. In the following, unless explicitly stated otherwise, the quantum information measure terms are with respect to the state $\rho_{RQ_1...Q_NB_1...B_{N_B}}$. Recall from (8) that our problem formulation requires perfect recovery for *every* pure state RQ_0, so in particular perfect recovery is required for a maximally entangled state RQ_0 where Q_0 is maximally mixed, i.e., $H(R,Q_0)_{|\varphi\rangle_{RQ_0}} = 0$ and $H(R) = H(Q_0)_{|\varphi\rangle_{RQ_0}} = \log_q |Q_0|$. In the converse proof, we assume throughout that RQ_0 is maximally entangled.

1) Proof of $\mathcal{R}_{cut}$ Bound: We need to prove that every achievable tuple (λ_0, λ_B) must satisfy the bound $\lambda_0 \leq \max(2K - N, 0) + \lambda_B \cdot \max(2K_B - N_B, 0)$. Let us proceed as follows. Consider any achievable tuple (λ_0, λ_B). Since this tuple is achievable, there must exist a feasible coding scheme $\mathfrak{S}$ such that

$$\lambda_0(\mathfrak{S}) \geq \lambda_0, \tag{162}$$

$$\lambda_B(\mathfrak{S}) \leq \lambda_B. \tag{163}$$

Consider this coding scheme $\mathfrak{S}$. Besides $\lambda_0(\mathfrak{S}), \lambda_B(\mathfrak{S})$, since there is no potential for ambiguity for the remaining parameters of the coding scheme, we will suppress the label $\mathfrak{S}$ and write, e.g., κ, q instead of $\kappa(\mathfrak{S}), q(\mathfrak{S})$ to simplify the notation.

The perfect recovery of RQ_0 implies the entropic condition [27], [4],

$$\forall \mathcal{K} \in \binom{[N]}{K}, \forall \mathcal{K}_B \in \binom{[N_B]}{K_B}, \quad I(R; Q_{\mathcal{K}}, B_{\mathcal{K}_B}) = 2H(R) = 2\kappa\lambda_0(\mathfrak{S}). \tag{164}$$

Then from weak monotonicity, we have

$$I(R; Q_{\mathcal{K}}, B_{\mathcal{K}_B}) + I(R; Q_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}) \leq 2H(R) = 2\kappa\lambda_0(\mathfrak{S}) \tag{165}$$

$$\overset{(164)}{\Longrightarrow} \quad I(R; Q_{\mathcal{K}^c}, B_{\mathcal{K}_B^c}) = 0, \quad \forall \mathcal{K}, \forall \mathcal{K}_B. \tag{166}$$

From (166), setting $\mathcal{K} = [N - K + 1 : N]$ and $\mathcal{K}_B = [N_B - K_B + 1 : N_B]$, we have

$$I(R; Q_{[N-K]}, B_{[N_B-K_B]}) = 0. \tag{167}$$

Then from (164), setting $\mathcal{K} = [K], \mathcal{K}_B = [K_B]$, we have

$$2\kappa\lambda_0(\mathfrak{S})$$

$$= I\left(R; Q_{[K]}, B_{[K_B]}\right) \tag{168}$$

$$\leq I\left(R; Q_{[N-K]}, Q_{[N-K+1:K]}, B_{[N_B-K_B]}, B_{[N_B-K_B+1:K_B]}\right) \tag{169}$$

$$\stackrel{(167)}{=} I\left(R; Q_{[N-K+1:K]}, B_{[N_B-K_B+1:K_B]} \mid Q_{[N-K]}, B_{[N_B-K_B]}\right) \tag{170}$$

$$\leq 2H\left(Q_{[N-K+1:K]}\right) + 2H\left(B_{[N_B-K_B+1:K_B]}\right) \tag{171}$$

$$\leq 2\log_q \prod_{n\in[N-K+1:K]} |Q_n| + 2\log_q \prod_{i\in[N_B-K_B+1:K_B]} |B_i| \tag{172}$$

$$\leq 2\kappa \cdot \max\left(2K-N, 0\right) + 2\kappa\lambda_B(\mathfrak{S}) \cdot \max\left(2K_B-N_B, 0\right) \tag{173}$$

$$\implies \lambda_0(\mathfrak{S}) \leq \max\left(2K-N, 0\right) + \lambda_B(\mathfrak{S}) \cdot \max\left(2K_B-N_B, 0\right) \tag{174}$$

$$\stackrel{(162)(163)}{\implies} \lambda_0 \leq \max\left(2K-N, 0\right) + \lambda_B \cdot \max\left(2K_B-N_B, 0\right). \tag{175}$$

(169) follows from the fact that quantum conditional mutual information is non-negative.

2) Proof of $\mathcal{R}_\infty$ Bound: Second, consider $\mathcal{R}_\infty$. Interestingly, the proof of the quantum setting parallels that of the classical setting in Section VI-A2. The differences are highlighted here while similarities are briefly described. Following exactly the same reasoning as that of the classical setting, the $K/N < 1/2$ case follows from the $K/N \geq 1/2$ case and it suffices to prove

$$\lambda_0 \leq N - (N-K)\frac{N_B}{K_B} \text{ when } K/N \geq 1/2. \tag{176}$$

Consider $\mathcal{K} = [K] = [N-K] \cup [N-K+1:K], \mathcal{K}_B = \mathcal{I} \cup [K_B+1:N_B]$ where $\mathcal{I} \subset [K_B], |\mathcal{I}| = 2K_B - N_B$. Note that $2K_B - N_B \leq K_B$ and $K/N \geq 1/2$. Consider any feasible scheme $\mathfrak{S}$. From the quantum entropic decodability constraint (164), we have

$$2\kappa\lambda_0 \leq 2\kappa\lambda_0(\mathfrak{S}) \stackrel{(164)}{=} I\left(R; Q_{[N-K]}, Q_{[N-K+1:K]}, B_{\mathcal{K}_B}\right) \tag{177}$$

$$\leq I\left(R; Q_{[N-K]}, B_{\mathcal{K}_B}\right) + 2H\left(Q_{[N-K+1:K]}\right) \tag{178}$$

$$\stackrel{(3)}{\leq} I\left(R, B_{\mathcal{I}}; Q_{[N-K]} \mid B_{[K_B+1:N_B]}\right) + 2\kappa(2K-N) \tag{179}$$

$$= \underbrace{I\left(R; Q_{[N-K]} \mid B_{[K_B+1:N_B]}\right)}_{\stackrel{(166)}{\leq} 0} + I\left(B_{\mathcal{I}}; Q_{[N-K]} \mid R, B_{[K_B+1:N_B]}\right)$$

$$+ 2\kappa(2K-N) \tag{180}$$

$$\implies 2\left(\kappa\lambda_0 - \kappa(2K-N)\right) \leq I\left(B_{\mathcal{I}}; Q_{[N-K]} \mid R, B_{[K_B+1:N_B]}\right). \tag{181}$$

(178) follows from the following quantum mutual information bound

$$I\left(R; Q_{[N-K+1:K]} \mid Q_{[N-K]}, B_{\mathcal{K}_B}\right) \leq 2H\left(Q_{[N-K+1:K]}\right),$$

where we have a factor of 2 before the entropy term $H\left(Q_{[N-K+1:K]}\right)$ because of the weak monotonicity of quantum entropy (in contrast to the strong monotonicity of classical entropy). The first term of (180) is zero because of the implicit quantum security constraint, proved in (166), which says that due to weak monotonicity (monogamy of entanglement), a decoding set preserves all entanglement with the reference system, leaving its complement in a product state with the reference system.

Next we add (181) for all $\mathcal{I} = \mathcal{I}_j, j \in [K_B]$ where $\mathcal{I}_j$ is defined in (103).

$$2\left(\kappa\lambda_0 - \kappa(2K-N)\right)K_B \leq \sum_{j\in[K_B]} I\left(B_{\mathcal{I}_j}; Q_{[N-K]} \mid R, B_{[K_B+1:N_B]}\right) \tag{182}$$

$$\stackrel{(106)}{\leq} (2K_B-N_B) I\left(B_{[K_B]}; Q_{[N-K]} \mid R, B_{[K_B+1:N_B]}\right) \tag{183}$$

$$\leq 2\kappa(N-K)(2K_B-N_B) \tag{184}$$

$$\implies \lambda_0 \leq N - (N-K)\frac{N_B}{K_B}. \tag{185}$$

In (183), we apply (106) in Lemma 1, proved in the classical setting because the proof of (106) only uses following two properties that hold in both classical and quantum settings.

1) $I(Y_0; B) = 0$ and $H(B_1, \ldots, B_{N_B}) = H(B_1) + \cdots + H(B_{N_B})$, while the corresponding quantum version also holds, i.e., $I(R; B) = 0$ as R and B are in a product state (see (3)) and the $B_i, i \in [N_B]$ entanglement is in a product state, i.e., $H(B_1, \ldots, B_{N_B}) = H(B_1) + \cdots + H(B_{N_B})$ (see (2)).
2) Strong sub-additivity of entropy, which holds for both quantum and classical entropy [28].

We may verify each step of the proof of (106) and will find that replacing Y_0 by R and replacing Y_n by Q_n, all the steps remain valid. Similar to above, the only difference lies in how to bound the mutual information term in (183), where for the quantum setting, we have a factor of 2. The proof of the quantum converse is thus complete.

VII. Conclusion

The problem of erasure-prone quantum storage with erasure-prone entanglement assistance, $\widetilde{\text{QSEA}}$, is explored by connecting it to an analogous problem of erasure-prone classical storage with erasure-prone shared-randomness assistance, $\widetilde{\text{CSSRA}}$. The capacity regions for both $\widetilde{\text{QSEA}}$ and $\widetilde{\text{CSSRA}}$ are characterized and shown to be identical in all parameter regimes, with the exception of one regime where the capacity remains open. It is conjectured that the capacity regions, $\mathcal{C}_Q$ and $\mathcal{C}$, respectively, are identical even in this regime, and that they match an inner bound (a feasible coding scheme) that is presented in Theorem 1. Let us conclude by listing some promising directions for future work.

1) The validity of the aforementioned conjecture is an important open question. Resolving this question may require a deeper understanding of the various converse arguments in order to find the right combination of bounds to cover the regime that remains open.
2) The connection between $\widetilde{\text{QSEA}}$ and $\widetilde{\text{CSSRA}}$, while clearly established in Theorem 2 from an achievability perspective, remains intriguing in terms of converse bounds. Since the capacity regions for the two settings seem to match, it is natural to ask if there is also a mechanism to translate an information theoretic converse bound from one setting to the other.
3) Figure 3 shows that there is much room to reduce the size requirements for our coding schemes. Observe that the field $\mathbb{F}_q$ in the specialized coding scheme of Figure 3 can be any field (even $\mathbb{F}_2$) but our generalizable construction for the same setting in Section IV-C assumes $q \geq 13$. The maximum storage possible under strict constraints on the sizes of storage and EA systems remains an important open question for future work.
4) Our formulation of $\widetilde{\text{QSEA}}$ does not allow any *precoding* (i.e., before the message appears at the encoder) across EA systems to counter the EA erasures. However precoding across EA systems may be possible in some settings, e.g., if the EA systems are co-located. The capacity for similar alternative formulations is also of interest.
5) Besides what is shown in Figure 2, the $\widetilde{\text{QSEA}}$ formulation does not allow any additional classical communication. On the other hand, it does allow joint processing of all unerased storage and EA systems at the decoder. Other formulations of interest may restrict access to a subset of unerased systems at the decoder while allowing additional classical communication among surviving systems [29].

Indeed, unreliable entanglement assistance is an important and underexplored topic with broad applicability across a wide variety of settings.

Appendix

We prove that $\mathcal{C}_Q$, the capacity region for $\widetilde{\text{QSEA}}$ is convex and note that the convexity of $\mathcal{C}$ for $\widetilde{\text{CSSRA}}$ follows from similar reasoning.

We show that $\mathcal{C}_Q$ is convex, i.e., if $(\lambda_0(1), \lambda_B(1)) \in \mathcal{C}_Q$ and $(\lambda_0(2), \lambda_B(2)) \in \mathcal{C}_Q$, then $(\mu\lambda_0(1) + (1-\mu)\lambda_0(2), \mu\lambda_B(1) + (1-\mu)\lambda_B(2)) \in \mathcal{C}_Q$ for $0 \leq \mu \leq 1$. The proof is based on a *space-sharing* argument, essentially a direct construction of a coding scheme as a convex combination of other coding schemes, analogous to the time-sharing argument that is quite common in information theory.

As $(\lambda_0(1), \lambda_B(1)) \in \mathcal{C}_Q$, there exists a feasible coding scheme $\mathfrak{S}_1$ with parameters

$$\left(\lambda_0(\mathfrak{S}_1), \lambda_B(\mathfrak{S}_1), \kappa(\mathfrak{S}_1), q(\mathfrak{S}_1), \text{ENC}(\mathfrak{S}_1), \text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S}_1) \right),$$

where $\lambda_0(\mathfrak{S}_1) \geq \lambda_0(1), \lambda_B(\mathfrak{S}_1) \leq \lambda_B(1)$. Similarly, $(\lambda_0(2), \lambda_B(2)) \in \mathcal{C}_Q$ indicates that there is a feasible coding scheme $\mathfrak{S}_2$ with parameters

$$\left(\lambda_0(\mathfrak{S}_2), \lambda_B(\mathfrak{S}_2), \kappa(\mathfrak{S}_2), q(\mathfrak{S}_2), \text{ENC}(\mathfrak{S}_2), \text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S}_2) \right),$$

where $\lambda_0(\mathfrak{S}_2) \geq \lambda_0(2), \lambda_B(\mathfrak{S}_2) \leq \lambda_B(2)$. Next, based on $\mathfrak{S}_1, \mathfrak{S}_2$, we construct a coding scheme $\mathfrak{S}$ as follows. As rationals are dense over reals, for any $\mu \in [0,1]$ and any $\epsilon \in \mathbb{R}_{\geq 0}$, we can find a rational $\mu_\epsilon = u/v$ with $u, v \in \mathbb{Z}_{\geq 0}$ and $u \leq v$ such that $|\mu - \mu_\epsilon| \leq \epsilon$.

A. $q(\mathfrak{S}_1) = q(\mathfrak{S}_2)$

First, let us start with the simpler case where $q(\mathfrak{S}_1) = q(\mathfrak{S}_2) \triangleq q$. The parameters of $\mathfrak{S}$ are

$$\left(\lambda_0(\mathfrak{S}), \lambda_B(\mathfrak{S}), \kappa(\mathfrak{S}), q(\mathfrak{S}) = q, \text{ENC}(\mathfrak{S}), \text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S}) \right), \tag{186}$$

$$\lambda_0(\mathfrak{S}) = \frac{u}{v}\lambda_0(\mathfrak{S}_1) + \frac{v-u}{v}\lambda_0(\mathfrak{S}_2), \tag{187}$$

$$\lambda_B(\mathfrak{S}) = \frac{u}{v}\lambda_B(\mathfrak{S}_1) + \frac{v-u}{v}\lambda_B(\mathfrak{S}_2), \tag{188}$$

$$\kappa(\mathfrak{S}) = v \cdot \kappa(\mathfrak{S}_1) \cdot \kappa(\mathfrak{S}_2), \tag{189}$$

$$\text{ENC}(\mathfrak{S}) = (\text{ENC}(\mathfrak{S}_1))^{\otimes u\kappa(\mathfrak{S}_2)} \otimes (\text{ENC}(\mathfrak{S}_2))^{\otimes (v-u)\kappa(\mathfrak{S}_1)}, \tag{190}$$

$$\text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S}) = \left(\text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S}_1) \right)^{\otimes u\kappa(\mathfrak{S}_2)} \otimes \left(\text{DEC}^{\mathcal{K}, \mathcal{K}_B}(\mathfrak{S}_2) \right)^{\otimes (v-u)\kappa(\mathfrak{S}_1)}. \tag{191}$$

The quantum message Q_0 has $\kappa(\mathfrak{S})\lambda_0(\mathfrak{S})$ qudits, and the EA $A_1 \ldots A_{N_B} \, B_1 \ldots B_{N_B}$, has $\kappa(\mathfrak{S})\lambda_B(\mathfrak{S})$ qudits,

$$\kappa(\mathfrak{S})\lambda_0(\mathfrak{S}) = \kappa(\mathfrak{S}_1) \cdot \kappa(\mathfrak{S}_2) \cdot \left(u\lambda_0(\mathfrak{S}_1) + (v-u)\lambda_0(\mathfrak{S}_2)\right), \tag{192}$$

$$\kappa(\mathfrak{S})\lambda_B(\mathfrak{S}) = \kappa(\mathfrak{S}_1) \cdot \kappa(\mathfrak{S}_2) \cdot \left(u\lambda_B(\mathfrak{S}_1) + (v-u)\lambda_B(\mathfrak{S}_2)\right). \tag{193}$$

Then ENC$(\mathfrak{S})$ and DEC$^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S})$ in (190) and (191) refer to the following encoding and decoding operations. $Q_0 = Q_0(1,1)\ldots$ $Q_0(1, u\kappa(\mathfrak{S}_2))Q_0(2,1)\ldots Q_0(2,(v-u)\kappa(\mathfrak{S}_1))$ is divided into $u\kappa(\mathfrak{S}_2) + (v-u)\kappa(\mathfrak{S}_1)$ blocks, where $Q_0(1,i), i \in [u\kappa(\mathfrak{S}_2)]$ has $\kappa(\mathfrak{S}_1)\lambda_0(\mathfrak{S}_1)$ qudits and $Q_0(2,j), j \in [(v-u)\kappa(\mathfrak{S}_1)]$ has $\kappa(\mathfrak{S}_2)\lambda_0(\mathfrak{S}_2)$ qudits. Similarly, $A_m, B_m, m \in [N_B]$ is divided into $u\kappa(\mathfrak{S}_2) + (v-u)\kappa(\mathfrak{S}_1)$ blocks where $A_m(1,i), B_m(1,i), i \in [u\kappa(\mathfrak{S}_2)]$ each has $\kappa(\mathfrak{S}_1)\lambda_B(\mathfrak{S}_1)$ qudits and $A_m(2,j), B_m(2,j), j \in [(v-u)\kappa(\mathfrak{S}_1)]$ each has $\kappa(\mathfrak{S}_2)\lambda_B(\mathfrak{S}_2)$ qudits.

Next, for each $i \in [u\kappa(\mathfrak{S}_2)]$, $Q_0(1,i), A_m(1,i), B_m(1,i)$ is encoded through the map ENC$(\mathfrak{S}_1)$ and decoded through the map DEC$^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S}_1)$ so that the final output $\widehat{Q}_0(1,i)$ preserves the same entanglements with the rest of the universe that were originally associated with $Q_0(1,i)$. Similarly, for each $j \in [(v-u)\kappa(\mathfrak{S}_1)]$, $Q_0(2,j), A_m(2,j), B_m(2,j)$ is encoded through the map ENC$(\mathfrak{S}_2)$ and decoded through the map DEC$^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S}_2)$ so that the final output $\widehat{Q}_0(2,j)$ preserves the same entanglements with the rest of the universe that were originally associated with $Q_0(2,j)$. Combining all outputs $\widehat{Q}_0 \triangleq$ $\widehat{Q}_0(1,1)\ldots \widehat{Q}_0(1,u\kappa(\mathfrak{S}_2))\widehat{Q}_0(2,1)\ldots \widehat{Q}_0(2,(v-u)\kappa(\mathfrak{S}_1))$, the quantum system $R\widehat{Q}_0$ is recovered whose state is identical to $|\varphi\rangle_{RQ_0}$.

Note that

$$\lambda_0(\mathfrak{S}) = \frac{u}{v}\lambda_0(\mathfrak{S}_1) + \frac{v-u}{v}\lambda_0(\mathfrak{S}_2) \geq \frac{u}{v}\lambda_0(1) + \frac{v-u}{v}\lambda_0(2), \tag{194}$$

$$\lambda_B(\mathfrak{S}) = \frac{u}{v}\lambda_B(\mathfrak{S}_1) + \frac{v-u}{v}\lambda_B(\mathfrak{S}_2) \leq \frac{u}{v}\lambda_B(1) + \frac{v-u}{v}\lambda_B(2). \tag{195}$$

Thus, the rate tuple $(\lambda_0, \lambda_B) = (\mu_\epsilon \lambda_0(1) + (1-\mu_\epsilon)\lambda_0(2), \mu_\epsilon \lambda_B(1) + (1-\mu_\epsilon)\lambda_B(2))$ is achievable. Letting $\epsilon \to 0$, the rate tuple $(\lambda_0, \lambda_B) = (\mu\lambda_0(1) + (1-\mu)\lambda_0(2), \mu\lambda_B(1) + (1-\mu)\lambda_B(2))$ is in the closure of the set of achievable rate tuples and the proof of convexity is complete.

B. General $q(\mathfrak{S}_1), q(\mathfrak{S}_2)$

Second, we consider the general case where $q(\mathfrak{S}_1), q(\mathfrak{S}_2)$ might be different. Here the key observation is that the closure of the set of achievable rate tuples is the same for all $q \geq 2$, i.e., for any $q \geq 2$, we may transform any feasible coding scheme $\mathfrak{S}$ with parameter $q(\mathfrak{S})$ to another scheme $\mathfrak{S}'$ such that $q(\mathfrak{S}') = q$ while achieving the same rate tuple. This result is stated in the following lemma.

Lemma 3. *For any ϵ, $0 < \epsilon < \lambda_0$, any $q \in \mathbb{Z}_{\geq 2}$ and any feasible coding scheme $\mathfrak{S}$ with parameters*

$$\left(\lambda_0(\mathfrak{S}), \lambda_B(\mathfrak{S}), \kappa(\mathfrak{S}), q(\mathfrak{S}), ENC(\mathfrak{S}), DEC^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S})\right),$$

that achieves rate tuple (λ_0, λ_B), i.e., $\lambda_0(\mathfrak{S}) \geq \lambda_0, \lambda_B(\mathfrak{S}) \leq \lambda_B$, there exists another feasible coding scheme $\mathfrak{S}'$ with parameters

$$\left(\lambda_0(\mathfrak{S}'), \lambda_B(\mathfrak{S}'), \kappa(\mathfrak{S}'), q(\mathfrak{S}') = q, ENC(\mathfrak{S}'), DEC^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S}')\right),$$

that achieves rate tuple $(\lambda_0 - \epsilon, \lambda_B + \epsilon)$, i.e., $\lambda_0(\mathfrak{S}') \geq \lambda_0 - \epsilon, \lambda_B(\mathfrak{S}') \leq \lambda_B + \epsilon$. Therefore, the closure of the set of achievable rate tuples does not depend on q.

Proof: Note that $\epsilon, \lambda_0(\mathfrak{S}), \lambda_B(\mathfrak{S}), \kappa(\mathfrak{S}), q$ are given and $\epsilon < \lambda_0 \leq \lambda_0(\mathfrak{S})$. Then we can find integers $T, T', \kappa' \in \mathbb{Z}_{\geq 1}$ such that

$$T\kappa(\mathfrak{S})\frac{\log_2 q(\mathfrak{S})}{\log_2 q}\frac{\lambda_B(\mathfrak{S})}{\lambda_B(\mathfrak{S}) + \epsilon} \leq T'\kappa' \leq T\kappa(\mathfrak{S})\frac{\log_2 q(\mathfrak{S})}{\log_2 q}\frac{\lambda_0(\mathfrak{S})}{\lambda_0(\mathfrak{S}) - \epsilon} \tag{196}$$

and the parameters of $\mathfrak{S}'$ are set as

$$\lambda_0(\mathfrak{S}') = \lambda_0(\mathfrak{S})\frac{\kappa(\mathfrak{S})}{\kappa'}\frac{T}{T'}\frac{\log_2 q(\mathfrak{S})}{\log_2 q}, \tag{197}$$

$$\lambda_B(\mathfrak{S}') = \lambda_B(\mathfrak{S})\frac{\kappa(\mathfrak{S})}{\kappa'}\frac{T}{T'}\frac{\log_2 q(\mathfrak{S})}{\log_2 q}, \tag{198}$$

$$\kappa(\mathfrak{S}') = \kappa'T', \tag{199}$$

$$ENC(\mathfrak{S}') = (ENC(\mathfrak{S}))^{\otimes T}, \tag{200}$$

$$DEC^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S}') = \left(DEC^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S})\right)^{\otimes T}. \tag{201}$$

For the coding scheme $\mathfrak{S}'$, the quantum message Q_0 has dimension

$$|Q_0| = q^{\kappa(\mathfrak{S}')\lambda_0(\mathfrak{S}')} \overset{(197),(199)}{=} q(\mathfrak{S})^{\kappa(\mathfrak{S})\lambda_0(\mathfrak{S})\times T}$$

and for the entanglement AB, each $A_m, B_m, m \in [N_B]$ has dimension

$$|A_m| = |B_m| = q^{\kappa(\mathfrak{S}')\lambda_B(\mathfrak{S}')} \overset{(198),(199)}{=} q(\mathfrak{S})^{\kappa(\mathfrak{S})\lambda_B(\mathfrak{S}) \times T}.$$

Q_0, A_m, B_m is encoded and decoded through T parallel concatenations of ENC($\mathfrak{S}$) and DEC$^{\mathcal{K},\mathcal{K}_B}(\mathfrak{S})$; perfect recovery is thus guaranteed. Furthermore,

$$\lambda_0(\mathfrak{S}') \overset{(196),(197)}{\geq} \lambda_0(\mathfrak{S}) - \epsilon \geq \lambda_0 - \epsilon, \tag{202}$$

$$\lambda_B(\mathfrak{S}') \overset{(196),(198)}{\leq} \lambda_B(\mathfrak{S}) + \epsilon \leq \lambda_B + \epsilon, \tag{203}$$

so that the rate tuple $(\lambda_0 - \epsilon, \lambda_B + \epsilon)$ is achieved. □

Equipped with Lemma 3, we may transform the two schemes $\mathfrak{S}_1, \mathfrak{S}_2$ to $\mathfrak{S}'_1, \mathfrak{S}'_2$ so that $q(\mathfrak{S}'_1) = q(\mathfrak{S}'_2) = q$. Then we can apply the same space sharing scheme in Appendix A to construct $\mathfrak{S}'$ so that letting $\epsilon \to 0$, any convex combination of rate tuples is achieved. The proof is thus complete.

Consider $\widetilde{\text{QSEA}}$ with $N_B = K_B = 1$ so that the entanglement B is not erasure-prone. The setting reduces to entanglement-assisted quantum MDS codes where the rate tuple $(\lambda_0, \lambda_B) = (K/2, K/2)$ is known to be achievable by a teleportation based scheme [5]. Here we specialize the classical code in Section VI-B2 and translate through Theorem 2 to provide an alternative quantum scheme that does not involve teleportation or measurement.

Consider encoding first. Set $\kappa = 2$ and choose $q \geq 2N$ as a prime power. The quantum message Q_0 has $\kappa\lambda_0 = K$ qudits and each qudit is q-dimensional. Suppose Q_0 is in an arbitrary state with density matrix ω_{Q_0}. Without loss of generality, suppose ω_{Q_0} has a spectral decomposition $\omega_{Q_0} = \sum_{\boldsymbol{a} \in \mathbb{F}_q^{1 \times K}} p_{\boldsymbol{a}} |\boldsymbol{a}\rangle \langle \boldsymbol{a}|$ and purification RQ_0 in the pure state $|\varphi\rangle_{RQ_0} = \sum_{\boldsymbol{a} \in \mathbb{F}_q^{1 \times K}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle |\boldsymbol{a}\rangle$. The EA B comprises $N_B\kappa\lambda_B = K$ qudits. The encoding proceeds as follows.

$$|\varphi\rangle_{RQ_0} |\phi\rangle_{AB} \tag{204}$$

$$= \sum_{\boldsymbol{a} \in \mathbb{F}_q^{1 \times K}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle_R |\boldsymbol{a}\rangle_{Q_0} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{1 \times K}} \frac{1}{\sqrt{q^K}} |\boldsymbol{b}\rangle_A |\boldsymbol{b}\rangle_B \tag{205}$$

$$\rightsquigarrow \sum_{\boldsymbol{a} \in \mathbb{F}_q^{1 \times K}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle_R |\boldsymbol{a}\rangle_{Q_0} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{1 \times K}} \frac{1}{\sqrt{q^K}} |\boldsymbol{b}\rangle_A |\boldsymbol{b}\rangle_B \sum_{\boldsymbol{z} \in \mathbb{F}_q^{1 \times (N-K)}} \frac{1}{\sqrt{q^{N-K}}} |\boldsymbol{z}\rangle \tag{206}$$

$$= \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b},\boldsymbol{z}} \frac{1}{\sqrt{q^N}} |\boldsymbol{a}\rangle_{Q_0} |\boldsymbol{b}\rangle_A |\boldsymbol{z}\rangle |\boldsymbol{b}\rangle_B \tag{207}$$

$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b},\boldsymbol{z}} \frac{1}{\sqrt{q^N}} |f_1(\boldsymbol{a}+\boldsymbol{b}), h_1(\boldsymbol{a},\boldsymbol{z})\rangle_{Q_1} \dots |f_N(\boldsymbol{a}+\boldsymbol{b}), h_N(\boldsymbol{a},\boldsymbol{z})\rangle_{Q_N} |\boldsymbol{b}\rangle_B . \tag{208}$$

Evidently, the encoded state $\rho_{RQ_1\dots Q_N B}$ in (5) is a pure state in this case. In (208), we define the functions $f_1, \dots, f_N$ as follows.

$$(f_1(\boldsymbol{a}+\boldsymbol{b}), \dots, f_N(\boldsymbol{a}+\boldsymbol{b})) = (\boldsymbol{a}+\boldsymbol{b}) \mathbf{V}, \qquad\qquad \forall \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^{1 \times K}. \tag{209}$$

The LHS is a vector in $\mathbb{F}_q^{1 \times N}$. On the RHS, $\boldsymbol{a}+\boldsymbol{b} \in \mathbb{F}_q^{1 \times K}$, and $\mathbf{V} \in \mathbb{F}_q^{K \times N}$ is defined as follows.

$$\mathbf{V} = \left[\alpha_j^{i-1}\right]_{ij}, i \in [K], j \in [N], \alpha_j \text{ are distinct in } \mathbb{F}_q. \tag{210}$$

The functions $h_1, \dots, h_N$ in (208) are defined as

$$(h_1(\boldsymbol{a},\boldsymbol{z}), \dots, h_N(\boldsymbol{a},\boldsymbol{z}))_{1 \times N} = (\boldsymbol{a},\boldsymbol{z})_{1 \times N} \times \mathbf{H}_{N \times N}, \qquad\qquad \forall \boldsymbol{a} \in \mathbb{F}_q^{1 \times K}, \boldsymbol{z} \in \mathbb{F}_q^{1 \times (N-K)}. \tag{211}$$

The LHS is a vector in $\mathbb{F}_q^{1 \times N}$. On the RHS, $(\boldsymbol{a},\boldsymbol{z}) \in \mathbb{F}_q^{1 \times N}$, and $\mathbf{H} \in \mathbb{F}_q^{N \times N}$ is defined as follows.

$$\mathbf{H}_{N \times N} = \left[\frac{1}{\beta_i - \gamma_j}\right]_{ij}, i \in [N], j \in [N], \beta_i, \gamma_j \text{ are distinct in } \mathbb{F}_q. \tag{212}$$

Note that (208) is an isometry because $(f_{[N]}(\boldsymbol{a}+\boldsymbol{b}), h_{[N]}(\boldsymbol{a},\boldsymbol{z}))$ determines $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{z}$. Note that $\mathbf{V}$ is a Vandermonde matrix and $\mathbf{H}$ is a Cauchy matrix so that both have full rank.

Consider decoding next. For any $\mathcal{K} \in \binom{[N]}{K}$, the state for $RQ_1 \dots Q_N B = RQ_{\mathcal{K}} Q_{\mathcal{K}^c} B$ is expressed as follows.

$$\sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b},\boldsymbol{z}} \frac{1}{\sqrt{q^N}} |f_{\mathcal{K}}(\boldsymbol{a}+\boldsymbol{b}), h_{\mathcal{K}}(\boldsymbol{a},\boldsymbol{z})\rangle_{Q_{\mathcal{K}}} |\boldsymbol{b}\rangle_B |f_{\mathcal{K}^c}(\boldsymbol{a}+\boldsymbol{b}), h_{\mathcal{K}^c}(\boldsymbol{a},\boldsymbol{z})\rangle_{Q_{\mathcal{K}^c}} \tag{213}$$

$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b},\boldsymbol{z}} \frac{1}{\sqrt{q^N}} \, |\boldsymbol{a}\mathbf{V}_{sub}^{K\times K}\rangle \, |h_{\mathcal{K}}(\boldsymbol{a},\boldsymbol{z})\rangle \, |\boldsymbol{b}\rangle \, |f_{\mathcal{K}^c}(\boldsymbol{a}+\boldsymbol{b}), h_{\mathcal{K}^c}(\boldsymbol{a},\boldsymbol{z})\rangle_{Q_{\mathcal{K}^c}} \tag{214}$$

$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b},\boldsymbol{z}} \frac{1}{\sqrt{q^N}} \, |\boldsymbol{a}\rangle \, |h_{\mathcal{K}}(\boldsymbol{a},\boldsymbol{z})\rangle \, |\boldsymbol{b}\rangle \, |f_{\mathcal{K}^c}(\boldsymbol{a}+\boldsymbol{b}), h_{\mathcal{K}^c}(\boldsymbol{a},\boldsymbol{z})\rangle_{Q_{\mathcal{K}^c}} \tag{215}$$

$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b},\boldsymbol{z}} \frac{1}{\sqrt{q^N}} \, |\boldsymbol{a}\rangle \, |\boldsymbol{z}\mathbf{H}_{sub}^{(N-K)\times K}\rangle \, |\boldsymbol{a}+\boldsymbol{b}\rangle \, \Big| f_{\mathcal{K}^c}(\underbrace{\boldsymbol{a}+\boldsymbol{b}}_{\triangleq \boldsymbol{b}'}), \underbrace{h_{\mathcal{K}^c}(\boldsymbol{a},\boldsymbol{z})}_{\triangleq \boldsymbol{z}'} \Big\rangle_{Q_{\mathcal{K}^c}} \tag{216}$$

$$\rightsquigarrow \sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \sum_{\boldsymbol{b}',\boldsymbol{z}'} \frac{1}{\sqrt{q^N}} \, |\boldsymbol{a}\rangle \, |\boldsymbol{z}'\overline{\mathbf{H}}_{sub}^{(N-K)\times K}\rangle \, |\boldsymbol{b}'\rangle \, |f_{\mathcal{K}^c}(\boldsymbol{b}'), \boldsymbol{z}'\rangle_{Q_{\mathcal{K}^c}} \tag{217}$$

$$= \left(\sum_{\boldsymbol{a}} \sqrt{p_{\boldsymbol{a}}} \, |\boldsymbol{a}\rangle_R \, |\boldsymbol{a}\rangle_{\widehat{Q}_0} \right) \otimes \left(\sum_{\boldsymbol{b}',\boldsymbol{z}'} \frac{1}{\sqrt{q^N}} \, |\boldsymbol{z}'\overline{\mathbf{H}}_{sub}^{(N-K)\times K}\rangle \, |\boldsymbol{b}'\rangle \, |f_{\mathcal{K}^c}(\boldsymbol{b}'), \boldsymbol{z}'\rangle_{Q_{\mathcal{K}^c}} \right). \tag{218}$$

Thus, $R\widehat{Q}_0$ is recovered in the same pure state as the original message and reference, RQ_0. In (214), $f_{\mathcal{K}}(\boldsymbol{a}+\boldsymbol{b}) = (\boldsymbol{a}+\boldsymbol{b}) \times \mathbf{V}(:,\mathcal{K})$. The matrix $\mathbf{V}(:,\mathcal{K}) \in \mathbb{F}_q^{K\times K}$ is denoted as $\mathbf{V}_{sub}^{K\times K}$. As $|b\rangle$ is available (from the EA B), we subtract the contribution of $\boldsymbol{b}$ and obtain $|\boldsymbol{a}\mathbf{V}_{sub}^{K\times K}\rangle \, |b\rangle$ through a unitary transformation of $|f_{\mathcal{K}}(\boldsymbol{a}+\boldsymbol{b})\rangle \, |b\rangle$. In the next step, (215) is obtained because $\mathbf{V}_{sub}^{K\times K}$ (comprised of K columns of the Vandermonde matrix $\mathbf{V}$) has full rank and thus a unitary map transforms $|\boldsymbol{a}\mathbf{V}_{sub}\rangle$ to $|\boldsymbol{a}\rangle$. In (216), $h_{\mathcal{K}}(\boldsymbol{a},\boldsymbol{z}) = (\boldsymbol{a},\boldsymbol{z}) \times \mathbf{H}(:,\mathcal{K}) = \boldsymbol{a} \times \mathbf{H}(1:K,\mathcal{K}) + \boldsymbol{z} \times \mathbf{H}(K+1:N,\mathcal{K})$, where $i:j$ denotes the index tuple $(i, i+1, \cdots, j)$ and the shorthand notation $:$ in $\mathbf{H}(:,\mathcal{K})$ denotes the tuple that contains all indices, i.e., all rows. The matrix $\mathbf{H}(K+1:N,\mathcal{K}) \in \mathbb{F}_q^{(N-K)\times K}$ is denoted as $\mathbf{H}_{sub}^{(N-K)\times K}$. To obtain (217), note that

$$\boldsymbol{z}' = h_{\mathcal{K}^c}(\boldsymbol{a},\boldsymbol{z}) = \boldsymbol{a} \times \mathbf{H}(1:K,\mathcal{K}^c) + \boldsymbol{z} \times \mathbf{H}(K+1:N,\mathcal{K}^c), \ \boldsymbol{z}' \in \mathbb{F}_q^{1\times(N-K)} \tag{219}$$

$$\implies \quad \boldsymbol{z} = (\boldsymbol{z}' - \boldsymbol{a} \times \mathbf{H}(1:K,\mathcal{K}^c)) \times \mathbf{H}^{-1}(K+1:N,\mathcal{K}^c)_{(N-K)\times(N-K)}, \tag{220}$$

and we define the $(N-K) \times K$ matrix $\overline{\mathbf{H}}_{sub}^{(N-K)\times K} \triangleq \mathbf{H}^{-1}(K+1:N,\mathcal{K}^c) \times \mathbf{H}_{sub}^{(N-K)\times K}$. Note that $\mathbf{H}(K+1:N,\mathcal{K}^c)$ has full rank as it is a square sub-matrix of the Cauchy matrix $\mathbf{H}$. A unitary map thus transforms $|\boldsymbol{a}\rangle \, |\boldsymbol{z}\mathbf{H}_{sub}^{(N-K)\times K}\rangle$ into $|\boldsymbol{a}\rangle \, |\boldsymbol{z}'\overline{\mathbf{H}}_{sub}^{(N-K)\times K}\rangle$. In (217), we also replace the sum over $\boldsymbol{b}, \boldsymbol{z}$ with the sum over $\boldsymbol{b}', \boldsymbol{z}'$ because for any given $\boldsymbol{a}$, the mapping between $(\boldsymbol{b}, \boldsymbol{z})$ and $(\boldsymbol{b}', \boldsymbol{z}')$ is invertible so that when $(\boldsymbol{b}, \boldsymbol{z})$ takes all values in $\mathbb{F}_q^{1\times N}$, $(\boldsymbol{b}', \boldsymbol{z}')$ also takes all values in $\mathbb{F}_q^{1\times N}$. Thus, the decoding is successful.

REFERENCES

[1] Y. Wu, S. Kolkowitz, S. Puri, and J. D. Thompson, "Erasure conversion for fault-tolerant quantum computing in alkaline earth rydberg atom arrays," *Nat. Commun.*, vol. 13, p. 4657, Aug. 2022.

[2] H. Levine, A. Haim, J. S. Hung, N. Alidoust, M. Kalaee, L. DeLorenzo, E. A. Wollack, P. Arrangoiz-Arriola, A. Khalajhedayati, R. Sanil, *et al.*, "Demonstrating a long-coherence dual-rail erasure qubit using tunable transmons," *Physical Review X*, vol. 14, no. 1, p. 011051, 2024.

[3] L. Golowich and V. Guruswami, "Quantum locally recoverable codes," in *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 5512–5522, Philadelphia, PA: Society for Industrial and Applied Mathematics, Jan. 2025.

[4] H. Sun and S. A. Jafar, "On the capacity of distributed quantum storage," *arXiv preprint arXiv:2510.10568*, 2025.

[5] M. Grassl, F. Huber, and A. Winter, "Entropic proofs of singleton bounds for quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 68, no. 6, pp. 3942–3950, 2022.

[6] M.-H. Hsieh and M. M. Wilde, "Trading classical communication, quantum communication, and entanglement in quantum shannon theory," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4705–4730, Sept. 2010.

[7] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[8] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2637–2655, Oct. 2002.

[9] C.-Y. Lai and T. A. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 86, no. 3, p. 032319, 2012.

[10] Y. Fujiwara, "Quantum error correction via less noisy qubits," *Physical Review Letters*, vol. 110, no. 17, p. 170501, 2013.

[11] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *science*, vol. 314, no. 5798, pp. 436–439, 2006.

[12] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3073–3089, 2014.

[13] C.-Y. Lai and A. Ashikhmin, "Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 622–639, 2017.

[14] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Designs, Codes and Cryptography*, vol. 86, no. 1, pp. 121–136, 2018.

[15] G. Luo, X. Cao, and X. Chen, "MDS codes with hulls of arbitrary dimensions and their quantum error correction," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 2944–2952, 2018.

[16] M. Grassl, "Entanglement-assisted quantum communication beating the quantum singleton bound," *Physical Review A*, vol. 103, no. 2, p. L020601, 2021.

[17] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical review letters*, vol. 76, no. 5, p. 722, 1996.

[18] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, p. 3824, 1996.

[19] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[20] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, p. 1098, 1996.

[21] A. Steane, "Multiple-particle interference and quantum error correction," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[22] A. D. Smith, "Quantum secret sharing for general access structures," *arXiv preprint quant-ph/0001087*, 2000.

[23] M. Hayashi and S. Song, "Unified approach to secret sharing and symmetric private information retrieval with colluding servers in quantum systems," *IEEE Transactions on Information Theory*, vol. 69, no. 10, pp. 6537–6563, 2023.

[24] M. Mamindlapally and A. Winter, "Singleton bounds for entanglement-assisted classical and quantum error correcting codes," *IEEE Trans. Inf. Theory*, vol. 69, pp. 5857–5868, Sept. 2023.

[25] T. Prasad and M. Grassl, "Codes for entanglement-assisted classical communication," *Npj Quantum Inf.*, vol. 11, Jan. 2025.

[26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, vol. 16. Elsevier, 1977.

[27] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Physical Review A*, vol. 54, no. 4, p. 2629, 1996.

[28] E. H. Lieb and M. B. Ruskai, "Proof of the strong subadditivity of quantum-mechanical entropy," *J. Math. Phys*, vol. 14, no. 12, 1973.

[29] X. Chen, S. Chessa, I. George, F. Leditzky, and E. Chitambar, "Capacities of entanglement distribution from a central source," *arXiv preprint arXiv:2411.04977*, 2024.