

Quantum Multiple-Access One-Time Pad

Eyuri Wakakuwa

Abstract—We introduce and analyze an information theoretical task that we call the *quantum multiple-access one-time pad*. Here, a number of senders initially share a correlated quantum state with a receiver and an eavesdropper. Each sender performs a local operation to encode a classical message and sends their system to the receiver, who subsequently performs a measurement to decode the messages. The receiver will be able to decode the messages almost perfectly, while the eavesdropper must not be able to extract information about the messages even if they have access to the quantum systems transmitted. We consider a “conditional” scenario in which a portion of the receiver’s side information is also accessible to the eavesdropper. We investigate the maximum amount of classical information that can be encoded by each of the senders. We derive a single-letter characterization for the achievable rate region in an asymptotic limit of infinitely many copies and vanishingly small error.

I. INTRODUCTION

Encoding and decoding of classical information into/from a composite quantum system under locality restrictions have been one of the central issues in quantum information theory. Superdense coding [1] is a task of encoding classical information to a bipartite quantum state by local operations on one of the two subsystems. Quantum secret sharing [2], [3] and quantum data hiding [4]–[7] are schemes that prevent anyone under locality restrictions from extracting the information encoded in a multipartite quantum system. The quantum one-time pad [8], [9] and the conditional quantum one-time pad [10] are hybrid of the two scenarios, in the sense that classical information is encoded by local operations on one of the subsystems so that it can be decoded only if the global access to the entire system is granted. These studies have led to a better understanding of correlation and entanglement in multipartite quantum states from an operational and information theoretical viewpoint.

This paper considers an extension of the conditional quantum one-time pad to a multi-sender scenario. We refer the task as the *quantum multiple-access one-time pad*. Here, a receiver, an eavesdropper and a number

of senders initially share a correlated quantum state. Each sender performs a local operation to encode a classical message on that state. The senders then send their systems to the receiver, who subsequently performs a measurement to decode the messages. We require that the receiver can decode the messages almost perfectly, while the eavesdropper can obtain almost no information about the messages even if they have access to the quantum systems transmitted. We focus on a “conditional” scenario as in [10], i.e., we assume that a portion of the receiver’s side information is accessible to the eavesdropper. We consider an asymptotic limit of infinitely many copies and vanishingly small error, and investigate the maximum amount of classical information that can be encoded by each of the senders. The main result is that we derive a single-letter characterization for the achievable rate region.

This paper is organized as follows. In Section II, we present the formulation of the problem and describe the main result. Section III introduces two subprotocols that we call *distributed encoding* and *distributed randomization*, and present the coding theorems thereof. Based on these results, we prove the main result in Section IV. The proofs of the coding theorems for distributed encoding and distributed randomization are provided in Section V and Section VI, respectively, and proofs of two lemmas that are used therein will be provided in Section VII. Conclusions are given in Section VIII.

Notations: For a natural number $N \in \mathbb{N}$, the set of natural numbers no greater than N is denoted by $[N]$, i.e., $[N] \equiv \{1, \dots, N\}$. The set of linear operators, unitary operators, normalized density operators and subnormalized ones on a Hilbert space \mathcal{H} are denoted by $\mathcal{L}(\mathcal{H})$, $\mathcal{U}(\mathcal{H})$, $\mathcal{S}(\mathcal{H})$ and $\mathcal{S}_{\leq}(\mathcal{H})$, respectively. The Hilbert space associated with a system A is denoted by \mathcal{H}^A , and its dimension is denoted by d_A . The identity operator on \mathcal{H}^A is denoted by I^A , and the completely mixed state on system A is denoted by π^A , i.e., $\pi^A = I^A/d_A$. The system composed of two subsystems A and B is denoted by AB . The Hilbert space associated with a composite system AB is denoted by \mathcal{H}^{AB} , i.e., $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$. When M and N are linear operators on \mathcal{H}^A and \mathcal{H}^B , respectively, their tensor product $M \otimes N$ is denoted by

E. Wakakuwa is with the Department of Computer Science, Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan (email: e.wakakuwa@gmail.com).

$M^A \otimes N^B$ for clarity. The identity operation on system A is denoted by id^A . When \mathcal{E} is a quantum operation on A and ρ is a state on AB , the state $(\mathcal{E} \otimes \text{id}^B)(\rho^{AB})$ is denoted simply by $\mathcal{E}^A(\rho^{AB})$. For ρ^{AB} , ρ^A represents $\text{Tr}_B[\rho^{AB}]$. The system composed of n identical systems of A is denoted by A^n , and the corresponding Hilbert space is denoted by $(\mathcal{H}^A)^{\otimes n}$ or \mathcal{H}^{A^n} . The trace norm of an operator $X \in \mathcal{L}(\mathcal{H})$ is defined by $\|X\|_1 := \text{Tr}[\sqrt{X^\dagger X}]$ and the trace distance between two states $\rho, \sigma \in \mathcal{S}(\mathcal{H}^A)$ is defined by $\frac{1}{2}\|\rho - \sigma\|_1$. $\log x$ represents the base 2 logarithm of x . The binary entropy is defined by $h(x) := -x \log x - (1-x) \log(1-x)$ and satisfies $\lim_{x \rightarrow 0} h(x) = 0$. The cardinality of a set S is denoted by $|S|$.

The von Neumann entropy of a state $\rho \in \mathcal{S}(\mathcal{H}^A)$ is defined by

$$S(A)_\rho = S(\rho^A) := -\text{Tr}[\rho^A \log \rho^A]. \quad (1)$$

For $\varrho \in \mathcal{S}(\mathcal{H}^{AB})$ and $\varsigma \in \mathcal{S}(\mathcal{H}^{ABC})$, the conditional entropy, the mutual information and the conditional mutual information are defined by

$$S(A|B)_\varrho := S(AB)_\varrho - S(B)_\varrho, \quad (2)$$

$$I(A : B)_\varrho := S(A)_\varrho - S(A|B)_\varrho, \quad (3)$$

$$I(A : B|C)_\varsigma := S(A|C)_\varsigma - S(A|BC)_\varsigma. \quad (4)$$

For the properties of the entropies and the mutual informations used in this paper, see e.g. [11].

II. FORMULATION AND RESULT

Suppose that $Z \in \mathbb{N}$ senders, a receiver and an eavesdropper are located distantly. Let A_1, \dots, A_Z, B and E be quantum systems in their possession, which are represented by finite-dimensional Hilbert spaces $\mathcal{H}^{A_1}, \dots, \mathcal{H}^{A_Z}, \mathcal{H}^B$ and \mathcal{H}^E , respectively. They initially share $n \in \mathbb{N}$ copies of a quantum state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z B E})$. Each sender encodes a classical message by performing an operation on their system locally. For $z \in [Z]$, let R_z be the bit length of the message that the z -th sender is to encode, divided by n , and let $M_z \equiv 2^{nR_z}$. The encoding scheme is represented by a finite-dimensional quantum system A'_z and a set of encoding quantum operations (completely positive trace-preserving maps) $\mathfrak{E}_z \equiv \{\mathcal{E}_{z, m_z}\}_{m_z=1}^{M_z}$ from A_z^n to A'_z , where $m_z \in [M_z]$ denotes the values of the message. For simplicity, we introduce the following notations:

$$\mathbf{M} \equiv [M_1] \times \dots \times [M_Z], \quad (5)$$

$$\mathbf{m} \equiv (m_1, \dots, m_Z). \quad (6)$$

After performing the encoding operations, the senders send their systems to the receiver, who subsequently

performs a measurement to decode the messages. We consider the ‘‘conditional’’ scenario of [10], in which the receiver has access to $A'_1 \dots A'_Z B^n E^n$ when decoding the messages and the eavesdropper has access to $A'_1 \dots A'_Z E^n$ when trying to extract the information about the messages. The decoding measurement by the receiver is represented by a POVM $\mathfrak{M} \equiv \{\Lambda_{\mathbf{m}}\}_{\mathbf{m} \in \mathbf{M}}$ on $A'_1 \dots A'_Z B^n E^n$. We refer to the tuple $\mathfrak{C} \equiv (\mathfrak{E}_1, \dots, \mathfrak{E}_Z, \mathfrak{M})$ as a (n, M_1, \dots, M_Z) code for ρ .

For each message value \mathbf{m} , the state after the encoding operations is represented by

$$\rho_{\mathbf{m}} := \left(\bigotimes_{z=1}^Z \mathcal{E}_{z, m_z}^{A_z^n \rightarrow A'_z} \right) (\rho^{\otimes n}). \quad (7)$$

We assume that the messages are distributed uniformly, in which case the average state is

$$\bar{\rho} := \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \rho_{\mathbf{m}}. \quad (8)$$

The average decoding error is defined by

$$\epsilon(\mathfrak{C}) := 1 - \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \text{Tr}[\rho_{\mathbf{m}} \Lambda_{\mathbf{m}}]. \quad (9)$$

The average information leakage is quantified by the trace distance as

$$\vartheta(\mathfrak{C}) := \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \left\| \rho_{\mathbf{m}}^{A'_{[Z]} E^n} - \bar{\rho}^{A'_{[Z]} E^n} \right\|_1. \quad (10)$$

We require that both the decoding error and the information leakage can be made arbitrarily small in the asymptotic limit of n to infinity. A rigorous definition of the achievable rate region is as follows:

Definition 1 A rate tuple (R_1, \dots, R_Z) is achievable for the state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z B E})$ if, for any $\epsilon, \vartheta > 0$ and any sufficiently large $n \in \mathbb{N}$, there exists a $(n, 2^{nR_1}, \dots, 2^{nR_Z})$ code \mathfrak{C} for ρ that satisfies the reliability condition $\epsilon(\mathfrak{C}) \leq \epsilon$ and the secrecy condition $\vartheta(\mathfrak{C}) \leq \vartheta$. The achievable rate region for ρ is the closure of the set of all achievable rate tuples in \mathbb{R}^Z .

The main result of this paper is the following theorem:

Theorem 2 The achievable rate region is equal to the set of all rate tuples $(R_1, \dots, R_Z) \in \mathbb{R}^Z$ that satisfy the following inequality for any $\Gamma \in [Z]$:

$$\sum_{z \in \Gamma} R_z \leq I(A_\Gamma : A_{\Gamma^c} B | E)_\rho, \quad (11)$$

where A_Γ and A_{Γ^c} denote the systems composed of $\{A_z\}_{z \in \Gamma}$ and $\{A_z\}_{z \in \Gamma^c}$, respectively, with $\Gamma^c \equiv [Z] \setminus \Gamma$.

A proof of Theorem 2 will be provided in Section IV based on the results presented in Section III.

III. DISTRIBUTED ENCODING AND DISTRIBUTED RANDOMIZATION

We introduce two subprotocols that we call *distributed encoding* and *distributed randomization*, and present the coding theorems thereof. We compare the results with those in the previous literature. The two subprotocols are combined in Section IV to prove the direct part of Theorem 2. The proofs of the two theorems will be provided in Section V and VI, respectively.

A. Distributed Encoding

Suppose that $Z \in \mathbb{N}$ senders and a receiver are located distantly. Let A_1, \dots, A_Z and V be quantum systems in their possession, which are represented by finite-dimensional Hilbert spaces $\mathcal{H}^{A_1}, \dots, \mathcal{H}^{A_Z}$ and \mathcal{H}^V , respectively. They initially share $n \in \mathbb{N}$ copies of a quantum state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z V})$. Distributed encoding is a task in which each sender encodes a classical message by performing a local unitary operation on A_z^n so that it can be decoded from $A_1^n \dots A_Z^n V^n$ almost perfectly. For $z \in [Z]$, let C_z be the bit length of the message that the z -th sender is to encode, divided by n , and let $K_z \equiv 2^{nC_z}$. We define $\mathbf{K} \equiv [K_1] \times \dots \times [K_Z]$. Each element of \mathbf{K} is denoted as $\mathbf{k} \equiv (k_1, \dots, k_Z)$, where $k_z \in [K_z]$. A rigorous definition is as follows:

Definition 3 For each $z \in [Z]$, let $\mathfrak{U}_z \equiv \{U_{z,k_z}\}_{k_z=1}^{K_z}$ be a set of unitaries on A_z^n . For each $\mathbf{k} \in \mathbf{K}$, define a unitary

$$U_{\mathbf{k}} := \bigotimes_{z=1}^Z U_{z,k_z} \quad (12)$$

and a state

$$\rho_{\mathbf{k}} := (U_{\mathbf{k}} \otimes I^{V^n}) \rho^{\otimes n} (U_{\mathbf{k}} \otimes I^{V^n})^\dagger. \quad (13)$$

A tuple $(\mathfrak{U}_1, \dots, \mathfrak{U}_Z)$ is a (n, K_1, \dots, K_Z) distributed encoding for ρ with error ϵ if there exists a measurement $\{\Lambda_{\mathbf{k}}\}_{\mathbf{k} \in \mathbf{K}}$ on $A_1^n \dots A_Z^n V^n$ such that

$$\frac{1}{|\mathbf{K}|} \sum_{\mathbf{k} \in \mathbf{K}} \text{Tr}[\rho_{\mathbf{k}} \Lambda_{\mathbf{k}}] \geq 1 - \epsilon. \quad (14)$$

Our interest is on how much classical information can be encoded in this manner. We consider a scenario where the encoding unitaries are chosen independently and randomly according to the Haar measure. A rigorous definition is as follows:

Definition 4 A rate tuple (C_1, \dots, C_Z) is achievable in distributed encoding on a state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z V})$ if, for any $\epsilon, \xi > 0$ and any sufficiently large $n \in \mathbb{N}$, the following statement holds:

Let $U_{z,k_z,i} \in \mathcal{U}(\mathcal{H}^{A_z})$ for $i \in [n]$ and suppose that we choose $U_{z,k_z,i}$ randomly and independently according to the Haar measure for each $i \in [n]$, $k_z \in [2^{nC_z}]$ and $z \in [Z]$. Let

$$U_{z,k} := \bigotimes_{i=1}^n U_{z,k_z,i} \quad (15)$$

and $\mathfrak{U}_z \equiv \{U_{z,k_z}\}_{k_z=1}^{K_z}$. Then, with probability no smaller than $1 - \xi$, the tuple $(\mathfrak{U}_1, \dots, \mathfrak{U}_Z)$ is a $(n, 2^{nC_1}, \dots, 2^{nC_Z})$ distributed encoding for ρ with error ϵ .

The achievable rate region for ρ is the closure of the set of all achievable rate tuples in \mathbb{R}^Z .

A single-letter characterization of the achievable rate region is provided by the following proposition:

Proposition 5 The achievable rate region for distributed encoding on ρ is equal to the set of all tuples $(C_1, \dots, C_Z) \in \mathbb{R}^Z$ that satisfy

$$\sum_{z \in \Gamma} C_z \leq \hat{C}(\Gamma)_\rho \quad (16)$$

for any $\Gamma \in [Z]$, where

$$\hat{C}(\Gamma)_\rho := \sum_{z \in \Gamma} \log d_{A_z} - S(A_\Gamma | A_{\Gamma^c} V)_\rho. \quad (17)$$

A proof of Proposition 5 will be presented in Section V. Although the converse part of Proposition 5 is not necessary to prove the main theorem, we provide its proof for the completeness. A few properties of $\hat{C}(\Gamma)_\rho$ are described in Section III-D and will be used in the following sections to prove the main results. We remark that the validity of the time sharing scheme used in the proof of the direct part of Proposition 5 (see Section V) follows from the fact that the encoding unitaries are in the form of the tensor product as (15).

B. Distributed Randomization

Consider quantum systems A_1, \dots, A_Z and W that are represented by finite-dimensional Hilbert spaces $\mathcal{H}^{A_1}, \dots, \mathcal{H}^{A_Z}$ and \mathcal{H}^W , respectively. Suppose that $n \in \mathbb{N}$ copies of a state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z W})$ are distributed to $Z + 1$ distant parties. The task of distributed randomization is to transform the state by applying a random unitary operation individually and independently on each A_z^n , so that the state will become the product of the maximally mixed state on $A_1^n \dots A_Z^n$ and a state on W^n . For $z \in [Z]$, let $L_z \equiv 2^{nD_z}$ be the number of unitaries that are randomly applied on A_z^n . A rigorous definition is as follows:

Definition 6 For each $z \in [Z]$, let $\mathfrak{U}_z \equiv \{U_{z,l_z}\}_{l_z=1}^{L_z}$ be a set of unitaries on A_z^n . Consider random unitary operations \mathcal{R}_z ($z \in [Z]$) defined by

$$\mathcal{R}_z(\cdot) := \frac{1}{L_z} \sum_{l_z=1}^{L_z} U_{z,l_z}(\cdot) U_{z,l_z}^\dagger \quad (18)$$

and let

$$\bar{\rho} := \left(\bigotimes_{z=1}^Z \mathcal{R}_z \right) (\rho^{\otimes n}). \quad (19)$$

A tuple $(\mathfrak{U}_1, \dots, \mathfrak{U}_Z)$ is a (n, L_1, \dots, L_Z) distributed randomization of ρ with error ϑ if it holds that

$$\left\| \bar{\rho}^{A_{[Z]}^n W^n} - \pi^{A_{[Z]}^n} \otimes (\rho^{\otimes n})^{W^n} \right\|_1 \leq \vartheta, \quad (20)$$

where π is the maximally mixed state on $A_{[Z]}^n$.

Our interest is on how much randomness is required to accomplish this task in an asymptotic limit of infinitely many copies and vanishingly small error. We consider a scenario where each element of the set of the unitaries is chosen randomly and independently according to the Haar measure. A rigorous definition is as follows:

Definition 7 A rate tuple (D_1, \dots, D_Z) is achievable in distributed randomization of a state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z W})$ if, for any $\vartheta, \xi > 0$ and any sufficiently large $n \in \mathbb{N}$, the following statement holds:

Let $U_{z,l_z,i} \in \mathcal{U}(\mathcal{H}^{A_z})$ for $i \in [n]$ and suppose that we choose $U_{z,l_z,i}$ randomly and independently according to the Haar measure for each $i \in [n]$, $l_z \in [2^{nD_z}]$ and $z \in [Z]$. Let

$$U_{z,l} := \bigotimes_{i=1}^n U_{z,l_z,i} \quad (21)$$

and $\mathfrak{U}_z \equiv \{U_{z,l}\}_{l=1}^{2^{nD_z}}$. Then, with probability no smaller than $1 - \xi$, the tuple $(\mathfrak{U}_1, \dots, \mathfrak{U}_Z)$ is a $(n, 2^{nD_1}, \dots, 2^{nD_Z})$ distributed randomization of ρ with error ϑ .

The achievable rate region for distributed randomization of ρ is the closure of the set of all achievable rate tuples in \mathbb{R}^Z .

A single-letter characterization of the achievable rate region is provided by the following proposition:

Proposition 8 The achievable rate region for distributed randomization of ρ is equal to the set of all tuples $(D_1, \dots, D_Z) \in \mathbb{R}^Z$ that satisfy

$$\sum_{z \in \Gamma} D_z \geq \hat{D}(\Gamma)_\rho \quad (22)$$

for any $\Gamma \in [Z]$, where

$$\hat{D}(\Gamma)_\rho := \sum_{z \in \Gamma} \log d_{A_z} - S(A_\Gamma | W)_\rho. \quad (23)$$

A proof of Proposition 8 will be given in Section VI. Although the converse part of Proposition 8 is not necessary to prove the main theorem, we provide its proof for the completeness. A few properties of $\hat{D}(\Gamma)_\rho$ are described in Section III-D and will be used in the following sections to prove the main results. We remark that the validity of the time sharing scheme used in the proof of the direct part of Proposition 8 (see Section VI) follows from the fact that the encoding unitaries are in the form of the tensor product as (21).

C. Comparison with Previous Results

Distributed encoding can be viewed as a Shannon theoretical generalization of local encoding [12], which is a task of encoding classical information to a multipartite pure quantum state by local unitary operations. Ref. [12] considered a one-shot and deterministic setting, and raised a question of whether it is possible to encode the maximum amount of information, i.e., the one determined by the dimension of the entire system, only by local unitary operations. Ref. [12] proved that this is possible for several classes of pure states, while it has been left open whether this is possible for *all* multipartite pure states. Proposition 5 above answers this question in the affirmative in the setting of asymptotic limit of infinitely many copies and vanishingly small error. Note that when B and E are trivial (one-dimensional) systems and ρ is a pure state, then $\hat{C}([Z])_\rho = \sum_{z \in [Z]} \log d_{A_z}$.

Refs. [13], [14] introduced a task called *distributed quantum dense coding*, which is a generalization of quantum superdense coding to a multi-sender scenario. They considered both of the case with one receiver and the case with multiple receivers. In the former, distributed quantum dense coding is similar to distributed encoding, i.e., the senders encode classical information to a multipartite quantum state only by local unitary operations. They proved that the maximum value of the Holevo information between the quantum system and the classical information to be encoded is equal to $C_{[Z]}^*$ defined by (17). Proposition 5 above and its proof in Section V improves upon this result in that (i) Proposition 5 not only deals with the total amount of information but also clarifies the trade-off relation between the maximum amounts of information that can be encoded by each of the senders, and (ii) in the proof in Section V, we explicitly show the existence of encoding operations and a decoding measurement that achieve the

optimal encoding rate. In the case of only one sender, Proposition 5 reduces to the result of [15].

Distributed randomization is similar to but is different from multi-sender decoupling [16] (see also Section 10 in [17]). In multi-sender decoupling, the goal is simply to destroy the correlation between $A_1 \cdots A_{[Z]}$ and W . In distributed randomization, we need not only to destroy the correlation between $A_1 \cdots A_{[Z]}$ and W but also to destroy the correlation among $A_1, \dots, A_{[Z]}$ and completely randomize these subsystems. Thus, distributed randomization costs more randomness than multi-sender decoupling in general. We remark that Ref. [18] considered distributed randomization that uses random projective measurements instead of random unitary operations (see Section 3.2.3 therein).

D. Properties of The Set Functions \hat{C} and \hat{D}

We describe properties of the set functions \hat{C} and \hat{D} , defined by (17) and (23), respectively. The properties will be used to prove the main results in Section IV, V and VI. We define

$$\check{D}(\Gamma)_\rho := 2 \sum_{z \in \Gamma} \log d_{A_z} - \hat{D}(\Gamma)_\rho \quad (24)$$

$$= \sum_{z \in \Gamma} \log d_{A_z} + S(A_\Gamma | W)_\rho. \quad (25)$$

Lemma 9 *The set functions $\hat{C}(\Gamma)_\rho$ and $\check{D}(\Gamma)_\rho$ are zero for the empty set, nonnegative, nondecreasing and strongly subadditive. I.e., for $f = \hat{C}, \check{D}$ and for any subsets $\Gamma, \Gamma', \Gamma'' \subseteq [Z]$ satisfying $\Gamma \subseteq \Gamma' \subseteq [Z]$, it holds that*

$$f(\emptyset)_\rho = 0, \quad (26)$$

$$f(\Gamma)_\rho \geq 0, \quad (27)$$

$$f(\Gamma)_\rho \leq f(\Gamma')_\rho, \quad (28)$$

$$f(\Gamma)_\rho + f(\Gamma'')_\rho \geq f(\Gamma \cup \Gamma'')_\rho + f(\Gamma \cap \Gamma'')_\rho. \quad (29)$$

Proof: Equality (26) immediately follows from the definitions of \hat{C} and \check{D} . Inequality (27) follows from the fact that the conditional entropy of a state $\varrho \in \mathcal{S}(\mathcal{H}^{AR})$ is bounded by the system dimension as $-\log d_A \leq S(A|R)_\varrho \leq \log d_A$. To prove (28) and (29), note that $A_{\bar{\Gamma}} A_{\bar{\Gamma}^c} = A_{[Z]}$ for any $\bar{\Gamma} \subseteq [Z]$. From the definition of the conditional entropy, we have

$$\begin{aligned} & S(A_{\Gamma'} | A_{\Gamma^c} V)_\rho - S(A_\Gamma | A_{\Gamma^c} V)_\rho \\ &= S(A_{\Gamma^c} V)_\rho - S(A_{\Gamma^c} V)_\rho \end{aligned} \quad (30)$$

$$= S(A_{\Gamma^c \setminus \Gamma'} | A_{\Gamma^c} V)_\rho \quad (31)$$

$$= S(A_{\Gamma' \setminus \Gamma} | A_{\Gamma^c} V)_\rho \quad (32)$$

$$\leq \sum_{z \in \Gamma' \setminus \Gamma} \log d_{A_z} \quad (33)$$

$$= \sum_{z \in \Gamma'} \log d_{A_z} - \sum_{z \in \Gamma} \log d_{A_z}, \quad (34)$$

which implies (28) for \hat{C} . In the same way, we have

$$\begin{aligned} & S(A_{\Gamma'} | W)_\rho - S(A_\Gamma | W)_\rho \\ &= S(A_{\Gamma'} W)_\rho - S(A_\Gamma W)_\rho \end{aligned} \quad (35)$$

$$= S(A_{\Gamma' \setminus \Gamma} | A_\Gamma W)_\rho \quad (36)$$

$$\geq - \sum_{z \in \Gamma' \setminus \Gamma} \log d_{A_z} \quad (37)$$

$$= \sum_{z \in \Gamma} \log d_{A_z} - \sum_{z \in \Gamma'} \log d_{A_z}, \quad (38)$$

which implies (28) for \check{D} . We also have

$$\begin{aligned} & \left(\hat{C}(\Gamma)_\rho + \hat{C}(\Gamma'')_\rho \right) - \left(\hat{C}(\Gamma \cup \Gamma'')_\rho + \hat{C}(\Gamma \cap \Gamma'')_\rho \right) \\ &= S(A_{\Gamma \cup \Gamma''} | A_{(\Gamma \cup \Gamma'')^c} V)_\rho + S(A_{\Gamma \cap \Gamma''} | A_{(\Gamma \cap \Gamma'')^c} V)_\rho \\ &\quad - S(A_\Gamma | A_{\Gamma^c} V)_\rho - S(A_{\Gamma''} | A_{\Gamma''^c} V)_\rho \end{aligned} \quad (39)$$

$$\begin{aligned} &= S(A_{\Gamma^c} V)_\rho + S(A_{\Gamma''^c} V)_\rho \\ &\quad - S(A_{\Gamma^c \cap \Gamma''^c} V)_\rho - S(A_{\Gamma^c \cup \Gamma''^c} V)_\rho. \end{aligned} \quad (40)$$

The last line is nonnegative due to the strong subadditivity of the von Neumann entropy, which implies (29) for \hat{C} . Similarly, we have

$$\begin{aligned} & S(A_\Gamma | W)_\rho + S(A_{\Gamma''} | W)_\rho \\ &= S(A_\Gamma W)_\rho + S(A_{\Gamma''} W)_\rho - 2S(W)_\rho \end{aligned} \quad (41)$$

$$\geq S(A_{\Gamma \cup \Gamma''} W)_\rho + S(A_{\Gamma \cap \Gamma''} W)_\rho - 2S(W)_\rho \quad (42)$$

$$= S(A_{\Gamma \cup \Gamma''} | W)_\rho + S(A_{\Gamma \cap \Gamma''} | W)_\rho, \quad (43)$$

which implies (29) for \check{D} . ■

The following corollary immediately follows from Lemma 9 and (24):

Corollary 10 *The set function $\hat{D}(\Gamma)_\rho$ is zero for the empty set and strongly superadditive, i.e., $\hat{D}(\emptyset) = 0$ and for any subsets $\Gamma, \Gamma' \subseteq [Z]$, it holds that*

$$\hat{D}(\Gamma)_\rho + \hat{D}(\Gamma')_\rho \leq \hat{D}(\Gamma \cup \Gamma')_\rho + \hat{D}(\Gamma \cap \Gamma')_\rho. \quad (44)$$

Due to Lemma 9, the extremal points of the regions defined by (16) and (22) are identified as follows:

Lemma 11 *The region defined by (16) is a polymatroid in \mathbb{R}^Z and every extremal point $(C_1^*, \dots, C_{[Z]}^*)$ is represented as*

$$C_{\sigma(z)}^* = \log d_{A_{\sigma(z)}} - S(A_{\sigma(z)} | A_{\sigma(1)} \cdots A_{\sigma(z-1)} V)_\rho, \quad (45)$$

where σ is a permutation on $[Z]$. Similarly, the region defined by (22) is a contrapolymatroid in \mathbb{R}^Z and every extremal point $(D_1^*, \dots, D_{[Z]}^*)$ is represented as

$$D_{\sigma(z)}^* = \log d_{A_{\sigma(z)}} - S(A_{\sigma(z)} | A_{\sigma(1)} \cdots A_{\sigma(z-1)} W)_\rho. \quad (46)$$

Proof: Due to Lemma 9 and the property of polymatroids (see Section 18.4 in [19]), the extremal points of the region defined by (16) are all points $(C_1^*, \dots, C_{[Z]}^*)$ that can be represented as

$$\begin{aligned} C_{\sigma(z)}^* &= \hat{C}(\{\sigma(z')\}_{z' \in [z]}) - \hat{C}(\{\sigma(z')\}_{z' \in [z-1]}) \\ &= \log d_{A_{\sigma(z)}} - S(A_{\sigma(z)} | A_{\sigma(z+1)} \cdots A_{\sigma(Z)} W)_\rho, \end{aligned} \quad (47)$$

where σ is a permutation on $[Z]$. Combining this with permutation of $[Z]$ in the inverse order, we obtain (45). In the same way, the set of all tuples $(\tilde{D}_1, \dots, \tilde{D}_Z) \in \mathbb{R}^Z$ that satisfy the condition $\sum_{z \in \Gamma} \tilde{D}_z \leq \check{D}(\Gamma)_\rho$ for any $\Gamma \in [Z]$ is a polymatroid, and all of its vertices $(\tilde{D}_1^*, \dots, \tilde{D}_{[Z]}^*)$ are given by

$$\begin{aligned} \tilde{D}_{\sigma(z)}^* &= \check{D}(\{\sigma(z')\}_{z' \in [z]}) - \check{D}(\{\sigma(z')\}_{z' \in [z-1]}) \quad (48) \\ &= \log d_{A_{\sigma(z)}} + S(A_{\sigma(z)} | A_{\sigma(1)} \cdots A_{\sigma(z-1)} W)_\rho \quad (49) \end{aligned}$$

for some permutation σ . Noting that \check{D} is defined by (24), the vertices of the region defined by (22) is represented as $D_{\sigma(z)}^* = 2 \log d_{A_{\sigma(z)}} - \tilde{D}_{\sigma(z)}^*$ and are equal to (46). ■

We remark that it is not possible to identify the extremal points of the region defined by (11) along the same argument as in Lemma 11. This is because the function $I(A_\Gamma : A_{\Gamma^c} B | E)_\rho$ is not a nondecreasing function of Γ , i.e., it does not satisfy the condition (28) in Lemma 9.

IV. PROOF OF THE MAIN THEOREM

In this section, we provide a proof of the main theorem (Theorem 2 in Section II). The proof of the converse part is based on a standard calculation of the entropies and the mutual informations. For the direct part, we invoke the direct part of the distributed encoding theorem and the distributed randomization theorem (Proposition 5 and Proposition 8).

A. Proof of The Converse Part

Suppose that a rate triplet (R_1, \dots, R_Z) is achievable for the state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \cdots A_Z B E})$. Fix arbitrary $\epsilon, \vartheta > 0$, choose sufficiently large n and let $M_z = 2^{nR_z}$ for each $z \in [Z]$. By definition, there exist a quantum system A'_z , a set of encoding CPTP maps $\mathfrak{E}_z \equiv \{\mathcal{E}_{z, m_z}\}_{m_z=1}^{M_z}$ from A_z^n to A'_z for each z and a measurement $\{\Lambda_{\mathbf{m}}\}_{\mathbf{m} \in \mathbf{M}}$ on $A'_1 \cdots A'_Z B^n E^n$ such that

$$1 - \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \text{Tr}[\rho_{\mathbf{m}} \Lambda_{\mathbf{m}}] \leq \epsilon \quad (50)$$

and

$$\frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \left\| \rho_{\mathbf{m}}^{A'_1 \cdots A'_Z E^n} - \bar{\rho}^{A'_1 \cdots A'_Z E^n} \right\|_1 \leq \vartheta, \quad (51)$$

where

$$\rho_{\mathbf{m}} := \left(\bigotimes_{z=1}^Z \mathcal{E}_{z, m_z}^{A_z^n \rightarrow A'_z} \right) (\rho^{\otimes n}) \quad (52)$$

and

$$\bar{\rho} := \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \rho_{\mathbf{m}}. \quad (53)$$

Fix an arbitrary subset $\Gamma \subseteq [Z]$. Let A'_Γ and A'_{Γ^c} denote the systems composed of $\{A'_z\}_{z \in \Gamma}$ and $\{A'_z\}_{z \in \Gamma^c}$, respectively. The set \mathbf{M} is divided into $\mathbf{M}_\Gamma \times \mathbf{M}_{\Gamma^c}$, where

$$\mathbf{M}_\Gamma := \times_{z \in \Gamma} [M_z], \quad \mathbf{M}_{\Gamma^c} := \times_{z \in \Gamma^c} [M_z]. \quad (54)$$

Correspondingly, each element $\mathbf{m} \in \mathbf{M}$ is represented as $\mathbf{m} = (\mathbf{m}_\Gamma, \mathbf{m}_{\Gamma^c})$ by $\mathbf{m}_\Gamma \in \mathbf{M}_\Gamma$ and $\mathbf{m}_{\Gamma^c} \in \mathbf{M}_{\Gamma^c}$. Let M_Γ and M_{Γ^c} be quantum systems with fixed orthonormal bases $\{|\mathbf{m}_\Gamma\rangle\}_{\mathbf{m}_\Gamma \in \mathbf{M}_\Gamma}$ and $\{|\mathbf{m}_{\Gamma^c}\rangle\}_{\mathbf{m}_{\Gamma^c} \in \mathbf{M}_{\Gamma^c}}$, respectively. We define CPTP maps $\mathcal{E}_{\Gamma, \mathbf{m}_\Gamma} : A_\Gamma^n \rightarrow A'_\Gamma$ and $\mathcal{E}_{\Gamma^c, \mathbf{m}_{\Gamma^c}} : A_{\Gamma^c}^n \rightarrow A'_{\Gamma^c}$ by

$$\mathcal{E}_{\Gamma, \mathbf{m}_\Gamma} := \bigotimes_{z \in \Gamma} \mathcal{E}_{z, m_z}, \quad \mathcal{E}_{\Gamma^c, \mathbf{m}_{\Gamma^c}} := \bigotimes_{z \in \Gamma^c} \mathcal{E}_{z, m_z}. \quad (55)$$

We also define $\tilde{\mathcal{E}}_\Gamma : A_\Gamma^n \rightarrow A'_\Gamma M_\Gamma$ and $\tilde{\mathcal{E}}_{\Gamma^c} : A_{\Gamma^c}^n \rightarrow A'_{\Gamma^c} M_{\Gamma^c}$ by

$$\begin{aligned} \tilde{\mathcal{E}}_\Gamma(\cdot) &:= \frac{1}{|\mathbf{M}_\Gamma|} \sum_{\mathbf{m}_\Gamma \in \mathbf{M}_\Gamma} |\mathbf{m}_\Gamma\rangle \langle \mathbf{m}_\Gamma|^{M_\Gamma} \otimes \mathcal{E}_{\Gamma, \mathbf{m}_\Gamma}(\cdot), \\ \tilde{\mathcal{E}}_{\Gamma^c}(\cdot) &:= \frac{1}{|\mathbf{M}_{\Gamma^c}|} \sum_{\mathbf{m}_{\Gamma^c} \in \mathbf{M}_{\Gamma^c}} |\mathbf{m}_{\Gamma^c}\rangle \langle \mathbf{m}_{\Gamma^c}|^{M_{\Gamma^c}} \otimes \mathcal{E}_{\Gamma^c, \mathbf{m}_{\Gamma^c}}(\cdot). \end{aligned}$$

The state after the encoding operation is represented by

$$\tilde{\rho} = \tilde{\mathcal{E}}_\Gamma \otimes \tilde{\mathcal{E}}_{\Gamma^c} (\rho^{\otimes n}). \quad (56)$$

It is straightforward to verify that

$$\bar{\rho} = \text{Tr}_{M_\Gamma M_{\Gamma^c}}[\tilde{\rho}], \quad \pi^{M_\Gamma M_{\Gamma^c}} = \text{Tr}_{A'_{[Z]} B^n E^n}[\tilde{\rho}]. \quad (57)$$

Noting that both $\tilde{\rho}$ and $\pi^{M_\Gamma M_{\Gamma^c}}$ are diagonal in $\{|\mathbf{m}_\Gamma\rangle\}$ and $\{|\mathbf{m}_{\Gamma^c}\rangle\}$, the secrecy condition (51) is equivalent to

$$\left\| \tilde{\rho}^{M_\Gamma M_{\Gamma^c} A'_\Gamma A'_{\Gamma^c} E^n} - \pi^{M_\Gamma M_{\Gamma^c}} \otimes \bar{\rho}^{A'_\Gamma A'_{\Gamma^c} E^n} \right\|_1 \leq \vartheta. \quad (58)$$

Tracing out $M_{\Gamma^c} A'_{\Gamma^c}$, we obtain

$$\left\| \tilde{\rho}^{M_\Gamma A'_\Gamma E^n} - \pi^{M_\Gamma} \otimes \bar{\rho}^{A'_\Gamma E^n} \right\|_1 \leq \vartheta. \quad (59)$$

We calculate the entropies and the mutual informations of $\tilde{\rho}$ along the same line of Appendix C in [10]. First, let M'_Γ be the system to which the Γ part of the decoding result is registered. Due to the reliability

condition (50) and Fano's inequality (see e.g. Theorem 2.10.1 in [20]), we have

$$\begin{aligned} I(M_\Gamma : M'_\Gamma) &= S(M_\Gamma) - S(M_\Gamma | M'_\Gamma) \\ &\geq (1 - \epsilon) \log |\mathbf{M}_\Gamma| - h(\epsilon) \end{aligned} \quad (60)$$

$$= n(1 - \epsilon) \sum_{z \in \Gamma} R_z - h(\epsilon). \quad (61)$$

Second, from (57), (59) and the Alicki-Fannes inequality ([21]: see [22] for an improved version), we obtain

$$\begin{aligned} I(M_\Gamma : A'_\Gamma E^n)_{\tilde{\rho}} &= S(M_\Gamma)_\pi - S(M_\Gamma | A'_\Gamma E^n)_{\tilde{\rho}} \end{aligned} \quad (62)$$

$$= S(M_\Gamma | A'_\Gamma E^n)_{\pi \otimes \tilde{\rho}} - S(M_\Gamma | A'_\Gamma E^n)_{\tilde{\rho}} \quad (63)$$

$$\leq 2\vartheta \log d_{M_\Gamma} + (1 + \vartheta)h\left(\frac{\vartheta}{1 + \vartheta}\right) \quad (64)$$

$$= 2n\vartheta \sum_{z \in \Gamma} R_z + (1 + \vartheta)h\left(\frac{\vartheta}{1 + \vartheta}\right). \quad (65)$$

Third, we have

$$I(M_\Gamma : M'_\Gamma) - I(M_\Gamma : A'_\Gamma E^n)_{\tilde{\rho}} \quad (66)$$

$$\leq I(M_\Gamma : A'_\Gamma A'_{\Gamma_c} B^n E^n)_{\tilde{\rho}} - I(M_\Gamma : A'_\Gamma E^n)_{\tilde{\rho}} \quad (67)$$

$$= I(M_\Gamma : A'_{\Gamma_c} B^n | A'_\Gamma E^n)_{\tilde{\rho}} \quad (68)$$

$$\leq I(M_\Gamma : A'_{\Gamma_c} B^n | A'_\Gamma E^n)_{\tilde{\mathcal{E}}_\Gamma(\rho^{\otimes n})} \quad (69)$$

$$= \sum_{i=1}^n I(M_\Gamma : A_{\Gamma_c, i} B_i | A'_\Gamma A_{\Gamma_c}^{i-1} B^{i-1} E^n)_{\tilde{\mathcal{E}}_\Gamma(\rho^{\otimes n})} \quad (70)$$

$$\begin{aligned} &= \sum_{i=1}^n \left[I(M_\Gamma A'_\Gamma A_{\Gamma_c}^{i-1} B^{i-1} E^n_{\setminus i} : A_{\Gamma_c, i} B_i | E_i)_{\tilde{\mathcal{E}}_\Gamma(\rho^{\otimes n})} \right. \\ &\quad \left. - I(A'_\Gamma A_{\Gamma_c}^{i-1} B^{i-1} E^n_{\setminus i} : A_{\Gamma_c, i} B_i | E_i)_{\tilde{\mathcal{E}}_\Gamma(\rho^{\otimes n})} \right] \end{aligned} \quad (71)$$

$$\leq \sum_{i=1}^n I(M_\Gamma A'_\Gamma A_{\Gamma_c}^{i-1} B^{i-1} E^n_{\setminus i} : A_{\Gamma_c, i} B_i | E_i)_{\tilde{\mathcal{E}}_\Gamma(\rho^{\otimes n})} \quad (72)$$

$$\leq \sum_{i=1}^n I(A_{\Gamma_c}^n A_{\Gamma_c}^{i-1} B^{i-1} E^n_{\setminus i} : A_{\Gamma_c, i} B_i | E_i)_{\rho^{\otimes n}} \quad (73)$$

$$= \sum_{i=1}^n I(A_{\Gamma_c, i} : A_{\Gamma_c, i} B_i | E_i)_{\rho^{\otimes n}} \quad (74)$$

$$= nI(A_\Gamma : A_{\Gamma_c} B | E)_\rho. \quad (75)$$

Here, (67) follows from the data processing inequality of the mutual information and the fact that M'_Γ is obtained by performing a measurement on $A'_\Gamma A'_{\Gamma_c} B^n E^n$; (68) due to the chain rule of the mutual information; (69) from (56) and the data processing inequality; (70) from the chain rule of the mutual information, where $A_{\Gamma_c}^{i-1}$ and B^{i-1} denotes the systems $A_{\Gamma_c, 1} \cdots A_{\Gamma_c, i-1}$ and $B_1 \cdots B_{i-1}$, respectively; (71) due to the chain rule of the mutual information, where $E^n_{\setminus i}$ denotes $E_1 \cdots E_{i-1} E_{i+1} \cdots E_n$; (72) from the non-negativity of

the conditional mutual information; (73) from the data processing inequality; (74) because $\rho^{\otimes n}$ is a product state between $A_{\Gamma_c, i} A_{\Gamma_c, i} B_i E_i$ and the other systems; and (75) because the state on $A_{\Gamma_c, i} A_{\Gamma_c, i} B_i E_i$ is ρ for each i . Substituting (61) and (65) into (66), we obtain

$$\begin{aligned} &n(1 - \epsilon - 2\vartheta) \sum_{z \in \Gamma} R_z \\ &\leq nI(A_\Gamma : A_{\Gamma_c} B | E)_\rho + h(\epsilon) + (1 + \vartheta)h\left(\frac{\vartheta}{1 + \vartheta}\right). \end{aligned} \quad (76)$$

Since this relation holds for any $\epsilon, \vartheta > 0$ and sufficiently large n , we arrive at

$$\sum_{z \in \Gamma} R_z \leq I(A_\Gamma : A_{\Gamma_c} B | E)_\rho. \quad (77)$$

Noting that the above inequality holds for any $\Gamma \subseteq [Z]$, we complete the proof of the converse part. \blacksquare

B. Proof of The Direct Part

We apply the distributed encoding theorem (Proposition 5) and the distributed randomization theorem (Proposition 8) under the correspondence $V \rightarrow BE$ and $W \rightarrow E$. Recall that $\hat{C}(\Gamma)_\rho$ and $\hat{D}(\Gamma)_\rho$ are defined by (17) and (23), respectively, which yields

$$\hat{C}(\Gamma)_\rho = \sum_{z \in \Gamma} \log d_{A_z} - S(A_\Gamma | A_{\Gamma_c} B E)_\rho, \quad (78)$$

$$\hat{D}(\Gamma)_\rho = \sum_{z \in \Gamma} \log d_{A_z} - S(A_\Gamma | E)_\rho. \quad (79)$$

It is straightforward to verify that

$$\hat{C}(\Gamma)_\rho - \hat{D}(\Gamma)_\rho = I(A_\Gamma : A_{\Gamma_c} B | E)_\rho. \quad (80)$$

Thus, the condition (11) is equivalent to

$$\sum_{z \in \Gamma} R_z \leq \hat{C}(\Gamma)_\rho - \hat{D}(\Gamma)_\rho. \quad (81)$$

We prove the direct part of Theorem 2 based on the following lemma:

Lemma 12 *For any rate tuple (R_1, \dots, R_Z) that satisfies the condition*

$$\sum_{z \in \Gamma} R_z < \hat{C}(\Gamma)_\rho - \hat{D}(\Gamma)_\rho, \quad (82)$$

there exists a pair of rate tuples (C_1, \dots, C_Z) and (D_1, \dots, D_Z) that satisfy

$$\sum_{z \in \Gamma} C_z < \hat{C}(\Gamma)_\rho, \quad \sum_{z \in \Gamma} D_z > \hat{D}(\Gamma)_\rho, \quad (83)$$

respectively, for any $\Gamma \in [Z]$, and it holds that

$$R_z = C_z - D_z \quad (84)$$

for all $z \in [Z]$.

A proof of Lemma 12 will be provided at the end of this subsection.

To prove the direct part of Theorem 2, let (R_1, \dots, R_Z) be an arbitrary rate tuple that satisfies the condition (82). Fix a pair of rate tuples (C_1, \dots, C_Z) and (D_1, \dots, D_Z) that satisfy (83) and (84). Fix arbitrary $\epsilon, \vartheta, \xi > 0$ and choose sufficiently large n . Let $K_z \equiv 2^{nC_z}$, $L_z \equiv 2^{nD_z}$ and $M_z \equiv 2^{nR_z}$ for each z . Note that $K_z = L_z M_z$. Let $U_{z,k_z,i} \in \mathcal{U}(\mathcal{H}^{A_z})$ for $i \in [n]$ and $U_{z,k_z} := \bigotimes_{i=1}^n U_{z,k_z,i}$. We let $A'_z = A_z^n$ and construct the encoding operation $\{\mathcal{E}_{z,m_z}\}_{m_z=1}^{M_z}$ by

$$\mathcal{E}_{z,m_z}(\cdot) = \frac{1}{L_z} \sum_{k_z=(m_z-1)L_z+1}^{m_z L_z} U_{z,k_z}(\cdot) U_{z,k_z}^\dagger. \quad (85)$$

In the following, we prove that if we choose $U_{z,k_z,i}$ randomly and independently according to the Haar measure for each $i \in [n]$, $k_z \in [K_z]$ and $z \in [Z]$, the set of encoding operations constructed as (85) satisfies both the reliability condition and the secrecy condition with a probability greater than $1 - 2\xi$. Recall that the state after the encoding operation corresponding to the message value \mathbf{m} is given by

$$\rho_{\mathbf{m}} := \left(\bigotimes_{z=1}^Z \mathcal{E}_{z,m_z}^{A_z^n} \right) (\rho^{\otimes n}). \quad (86)$$

To prove the reliability condition, define $U_{\mathbf{k}} = \bigotimes_{z=1}^Z U_{z,k_z}$ and $\rho_{\mathbf{k}} := (U_{\mathbf{k}} \otimes I^{B^n E^n}) \rho^{\otimes n} (U_{\mathbf{k}} \otimes I^{B^n E^n})^\dagger$ for $\mathbf{k} \equiv (k_1, \dots, k_Z)$. Due to the distributed encoding theorem (Proposition 5), with probability no smaller than $1 - \xi$, there exists a measurement $\{\Lambda_{\mathbf{k}}\}_{\mathbf{k} \in \mathbf{K}}$ on $A_1^n \dots A_Z^n B^n E^n$ and it holds that

$$1 - \frac{1}{|\mathbf{K}|} \sum_{\mathbf{k} \in \mathbf{K}} \text{Tr}[\rho_{\mathbf{k}} \Lambda_{\mathbf{k}}] \leq \epsilon. \quad (87)$$

We construct the decoding measurement by

$$\Lambda_{\mathbf{m}} := \sum_{k_1=(m_1-1)L_1+1}^{m_1 L_1} \cdots \sum_{k_Z=(m_Z-1)L_Z+1}^{m_Z L_Z} \Lambda_{\mathbf{k}}. \quad (88)$$

It is straightforward to verify that

$$\frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \Lambda_{\mathbf{m}} = \frac{1}{|\mathbf{K}|} \sum_{\mathbf{k} \in \mathbf{K}} \Lambda_{\mathbf{k}} = I, \quad (89)$$

thus $\{\Lambda_{\mathbf{m}}\}_{\mathbf{m} \in \mathbf{M}}$ is indeed a POVM. Noting that $\rho_{\mathbf{m}}$ in (86) is calculated to be

$$\rho_{\mathbf{m}} = \frac{1}{L_1 \cdots L_Z} \sum_{k_1=(m_1-1)L_1+1}^{m_1 L_1} \cdots \sum_{k_Z=(m_Z-1)L_Z+1}^{m_Z L_Z} \rho_{\mathbf{k}}, \quad (90)$$

we have

$$\begin{aligned} & \text{Tr}[\rho_{\mathbf{m}} \Lambda_{\mathbf{m}}] \\ & \geq \frac{1}{L_1 \cdots L_Z} \sum_{k_1=(m_1-1)L_1+1}^{m_1 L_1} \cdots \sum_{k_Z=(m_Z-1)L_Z+1}^{m_Z L_Z} \text{Tr}[\rho_{\mathbf{k}} \Lambda_{\mathbf{k}}]. \end{aligned} \quad (91)$$

Thus

$$\frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \text{Tr}[\rho_{\mathbf{m}} \Lambda_{\mathbf{m}}] \geq \frac{1}{|\mathbf{K}|} \sum_{\mathbf{k} \in \mathbf{K}} \text{Tr}[\rho_{\mathbf{k}} \Lambda_{\mathbf{k}}] \geq 1 - \epsilon, \quad (92)$$

which implies the reliability condition.

To prove the secrecy condition, we evaluate the information leakage as

$$\begin{aligned} & \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \left\| \rho_{\mathbf{m}}^{A_{[Z]}^n E^n} - \bar{\rho}^{A_{[Z]}^n E^n} \right\|_1 \\ & \leq \frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \left\| \rho_{\mathbf{m}}^{A_{[Z]}^n E^n} - \pi^{A_{[Z]}^n} \otimes \bar{\rho}^{E^n} \right\|_1 \\ & \quad + \left\| \bar{\rho}^{A_{[Z]}^n E^n} - \pi^{A_{[Z]}^n} \otimes \bar{\rho}^{E^n} \right\|_1 \end{aligned} \quad (93)$$

$$\leq \frac{2}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \left\| \rho_{\mathbf{m}}^{A_{[Z]}^n E^n} - \pi^{A_{[Z]}^n} \otimes \bar{\rho}^{E^n} \right\|_1, \quad (94)$$

where (93) follows from the triangle inequality and (94) from the convexity of the trace distance. Hence, by the distributed randomization theorem (Proposition 8), we have

$$\frac{1}{|\mathbf{M}|} \sum_{\mathbf{m} \in \mathbf{M}} \left\| \rho_{\mathbf{m}}^{A_{[Z]}^n E^n} - \bar{\rho}^{A_{[Z]}^n E^n} \right\|_1 \leq 2\vartheta \quad (95)$$

with a probability no smaller than $1 - \xi$.

In total, with a probability no smaller than $(1 - \xi)^2 > 1 - 2\xi$, the reliability condition and the secrecy condition are both satisfied. Since this relation holds for any $\epsilon, \vartheta, \xi > 0$ and sufficiently large n , we conclude that any rate tuple satisfying the condition (82) is achievable. Taking the closure of the region defined by (82), we obtain (81) and complete the proof of the direct part. ■

It remains to prove Lemma 12. Let S be a finite set. A function $f : 2^S \rightarrow \mathbb{R}$ is said to be a *submodular function* if it holds that

$$f(A) + f(B) \geq f(A \cup B) + f(A \cap B) \quad (96)$$

for any $A, B \subseteq S$. A function $g : 2^S \rightarrow \mathbb{R}$ is said to be a *supermodular function* if $-g$ is submodular. We prove Lemma 12 based on the following lemma:

Lemma 13 *Let $f : 2^S \rightarrow \mathbb{R}$ a submodular function and $g : 2^S \rightarrow \mathbb{R}$ be a supermodular function such that*

$$f(\emptyset) = g(\emptyset) = 0, \quad (97)$$

$$g(A) \leq f(A) \quad (\forall A \subseteq S, A \neq \emptyset). \quad (98)$$

There exists $\{R_s\}_{s \in S}$ such that

$$g(A) \leq \sum_{s \in A} R_s \leq f(A) \quad (99)$$

for any $A \subseteq S$ satisfying $A \neq \emptyset$. If the condition (98) is strict inequalities, both inequalities in (99) can be strict inequalities.

Proof: The former statement was proved in Section 4 of [23]. To prove the latter statement, suppose that $g(A) < f(A)$ for any $A \subseteq S$ such that $A \neq \emptyset$. Let

$$\Delta := \min_{A \subseteq S, A \neq \emptyset} \frac{1}{2|A|} (f(A) - g(A)) \quad (100)$$

and define $f', g' : 2^S \rightarrow \mathbb{R}$ by

$$f'(A) = f(A) - |A|\Delta, \quad g'(A) = g(A) + |A|\Delta. \quad (101)$$

Applying the former statement to f' and g' , we complete the proof. ■

Proof of Lemma 12: Due to Lemma 9 and Corollary 10, the set functions $\hat{C}(\Gamma)_\rho - \sum_{z \in \Gamma} R_z$ and $\hat{D}(\Gamma)_\rho$ are submodular and supermodular, respectively, and are equal to zero for $\Gamma = \emptyset$. From (82), we have $\hat{D}(\Gamma)_\rho < \hat{C}(\Gamma)_\rho - \sum_{z \in \Gamma} R_z$. Hence, due to Lemma 13, there exists $\{D_z\}_{z \in [Z]}$ such that $\hat{D}(\Gamma)_\rho < \sum_{z \in \Gamma} D_z < \hat{C}(\Gamma)_\rho - \sum_{z \in \Gamma} R_z$ for any nonempty $\Gamma \subseteq [Z]$. Letting $C_z = D_z + R_z$ completes the proof. We remark that the same argument was used in [24] to prove the achievability of the private classical capacity of a classical-quantum multiple-access channel (see Inequality (19) therein). ■

V. PROOF OF PROPOSITION 5

In this section, we prove the distributed encoding theorem (Proposition 5). We will use the same notations as in Section III-A.

A. Proof of The Converse Part

Suppose that a triplet (C_1, \dots, C_Z) is achievable for distributed encoding on the state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z V})$. Fix arbitrary $\epsilon > 0$, choose sufficiently large n and let $K_z = 2^{nC_z}$. By definition, there exist a set of unitaries $\mathcal{U}_z \equiv \{U_{z, k_z}\}_{k_z=1}^{K_z}$ on A_z^n for each z and a measurement $\{\Lambda_{\mathbf{k}}\}_{\mathbf{k} \in \mathbf{K}}$ on $A_{[Z]}^n V^n$ such that

$$1 - \frac{1}{|\mathbf{K}|} \sum_{\mathbf{k} \in \mathbf{K}} \text{Tr}[\rho_{\mathbf{k}} \Lambda_{\mathbf{k}}] \leq \epsilon, \quad (102)$$

where $\rho_{\mathbf{k}} := (U_{\mathbf{k}} \otimes I^{V^n}) \rho^{\otimes n} (U_{\mathbf{k}} \otimes I^{V^n})^\dagger$ and $U_{\mathbf{k}} := \bigotimes_{z=1}^Z U_{z, k_z}$.

Let $\Gamma \in [Z]$ be any subset. The set \mathbf{K} is represented as $\mathbf{K}_\Gamma \times \mathbf{K}_{\Gamma^c}$, where $\mathbf{K}_\Gamma := \times_{z \in \Gamma} [K_z]$, $\mathbf{K}_{\Gamma^c} := \times_{z \in \Gamma^c} [K_z]$.

Each element $\mathbf{k} \in \mathbf{K}$ is written as $\mathbf{k} = (\mathbf{k}_\Gamma, \mathbf{k}_{\Gamma^c})$ by $\mathbf{k}_\Gamma \in \mathbf{K}_\Gamma$ and $\mathbf{k}_{\Gamma^c} \in \mathbf{K}_{\Gamma^c}$. We define $U_{\mathbf{k}_\Gamma} := \bigotimes_{z \in \Gamma} U_{z, k_z}$ and $U_{\mathbf{k}_{\Gamma^c}} := \bigotimes_{z \in \Gamma^c} U_{z, k_z}$, by which $U_{\mathbf{k}}$ is represented as $U_{\mathbf{k}_\Gamma}^{A_\Gamma} \otimes U_{\mathbf{k}_{\Gamma^c}}^{A_{\Gamma^c}}$ and $\rho_{\mathbf{k}}$ as $\rho_{\mathbf{k}_\Gamma, \mathbf{k}_{\Gamma^c}}$. It is straightforward to verify that

$$\begin{aligned} \text{Tr}_{A_\Gamma^n} [\rho_{\mathbf{k}_\Gamma, \mathbf{k}_{\Gamma^c}}] &= \rho_{\mathbf{k}_{\Gamma^c}}^{A_{\Gamma^c}^n V^n} \\ &:= (U_{\mathbf{k}_{\Gamma^c}}^{A_{\Gamma^c}} \otimes I^{V^n}) (\rho^{A_{\Gamma^c} V})^{\otimes n} (U_{\mathbf{k}_{\Gamma^c}}^{A_{\Gamma^c}} \otimes I^{V^n})^\dagger. \end{aligned} \quad (103)$$

Let K_Γ and K_{Γ^c} be the systems with fixed orthonormal bases $\{|\mathbf{k}_\Gamma\rangle\}_{\mathbf{k}_\Gamma}$ and $\{|\mathbf{k}_{\Gamma^c}\rangle\}_{\mathbf{k}_{\Gamma^c}}$, respectively. The state after the encoding operation is represented by

$$\tilde{\rho} = \frac{1}{|\mathbf{K}|} \sum_{\mathbf{k}_\Gamma, \mathbf{k}_{\Gamma^c}} |\mathbf{k}_\Gamma\rangle\langle\mathbf{k}_\Gamma|^{K_\Gamma} \otimes |\mathbf{k}_{\Gamma^c}\rangle\langle\mathbf{k}_{\Gamma^c}|^{K_{\Gamma^c}} \otimes \rho_{\mathbf{k}_\Gamma, \mathbf{k}_{\Gamma^c}}. \quad (104)$$

Using (103), it is straightforward to verify that

$$\text{Tr}_{K_\Gamma A_\Gamma^n} [\tilde{\rho}] = \frac{1}{|\mathbf{K}_{\Gamma^c}|} \sum_{\mathbf{k}_{\Gamma^c}} |\mathbf{k}_{\Gamma^c}\rangle\langle\mathbf{k}_{\Gamma^c}|^{K_{\Gamma^c}} \otimes \rho_{\mathbf{k}_{\Gamma^c}}^{A_{\Gamma^c}^n V^n}. \quad (105)$$

To prove the converse part, we calculate the conditional entropies of $\tilde{\rho}$. We have

$$S(K_\Gamma | A_{[Z]}^n V^n)_{\tilde{\rho}} \quad (106)$$

$$\geq S(K_\Gamma | A_{[Z]}^n V^n K_{\Gamma^c})_{\tilde{\rho}} \quad (107)$$

$$\begin{aligned} &= S(K_\Gamma K_{\Gamma^c})_{\tilde{\rho}} + S(A_{[Z]}^n V^n | K_\Gamma K_{\Gamma^c})_{\tilde{\rho}} \\ &\quad - S(A_{[Z]}^n V^n K_{\Gamma^c})_{\tilde{\rho}} \end{aligned} \quad (108)$$

$$\begin{aligned} &\geq S(K_\Gamma K_{\Gamma^c})_{\tilde{\rho}} + S(A_{[Z]}^n V^n | K_\Gamma K_{\Gamma^c})_{\tilde{\rho}} + S(K_{\Gamma^c})_{\tilde{\rho}} \\ &\quad - S(A_{\Gamma^c}^n V^n K_{\Gamma^c})_{\tilde{\rho}} - S(A_{\Gamma^c}^n K_{\Gamma^c})_{\tilde{\rho}} \end{aligned} \quad (109)$$

$$\begin{aligned} &= S(K_\Gamma | K_{\Gamma^c})_{\tilde{\rho}} + S(A_{[Z]}^n V^n | K_{[Z]})_{\tilde{\rho}} \\ &\quad - S(A_{\Gamma^c}^n V^n | K_{\Gamma^c})_{\tilde{\rho}} - S(A_{\Gamma^c}^n | K_{\Gamma^c})_{\tilde{\rho}}, \end{aligned} \quad (110)$$

where (107) follows from the data processing inequality; (108) from the chain rule; (109) from the strong subadditivity and $A_\Gamma A_{\Gamma^c} = A_{[Z]}$; and (110) from the definition of the conditional entropy and $K_\Gamma K_{\Gamma^c} = K_{[Z]}$. Noting that K_{Γ^c} is uncorrelated with K_Γ , the first term in (110) is evaluated as

$$S(K_\Gamma | K_{\Gamma^c})_{\tilde{\rho}} = S(K_\Gamma)_{\tilde{\rho}} = \sum_{z \in \Gamma} \log K_z = n \sum_{z \in \Gamma} C_z. \quad (111)$$

The fourth term is bounded by the system dimension as

$$S(A_{\Gamma^c}^n | K_{\Gamma^c})_{\tilde{\rho}} \leq \log d_{A_{\Gamma^c}^n} = n \sum_{z \in \Gamma^c} \log d_{A_z}. \quad (112)$$

Due to (104) and the unitary invariance of the von Neumann entropy, the second term in (110) is evaluated to be

$$S(A_{[Z]}^n V^n | K_{[Z]})_{\tilde{\rho}} = \frac{1}{|\mathbf{K}|} \sum_{\mathbf{k} \in \mathbf{K}} S(\rho_{\mathbf{k}}^{A_{[Z]}^n V^n}) \quad (113)$$

$$= S((\rho^{A_{[Z]} V})^{\otimes n}) = n S(A_{[Z]} V)_\rho. \quad (114)$$

Similarly, due to (105) we have

$$S(A_{\Gamma_c}^n V^n | K_{\Gamma_c})_{\bar{\rho}} = \frac{1}{|\mathbf{K}_{\Gamma_c}|} \sum_{\mathbf{k}_{\Gamma_c} \in \mathbf{K}_{\Gamma_c}} S\left(\rho_{\mathbf{k}_{\Gamma_c}}^{A_{\Gamma_c}^n V^n}\right) \quad (115)$$

$$= S((\rho^{A_{\Gamma_c} V})^{\otimes n}) = nS(A_{\Gamma_c} V)_{\rho}. \quad (116)$$

Let K_{Γ}' be the system to which the Γ part of the decoding result is recorded. Since K_{Γ}' is obtained as a result of a measurement on $A_{[Z]}^n V^n$, the data processing inequality yields

$$S(K_{\Gamma} | K_{\Gamma}') \geq S(K_{\Gamma} | A_{[Z]}^n V^n)_{\bar{\rho}}. \quad (117)$$

Furthermore, due to the condition (102) and Fano's inequality (see e.g. Theorem 2.10.1 in [20]), we have

$$\begin{aligned} S(K_{\Gamma} | K_{\Gamma}') &\leq \epsilon \log |\mathbf{K}_{\Gamma}| + h(\epsilon) \\ &= n\epsilon \sum_{z \in \Gamma} C_z + h(\epsilon). \end{aligned} \quad (118)$$

We substitute (111), (112), (114) and (116) all into (109), and (117) and (118) into (106). Noting that $S(A_{[Z]} V)_{\rho} - S(A_{\Gamma_c} V)_{\rho} = S(A_{\Gamma} | A_{\Gamma_c} V)_{\rho}$, we obtain

$$\begin{aligned} n(1 - \epsilon) \sum_{z \in \Gamma} C_z \\ \leq n \left(\sum_{z \in \Gamma} \log d_{A_z} - S(A_{\Gamma} | A_{\Gamma_c} V)_{\rho} \right) + h(\epsilon). \end{aligned} \quad (119)$$

Since this relation holds for any $\epsilon > 0$ and any sufficiently large n , we arrive at

$$\sum_{z \in \Gamma} C_z \leq \sum_{z \in \Gamma} \log d_{A_z} - S(A_{\Gamma} | A_{\Gamma_c} V)_{\rho}. \quad (120)$$

Noting that the above inequality holds for any $\Gamma \subseteq [Z]$, we complete the proof of the converse part. ■

B. Proof of The Direct Part

Recall that the region defined by (16) is a polymatroid in \mathbb{R}^Z and every extremal point $(C_1^*, \dots, C_{[Z]}^*)$ is represented as

$$C_{\sigma(z)}^* = \log d_{A_{\sigma(z)}} - S(A_{\sigma(z)} | A_{\sigma(1)} \cdots A_{\sigma(z-1)} V)_{\rho}, \quad (121)$$

where σ is a permutation on $[Z]$ (see Lemma 11). Due to the time-sharing scheme, it suffices to prove that all these extremal points are in the achievable rate region. Without loss of generality, it suffices to prove that a rate tuple $(C_1, \dots, C_{[Z]})$ is achievable if

$$C_z < \log d_{A_z} - S(A_z | A_1 \cdots A_{z-1} V)_{\rho} \quad (122)$$

for all $z \in [Z]$. The proof is based on the following two lemmas:

Lemma 14 *Let A and Q be finite-dimensional quantum systems represented by Hilbert spaces \mathcal{H}^A and \mathcal{H}^Q , respectively, and let $\rho \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^Q)$ be a quantum state thereon. Fix arbitrary $C < \log d_A - S(A|Q)_{\rho}$, $\epsilon, \xi > 0$ and choose sufficiently large $n \in \mathbb{N}$. Let $U_{k,i}$ be unitaries on \mathcal{H}^A that are chosen independently and randomly according to the Haar measure for each $i \in [n]$ and $k \in [2^{nC}]$, and $U_k := \bigotimes_{i=1}^n U_{k,i}$. Then, with probability no smaller than $1 - \xi$, there exists a POVM $\{\Lambda_k\}_{k=1}^{2^{nC}}$ on $A^n Q^n$ and it holds that*

$$1 - \frac{1}{2^{nC}} \sum_{k=1}^{2^{nC}} \text{Tr}[\Lambda_k (U_k^{A^n} \otimes I^{Q^n}) \rho^{\otimes n} (U_k^{A^n} \otimes I^{Q^n})^\dagger] \leq \epsilon. \quad (123)$$

Lemma 15 *Let S be a finite-dimensional quantum system and let $\Lambda_1, \dots, \Lambda_J$ be any sequence of positive semidefinite operators on \mathcal{H}^S such that $0 \leq \Lambda_j \leq I$. Let M_j be a qubit system for each $1 \leq j \leq J$ and define a linear operator $\Pi_{\Lambda_j} : \mathcal{H}^S \rightarrow \mathcal{H}^S \otimes \mathcal{H}^{M_j}$ by $\Pi_{\Lambda_j} := \Lambda_j \otimes |0\rangle + \sqrt{\Lambda_j} \sqrt{I - \Lambda_j} \otimes |1\rangle$. For any subnormalized state $\varrho \in \mathcal{S}(\mathcal{H}^S)$, it holds that*

$$\text{Tr}[\varrho] - \text{Tr}[\hat{\Pi} \varrho \hat{\Pi}^\dagger] \leq 2 \sqrt{\sum_{i=1}^J \text{Tr}[(I - \Lambda_j) \varrho]}, \quad (124)$$

where $\hat{\Pi} := \Pi_{\Lambda_J} \cdots \Pi_{\Lambda_1}$. In addition, we have $\text{Tr}[\hat{\Pi} \varrho \hat{\Pi}^\dagger] = \text{Tr}[\hat{\Lambda} \varrho]$, where

$$\hat{\Lambda} := \sum_{x_1, \dots, x_J=0,1} \Lambda_1^{(x_1)} \cdots \Lambda_J^{(x_J)} \cdot \Lambda_J^{(x_J)} \cdots \Lambda_1^{(x_1)} \quad (125)$$

and $\Lambda_j^{(0)} = \Lambda_j$, $\Lambda_j^{(1)} = \sqrt{\Lambda_j} \sqrt{I - \Lambda_j}$.

A proof of Lemma 14 will be provided in Section VII. The former half of Lemma 15 was proved in Section 3 of [25] based on the non-commutative union bound for projective measurements [26]. The latter half follows by a straightforward calculation.

To prove the achievability of the rate tuple satisfying the condition (122), we invoke the notion of successive decoding which has been used e.g. in the achievability proof of the classical capacity of a classical-quantum multiple access channel [27]: The receiver first decodes M_1 by performing a measurement on $A_1^n V^n$. The measurement does not much change the state of the whole system as long as the error probability in decoding M_1 is sufficiently small. The receiver then performs U_{1,m_1}^\dagger on A_1^n to reverse the encoding operation by Sender 1. In the second step, the receiver decodes M_2 by performing a measurement on $A_1^n A_2^n V^n$. Since the encoding operation on A_1^n has already been cancelled, in this step, $A_1^n V^n$ plays the same role as that of V^n in the first step.

This time, the receiver then performs U_{2,m_2}^\dagger on A_2^n to reverse the encoding operation by Sender 2. Repeating this procedure Z times, the receiver can decode all of the messages M_1, \dots, M_Z within a small error.

To be more precise, fix arbitrary $\epsilon > 0$, arbitrary rate tuple (C_1, \dots, C_Z) satisfying the condition (122) and choose sufficiently large n . For each $z \in [Z]$, we apply Lemma 14 under the following correspondence:

$$A \rightarrow A_z, \quad Q \rightarrow A_1 \cdots A_{z-1} V. \quad (126)$$

Let $U_{z,k_z,i}$ be unitaries on \mathcal{H}^{A_z} that are chosen independently and randomly according to the Haar measure for $i \in [n]$, $k_z \in 2^{c_z}$ and $z \in [Z]$, and let $U_{z,k_z} := \bigotimes_{i=1}^n U_{z,k_z,i}$. Let $I_{z,k_z}^{A_z}$ be the identity operator on $(\bigotimes_{z'=1}^{z-1} \mathcal{H}^{A_{z'}})^{\otimes n}$, and define

$$\rho_{z,k_z} := (U_{z,k_z} \otimes I_{z,k_z}^{A_z}) (\rho^{A_{[z]} V})^{\otimes n} (U_{z,k_z} \otimes I_{z,k_z}^{A_z})^\dagger, \quad (127)$$

It follows that, for any z and with a probability no smaller than $1 - \xi$, there exists a POVM $\{\Lambda_{z,k_z}\}_{k_z=1}^{2^{n c_z}}$ on $A_{[z]}^n V^n$ that satisfies

$$1 - \frac{1}{2^{n C_z}} \sum_{k_z=1}^{2^{n C_z}} \text{Tr}[\Lambda_{z,k_z} \rho_{z,k_z}] \leq \epsilon. \quad (128)$$

Thus, with a probability no smaller than $(1 - \xi)^Z \geq 1 - Z\xi$, there exist POVMs $\{\Lambda_{z,k_z}\}_{k_z=1}^{2^{n c_z}}$ satisfying (128) for every $z \in [Z]$.

We construct a decoding measurement $\{\Lambda_{\mathbf{k}}\}_{\mathbf{k} \in \mathbf{K}}$ from $\{U_{z,k_z}\}_{k_z=1}^{2^{n c_z}}$ and $\{\Lambda_{z,k_z}\}_{k_z=1}^{2^{n c_z}}$ as follows. First, define

$$\Upsilon_{z,k_z} := (U_{z,k_z} \otimes I_{z,k_z}^{A_z})^\dagger \sqrt{\Lambda_{z,k_z}} (U_{z,k_z} \otimes I_{z,k_z}^{A_z}). \quad (129)$$

It follows that

$$(\Upsilon_{z,k_z})^2 := (U_{z,k_z} \otimes I_{z,k_z}^{A_z})^\dagger \Lambda_{z,k_z} (U_{z,k_z} \otimes I_{z,k_z}^{A_z}). \quad (130)$$

Thus, we have

$$\sum_{k_z \in [K_z]} (U_{z,k_z} \otimes I_{z,k_z}^{A_z}) (\Upsilon_{z,k_z})^2 (U_{z,k_z} \otimes I_{z,k_z}^{A_z})^\dagger = I_{z,k_z}^{A_z}. \quad (131)$$

Let $I_{z,k_z}^{A_z}$ denote the identity operator on $(\bigotimes_{z'=z+1}^Z \mathcal{H}^{A_{z'}})^{\otimes n}$. From (127) and (128), we have

$$1 - \frac{1}{2^{n C_z}} \sum_{k_z=1}^{2^{n C_z}} \text{Tr}[(\Upsilon_{z,k_z})^2 \otimes I_{z,k_z}^{A_z}] \rho^{\otimes n} \leq \epsilon. \quad (132)$$

Second, define

$$\Upsilon_{z,k_z}^{(0)} := \Upsilon_{z,k_z}^2, \quad \Upsilon_{z,k_z}^{(1)} := \Upsilon_{z,k_z} \sqrt{I - \Upsilon_{z,k_z}^2} \quad (133)$$

for each z and k_z . It is straightforward to verify that

$$(\Upsilon_{z,k_z}^{(0)})^2 + (\Upsilon_{z,k_z}^{(1)})^2 = \Upsilon_{z,k_z}^2. \quad (134)$$

Third, we define

$$\Upsilon_{\mathbf{k}}^{x_1 \cdots x_z} := \Upsilon_{Z,k_Z}^{(x_Z)} (\Upsilon_{Z-1,k_{Z-1}}^{(x_{Z-1})} \otimes I^{A_Z}) \cdots (\Upsilon_{1,k_1}^{(x_1)} \otimes I^{A_{>1}}) \quad (135)$$

for $x_1, \dots, x_Z \in \{0, 1\}$, where $\mathbf{k} = (k_1, \dots, k_Z)$. We apply Lemma 15 under the correspondence $S \rightarrow A_{[Z]}^n V^n$, $J \rightarrow Z$, $j \rightarrow z$, $\Lambda_j \rightarrow \Upsilon_{z,k_z}^2 \otimes I^{A_{>z}}$ and $\varrho \rightarrow \rho^{\otimes n}$. It follows that

$$1 - \sum_{x_1, \dots, x_Z=0,1} \text{Tr}[\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z} \rho^{\otimes n} (\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z})^\dagger] \leq 2 \sqrt{\sum_{z=1}^Z (1 - \text{Tr}[(\Upsilon_{z,k_z})^2 \otimes I^{A_{>z}}] \rho^{\otimes n})}. \quad (136)$$

Thus, from (132) and the concavity of the squareroot function, we have

$$1 - \frac{1}{2^{n C_{[Z]}}} \sum_{\mathbf{k} \in \mathbf{K}} \sum_{x_1, \dots, x_Z=0,1} \text{Tr}[\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z} \rho^{\otimes n} (\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z})^\dagger] \leq 2\sqrt{Z}\epsilon. \quad (137)$$

Now, we construct a decoding measurement by

$$\Lambda_{\mathbf{k}} := \tilde{U}_{\mathbf{k}} \left(\sum_{x_1, \dots, x_Z=0,1} (\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z})^\dagger \Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z} \right) \tilde{U}_{\mathbf{k}}^\dagger, \quad (138)$$

where $\tilde{U}_{\mathbf{k}} := (\bigotimes_{z=1}^Z U_{z,k_z}) \otimes I^{V^n}$. From (131), (134) and (135), it follows that

$$\sum_{\mathbf{k} \in \mathbf{K}} \Lambda_{\mathbf{k}} = I, \quad (139)$$

which implies that $\{\Lambda_{\mathbf{k}}\}_{\mathbf{k} \in \mathbf{K}}$ is indeed a POVM. Noting that $\rho_{\mathbf{k}} = \tilde{U}_{\mathbf{k}} \rho^{\otimes n} \tilde{U}_{\mathbf{k}}^\dagger$, we also have

$$\text{Tr}[\Lambda_{\mathbf{k}} \rho_{\mathbf{k}}] = \sum_{x_1, \dots, x_Z=0,1} \text{Tr}[\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z} \rho^{\otimes n} (\Upsilon_{\mathbf{k}}^{x_1 \cdots x_Z})^\dagger]. \quad (140)$$

Substituting this to (137), we arrive at

$$1 - \frac{1}{2^{n C_{[Z]}}} \sum_{\mathbf{k} \in \mathbf{K}} \text{Tr}[\Lambda_{\mathbf{k}} \rho_{\mathbf{k}}] \leq 2\sqrt{Z}\epsilon. \quad (141)$$

Since this relation holds for any small $\epsilon, \xi > 0$ and any sufficiently large n , we complete the proof of the direct part. \blacksquare

VI. PROOF OF PROPOSITION 8

In this section, we prove the distributed randomization theorem (Proposition 8). We will use the same notations as in Section III-B.

A. Proof of The Converse Part

Suppose that a rate tuple (D_1, \dots, D_Z) is achievable in distributed randomization of the state $\rho \in \mathcal{S}(\mathcal{H}^{A_1 \dots A_Z W})$. Fix arbitrary $\vartheta > 0$, choose sufficiently large n , and let $L_z = 2^{nD_z}$ for each z . By definition, there exists a set of unitaries $\mathfrak{U}_z \equiv \{U_{z,l_z}\}_{l_z=1}^{L_z}$ on A_z^n for every z such that

$$\left\| \bar{\rho}^{A_{[z]}^n W^n} - \pi^{A_{[z]}^n} \otimes (\rho^{\otimes n})^{W^n} \right\|_1 \leq \vartheta, \quad (142)$$

where

$$\bar{\rho} := \left(\bigotimes_{z=1}^Z \mathcal{R}_z \right) (\rho^{\otimes n}) \quad (143)$$

and

$$\mathcal{R}_z(\cdot) := \frac{1}{L_z} \sum_{l_z=1}^{L_z} U_{z,l_z}(\cdot) U_{z,l_z}^\dagger. \quad (144)$$

Fix an arbitrary subset $\Gamma \subseteq [Z]$. By tracing out $A_{\Gamma^c}^n$ in (142), we have

$$\left\| \bar{\rho}^{A_\Gamma^n W^n} - \pi^{A_\Gamma^n} \otimes (\rho^{\otimes n})^{W^n} \right\|_1 \leq \vartheta. \quad (145)$$

Define $\mathbf{L}_\Gamma := \times_{z \in \Gamma} [L_z]$. Each element of \mathbf{L}_Γ is denoted as $\mathbf{l}_\Gamma = (l_z)_{z \in \Gamma}$, where $l_z \in [L_z]$ for each z . Correspondingly, define $U_{\mathbf{l}_\Gamma} = \bigotimes_{z \in \Gamma} U_{z,l_z}$ and

$$\rho_{\mathbf{l}_\Gamma}^{A_\Gamma^n W^n} := (U_{\mathbf{l}_\Gamma} \otimes I^{W^n}) (\rho^{A_\Gamma W})^{\otimes n} (U_{\mathbf{l}_\Gamma} \otimes I^{W^n})^\dagger. \quad (146)$$

Let L_Γ be a quantum system with a fixed orthonormal basis $\{|\mathbf{l}_\Gamma\rangle\}_{\mathbf{l}_\Gamma \in \mathbf{L}_\Gamma}$. Consider a state

$$\tilde{\rho}_\Gamma := \frac{1}{|\mathbf{L}_\Gamma|} \sum_{\mathbf{l}_\Gamma \in \mathbf{L}_\Gamma} |\mathbf{l}_\Gamma\rangle\langle \mathbf{l}_\Gamma|^{L_\Gamma} \otimes \rho_{\mathbf{l}_\Gamma}^{A_\Gamma^n W^n}. \quad (147)$$

It is straightforward to verify that

$$(\rho^W)^{\otimes n} = \text{Tr}_{L_\Gamma A_\Gamma^n} [\tilde{\rho}_\Gamma], \quad (148)$$

$$\bar{\rho}^{A_\Gamma^n W^n} = \text{Tr}_{L_\Gamma} [\tilde{\rho}_\Gamma]. \quad (149)$$

The entropies of $\tilde{\rho}_\Gamma$ is calculated as follows. We have

$$\begin{aligned} & \log d_{L_\Gamma} \\ & \geq I(L_\Gamma : A_\Gamma^n W^n)_{\tilde{\rho}_\Gamma} \end{aligned} \quad (150)$$

$$= S(A_\Gamma^n W^n)_{\tilde{\rho}_\Gamma} - S(A_\Gamma^n W^n | L_\Gamma)_{\tilde{\rho}_\Gamma} \quad (151)$$

$$= S(W^n)_{\tilde{\rho}_\Gamma} + S(A_\Gamma^n | W^n)_{\tilde{\rho}_\Gamma} - S(A_\Gamma^n W^n | L_\Gamma)_{\tilde{\rho}_\Gamma} \quad (152)$$

$$= nS(W)_\rho + S(A_\Gamma^n | W^n)_\rho - S(A_\Gamma^n W^n | L_\Gamma)_{\tilde{\rho}_\Gamma}, \quad (153)$$

where (150) follows from the fact that $\tilde{\rho}_\Gamma$ is a classical-quantum state between L_Γ and $A_\Gamma^n W^n$; (151) from the definition of the mutual information; (152) due to the chain rule; and (153) from (148) and (149). Due to the

condition (145) and the Alicki-Fannes inequality [21], [22], the second term in (153) is bounded as

$$S(A_\Gamma^n | W^n)_{\tilde{\rho}_\Gamma} \quad (154)$$

$$\begin{aligned} & \geq S(A_\Gamma^n | W^n)_{\pi^{A_\Gamma^n} \otimes \rho^{W^n}} - 2\vartheta \log d_{A_\Gamma^n} \\ & \quad - (1 + \vartheta) h \left(\frac{\vartheta}{1 + \vartheta} \right) \end{aligned} \quad (155)$$

$$= n(1 - 2\vartheta) \log d_{A_\Gamma} - (1 + \vartheta) h \left(\frac{\vartheta}{1 + \vartheta} \right). \quad (156)$$

Due to (147), (146) and the unitary invariance of the von Neumann entropy, the third term in (153) is evaluated as

$$S(A_\Gamma^n W^n | L_\Gamma)_{\tilde{\rho}_\Gamma} = \frac{1}{|\mathbf{L}_\Gamma|} \sum_{\mathbf{l}_\Gamma \in \mathbf{L}_\Gamma} S(\rho_{\mathbf{l}_\Gamma}^{A_\Gamma^n W^n}) \quad (157)$$

$$= \frac{1}{|\mathbf{L}_\Gamma|} \sum_{\mathbf{l}_\Gamma \in \mathbf{L}_\Gamma} S((\rho^{A_\Gamma W})^{\otimes n}) = nS(A_\Gamma W)_\rho. \quad (158)$$

In addition, we have

$$\log d_{A_\Gamma} = \sum_{z \in \Gamma} \log d_{A_z} \quad (159)$$

and

$$\log d_{L_\Gamma} = \sum_{z \in \Gamma} \log d_{L_z} = n \sum_{z \in \Gamma} D_z. \quad (160)$$

Combining the above relations, we obtain

$$\begin{aligned} n \sum_{z \in \Gamma} D_z & \geq n \left((1 - 2\vartheta) \sum_{z \in \Gamma} \log d_{A_z} - S(A_\Gamma | W)_\rho \right) \\ & \quad - (1 + \vartheta) h \left(\frac{\vartheta}{1 + \vartheta} \right). \end{aligned} \quad (161)$$

Since this relation holds for any $\vartheta > 0$ and sufficiently large n , we arrive at

$$\sum_{z \in \Gamma} D_z \geq \sum_{z \in \Gamma} \log d_{A_z} - S(A_\Gamma | W)_\rho. \quad (162)$$

Noting that this relation holds for any $\Gamma \subseteq [Z]$, we complete the proof of the converse part. \blacksquare

B. Proof of The Direct Part

Recall that the region defined by (22) is a contrapoly-matroid in \mathbb{R}^Z and every extremal point $(D_1^*, \dots, D_{[Z]}^*)$ is represented as

$$D_{\sigma(z)}^* = \log d_{A_{\sigma(z)}} - S(A_{\sigma(z)} | A_{\sigma(1)} \dots A_{\sigma(z-1)} W)_\rho, \quad (163)$$

where σ is a permutation on $[Z]$ (see Lemma 11). Owing to the time-sharing scheme, it suffices to prove that all extremal points are in the achievable rate region. Without loss of generality, it suffices to prove that a rate tuple $(D_1, \dots, D_{[Z]})$ is achievable if

$$D_z > \log d_{A_z} - S(A_z | A_1 \dots A_{z-1} W)_\rho \quad (164)$$

for all $z \in [Z]$. The proof is based on the following lemma:

Lemma 16 *Let A and Q be finite-dimensional quantum systems represented by Hilbert spaces \mathcal{H}^A and \mathcal{H}^Q , respectively, and let $\rho \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^Q)$ be a quantum state thereon. Fix arbitrary $D > \log d_A - S(A|Q)_\rho$, $\vartheta, \xi > 0$ and choose sufficiently large $n \in \mathbb{N}$. Let $U_{l,i}$ be unitaries on \mathcal{H}^A that are chosen independently and randomly according to the Haar measure for each $i \in [n]$ and $l \in [2^{nD}]$. Let $U_l := \bigotimes_{i=1}^n U_{l,i}$ and $\mathcal{R}(\cdot) := \frac{1}{2^{nD}} \sum_{l=1}^{2^{nD}} U_l(\cdot)U_l^\dagger$. Then, with probability no smaller than $1 - \xi$, it holds that*

$$\|\mathcal{R}(\rho^{\otimes n}) - \pi^{A^n} \otimes (\rho^{\otimes n})^{Q^n}\|_1 \leq \vartheta. \quad (165)$$

A proof of Lemma 16 will be provided in Section VII.

To prove the achievability of the rate tuple satisfying the condition (164), we consider a successive protocol that proceeds as follows: In the first step, a random unitary operation is applied on system A_1^n so that the state on A_1^n is completely randomized and is decorrelated from the remaining system $A_2^n \cdots A_Z^n E^n$. Note that this operation does not affect the reduced state on $A_2^n \cdots A_Z^n E^n$. In the second step, a random unitary operation is applied on A_2^n to completely randomize A_2^n and decorrelate it from $A_3^n \cdots A_Z^n E^n$. Repeating this procedure Z times, all subsystems A_z^n are completely randomized and decoupled from each other and W^n .

To be more precise, fix arbitrary $\epsilon > 0$, arbitrary rate tuple (D_1, \dots, D_Z) satisfying the condition (164) and choose sufficiently large n . For each $z \in [Z]$, we apply Lemma 16 under the following correspondence:

$$A \rightarrow A_z, \quad Q \rightarrow A_{z+1} \cdots A_Z W. \quad (166)$$

Let $U_{z,l_z,i}$ be unitaries on \mathcal{H}^{A_z} that are chosen independently and randomly according to the Haar measure for each $i \in [n]$, $l_z \in [2^{nD_z}]$ and $z \in [Z]$. Let $U_{z,l_z} := \bigotimes_{i=1}^n U_{z,l_z,i}$ and $\mathcal{R}_z(\cdot) := \frac{1}{2^{nD_z}} \sum_{l=1}^{2^{nD_z}} U_{z,l_z}(\cdot)U_{z,l_z}^\dagger$. It follows that, for each z and with a probability no smaller than $1 - \xi$, it holds that

$$\|\mathcal{R}_z((\rho^{A_z \cdots A_Z W})^{\otimes n}) - \pi^{A_z} \otimes (\rho^{A_{z+1} \cdots A_Z W})^{\otimes n}\|_1 \leq \vartheta. \quad (167)$$

Thus, with a probability no smaller than $(1 - \xi)^Z \geq 1 - Z\xi$, the condition (167) holds for every $z \in [Z]$. Let $A_{>z}$ denote the system $A_{z+1} \cdots A_Z$. By the triangle inequality and the monotonicity of the trace distance, we

have

$$\begin{aligned} & \left\| \left(\bigotimes_{z=1}^Z \mathcal{R}_z \right) ((\rho^{A_{[z]}W})^{\otimes n}) - \pi^{A_{[z]}} \otimes (\rho^W)^{\otimes n} \right\|_1 \\ & \leq \sum_{z=1}^Z \left\| \pi^{A_{[z-1]}} \otimes \left(\bigotimes_{z'=z}^Z \mathcal{R}_{z'} \right) ((\rho^{A_{\geq z}W})^{\otimes n}) \right. \\ & \quad \left. - \pi^{A_{[z]}} \otimes \left(\bigotimes_{z'=z+1}^Z \mathcal{R}_{z'} \right) ((\rho^{A_{\geq z+1}W})^{\otimes n}) \right\|_1 \end{aligned} \quad (168)$$

$$\begin{aligned} & \leq \sum_{z=1}^Z \left\| \mathcal{R}_z((\rho^{A_{\geq z}W})^{\otimes n}) - \pi^{A_z} \otimes (\rho^{A_{\geq z+1}W})^{\otimes n} \right\|_1 \quad (169) \\ & \leq Z\vartheta. \end{aligned} \quad (170)$$

Since this relation holds for any small $\vartheta, \xi > 0$ and any sufficiently large n , we complete the proof of the direct part. \blacksquare

VII. PROOF OF LEMMA 14 AND 16

We prove Lemma 14 and 16 based on the packing lemma and the covering lemma, respectively. For the simplicity of presentations, we describe the two lemmas as a single one. For the details, see Chapter 15 and 16 in [11].

Lemma 17 *Consider an ensemble of states $\{p_x, \tau_x\}_{x \in \mathcal{X}}$ on a Hilbert space \mathcal{H} , and define*

$$\tau := \sum_{x \in \mathcal{X}} p_x \tau_x. \quad (171)$$

Suppose there exists a projector Π and a set of projectors $\{\Pi_x\}_{x \in \mathcal{X}}$ that satisfy

$$\sum_{x \in \mathcal{X}} p_x \text{Tr}[\Pi \tau_x] \geq 1 - \epsilon, \quad (172)$$

$$\sum_{x \in \mathcal{X}} p_x \text{Tr}[\Pi_x \tau_x] \geq 1 - \epsilon, \quad (173)$$

and there exist $\omega, \Omega, \omega', \Omega' > 0$ such that

$$\text{Tr}[\Pi_x] \leq \omega, \quad \Pi \tau \Pi \leq \frac{1}{\Omega} \Pi \quad (174)$$

and

$$\text{Tr}[\Pi] \leq \Omega', \quad \Pi_x \tau_x \Pi_x \leq \frac{1}{\omega'} \Pi_x. \quad (175)$$

Let \mathcal{M} and \mathcal{M}' be finite sets, and $\mathcal{C} \equiv \{C_m\}_{m \in \mathcal{M}}$ and $\mathcal{C}' \equiv \{C'_m\}_{m' \in \mathcal{M}'}$ be sets of random variables that take values in \mathcal{X} independently according to a probability distribution $\{p_x\}_{x \in \mathcal{X}}$. Then,

1) *There exists a POVM $\{\Lambda_m^C\}_{m \in \mathcal{M}}$ for each C and satisfies*

$$\mathbb{E}_C \left\{ \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \text{Tr}[\Lambda_m^C \tau_{C_m}] \right\} \geq 1 - 2(\varepsilon + 2\sqrt{\varepsilon}) - \frac{4\omega|\mathcal{M}|}{\Omega}. \quad (176)$$

2) *It holds that*

$$\Pr_{C'} \left\{ \|\bar{\tau} - \tau\|_1 \leq \varepsilon + 4\sqrt{\varepsilon} + 24\sqrt[4]{\varepsilon} \right\} \geq 1 - 2\Omega' \exp\left(-\frac{\varepsilon^3}{4 \ln 2} \frac{|\mathcal{M}'|\omega'}{\Omega'}\right), \quad (177)$$

where $\bar{\tau} := |\mathcal{M}'|^{-1} \sum_{m' \in \mathcal{M}'} \tau_{C_{m'}}$.

Proof of Lemma 14 and 16: Fix arbitrary $\delta, \varepsilon > 0$ such that

$$C + 3\delta \leq \log d_A - S(A|Q)_\rho, \quad (178)$$

$$D - 3\delta \geq \log d_A - S(A|Q)_\rho \quad (179)$$

and

$$3\varepsilon + 4\sqrt{\varepsilon} < \varepsilon\xi, \quad (180)$$

$$\varepsilon + 4\sqrt{\varepsilon} + 24\sqrt[4]{\varepsilon} < \vartheta, \quad (181)$$

and choose sufficiently large n . Let $\Pi_{n,\delta}^{Q^n}$ and $\Pi_{n,\delta}^{A^n Q^n}$ be projectors onto the δ typical subspaces of $(\mathcal{H}^Q)^{\otimes n}$ and $(\mathcal{H}^{AQ})^{\otimes n}$ with respect to $(\rho^Q)^{\otimes n}$ and $(\rho^{AQ})^{\otimes n}$, respectively. For each unitary U on $(\mathcal{H}^A)^{\otimes n}$ that is decomposed into $U = \bigotimes_{i=1}^n U_i$, define

$$\Pi_{n,\delta,U}^{A^n Q^n} := (U \otimes I^{Q^n}) \Pi_{n,\delta}^{A^n Q^n} (U \otimes I^{Q^n})^\dagger, \quad (182)$$

$$\rho_{n,U} := (U \otimes I^{Q^n}) \rho^{\otimes n} (U \otimes I^{Q^n})^\dagger. \quad (183)$$

It is straightforward to verify that

$$\bar{\rho}_n := \mathbb{E}_U [\rho_{n,U}] = \pi^{A^n} \otimes (\rho^Q)^{\otimes n}, \quad (184)$$

where the expectation is taken with respect to the Haar measure for each U_i . We denote $I^{A^n} \otimes \Pi_{n,\delta}^{Q^n}$ simply by $\tilde{\Pi}_{n,\delta}^{A^n Q^n}$. Due to the property of the typical subspace, it holds that

$$\mathbb{E}_U \text{Tr}[\tilde{\Pi}_{n,\delta}^{A^n Q^n} \rho_{n,U}^{A^n Q^n}] = \text{Tr}[\Pi_{n,\delta}^{Q^n} (\rho^Q)^{\otimes n}] \geq 1 - \varepsilon,$$

$$\mathbb{E}_U \text{Tr}[\Pi_{n,\delta,U}^{A^n Q^n} \rho_{n,U}^{A^n Q^n}] = \text{Tr}[\Pi_{n,\delta}^{A^n Q^n} (\rho^{AQ})^{\otimes n}] \geq 1 - \varepsilon.$$

In addition, we have

$$\text{Tr}[\Pi_{n,\delta,U}^{A^n Q^n}] = \text{Tr}[\Pi_{n,\delta}^{A^n Q^n}] \leq 2^{n(S(AQ)_\rho + \delta)}, \quad (185)$$

$$\text{Tr}[\tilde{\Pi}_{n,\delta}^{A^n Q^n}] \leq 2^{n(\log d_A + S(Q)_\rho + \delta)} \quad (186)$$

and

$$\tilde{\Pi}_{n,\delta}^{A^n Q^n} \bar{\rho}_n \tilde{\Pi}_{n,\delta}^{A^n Q^n} \leq 2^{-n(\log d_A + S(Q)_\rho - \delta)} \tilde{\Pi}_{n,\delta}^{A^n Q^n}, \quad (187)$$

$$\Pi_{n,\delta,U}^{A^n Q^n} \rho_{n,U}^{A^n Q^n} \Pi_{n,\delta,U}^{A^n Q^n} \leq 2^{-n(S(AQ)_\rho - \delta)} \Pi_{n,\delta,U}^{A^n Q^n}. \quad (188)$$

We apply Lemma 17 under the following correspondence:

$$\mathcal{X} \rightarrow \mathcal{U}((\mathcal{H}^A)^{\otimes n}), \quad p_x \rightarrow p(dU) \quad (189)$$

$$\tau_x \rightarrow \rho_{n,U}, \quad \tau \rightarrow \bar{\rho}_n, \quad (190)$$

$$\Pi \rightarrow \tilde{\Pi}_{n,\delta}, \quad \Pi_x \rightarrow \Pi_{n,\delta,U}. \quad (191)$$

We let

$$\omega \rightarrow 2^{n(S(AQ)_\rho + \delta)}, \quad \Omega \rightarrow 2^{n(\log d_A + S(Q)_\rho - \delta)}, \quad (192)$$

$$\mathcal{M} \rightarrow [2^{nC}], \quad \mathcal{C} \rightarrow \mathfrak{U} \quad (193)$$

and

$$\omega' \rightarrow 2^{n(S(AQ)_\rho - \delta)}, \quad \Omega' \rightarrow 2^{n(\log d_A + S(Q)_\rho + \delta)}, \quad (194)$$

$$\mathcal{M}' \rightarrow [2^{nD}], \quad \mathcal{C}' \rightarrow \mathfrak{U}. \quad (195)$$

It follows that there exists a POVM $\{\Lambda_k^{\mathfrak{U}}\}_{k=1}^{2^{nC}}$ on $A^n Q^n$ for each \mathfrak{U} and it holds that

$$\mathbb{E}_{\mathfrak{U}} \left\{ \frac{1}{2^{nC}} \sum_{m=1}^{2^{nC}} \text{Tr}[\Lambda_k^{\mathfrak{U}} U_k \rho^{\otimes n} U_k^\dagger] \right\} \geq 1 - 2(\varepsilon + 2\sqrt{\varepsilon}) - 4 \cdot 2^{n(C - \log d_A + S(A|Q)_\rho + 2\delta)} \geq 1 - 2(\varepsilon + 2\sqrt{\varepsilon}) - 4 \cdot 2^{-n\delta}. \quad (196)$$

By taking n sufficiently large, and by applying Markov's inequality, we complete the proof of Lemma 14. With \mathcal{R} define as in Lemma 16, we also have

$$\Pr \left\{ \|\mathcal{R}(\rho^{\otimes n}) - \pi^{A^n} \otimes (\rho^{\otimes n})^{Q^n}\|_1 \leq \vartheta \right\} \geq 1 - 2 \cdot 2^{n(\log d_A + S(Q)_\rho + \delta)} \exp\left(-\frac{\varepsilon^3}{4 \ln 2} \cdot 2^{n\delta}\right). \quad (197)$$

This yields Lemma 16 by taking n sufficiently large. ■

VIII. CONCLUSION AND DISCUSSION

In this paper, we introduced the task of the quantum multiple-access one-time pad. We considered an asymptotic limit of infinitely many copies and vanishingly small error, and derived a single-letter characterization of the achievable rate region. Thereby we have provided a generalization of the quantum one-time pad [8], [9] and the conditional quantum one-time pad [10] to a multi-sender scenario. The proof of the converse part is based on a standard calculation of the entropies and the mutual informations, and that of the direct part is obtained by combining two subprotocols, i.e., distributed encoding and distributed randomization. It is left open to obtain a similar characterization for the achievable rate region when the eavesdropper's side information is not necessarily a subsystem of the receiver's one.

A future direction is to extend the result to a one-shot scenario. As in the case of the quantum multiple-access

channels, successive decoding and time sharing may not be sufficient to derive the optimal one-shot rate region. It would be necessary to employ the quantum joint typicality lemma [28] (see also the quantum multipartite packing lemma in [29]), which has played a central role in the proof of the one-shot capacity theorems of the classical-quantum multiple-access channels [16], [28], [30], [31], and to address the simultaneous smoothing conjecture [32], which has been one of the major open problems in quantum Shannon theory.

ACKNOWLEDGEMENT

The author thanks Atsushi Shimbo, Akihito Soeda and Mio Muraio for useful discussions about local encoding.

REFERENCES

- [1] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,” *Phys. Rev. Lett.*, vol. 69, no. 20, p. 2881, 1992.
- [2] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.
- [3] A. Karlsson, M. Koashi, and N. Imoto, “Quantum entanglement for secret sharing and secret splitting,” *Physical Review A*, vol. 59, no. 1, p. 162, 1999.
- [4] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, “Hiding bits in Bell states,” *Physical Review Letters*, vol. 86, no. 25, p. 5807, 2001.
- [5] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, “Quantum data hiding,” *arXiv preprint quant-ph/0103098*, 2001.
- [6] T. Eggeling and R. F. Werner, “Hiding classical data in multipartite quantum states,” *Physical Review Letters*, vol. 89, no. 9, p. 097905, 2002.
- [7] D. P. DiVincenzo, P. Hayden, and B. M. Terhal, “Hiding quantum data,” *Foundations of Physics*, vol. 33, no. 11, pp. 1629–1647, 2003.
- [8] B. Schumacher and M. D. Westmoreland, “Quantum mutual information and the one-time pad,” *Physical Review A*, vol. 74, no. 4, p. 042305, 2006.
- [9] F. G. Brandao and J. Oppenheim, “Quantum one-time pad in the presence of an eavesdropper,” *Physical Review Letters*, vol. 108, no. 4, p. 040504, 2012.
- [10] K. Sharma, E. Wakakuwa, and M. M. Wilde, “Conditional quantum one-time pad,” *Phys. Rev. Lett.*, vol. 124, no. 5, p. 050503, 2020.
- [11] M. Wilde, *Quantum Information Theory*. Camb. Univ. Press, 2013.
- [12] Y. Tanaka, D. Markham, and M. Muraio, “Local encoding of classical information onto quantum states,” *Journal of Modern Optics*, vol. 54, no. 13-15, pp. 2259–2273, 2007.
- [13] D. Bruß, G. M. D’Ariano, M. Lewenstein, C. Macchiavello, A. Sen, U. Sen *et al.*, “Distributed quantum dense coding,” *Physical Review Letters*, vol. 93, no. 21, p. 210501, 2004.
- [14] D. Bruß, M. Lewenstein, A. Sen, U. Sen, G. M. D’Ariano, and C. Macchiavello, “Dense coding with multipartite quantum states,” *International Journal of Quantum Information*, vol. 4, no. 03, pp. 415–428, 2006.
- [15] T. Hiroshima, “Optimal dense coding with mixed state entanglement,” *Journal of Physics A: Mathematical and General*, vol. 34, no. 35, p. 6907, 2001.
- [16] S. Chakraborty, A. Nema, and P. Sen, “One-shot multi-sender decoupling and simultaneous decoding for the quantum mac,” *arXiv preprint arXiv:2102.02187*, 2021.
- [17] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, “The mother of all protocols: restructuring quantum information’s family tree,” *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 465, no. 2108, pp. 2537–2563, AUG 8 2009.
- [18] N. Dutil, “Multipartite quantum protocols for assisted entanglement distillation,” *arXiv preprint arXiv:1105.4657*, 2011.
- [19] D. J. Welsh, *Matroid theory*. Courier Corporation, 2010.
- [20] T. M. Cover and J. A. Thomas, *Elements of Information Theory (2nd ed.)*. Wiley-Interscience, 2005.
- [21] R. Alicki and M. Fannes, “Continuity of quantum conditional information,” *J. Phys. A: Math. Gen.*, vol. 37.5, pp. L55–L57, 2004.
- [22] A. Winter, “Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints,” *Comm. Math. Phys.*, vol. 347, no. 1, pp. 291–313, 2016.
- [23] L. Lovász, “Submodular functions and convexity,” in *Mathematical programming the state of the art*. Springer, 1983, pp. 235–257.
- [24] R. A. Chou, “Private classical communication over quantum multiple-access channels,” *IEEE Transactions on Information Theory*, vol. 68, no. 3, pp. 1782–1794, 2021.
- [25] M. M. Wilde, “Sequential decoding of a general classical-quantum channel,” *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 469, no. 2157, p. 20130259, 2013.
- [26] P. Sen, “Achieving the Han-Kobayashi inner bound for the quantum interference channel by sequential decoding,” *arXiv preprint arXiv:1109.0802*, 2011.
- [27] A. Winter, “The capacity of the quantum multiple-access channel,” *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3059–3065, 2001.
- [28] P. Sen, “Unions, intersections and a one-shot quantum joint typicality lemma,” *Sādhanā*, vol. 46, no. 1, p. 57, 2021.
- [29] D. Ding, H. Gharibyan, P. Hayden, and M. Walter, “A quantum multipartite packing lemma and the relay channel,” *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3500–3519, 2019.
- [30] P. Sen, “Inner bounds via simultaneous decoding in quantum network information theory,” *Sādhanā*, vol. 46, no. 1, p. 18, 2021.
- [31] S. Chakraborty, A. Nema, and P. Sen, “One-shot inner bounds for sending private classical information over a quantum mac,” in *2021 IEEE Information Theory Workshop (ITW)*. IEEE, 2021, pp. 1–6.
- [32] L. Drescher and O. Fawzi, “On simultaneous min-entropy smoothing,” in *2013 IEEE International Symposium on Information Theory*. IEEE, 2013, pp. 161–165.