Private Classical Communication Over Quantum Multiple-Access Channels

Rémi A. Chou, *Member, IEEE*

***Abstract*— We study private classical communication over quantum multiple-access channels. For an arbitrary number of transmitters, we derive a regularized expression of the capacity region. In the case of degradable channels, we establish a single-letter expression for the best achievable sum-rate and prove that this quantity also corresponds to the best achievable sum-rate for quantum communication over degradable quantum multiple-access channels. In our achievability result, we decouple the reliability and privacy constraints, which are handled via source coding with quantum side information and universal hashing, respectively. Hence, we also establish that the multi-user coding problem under consideration can be handled solely via point-to-point coding techniques. As a by-product of independent interest, we derive a distributed leftover hash lemma against quantum side information that ensures privacy in our achievability result.**

***Index Terms*— Private communication, multiple-access channels, wiretap channels, leftover hash lemma, source coding with quantum side information.**

I. Introduction

THE capacity of private classical communication over point-to-point quantum channels has been characterized in [2], [3]. While only a regularized expression of this capacity is known, a single-letter expression has been obtained in the case of degradable quantum channels [4], and coincides with the coherent information of the channel. In this paper, we define private classical communication over quantum multiple-access channels, and determine a regularized expression of the capacity region for an arbitrary number of transmitters. As formally described in the next sections, we consider message indistinguishability as privacy metric. Our proposed setting can be seen as a quantum counterpart to the classical multiple-access wiretap channel, first introduced in [5] and further studied in [6]–[10]. Note that for the special case of classical communication over multiple-access quantum channels *without privacy constraint*, the capacity region has already been characterized in [11].

Often, for simplicity and to facilitate the design of good codes, coding for multiple-access channels is reduced to point-point coding techniques, for instance, with successive decoding or rate-splitting [12], [13]. However, in the presence of a privacy constraint these techniques are challenging to apply. In a successive decoding approach, the transmitters' messages are decoded one after another at the receiver. This approach works well in the absence of privacy constraints [11] because the capacity region is a polymatroid. Unfortunately, in the presence of privacy constraints, this task is challenging, even in the classical case and for only two transmitters [14], because the capacity region is not known to be a polymatroid in general. With a rate-splitting approach, again, the presence of privacy constraints renders the technique challenging to apply, even in the classical case and for only two transmitters, because the rate-splitting procedure may result in negative "rates" for some virtual users [15].

Instead of relying on successive decoding or rate-splitting, we investigate another method (because of the challenges described above) but will still only rely on point-to-point coding techniques. Specifically, our approach in this paper relies on ideas from random binning techniques, first developed in [16], which have demonstrated that three primitives are sufficient to build good codes for classical point-to-point wiretap channels. Namely, source coding with side information at the decoder [17], privacy amplification [18] (which may or may not be implemented with universal hashing), and distribution approximation, i.e., the problem of creating from a random variable that is uniformly distributed, another random variable whose distribution is close (for instance with respect to relative entropy or variational distance) to a fixed target distribution, e.g. [19]. Random binning ideas has been successfully applied to construct optimal coding schemes for point-to-point private classical communication over quantum channels [20] from universal hash functions (used to implement privacy amplification and distribution approximation) and schemes for source coding with quantum side information [21], [22]. Random binning ideas have also been put forward in [23] as a means to prove the existence of good codes for classical wiretap channels, and have been applied in the context of polar coding to provide efficient and optimal codes for several classical point-to-point wiretap channel models [24]–[26]. Note that a capacity-achieving approach that separately handles the reliability constraint and the privacy constraint in the classical point-to-point wiretap channel and the classical-quantum wiretap channel has also been developped in [27] and [28], respectively. [27] and [28] handle the reliability constraint via channel coding and the privacy constraint via universal hashing. We remark that the approaches in [27] and [28] differ

Manuscript received February 17, 2021; revised September 9, 2021; accepted November 8, 2021. Date of publication November 23, 2021; date of current version February 17, 2022. This work was supported in part by NSF under Grant CCF-1850227 and Grant CCF-2047913. An earlier version of this paper was presented in part at the 2021 IEEE International Symposium on Information Theory (ISIT) [DOI: 10.1109/ISIT45174.2021.9517802].

The author is with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260 USA (e-mail: remi.chou@wichita.edu).

Communicated by S. Beigi, Associate Editor for Quantum.
Digital Object Identifier 10.1109/TIT.2021.3130151

from a random binning approach in that [27] and [28] rely on channel coding to handle the reliability constraint, whereas the random binning approach relies on source coding. Despite this difference, we believe that both approaches are interesting: The approach based on channel coding seems more natural as the wiretap channel model is a generalization of a channel coding problem, whereas the approach based on source coding uses a simpler building block, since source coding with quantum side information can be used to obtain classical-quantum channel coding, e.g., [20].

In this paper, following random binning ideas, we establish the sufficiency of the three same primitives (source coding with quantum side information, privacy amplification, and distribution approximation) to achieve the capacity region of private classical communication over quantum multiple-access channels. Additionally, universal hashing will be sufficient to handle privacy amplification and distribution approximation. More specifically, in our coding scheme, the reliability and privacy constraints are decoupled and handled via source coding with quantum side information at the receiver, and two-universal hash functions [29], respectively. The challenge for the transmitters is to encode their private messages without the knowledge of the other users messages, and still guarantee privacy for all the messages jointly. We establish a distributed version of the leftover hash lemma against quantum side information as a tool for this task. While simultaneously smoothing the min-entropies that appears in the distributed leftover hash lemma is challenging [30], we are still able to approximate these min-entropies by Von Neumann entropies in the case of product states. Next, to ensure reliability of the messages at the receivers we design and appropriately combine with universal hashing a multiple-access channel code designed from distributed source coding with quantum side information at the decoder. The crux of our analysis is to precisely control the joint state of the encoders output by ensuring a close trace distance between this joint state and a fixed target state in the different steps of the coding scheme, as it not only affects the rates at which the users can transmit but also the privacy guarantees. Finally, a non-trivial Fourier-Motzkin elimination that leverages submodularity properties associated with our achievable rates is performed to obtain the final expression of our achievability region.

We summarize our main contributions as follows. (i) We first derive a regularized expression for the private classical capacity region of quantum multiple-access channels *for an arbitrary number of transmitters*. (ii) Then, we derive a single-letter expression of the best achievable sum-rate for degradable channels by leveraging properties of the polymatroidal structure of the regularized capacity region. (iii) We establish that the latter quantity is also equal to the best achievable sum-rate for quantum communication over degradable quantum multiple-access channels. (iv) As a byproduct of independent interest, we derive a distributed version of the leftover hash lemma against quantum side information, that is used in our analysis of distributed hashing to ensure privacy. (v) Finally, our achievability scheme, which decouples reliability and privacy via distributed source coding and distributed hashing, establishes that the multi-user coding problem under consideration can be handled solely via point-to-point coding techniques. Namely, source coding with quantum side information between two parties and universal hashing. Even in the classical case, i.e., the classical multiple-access wiretap channel, the reduction of this multi-user coding problem to point-to-point coding techniques was only established for two transmitters but not an arbitrary number of transmitters.

Finally, we refer to the recent work [31] for the study of a one-shot achievability scheme for the problem considered in this paper in the case of two transmitters.

The remainder of the paper is organized as follows. We formally define the problem in Section III and present our main results in Section IV. Before we prove our inner bound for the capacity region in Section VI, we present in Section V preliminary results that will be used in our achievability scheme. Specifically, in Section V, we discuss (i) distributed universal hashing against quantum side information, (ii) distributed source coding with quantum side information, and (iii) classical data transmission over classical-quantum multiple-access channels from distributed source coding. We prove an outer bound for the capacity region in Section VII. We prove our results regarding the best achievable sum-rate in Section VIII. Finally, we provide concluding remarks in Section IX.

II. Notation

For $x \in \mathbb{R}$, define $[x] \triangleq [1, \lceil x \rceil] \cap \mathbb{N}$ and $[x]^+ \triangleq \max(0, x)$. For $\mathcal{H}$, a finite-dimensional Hilbert space, let $\mathcal{P}(\mathcal{H})$ be the set of positive semi-definite operators on $\mathcal{H}$. Then, let $\mathcal{S}_=(\mathcal{H}) \triangleq \{\rho \in \mathcal{P}(\mathcal{H}) : \operatorname{Tr}\rho = 1\}$ and $\mathcal{S}_\leqslant(\mathcal{H}) \triangleq \{\rho \in \mathcal{P}(\mathcal{H}) : 0 < \operatorname{Tr}\rho \leqslant 1\}$ be the set of normalized and subnormalized, respectively, quantum states. Let also $\mathcal{B}(\mathcal{H})$ denote the space of bounded linear operators on $\mathcal{H}$. For any $\rho_{XE} \in \mathcal{S}_\leqslant(\mathcal{H}_X \otimes \mathcal{H}_E)$ and $\sigma_E \in \mathcal{S}_=(\mathcal{H}_E)$, the min-entropy of ρ_{XE} relative to σ_E [32] is defined as $H_{\min}(\rho_{XE}|\sigma_E) \triangleq \sup\left\{\lambda \in \mathbb{R} : \rho_{XE} \leqslant 2^{-\lambda} I_X \otimes \sigma_E\right\}$, where I_X denotes the identity operator on $\mathcal{H}_X$, and the max-entropy of ρ_E [32] is defined as $H_{\max}(\rho_E) \triangleq \log \operatorname{rank}(\rho_E)$. For any $\rho_{ABC} \in \mathcal{S}_=(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, define the quantum entropy $H(A)_\rho \triangleq -\operatorname{Tr}[\rho_A \log_2 \rho_A]$, the conditional quantum entropy $H(A|B)_\rho \triangleq H(AB)_\rho - H(B)_\rho$, the quantum mutual information $I(A;B)_\rho \triangleq H(A)_\rho + H(B)_\rho - H(AB)_\rho$, the quantum conditional mutual information $I(A;B|C)_\rho \triangleq H(A|C)_\rho + H(B|C)_\rho - H(AB|C)_\rho$, and the coherent information $I(A\rangle B)_\rho \triangleq H(B)_\rho - H(AB)_\rho$. For two probability distributions p and q defined over the same finite alphabet $\mathcal{X}$, define the variational distance between p and q as $\mathbb{V}(p,q) \triangleq \sum_{x\in\mathcal{X}} |p(x) - q(x)|$. Finally, the power set of a set $\mathcal{S}$ is denoted by $2^{\mathcal{S}}$.

III. Problem Statement

Let $L \in \mathbb{N}^*$ and define $\mathcal{L} \triangleq [L]$. Consider a quantum multiple-access channel $\mathcal{N}_{A'_\mathcal{L}\to B} : \bigotimes_{l\in\mathcal{L}} \mathcal{B}(\mathcal{H}_{A'_l}) \to \mathcal{B}(\mathcal{H}_B)$ with L transmitters, where $A'_\mathcal{L} \triangleq (A'_l)_{l\in\mathcal{L}}$. Let $U^{\mathcal{N}}_{A'_\mathcal{L}\to BE}$ be an isometric extension of the channel $\mathcal{N}_{A'_\mathcal{L}\to B}$ such that the complementary channel to the environment $\mathcal{N}^c_{A'_\mathcal{L}\to E}$ satisfies $\mathcal{N}^c_{A'_\mathcal{L}\to E}(\rho) = \operatorname{Tr}_B[\mathcal{U}^{\mathcal{N}}_{A'_\mathcal{L}\to BE}(\rho)]$ for $\rho \in \bigotimes_{l\in\mathcal{L}} \mathcal{B}(\mathcal{H}_{A'_l})$.

Definition 1: An $(n, (2^{nR_l})_{l\in\mathcal{L}})$ private classical multiple-access code for the channel $\mathcal{N}_{A'_{\mathcal{L}}\to B}$ consists of

- L message sets $\mathcal{M}_l \triangleq [2^{nR_l}]$, $l \in \mathcal{L}$;
- L encoding maps $\phi_l : \mathcal{M}_l \to \mathcal{B}(\mathcal{H}_{A'^n_l})$, $l \in \mathcal{L}$;
- A decoding positive operator-valued measure (POVM) $(\Lambda_{m_{\mathcal{L}}})_{m_{\mathcal{L}}\in\mathcal{M}_{\mathcal{L}}}$, where $\mathcal{M}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}}\mathcal{M}_l$;

and operates as follows: Transmitter $l \in \mathcal{L}$ selects a message $m_l \in \mathcal{M}_l$ and prepares the state $\rho^{m_l}_{A'^n_l} \triangleq \phi_l(m_l)$, which is sent over $\mathcal{N}_{A'^n_{\mathcal{L}}\to B^n} \triangleq (\mathcal{N}_{A'_{\mathcal{L}}\to B})^{\otimes n}$. The channel output is $\omega^{m_{\mathcal{L}}}_{B^n} \triangleq \mathcal{N}_{A'^n_{\mathcal{L}}\to B^n}(\rho^{m_{\mathcal{L}}}_{A'^n_{\mathcal{L}}})$ where $\rho^{m_{\mathcal{L}}}_{A'^n_{\mathcal{L}}} \triangleq \bigotimes_{l\in\mathcal{L}}\rho^{m_l}_{A'^n_l}$ and $m_{\mathcal{L}} \triangleq (m_l)_{l\in\mathcal{L}}$. The decoding POVM $(\Lambda_{m_{\mathcal{L}}})_{m_{\mathcal{L}}\in\mathcal{M}_{\mathcal{L}}}$ is then used at the receiver to detect the messages sent. The complementary channel output is denoted by $\omega^{m_{\mathcal{L}}}_{E^n} \triangleq \mathcal{N}^c_{A'^n_{\mathcal{L}}\to E^n}(\rho^{m_{\mathcal{L}}}_{A'^n_{\mathcal{L}}})$.

Definition 2: A rate-tuple $(R_l)_{l\in\mathcal{L}}$ is achievable if there exists a sequence of $(n, (2^{nR_l})_{l\in\mathcal{L}})$ private classical multiple-access codes such that for some sequence of constant states (σ_{E^n}), we have

$$\lim_{n\to\infty}\max_{m_{\mathcal{L}}\in\mathcal{M}_{\mathcal{L}}}\operatorname{Tr}[(I-\Lambda_{m_{\mathcal{L}}})\omega^{m_{\mathcal{L}}}_{B^n}] = 0, \text{ (Reliability)} \tag{1}$$

$$\lim_{n\to\infty}\max_{m_{\mathcal{L}}\in\mathcal{M}_{\mathcal{L}}}\|\omega^{m_{\mathcal{L}}}_{E^n} - \sigma_{E^n}\|_1 = 0. \text{ (Indistinguishability)} \tag{2}$$

The private classical capacity region $C_{\text{P-MAC}}$ of a quantum multiple-access channel $\mathcal{N}_{A'_{\mathcal{L}}\to B}$ is defined as the closure of the set of achievable rate-tuples $(R_l)_{l\in\mathcal{L}}$.

IV. Main Results

We first propose a regularized expression for the private classical capacity region.

Theorem 1: The private classical capacity region $C_{\text{P-MAC}}$ of a quantum multiple-access channel $\mathcal{N}_{A'_{\mathcal{L}}\to B}$ is

$$C_{\text{P-MAC}}(\mathcal{N}) = \text{cl}\left(\bigcup_{n=1}^{\infty}\frac{1}{n}\mathcal{P}(\mathcal{N}^{\otimes n})\right),$$

where cl denotes the closure operator and $\mathcal{P}(\mathcal{N})$ is the set of rate-tuples $(R_l)_{l\in\mathcal{L}}$ that satisfy

$$R_{\mathcal{S}} \triangleq \sum_{l\in\mathcal{S}} R_l \leqslant [I(X_{\mathcal{S}}; B|X_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}}; E)_\rho]^+, \forall \mathcal{S}\subseteq\mathcal{L},$$

for some classical-quantum state $\rho_{X_{\mathcal{L}}A'_{\mathcal{L}}}$ of the form

$$\rho_{X_{\mathcal{L}}A'_{\mathcal{L}}} \triangleq \bigotimes_{l\in\mathcal{L}}\left(\sum_{x_l} p_{X_l}(x_l)|x_l\rangle\langle x_l|_{X_l}\otimes\rho^{x_l}_{A'_l}\right),$$

and $\rho_{X_{\mathcal{L}}BE} \triangleq \mathcal{U}^{\mathcal{N}}_{A'_{\mathcal{L}}\to BE}(\rho_{X_{\mathcal{L}}A'_{\mathcal{L}}})$ with $U^{\mathcal{N}}_{A'_{\mathcal{L}}\to BE}$ an isometric extension of $\mathcal{N}_{A'_{\mathcal{L}}\to B}$, and the notation $X_{\mathcal{S}} \triangleq (X_l)_{l\in\mathcal{S}}$ for any $\mathcal{S}\subseteq\mathcal{L}$.

Proof: The achievability and converse are proved in Sections VI and VII, respectively. ∎

In the next result, for the case of degradable channels, we propose a single-letter expression for the best achievable sum-rate in the private classical capacity region.

Theorem 2: Consider a degradable quantum multiple-access channel $\mathcal{N}_{A'_{\mathcal{L}}\to B}$, i.e., there exists a channel $\mathcal{D}_{B\to E}$ such that $\mathcal{D}_{B\to E}\circ\mathcal{N}_{A'_{\mathcal{L}}\to B} = \mathcal{N}^c_{A'_{\mathcal{L}}\to E}$. Define $C^{\text{sum}}_{\text{P-MAC}}$ as the supremum of all achievable sum-rates in $C_{\text{P-MAC}}(\mathcal{N})$. Then, we have

$$C^{\text{sum}}_{\text{P-MAC}}(\mathcal{N}) = P^{\text{sum}}_{\text{MAC}}(\mathcal{N}),$$

with

$$P^{\text{sum}}_{\text{MAC}}(\mathcal{N}) \triangleq \max_{\rho}[I(X_{\mathcal{L}}; B)_\rho - I(X_{\mathcal{L}}; E)_\rho]^+, \tag{3}$$

where the maximization is over classical-quantum states that have the same form as in Theorem 1.

Proof: See Section VIII. ∎

We now propose another single-letter characterization of $C^{\text{sum}}_{\text{P-MAC}}$ for degradable channels. We first define the quantity $Q^{\text{sum}}_{\text{MAC}}$.

Definition 3: Consider a quantum multiple-access channel $\mathcal{N}_{A'_{\mathcal{L}}\to B}$. Define

$$Q^{\text{sum}}_{\text{MAC}}(\mathcal{N}) \triangleq \max_{\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}}} I(A_{\mathcal{L}}\rangle B)_\rho, \tag{4}$$

where the maximization is over states of the form $\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}} \triangleq \bigotimes_{l\in\mathcal{L}}\phi_{A_lA'_l}$ with $\phi_{A_lA'_l}$, $l \in \mathcal{L}$, a pure state, and $\rho_{A_{\mathcal{L}}B} \triangleq \mathcal{N}_{A'_{\mathcal{L}}\to B}(\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}})$.

Note that by [33], $\lim_{n\to\infty}\frac{1}{n}Q^{\text{sum}}_{\text{MAC}}(\mathcal{N}^{\otimes n})$ is a regularized expression for the largest achievable sum-rate for quantum communication over quantum multiple-access channels.

Theorem 3: Consider a degradable quantum multiple-access channel $\mathcal{N}_{A'_{\mathcal{L}}\to B}$. Then, we have

$$C^{\text{sum}}_{\text{P-MAC}}(\mathcal{N}) = Q^{\text{sum}}_{\text{MAC}}(\mathcal{N}).$$

Proof: See Section VIII. ∎

Note that in the case of point-to-point channels Theorem 3 recovers the result in [4, Th. 2].

V. Preliminary Results

We establish in this section preliminary results that we will use to show in Section VI the achievability part of Theorem 1.

A. Distributed Leftover Hash Lemma Against Quantum Side Information

Define $\mathcal{L} \triangleq [L]$. Consider the random variables $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$, defined over the Cartesian product $\mathcal{X}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}}\mathcal{X}_l$ with probability distribution $p_{X_{\mathcal{L}}}$, and a quantum system E whose state depends on $X_{\mathcal{L}}$, described by the following classical-quantum state:

$$\rho_{X_{\mathcal{L}}E} \triangleq \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}}|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}|\otimes\rho^{x_{\mathcal{L}}}_E, \tag{5}$$

where $|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}}|x_l\rangle\langle x_l|$ and $\rho^{x_{\mathcal{L}}}_E \triangleq p_{X_{\mathcal{L}}}(x_{\mathcal{L}})\bar{\rho}^{x_{\mathcal{L}}}_E$ with $\bar{\rho}^{x_{\mathcal{L}}}_E$ the state of the system E conditioned on the realization $x_{\mathcal{L}}$. Next, consider $F_l : \mathcal{X}_l \to \{0,1\}^{r_l}$ a hash function chosen uniformly at random in a family $\mathcal{F}_l$, $l \in \mathcal{L}$, of two-universal hash functions [18], i.e.,

$$\forall x_l, x'_l \in \mathcal{X}_l, x_l \neq x'_l \implies \mathbb{P}[F_l(x_l) = F_l(x'_l)] \leqslant 2^{-r_l}.$$

For any $\mathcal{S}\subseteq\mathcal{L}$, define $\mathcal{X}_{\mathcal{S}} \triangleq \bigtimes_{l\in\mathcal{S}}\mathcal{X}_l$, $F_{\mathcal{S}} \triangleq (F_l)_{l\in\mathcal{S}}$, $\mathcal{F}_{\mathcal{S}} \triangleq \bigtimes_{l\in\mathcal{S}}\mathcal{F}_l$, $\mathcal{A}_{\mathcal{S}} \triangleq \bigtimes_{l\in\mathcal{S}}\{0,1\}^{r_l}$, and for $a_{\mathcal{S}} \in \mathcal{A}_{\mathcal{S}}$, $f_{\mathcal{S}} \in \mathcal{F}_{\mathcal{S}}$, $f^{-1}_{\mathcal{S}}(a_{\mathcal{S}}) \triangleq \{x_{\mathcal{S}} \in \mathcal{X}_{\mathcal{S}} : f_l(x_l) = a_l, \forall l \in \mathcal{S}\}$.

The hash functions outputs $f_{\mathcal{L}}(x_{\mathcal{L}}) \triangleq (f_l(x_l))_{l\in\mathcal{L}}$, the state of the quantum system, and the choice of the functions $f_{\mathcal{L}}$ are described by the following operator

$$\rho_{F_{\mathcal{L}}(X_{\mathcal{L}})EF_{\mathcal{L}}} \triangleq \frac{1}{|\mathcal{F}_{\mathcal{L}}|}\sum_{f_{\mathcal{L}}\in\mathcal{F}_{\mathcal{L}}}\sum_{a_{\mathcal{L}}\in\mathcal{A}_{\mathcal{L}}} |a_{\mathcal{L}}\rangle\langle a_{\mathcal{L}}|\otimes\rho_E^{f_{\mathcal{L}},a_{\mathcal{L}}}\otimes|f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|, \quad (6)$$

where $\rho_E^{f_{\mathcal{L}},a_{\mathcal{L}}} \triangleq \sum_{x_{\mathcal{L}}\in f_{\mathcal{L}}^{-1}(a_{\mathcal{L}})}\rho_E^{x_{\mathcal{L}}}$, $|a_{\mathcal{L}}\rangle\langle a_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}}|a_l\rangle\langle a_l|$, and $|f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}}|f_l\rangle\langle f_l|$.

Lemma 1 (Distributed leftover hash lemma): Let ρ_U be the fully mixed state on $\mathcal{H}_{F_{\mathcal{L}}(X_{\mathcal{L}})}$. Define for any $\mathcal{S}\subseteq\mathcal{L}$, $r_{\mathcal{S}} \triangleq \sum_{s\in\mathcal{S}} r_s$. For any $\sigma_E\in\mathcal{S}_=(\mathcal{H}_E)$, we have

$$\|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}})EF_{\mathcal{L}}} - \rho_U\otimes\rho_{EF_{\mathcal{L}}}\|_1 \leqslant \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-H_{\min}(\rho_{X_{\mathcal{S}}E}|\sigma_E)}}.$$

Proof: See Appendix A. ∎

Note that a similar lemma was known in the classical case, e.g., [34], and had found applications to oblivious transfer [34]–[36], secret generation [37]–[39], and multiple-access channel resolvability [40]. We are now interested in deriving a distributed leftover hash lemma for product states. We will use the following result on product probability distributions, which is a kind of asymptotic equipartition property (AEP) that holds simultaneously for a set of min-entropies.

Lemma 2: Consider the random variables $X_{\mathcal{L}}^n \triangleq (X_l)_{l\in\mathcal{L}}$, Y^n defined over $\mathcal{X}_{\mathcal{L}}^n\times\mathcal{Y}^n$ with probability distribution $p_{X_{\mathcal{L}}^nY^n} \triangleq \prod_{i=1}^n p_{X_{\mathcal{L}}Y}$. In this lemma, let $H(\cdot)$ denote the Shannon entropy for random variables following $p_{X_{\mathcal{L}}Y}$ or its marginals. For any $\epsilon>0$, there exists a subnormalized non-negative function $q_{X_{\mathcal{L}}^nY^n}$ defined over $\mathcal{X}_{\mathcal{L}}^n\times\mathcal{Y}^n$ such that $\mathbb{V}(p_{X_{\mathcal{L}}^nY^n}, q_{X_{\mathcal{L}}^nY^n})\leqslant\epsilon$ and

$$\forall\mathcal{S}\subseteq\mathcal{L}, H_{\min}(q_{X_{\mathcal{S}}^nY^n}) \geqslant nH(X_{\mathcal{S}}Y) - n\delta_{\mathcal{S}}(n),$$
$$H_{\max}(q_{Y^n}) \leqslant nH(Y) + n\delta(n),$$

where $\delta_{\mathcal{S}}(n) \triangleq \log(|\mathcal{X}_{\mathcal{S}}||\mathcal{Y}|+3)\sqrt{\frac{2}{n}(L+1+\log(\frac{1}{\epsilon}))}$, $\forall\mathcal{S}\subseteq\mathcal{L}$, $\delta(n) \triangleq \log(|\mathcal{Y}|+3)\sqrt{\frac{2}{n}(1+\log(\frac{1}{\epsilon}))}$.

Proof: See Appendix B. ∎

From Lemmas 1 and 2, we then obtain the following result.

Lemma 3 (Distributed leftover hash lemma for product states): Consider the product state $\rho_{X_{\mathcal{L}}^nE^n} \triangleq \rho_{X_{\mathcal{L}}E}^{\otimes n}$, where $\rho_{X_{\mathcal{L}}E}$ is defined in (5). With the same notation as in Lemma 1, we have

$$\|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}} - \rho_U\otimes\rho_{E^nF_{\mathcal{L}}}\|_1 \leqslant 2\epsilon + \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-nH(X_{\mathcal{S}}|E)_\rho+n(\delta_{\mathcal{S}}(n)+\delta(n))}},$$

where $\delta_{\mathcal{S}}(n) \triangleq \log(|\mathcal{X}_{\mathcal{S}}|d_E+3)\sqrt{\frac{2}{n}(L+1+\log(\frac{1}{\epsilon}))}$, $\delta(n) \triangleq \log(d_E+3)\sqrt{\frac{2}{n}(1+\log(\frac{1}{\epsilon}))}$, with $d_E \triangleq \dim\mathcal{H}_E$.

Proof: See Appendix C. ∎

B. Distributed Classical Source Coding With Quantum Side Information

Consider $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$, defined over $\mathcal{X}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}}\mathcal{X}_l$ with probability distribution $p_{X_{\mathcal{L}}}$, and a quantum system B whose state depends on the random variable $X_{\mathcal{L}}$, described by the following classical-quantum state

$$\rho_{X_{\mathcal{L}}B} \triangleq \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} |x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}|\otimes\rho_B^{x_{\mathcal{L}}},$$

where $\rho_B^{x_{\mathcal{L}}} \triangleq p_{X_{\mathcal{L}}}(x_{\mathcal{L}})\bar{\rho}_B^{x_{\mathcal{L}}}$ with $\bar{\rho}_B^{x_{\mathcal{L}}}$ the state of the system B conditioned on the realization $x_{\mathcal{L}}$, and we have used the same notation as in Section V-A.

Definition 4: A $(2^{nR_l})_{l\in\mathcal{L}}$ distributed source code for a classical-quantum product state $\rho_{X_{\mathcal{L}}B}^{\otimes n}$ consists of

- L sets $\mathcal{C}_l \triangleq [2^{nR_l}]$, $l\in\mathcal{L}$;
- L encoders $g_l : \mathcal{X}_l^n\to\mathcal{C}_l$, $l\in\mathcal{L}$;
- One decoder $h : \mathcal{S}_=(\mathcal{H}_{B^n})\times\mathcal{C}_{\mathcal{L}}\to\mathcal{X}_{\mathcal{L}}^n$, where $\mathcal{C}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}}\mathcal{C}_l$.

A rate-tuple $(R_l)_{l\in\mathcal{L}}$ is said to be achievable when the average error probability $P_e(n) \triangleq \sum_{x_{\mathcal{L}}^n\in\mathcal{X}_{\mathcal{L}}^n} p_{X_{\mathcal{L}}^n}(x_{\mathcal{L}}^n)\mathbb{P}\left[h(\bar{\rho}_{B^n}^{x_{\mathcal{L}}^n}, g_{\mathcal{L}}(x_{\mathcal{L}}^n)) \neq x_{\mathcal{L}}^n\right]$ satisfies $\lim_{n\to\infty}P_e(n) = 0$, where for all $x_{\mathcal{L}}^n\in\mathcal{X}_{\mathcal{L}}^n$, $g_{\mathcal{L}}(x_{\mathcal{L}}^n) \triangleq (g_l(x_l^n))_{l\in\mathcal{L}}$. Let $\mathcal{C}(\rho_{X_{\mathcal{L}}B})$ be the set of all achievable rate-tuples.

Lemma 4 ([41]): We have

$$\mathcal{C}(\rho_{X_{\mathcal{L}}B}) = \{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{S}} \geqslant H(X_{\mathcal{S}}|X_{\mathcal{S}^c}B)_\rho, \forall\mathcal{S}\subseteq\mathcal{L}\}.$$

Note that the set $\{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{S}} \geqslant H(X_{\mathcal{S}}|X_{\mathcal{S}^c}B)_\rho, \forall\mathcal{S}\subseteq\mathcal{L}\}$ associated with the set function $\mathcal{S}\mapsto H(X_{\mathcal{S}}|X_{\mathcal{S}^c}B)_\rho$ defines a contrapolymatroid. Using the fact that its dominant face, i.e., $\{(R_l)_{l\in\mathcal{L}}\in\mathcal{C}(\rho_{X_{\mathcal{L}}B}) : R_{\mathcal{L}} = H(X_{\mathcal{L}}|B)_\rho\}$ is the convex hull of its extreme points [42], one can easily verify that the region $\mathcal{C}(\rho_{X_{\mathcal{L}}B})$ is achievable using source coding with quantum side information for two parties [21] and time-sharing. This is exactly the coding technique employed in [41] to prove Lemma 4.

C. Multiple-Access Channel Coding From Distributed Source Coding

Consider L finite sets $\mathcal{U}_l$, $l\in\mathcal{L}$, such that $|\mathcal{U}_l| = 2^{R_l^{\mathrm{U}}}$ for some $R_l^{\mathrm{U}}\in\mathbb{R}_+$ and define $\mathcal{U}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}}\mathcal{U}_l$. Consider a classical-quantum multiple-access channel, i.e., a map $W : \mathcal{U}_{\mathcal{L}}\to\mathcal{S}_=(\mathcal{H}_B)$, which maps $u_{\mathcal{L}}\in\mathcal{U}_{\mathcal{L}}$ to the state $\bar{\rho}_B^{u_{\mathcal{L}}}\in\mathcal{S}_=(\mathcal{H}_B)$. Let $\rho_{U_{\mathcal{L}}B} \triangleq \frac{1}{|\mathcal{U}_{\mathcal{L}}|}\sum_{u_{\mathcal{L}}\in\mathcal{U}_{\mathcal{L}}}|u_{\mathcal{L}}\rangle\langle u_{\mathcal{L}}|\otimes\bar{\rho}_B^{u_{\mathcal{L}}}$ describe the input and output of W when the input $U_{\mathcal{L}}$ is uniformly distributed over $\mathcal{U}_{\mathcal{L}}$, and where we have used the notation $|u_{\mathcal{L}}\rangle\langle u_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}}|u_l\rangle\langle u_l|$.

Lemma 5 (Multiple-access channel coding from distributed source coding): Consider L uniformly distributed messages $(M_l)_{l\in\mathcal{L}}\in\mathcal{M}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}}\mathcal{M}_l$, where $\mathcal{M}_l \triangleq [2^{nR_l}]$ for some $R_l\in\mathbb{R}_+$, $l\in\mathcal{L}$. If there exists a $(2^{nR_l^{\mathrm{DC}}})_{l\in\mathcal{L}}$ distributed source code (as defined in Definition 4) for the classical-quantum product state $\rho_{U_{\mathcal{L}}B}^{\otimes n}$, then there exist L encoders $e_l : \mathcal{M}_l\to\mathcal{U}_l^n$, $l\in\mathcal{L}$, and one decoder $d : \mathcal{S}_=(\mathcal{H}_{B^n})\to\mathcal{M}_{\mathcal{L}}$ such that one can choose $R_l = R_l^{\mathrm{U}} - R_l^{\mathrm{DC}}$ as $n\to\infty$, $l\in\mathcal{L}$, and $\lim_{n\to\infty}\mathbb{P}[d(\bar{\rho}_{B^n}^{e_{\mathcal{L}}(M_{\mathcal{L}})}) \neq M_{\mathcal{L}}] = 0$, where $e_{\mathcal{L}}(M_{\mathcal{L}}) \triangleq (e_l(M_l))_{l\in\mathcal{L}}$.

Proof: See Appendix D. ∎

Note that this lemma recovers [20, Lemma 2], which treats the case of point-to-point channels.

VI. Achievability of Theorem 1

Consider a classical-quantum multiple-access wiretap channel, i.e., a map $W : \mathcal{X}_{\mathcal{L}} \to \mathcal{S}_{=}(\mathcal{H}_B \otimes \mathcal{H}_E)$, which maps $x_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}$ to $\bar{\rho}_{BE}^{x_{\mathcal{L}}} \in \mathcal{S}_{=}(\mathcal{H}_B \otimes \mathcal{H}_E)$. The achievability part of Theorem 1 reduces to another achievability result (with a slight adaptation of Definitions 1, 2) for this classical-quantum multiple-access wiretap channel. Specifically, we show in this section that, for any probability distribution $p_{X_{\mathcal{L}}} \triangleq \prod_{l\in\mathcal{L}} p_{X_l}$, the following region is achievable

$$\begin{aligned}&\mathcal{R}(W, p_{X_{\mathcal{L}}})\\ &\triangleq \{(R_{l\in\mathcal{L}}) : R_{\mathcal{S}} \leqslant [I(X_{\mathcal{S}}; B|X_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}}; E)_\rho]^+, \forall \mathcal{S} \subseteq \mathcal{L}\},\end{aligned}$$

where $\rho_{X_{\mathcal{L}}BE} \triangleq \sum_{x_{\mathcal{L}}} p_{X_{\mathcal{L}}}(x_{\mathcal{L}})|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \otimes \bar{\rho}_{BE}^{x_{\mathcal{L}}}$. Note that, compared to the setting of Section III, the signal states sent by the transmitters are now part of the channel definition. Hence, achievability of $\mathcal{R}(W, p_{X_{\mathcal{L}}})$ and regularization lead to the achievability part of Theorem 1.

A. Coding Scheme

The main idea of the coding scheme is to combine distributed source coding and distributed randomness extraction to emulate a random binning-like proof. We proceed in three steps.

Step 1: We create a stochastic channel that simulates the inversion of multiple hash functions while approximating the joint distribution of the inputs and outputs of the hash functions. Approximating this joint distribution is crucial for the message indistinguishability analysis. In the special case of a single hash function, this operation is referred to as shaping in [20] and distribution approximation in [25].

Consider $X_{\mathcal{L}}^n$ distributed according to some arbitrary product distribution $p_{X_{\mathcal{L}}^n} \triangleq \prod_{l\in\mathcal{L}} p_{X_l^n}$, and L two-universal hash functions $F_{\mathcal{L}}$ uniformly distributed over $\mathcal{F}_{\mathcal{L}}$, where we use the same notation as in Section V-A. The output lengths of the hash functions, denoted by $(nR_l^{\mathrm{U}})_{l\in\mathcal{L}}$, will be defined later. Let $\widetilde{W}_{\mathcal{L}}$ be the channel described by the conditional probability distribution $p_{X_{\mathcal{L}}^n|F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}} \triangleq \prod_{l\in\mathcal{L}} p_{X_l^n|F_l(X_l^n)F_l}$ and $\widetilde{W}_l$ be the channel described by the conditional probability distribution $p_{X_l^n|F_l(X_l^n)F_l}$, $l \in \mathcal{L}$. For $l \in \mathcal{L}$, let U_l^n be uniformly distributed over $\mathcal{U}_l^n \triangleq [2^{nR_l^{\mathrm{U}}}]$, and define

$$\widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}} \triangleq p_{X_{\mathcal{L}}^n|F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}} p_{U_{\mathcal{L}}^n} p_{F_{\mathcal{L}}}, \tag{7}$$

where $p_{U_{\mathcal{L}}^n}$ is the uniform distribution over $\mathcal{U}_{\mathcal{L}}^n$ with the same notation as in Section V-C. Hence, $\widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}$ denotes the joint probability distribution of the input $(U_{\mathcal{L}}^n, F_{\mathcal{L}})$ and output $\widetilde{X}_{\mathcal{L}}^n \triangleq \widetilde{W}_{\mathcal{L}}(U_{\mathcal{L}}^n, F_{\mathcal{L}})$ of the channel $\widetilde{W}_{\mathcal{L}}$. To simplify notation in the following, we write $\widetilde{W}_{\mathcal{L}}(U_{\mathcal{L}}^n)$ instead of $\widetilde{W}_{\mathcal{L}}(U_{\mathcal{L}}^n, F_{\mathcal{L}})$ by redefining $\widetilde{W}_{\mathcal{L}}$ and including $F_{\mathcal{L}}$ in its definition.

Step 2: Using Lemma 5, we construct a multiple-access channel code for jointly uniform input distributions (in the absence of any privacy constraint) for the channel $W \circ \widetilde{W}_{\mathcal{L}}$.

Let $m \in \mathbb{N}$. By Lemma 4, there exists a $(2^{mnR_l^{\mathrm{DC}}})_{l\in\mathcal{L}}$ distributed source code (as defined in Definition 4) for the classical-quantum product state $\widetilde{\rho}_{U_{\mathcal{L}}^n B^n}^{\otimes m}$, where

$$\widetilde{\rho}_{U_{\mathcal{L}}^n B^n} \triangleq \frac{1}{|\mathcal{U}_{\mathcal{L}}^n|} \sum_{u_{\mathcal{L}}^n \in \mathcal{U}_{\mathcal{L}}^n} |u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes \bar{\rho}_{B^n}^{\widetilde{W}_{\mathcal{L}}(u_{\mathcal{L}}^n)}, \tag{8}$$

and where $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}}$ belongs to $\mathcal{C}(\widetilde{\rho}_{U_{\mathcal{L}}^n B^n})$. Then, by Lemma 5, there exist L encoders $e_l : \mathcal{M}_l^m \to \mathcal{U}_l^{mn}, l \in \mathcal{L}$, and one decoder $d : \mathcal{S}_{=}(\mathcal{H}_{B^{mn}}) \to \mathcal{M}_{\mathcal{L}}^m$, where we have defined for $l \in \mathcal{L}$, $\mathcal{M}_l^m \triangleq [2^{mnR_l}]$ such that $R_l = R_l^{\mathrm{U}} - R_l^{\mathrm{DC}}$ as $m \to \infty$, and

$$\lim_{m\to\infty} \mathbb{P}\left[d\left(\bar{\rho}_{B^{mn}}^{\widetilde{W}_{\mathcal{L}}^{\otimes m}(e_{\mathcal{L}}(M_{\mathcal{L}}^m))}\right) \neq M_{\mathcal{L}}^m\right] = 0, \tag{9}$$

with $e_{\mathcal{L}}(M_{\mathcal{L}}^m) \triangleq (e_l(M_l^m))_{l\in\mathcal{L}}$.

Step 3: We combine Step 1 and Step 2 to define our encoders and decoder for the classical-quantum multiple-access wiretap channel. Specifically, the encoders are defined as

$$\phi_l : M_l^m \mapsto \widetilde{W}_l^{\otimes m}(e_l(M_l^m)), l \in \mathcal{L}, \tag{10}$$

and the decoder is defined as

$$\psi : \bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)} \mapsto d(\bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)}), \tag{11}$$

where $\phi_{\mathcal{L}}(M_{\mathcal{L}}^m) \triangleq (\phi_l(M_l^m))_{l\in\mathcal{L}}$.

Remark 1: In Step 2, Lemma 4 cannot be directly applied to $\widetilde{\rho}_{U_{\mathcal{L}}^n B^n}$ as it is not a product state.

B. Coding Scheme Analysis

1) Average Reliability: We have

$$\begin{aligned}&\mathbb{P}\left[\psi(\bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)}) \neq M_{\mathcal{L}}^m\right]\\ &= \mathbb{P}\left[d(\bar{\rho}_{B^{mn}}^{\widetilde{W}_{\mathcal{L}}^{\otimes m}(e_{\mathcal{L}}(M_{\mathcal{L}}^m))}) \neq M_{\mathcal{L}}^m\right] \xrightarrow{m\to\infty} 0,\end{aligned} \tag{12}$$

where the equality holds by definition of ψ and $(\phi_l)_{l\in\mathcal{L}}$ in (10), (11), and the limit holds by (9).

2) Average Message Indistinguishability: Note that by a random choice of the encoder in the proof of Lemma 5, $e_{\mathcal{L}}(M_{\mathcal{L}}^m)$ is uniformly distributed, hence, $\widetilde{W}_{\mathcal{L}}^{\otimes m}(e_{\mathcal{L}}(M_{\mathcal{L}}^m))$ follows a product distribution and $\widetilde{\rho}_{e_{\mathcal{L}}(M_{\mathcal{L}}^m)E^{mn}F_{\mathcal{L}}^m}$ is a product state, which one can write $\widetilde{\rho}_{e_{\mathcal{L}}(M_{\mathcal{L}}^m)E^{mn}F_{\mathcal{L}}^m} = \widetilde{\rho}_{U_{\mathcal{L}}^n E^n F_{\mathcal{L}}}^{\otimes m}$, where

$$\begin{aligned}\widetilde{\rho}_{U_{\mathcal{L}}^n E^n F_{\mathcal{L}}} \triangleq \sum_{f_{\mathcal{L}}} \sum_{u_{\mathcal{L}}^n} \sum_{x_{\mathcal{L}}^n} &\widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}(x_{\mathcal{L}}^n, u_{\mathcal{L}}^n, f_{\mathcal{L}})\\ &|u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes \bar{\rho}_{E^n}^{x_{\mathcal{L}}^n} \otimes |f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|.\end{aligned} \tag{13}$$

Next, define the following classical-quantum state

$$\begin{aligned}\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^n F_{\mathcal{L}}} \triangleq \sum_{f_{\mathcal{L}}} \sum_{u_{\mathcal{L}}^n} \sum_{x_{\mathcal{L}}^n} &p_{X_{\mathcal{L}}^n F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}(x_{\mathcal{L}}^n, u_{\mathcal{L}}^n, f_{\mathcal{L}})\\ &|u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes \bar{\rho}_{E^n}^{x_{\mathcal{L}}^n} \otimes |f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|.\end{aligned} \tag{14}$$

Then, for $\bar{\rho}_U$ the fully mixed state on $\mathcal{H}_{U_{\mathcal{L}}^n}$ and ρ_U the fully mixed state on $\mathcal{H}_{M_{\mathcal{L}}}$, we have

$$\begin{aligned}&\|\widetilde{\rho}_{M_{\mathcal{L}}^m E^{mn} F_{\mathcal{L}}^m} - \rho_U^{\otimes m} \otimes \widetilde{\rho}_{E^{mn}F_{\mathcal{L}}^m}\|_1\\ &\leqslant \|\widetilde{\rho}_{e_{\mathcal{L}}(M_{\mathcal{L}}^m)E^{mn}F_{\mathcal{L}}^m} - \bar{\rho}_U^{\otimes m} \otimes \widetilde{\rho}_{E^{mn}F_{\mathcal{L}}^m}\|_1\\ &= \|\widetilde{\rho}_{U_{\mathcal{L}}^n E^n F_{\mathcal{L}}}^{\otimes m} - \bar{\rho}_U^{\otimes m} \otimes \widetilde{\rho}_{E^n F_{\mathcal{L}}}^{\otimes m}\|_1\\ &\overset{(a)}{\leqslant} m\|\widetilde{\rho}_{U_{\mathcal{L}}^n E^n F_{\mathcal{L}}} - \bar{\rho}_U \otimes \widetilde{\rho}_{E^n F_{\mathcal{L}}}\|_1\\ &\overset{(b)}{\leqslant} m(\|\widetilde{\rho}_{U_{\mathcal{L}}^n E^n F_{\mathcal{L}}} - \rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^n F_{\mathcal{L}}}\|_1\end{aligned}$$

$$
\begin{aligned}
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}} - \bar{\rho}_U \otimes \rho_{E^nF_{\mathcal{L}}}\|_1 \\
&\quad + \|\bar{\rho}_U \otimes \rho_{E^nF_{\mathcal{L}}} - \bar{\rho}_U \otimes \widetilde{\rho}_{E^nF_{\mathcal{L}}}\|_1) \\
&\leqslant m(2\|\widetilde{\rho}_{U_{\mathcal{L}}^n E^nF_{\mathcal{L}}} - \rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}}\|_1 \\
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}} - \bar{\rho}_U \otimes \rho_{E^nF_{\mathcal{L}}}\|_1) \\
&\overset{(c)}{\leqslant} m(2\mathbb{V}(\widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}, p_{X_{\mathcal{L}}^n F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}) \\
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}} - \bar{\rho}_U \otimes \rho_{E^nF_{\mathcal{L}}}\|_1) \\
&\overset{(d)}{=} m(2\mathbb{V}(p_{U_{\mathcal{L}}^n}p_{F_{\mathcal{L}}}, p_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}) \\
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}} - \bar{\rho}_U \otimes \rho_{E^nF_{\mathcal{L}}}\|_1) \\
&\overset{(e)}{\leqslant} 3m\|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}} - \bar{\rho}_U \otimes \rho_{E^nF_{\mathcal{L}}}\|_1 \\
&\overset{(f)}{\leqslant} 3m\left(2\cdot 2^{-n^{\xi}} + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset} 2^{n[R_{\mathcal{S}}^{\mathrm{U}} - H(X_{\mathcal{S}}|E)_\rho + \delta_{\mathcal{S}}(n)+\delta(n)]}}\right) \\
&\overset{(g)}{\leqslant} 3m\left(2\cdot 2^{-n^{\xi}} + \sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset} 2^{-n\eta}}\right) \\
&= 3m\left(2\cdot 2^{-n^{\xi}} + \sqrt{(2^L-1)\cdot 2^{-n\eta}}\right) \\
&\xrightarrow{n\to\infty} 0, \qquad (15)
\end{aligned}
$$

where (a) and (b) hold by the triangle inequality, (c) holds by strong convexity of the trace distance and the definitions of $\widetilde{\rho}_{U_{\mathcal{L}}^n E^nF_{\mathcal{L}}}$ and $\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^nF_{\mathcal{L}}}$ in (13) and (14), (d) holds by the definition of $\widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}$ in (7), (e) holds because $\mathbb{V}(p_{U_{\mathcal{L}}^n}p_{F_{\mathcal{L}}}, p_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}) \leqslant \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}} - \bar{\rho}_U \otimes \rho_{F_{\mathcal{L}}}\|_1$, (f) holds for $\xi \in]0,1[$ by Lemma 3 with the substitution $\epsilon \leftarrow 2^{-n^{\xi}}$ such that $\delta(n) = \log(d_E+3)\sqrt{2(\frac{1}{n}+\frac{1}{n^{1-\xi}})}$, and $\delta_{\mathcal{S}}(n) \triangleq \log(|\mathcal{X}_{\mathcal{S}}|d_E+3)\sqrt{2(\frac{L+1}{n}+\frac{1}{n^{1-\xi}})}$, $\forall \mathcal{S}\subseteq\mathcal{L}$, (g) holds provided that $R_{\mathcal{S}}^{\mathrm{U}} \leqslant H(X_{\mathcal{S}}|E)_\rho - \delta_{\mathcal{S}}(n) - \delta(n) - \eta$, $\forall \mathcal{S}\subseteq\mathcal{L}$, $\eta>0$.

3) Achievable Rate-Tuples: Consider the following extension of the state described in (8)

$$
\begin{aligned}
\widetilde{\rho}_{U_{\mathcal{L}}^n X_{\mathcal{L}}^n B^n F_{\mathcal{L}}} \triangleq \sum_{u_{\mathcal{L}}^n\in\mathcal{U}_{\mathcal{L}}^n}\sum_{x_{\mathcal{L}}^n\in\mathcal{X}_{\mathcal{L}}^n}\sum_{f_{\mathcal{L}}\in\mathcal{F}_{\mathcal{F}}} \widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}(x_{\mathcal{L}}^n, u_{\mathcal{L}}^n, f_{\mathcal{L}}) \\
|u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes |x_{\mathcal{L}}^n\rangle\langle x_{\mathcal{L}}^n| \otimes \bar{\rho}_{B^n}^{x_{\mathcal{L}}^n} \otimes |f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|.
\end{aligned}
$$

Define also the state

$$
\begin{aligned}
\rho_{U_{\mathcal{L}}^n X_{\mathcal{L}}^n B^n F_{\mathcal{L}}} \triangleq \sum_{u_{\mathcal{L}}^n\in\mathcal{U}_{\mathcal{L}}^n}\sum_{x_{\mathcal{L}}^n\in\mathcal{X}_{\mathcal{L}}^n}\sum_{f_{\mathcal{L}}\in\mathcal{F}_{\mathcal{F}}} p_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}(x_{\mathcal{L}}^n, u_{\mathcal{L}}^n, f_{\mathcal{L}}) \\
|u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes |x_{\mathcal{L}}^n\rangle\langle x_{\mathcal{L}}^n| \otimes \bar{\rho}_{B^n}^{x_{\mathcal{L}}^n} \otimes |f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|.
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
&\max\left(\|\widetilde{\rho}_{X_{\mathcal{L}}^n B^n} - \rho_{X_{\mathcal{L}}^n B^n}\|_1, \max_{\mathcal{S}\subseteq\mathcal{L}}\|\widetilde{\rho}_{U_{\mathcal{S}}^n B^n} - \rho_{U_{\mathcal{S}}^n B^n}\|_1\right) \\
&\leqslant \|\widetilde{\rho}_{U_{\mathcal{L}}^n X_{\mathcal{L}}^n B^n F_{\mathcal{L}}} - \rho_{U_{\mathcal{L}}^n X_{\mathcal{L}}^n B^n F_{\mathcal{L}}}\|_1 \\
&\overset{(a)}{\leqslant} \mathbb{V}(\widetilde{p}_{X_{\mathcal{L}}^n U_{\mathcal{L}}^n F_{\mathcal{L}}}, p_{X_{\mathcal{L}}^n F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}) \\
&\overset{(b)}{=} \mathbb{V}(p_{U_{\mathcal{L}}^n}p_{F_{\mathcal{L}}}, p_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}) \\
&\xrightarrow{n\to\infty} 0 \qquad (16)
\end{aligned}
$$

where (a) holds by strong convexity of the trace distance, (b) holds by (7), and the limit holds by the proof of (15).

Next, by Step 2 in Section VI-A, $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}}$ must belong to $\mathcal{C}(\widetilde{\rho}_{U_{\mathcal{L}}^n B^n})$. One can choose $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}} \in \mathcal{C}(\rho_{X_{\mathcal{L}}^n B^n})$ because, as proved next, we have $\mathcal{C}(\rho_{X_{\mathcal{L}}^n B^n}) \subseteq \mathcal{C}(\widetilde{\rho}_{U_{\mathcal{L}}^n B^n})$. For $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}}$ in $\mathcal{C}(\rho_{X_{\mathcal{L}}^n B^n})$ and any $\mathcal{S}\subseteq\mathcal{L}$, we have

$$
\begin{aligned}
nR_{\mathcal{S}}^{\mathrm{DC}} &\overset{(a)}{\geqslant} H(X_{\mathcal{S}}^n|B^n X_{\mathcal{S}^c}^n)_\rho \\
&= H(X_{\mathcal{L}}^n B^n)_\rho - H(B^n X_{\mathcal{S}^c}^n)_\rho \\
&= H(B^n|X_{\mathcal{L}}^n)_\rho - H(B^n|X_{\mathcal{S}^c}^n)_\rho + H(X_{\mathcal{S}}^n)_\rho \\
&\overset{(b)}{\geqslant} H(B^n|X_{\mathcal{L}}^n)_\rho - H(B^n|U_{\mathcal{S}^c}^n)_\rho + H(X_{\mathcal{S}}^n)_\rho \\
&\overset{(c)}{\geqslant} H(B^n|X_{\mathcal{L}}^n)_\rho - H(B^n|U_{\mathcal{S}^c}^n)_\rho + H(U_{\mathcal{S}}^n)_\rho \\
&\geqslant H(B^n|X_{\mathcal{L}}^n)_{\widetilde{\rho}} - H(B^n|U_{\mathcal{S}^c}^n)_{\widetilde{\rho}} + H(U_{\mathcal{S}}^n)_{\widetilde{\rho}} \\
&\quad - |H(B^n|X_{\mathcal{L}}^n)_{\widetilde{\rho}} - H(B^n|X_{\mathcal{L}}^n)_\rho| \\
&\quad - |H(B^n|U_{\mathcal{S}^c}^n)_{\widetilde{\rho}} - H(B^n|U_{\mathcal{S}^c}^n)_\rho| \\
&\quad - |H(U_{\mathcal{S}}^n)_{\widetilde{\rho}} - H(U_{\mathcal{S}}^n)_\rho| \\
&\overset{(d)}{\geqslant} H(B^n|X_{\mathcal{L}}^n)_{\widetilde{\rho}} - H(B^n|U_{\mathcal{S}^c}^n)_{\widetilde{\rho}} + H(U_{\mathcal{S}}^n)_{\widetilde{\rho}} - o(n) \\
&\overset{(e)}{\geqslant} H(B^n|U_{\mathcal{L}}^n)_{\widetilde{\rho}} - H(B^n|U_{\mathcal{S}^c}^n)_{\widetilde{\rho}} + H(U_{\mathcal{S}}^n)_{\widetilde{\rho}} - o(n) \\
&= H(U_{\mathcal{S}}^n|B^n U_{\mathcal{S}^c}^n)_{\widetilde{\rho}} - o(n),
\end{aligned}
$$

where (a) holds because $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}}$ in $\mathcal{C}(\rho_{X_{\mathcal{L}}^n B^n})$, (b) holds by the quantum data processing inequality because, by definition of ρ, for any $\mathcal{S}\subseteq\mathcal{L}$, $U_{\mathcal{S}}^n$ is a function of $X_{\mathcal{S}}^n$, (c) holds by Lemma 3 because, by definition of ρ, for any $\mathcal{S}\subseteq\mathcal{L}$, $U_{\mathcal{S}}^n$ is the output of hash functions when $X_{\mathcal{S}}^n$ is the input, (d) holds by the Alicki-Fannes inequality and (16), (e) holds by the quantum data processing inequality because, by definition of $\widetilde{\rho}$, $X_{\mathcal{L}}^n$ is a function of $U_{\mathcal{L}}^n$.

Hence, by having chosen $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}} \in \mathcal{C}(\rho_{X_{\mathcal{L}}^n B^n})$ and the choice of $(R_l^{\mathrm{U}})_{l\in\mathcal{L}}$ in (15), we have the system

$$
\begin{pmatrix} R_{\mathcal{S}}^{\mathrm{DC}} \geqslant H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho, \forall \mathcal{S}\subseteq\mathcal{L} \\ R_{\mathcal{S}}^{\mathrm{U}} \leqslant H(X_{\mathcal{S}}|E)_\rho, \forall \mathcal{S}\subseteq\mathcal{L} \end{pmatrix}, \qquad (17)
$$

which we rewrite, by Step 3 in Section VI-A, as

$$
\begin{pmatrix} R_{\mathcal{S}}^{\mathrm{DC}} \geqslant H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho, \forall \mathcal{S}\subseteq\mathcal{L} \\ R_{\mathcal{S}} + R_{\mathcal{S}}^{\mathrm{DC}} \leqslant H(X_{\mathcal{S}}|E)_\rho, \forall \mathcal{S}\subseteq\mathcal{L} \end{pmatrix}. \qquad (18)
$$

Next, by Lemma 14, the set functions $\mathcal{S} \mapsto -H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho$ and $\mathcal{S}\mapsto H(X_{\mathcal{S}}|E)_\rho - R_{\mathcal{S}}$ are submodular. Hence, by Lemma 15, the system (18) has a solution if and only if

$$
H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho \leqslant H(X_{\mathcal{S}}|E)_\rho - R_{\mathcal{S}}, \forall \mathcal{S}\subseteq\mathcal{L}, \qquad (19)
$$

which we rewrite as

$$
\begin{aligned}
R_{\mathcal{S}} &\leqslant H(X_{\mathcal{S}}|E)_\rho - H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho \\
&= I(X_{\mathcal{S}};B|X_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}};E)_\rho, \forall \mathcal{S}\subseteq\mathcal{L}.
\end{aligned}
$$

4) Expurgation: We write the average probability of error and average message indistinguishability of the coding scheme in Section VI-A as $\mathbf{S}_n \triangleq \|\widetilde{\rho}_{M_{\mathcal{L}}^m E^{mn}F_{\mathcal{L}}^m} - \rho_U^{\otimes m} \otimes \widetilde{\rho}_{E^{mn}F_{\mathcal{L}}^m}\|_1$ and $\mathbf{P}_n \triangleq \mathbb{P}\left[\psi(\bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)}) \neq M_{\mathcal{L}}^m\right]$, respectively. To simplify

notation, we write $\mathbf{m}_{\mathcal{L}} \triangleq m_{\mathcal{L}}^m$ for $m_{\mathcal{L}}^m \in \mathcal{M}_{\mathcal{L}}^m$. Then, we have

$$\mathbf{S}_n = \sum_{\mathbf{m}_{\mathcal{L}}} \frac{1}{|\mathcal{M}_{\mathcal{L}}^m|} S_n(\mathbf{m}_{\mathcal{L}}),$$
$$\mathbf{P}_n = \sum_{\mathbf{m}_{\mathcal{L}}} \frac{1}{|\mathcal{M}_{\mathcal{L}}^m|} P_n(\mathbf{m}_{\mathcal{L}}),$$

where for $\mathbf{m}_{\mathcal{L}} \in \mathcal{M}_{\mathcal{L}}^m$, we have defined

$$S_n(\mathbf{m}_{\mathcal{L}}) \triangleq \|\widetilde{\rho}_{E^{nm}F_{\mathcal{L}}^m}^{\mathbf{m}_{\mathcal{L}}} - \widetilde{\rho}_{E^{nm}F_{\mathcal{L}}^m}\|_1,$$
$$P_n(\mathbf{m}_{\mathcal{L}}) \triangleq \mathbb{P}\left[\psi(\bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(\mathbf{M}_{\mathcal{L}})}) \neq \mathbf{M}_{\mathcal{L}} | \mathbf{M}_{\mathcal{L}} = \mathbf{m}_{\mathcal{L}}\right].$$

Let $\alpha \in]0,1[$. By Markov's inequality and (12), (15), for at least a fraction $1-\alpha$ of the codewords, $P_n(\mathbf{m}_{\mathcal{L}}) \leqslant \alpha^{-1}\mathbf{P}_n$ and for at least a fraction $1-\alpha$ of the codewords, $S_n(\mathbf{m}_{\mathcal{L}}) \leqslant \alpha^{-1}\mathbf{S}_n$. Hence, for a fraction of the codewords at least $1-2\alpha$, $P_n(\mathbf{m}_{\mathcal{L}}) \leqslant \alpha^{-1}\mathbf{P}_n \xrightarrow{n\to\infty} 0$ and $S_n(\mathbf{m}_{\mathcal{L}}) \leqslant \alpha^{-1}\mathbf{S}_n \xrightarrow{n\to\infty} 0$. Finally, we expurgate the code to only retain this fraction $1-2\alpha$ of messages, which has a negligible impact on the asymptotic communication rates.

VII. Converse of Theorem 1

Similar to the case of point-to-point channels, e.g., [43, Sec. 23.4], it is sufficient to consider the task of exchanging private randomness between the transmitters and the legitimate receiver, which is a weaker task than private classical communication. Specifically, assume that Transmitter $l \in \mathcal{L}$ prepares a maximally correlated state $\rho_{M_l M_l'}$ and encodes M_l' as $\rho_{A_l'^n}^{m_l}$, $m_l \in \mathcal{M}_l$, such that the legitimate receiver can recover the share $M_{\mathcal{L}}'$ of the state $\rho_{M_{\mathcal{L}}M_{\mathcal{L}}'} \triangleq \bigotimes_{l\in\mathcal{L}} \rho_{M_l M_l'}$ with some decoder $\mathcal{D}_{B^n \to M_{\mathcal{L}}'}$. The state resulting from this encoding and n independent uses of the channel, i.e., $\mathcal{N}_{A_{\mathcal{L}}'^n \to B^n}$, is

$$\omega_{M_{\mathcal{L}}B^nE^n} \triangleq \frac{1}{|\mathcal{M}_{\mathcal{L}}|} \sum_{m_{\mathcal{L}}\in\mathcal{M}_{\mathcal{L}}} |m_{\mathcal{L}}\rangle\langle m_{\mathcal{L}}| \otimes \mathcal{U}_{A_{\mathcal{L}}'^n \to B^nE^n}^{\mathcal{N}}(\rho_{A_{\mathcal{L}}'^n}^{m_{\mathcal{L}}}),$$

where $\rho_{A_{\mathcal{L}}'^n}^{m_{\mathcal{L}}} \triangleq \bigotimes_{l\in\mathcal{L}} \rho_{A_l'^n}^{m_l}$ and $|m_{\mathcal{L}}\rangle\langle m_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}} |m_l\rangle\langle m_l|$, with $m_{\mathcal{L}} = (m_l)_{l\in\mathcal{L}} \in \mathcal{M}_{\mathcal{L}}$. Then, the decoder of the legitimate receiver produces

$$\omega_{M_{\mathcal{L}}M_{\mathcal{L}}'E^n} \triangleq \mathcal{D}_{B^n \to M_{\mathcal{L}}'}(\omega_{M_{\mathcal{L}}B^nE^n}),$$

and privacy with respect to the environment is assumed, i.e., there exists a constant state σ_{E^n} independent of $\rho_{M_{\mathcal{L}}M_{\mathcal{L}}'}$ such that

$$\|\omega_{M_{\mathcal{L}}M_{\mathcal{L}}'E^n} - \rho_{M_{\mathcal{L}}M_{\mathcal{L}}'} \otimes \sigma_{E^n}\|_1 \leqslant \delta(n), \tag{20}$$

where $\lim_{n\to\infty} \delta(n) = 0$. Next, for $\mathcal{S} \subseteq \mathcal{L}$, we have

$$\begin{aligned}
nR_{\mathcal{S}} &= \sum_{l\in\mathcal{S}} \log|\mathcal{M}_l| \\
&= \sum_{l\in\mathcal{S}} I(M_l; M_l')_\rho \\
&\overset{(a)}{=} I(M_{\mathcal{S}}; M_{\mathcal{S}}')_\rho \\
&= H(M_{\mathcal{S}})_\rho - H(M_{\mathcal{S}}|M_{\mathcal{S}}')_\rho \\
&\overset{(b)}{=} H(M_{\mathcal{S}}|M_{\mathcal{S}^c})_\rho - H(M_{\mathcal{S}}|M_{\mathcal{S}}')_\rho \\
&\overset{(c)}{\leqslant} H(M_{\mathcal{S}}|M_{\mathcal{S}^c})_\rho - H(M_{\mathcal{S}}|M_{\mathcal{S}}'M_{\mathcal{S}^c})_\rho \\
&\leqslant H(M_{\mathcal{S}}|M_{\mathcal{S}^c})_\omega - H(M_{\mathcal{S}}|M_{\mathcal{S}}'M_{\mathcal{S}^c})_\omega \\
&\quad + |H(M_{\mathcal{S}}|M_{\mathcal{S}^c})_\omega - H(M_{\mathcal{S}}|M_{\mathcal{S}^c})_\rho| \\
&\quad + |H(M_{\mathcal{S}}|M_{\mathcal{S}}'M_{\mathcal{S}^c})_\omega - H(M_{\mathcal{S}}|M_{\mathcal{S}}'M_{\mathcal{S}^c})_\rho| \\
&\overset{(d)}{\leqslant} H(M_{\mathcal{S}}|M_{\mathcal{S}^c})_\omega - H(M_{\mathcal{S}}|M_{\mathcal{S}}'M_{\mathcal{S}^c})_\omega + o(n) \\
&= I(M_{\mathcal{S}}; M_{\mathcal{S}}'|M_{\mathcal{S}^c})_\omega + o(n) \\
&\overset{(e)}{\leqslant} I(M_{\mathcal{S}}; B^n|M_{\mathcal{S}^c})_\omega + o(n) \\
&\overset{(f)}{\leqslant} I(M_{\mathcal{S}}; B^n|M_{\mathcal{S}^c})_\omega - I(M_{\mathcal{S}}; E^n)_\omega + o(n),
\end{aligned} \tag{21}$$

where (a) holds because $\rho_{M_{\mathcal{S}}M_{\mathcal{S}}'} = \bigotimes_{l\in\mathcal{S}} \rho_{M_l M_l'}$, (b) holds because for any $\mathcal{S}, \mathcal{T} \subseteq \mathcal{L}$ such that $\mathcal{S} \cap \mathcal{T} = \emptyset$, we have $\rho_{M_{\mathcal{S}}M_{\mathcal{T}}} = \rho_{M_{\mathcal{S}}} \otimes \rho_{M_{\mathcal{T}}}$, (c) holds because conditioning does not increase entropy, (d) holds by (20) and Alicki-Fannes inequality, (e) holds by the quantum data processing inequality, (f) holds because $I(M_{\mathcal{S}}; E^n)_\omega = H(M_{\mathcal{S}}|E^n)_{\rho\otimes\sigma} - H(M_{\mathcal{S}}|E^n)_\omega$ is upper bounded by $o(n)$ using Alicki-Fannes inequality and (20). Finally, from (21) we conclude that $(R_l)_{l\in\mathcal{L}}$ belongs to $\mathrm{cl}\left(\bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{P}(\mathcal{N}^{\otimes n})\right)$.

VIII. Proof of Theorems 2 and 3

We first prove the following lemma, which provides a regularized expression of the best achievable sum-rate in $C_{\text{P-MAC}}$ for degradable channels.

Lemma 6: Let $\mathcal{N}$ be a degradable quantum multiple-access channel. We have

$$C_{\text{P-MAC}}^{\text{sum}}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} P_{\text{MAC}}^{\text{sum}}(\mathcal{N}^{\otimes n}), \tag{22}$$

where $P_{\text{MAC}}^{\text{sum}}$ is defined in (3).

Proof: Note that by Theorem 1 the inequality $C_{\text{P-MAC}}^{\text{sum}}(\mathcal{N}) \leqslant \lim_{n\to\infty} \frac{1}{n} P_{\text{MAC}}^{\text{sum}}(\mathcal{N}^{\otimes n})$ is trivial. It is thus sufficient to show the achievability of the sum-rate $\lim_{n\to\infty} \frac{1}{n} P_{\text{MAC}}^{\text{sum}}(\mathcal{N}^{\otimes n})$. Consider the set function $f_\rho : \mathcal{S} \mapsto I(X_{\mathcal{S}}; B|X_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}}; E)_\rho$, where ρ is a state as defined in Theorem 1. By Lemma 14 in Appendix F, f_ρ is submodular. Next, f_ρ is also non-negative because for any $\mathcal{S} \subseteq \mathcal{L}$

$$\begin{aligned}
f_\rho(\mathcal{S}) &= I(X_{\mathcal{S}}; B|X_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}}; E)_\rho \\
&\overset{(a)}{=} I(X_{\mathcal{S}}; BX_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}}; E)_\rho \\
&\overset{(b)}{\geqslant} I(X_{\mathcal{S}}; B)_\rho - I(X_{\mathcal{S}}; E)_\rho \\
&\overset{(c)}{\geqslant} 0,
\end{aligned}$$

where (a) holds because for any $\mathcal{S} \subseteq \mathcal{L}$, we have $\rho_{X_{\mathcal{S}}X_{\mathcal{S}^c}} = \rho_{X_{\mathcal{S}}} \otimes \rho_{X_{\mathcal{S}^c}}$, (b) holds by the chain rule and positivity of mutual information, (c) holds by the quantum data processing inequality because $\mathcal{N}$ is degradable.

Hence, f_ρ is submodular and non-negative. However, f_ρ is not necessarily non-decreasing, which means that $\mathcal{R}(f_\rho) \triangleq \{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{S}} \leqslant f_\rho(\mathcal{S}), \forall \mathcal{S} \subseteq \mathcal{L}\}$ associated with the function f_ρ does not describe a polymatroid in general – see Definition 5 in Appendix F. To overcome this difficulty, we define the set function f_ρ^* with

$$f_\rho^* : \mathcal{S} \mapsto \min_{\substack{\mathcal{A}\subseteq\mathcal{L} \\ \text{s.t. } \mathcal{A}\supseteq\mathcal{S}}} f_\rho(\mathcal{A}).$$

By Lemma 16 in Appendix F, the set function f_ρ^* is normalized, i.e., $f_\rho^*(\emptyset) = 0$, non-decreasing, and submodular because f_ρ is normalized, non-negative, and submodular. Hence, $\mathcal{R}(f_\rho^*)$ associated with the function f_ρ^* describes a polymatroid and by [42] its dominant face, i.e., $\{(R_l)_{l\in\mathcal{L}} \in \mathcal{R}(f_\rho^*) : R_\mathcal{L} = f_\rho^*(\mathcal{L})\}$ is non-empty. Consequently, there exists a rate-tuple $(R_l)_{l\in\mathcal{L}} \in \mathcal{R}(f_\rho^*)$ such that $R_\mathcal{L} = f_\rho^*(\mathcal{L})$. Next, by inspecting $\mathcal{R}(f_\rho^*)$ and $\mathcal{R}(f_\rho)$, we have that $\mathcal{R}(f_\rho^*) = \mathcal{R}(f_\rho)$ by the construction of f_ρ^*. We also have $f_\rho^*(\mathcal{L}) = f_\rho(\mathcal{L})$ by the construction of f_ρ^*. Hence, we conclude that there exists a rate-tuple $(R_l)_{l\in\mathcal{L}} \in \mathcal{R}(f_\rho)$ such that $R_\mathcal{L} = f_\rho(\mathcal{L})$. Finally, from Theorem 1, we conclude that the sum-rate $\lim_{n\to\infty}\frac{1}{n}P_{\text{MAC}}^{\text{sum}}(\mathcal{N}^{\otimes n})$ is achievable, and thus that (22) holds. ∎

Next, we prove the following equality.

Lemma 7: Let $\mathcal{N}$ be a degradable quantum multiple-access channel. We have

$$P_{\text{MAC}}^{\text{sum}}(\mathcal{N}) = Q_{\text{MAC}}^{\text{sum}}(\mathcal{N}).$$

Proof: See Appendix E. ∎

Finally, we have that $Q_{\text{MAC}}^{\text{sum}}$ is additive for degradable channels. The proof of Lemma 8 is similar to the proof of additivity for the coherent information of degradable channels. Note that Lemma 8 is also referenced in [33].

Lemma 8: Let $\mathcal{N}$ and $\mathcal{M}$ be two degradable quantum multiple-access channels. Then, we have

$$Q_{\text{MAC}}^{\text{sum}}(\mathcal{N}\otimes\mathcal{M}) = Q_{\text{MAC}}^{\text{sum}}(\mathcal{N}) + Q_{\text{MAC}}^{\text{sum}}(\mathcal{M}).$$

All in all, from Lemmas 6, 7, 8, we obtain Theorems 2 and 3.

IX. Concluding Remarks

We introduced the notion of private capacity region for quantum multiple-access channels. For an arbitrary number of transmitters, we derived a regularized expression for this private capacity region. In the case of degradable channels, we also derived two single-letter expressions for the best achievable sum-rate. One of these expressions coincides with the best achievable sum-rate for quantum communication over degradable quantum multiple-access channels.

Our proof technique for the achievability part relies on an emulation of a proof based on random binning. Specifically, our achievability result decouples the reliability and privacy constraints, which are handled via distributed source coding with quantum side information at the receiver and distributed hashing, respectively. Consequently, we reduced a multiuser coding problem into multiple single-user coding problems. Indeed, distributed source coding with quantum side information at the receiver can be reduced to single-user source coding with quantum side information at the receiver, and distributed hashing is, by construction, performed independently at each transmitter.

As part of our proof, we derived a distributed leftover hash lemma in the presence of quantum side information, which may be of independent interest. Note that in our setting the seeds size needed to choose the hash functions is irrelevant. However, for other applications, it may be desirable to reduce the necessary seeds size. Specifically, it remains open to extend our result to δ-almost two-universal hash functions, which are known to enable a reduction of the necessary seed size for the non-distributed setting, i.e., the special case $L = 1$, [44].

Appendix A
Proof of Lemma 1

For any $\rho_{XE} \in \mathcal{S}_\leqslant(\mathcal{H}_X\otimes\mathcal{H}_E)$ and $\sigma_E \in \mathcal{S}_=(\mathcal{H}_E)$, the collision entropy of ρ_{XE} relative to σ_E [32] is defined as

$$H_2(\rho_{XE}|\sigma_E) \triangleq -\log\frac{\text{Tr}[\left(\rho_{XE}(I_X\otimes\sigma_E^{-1/2})\right)^2]}{\text{Tr}\,\rho_{XE}}. \tag{23}$$

Next, define $A_\mathcal{L} \triangleq F_\mathcal{L}(X_\mathcal{L})$. We then have

$$\begin{aligned}
&\|\rho_{A_\mathcal{L}EF_\mathcal{L}} - \rho_U\otimes\rho_{EF_\mathcal{L}}\|_1\\
&\overset{(a)}{=} \mathbb{E}_{F_\mathcal{L}}\left\|\rho_{A_\mathcal{L}E}^{F_\mathcal{L}} - \rho_U\otimes\rho_E\right\|_1\\
&\overset{(b)}{\leqslant} \mathbb{E}_{F_\mathcal{L}}\sqrt{2^{r_\mathcal{L}}}\sqrt{\text{Tr}[\left((\rho_{A_\mathcal{L}E}^{F_\mathcal{L}} - \rho_U\otimes\rho_E)(I_{A_\mathcal{L}}\otimes\sigma_E^{-1/2})\right)^2]}\\
&\overset{(c)}{\leqslant} \sqrt{2^{r_\mathcal{L}}}\sqrt{\mathbb{E}_{F_\mathcal{L}}\,\text{Tr}[\left((\rho_{A_\mathcal{L}E}^{F_\mathcal{L}} - \rho_U\otimes\rho_E)(I_{A_\mathcal{L}}\otimes\sigma_E^{-1/2})\right)^2]}\\
&\overset{(d)}{=} \sqrt{2^{r_\mathcal{L}}}\left(\mathbb{E}_{F_\mathcal{L}}\,\text{Tr}\left[\left(\sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}|a_\mathcal{L}\rangle\langle a_\mathcal{L}|\right.\right.\right.\\
&\qquad\left.\left.\left.\otimes\left(\sigma_E^{-1/4}\rho_E^{F_\mathcal{L},a_\mathcal{L}}\sigma_E^{-1/4} - 2^{-r_\mathcal{L}}\sigma_E^{-1/4}\rho_E\sigma_E^{-1/4}\right)\right)^2\right]\right)^{1/2}\\
&= \sqrt{2^{r_\mathcal{L}}}\left(\mathbb{E}_{F_\mathcal{L}}\sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}\text{Tr}\left[\left(\sigma_E^{-1/4}\rho_E^{F_\mathcal{L},a_\mathcal{L}}\sigma_E^{-1/4}\right.\right.\right.\\
&\qquad\left.\left.\left.-2^{-r_\mathcal{L}}\sigma_E^{-1/4}\rho_E\sigma_E^{-1/4}\right)^2\right]\right)^{1/2}\\
&\overset{(e)}{=} \sqrt{2^{r_\mathcal{L}}}\left(\mathbb{E}_{F_\mathcal{L}}\sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}\text{Tr}\left[\left(\sigma_E^{-1/4}\rho_E^{F_\mathcal{L},a_\mathcal{L}}\sigma_E^{-1/4}\right)^2\right]\right.\\
&\qquad\left.-2^{-r_\mathcal{L}}\,\text{Tr}\left[\left(\sigma_E^{-1/4}\rho_E\sigma_E^{-1/4}\right)^2\right]\right)^{1/2},
\end{aligned}\tag{24}$$

where (a) holds with $\rho_{A_\mathcal{L}E}^{F_\mathcal{L}} \triangleq \sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}|a_\mathcal{L}\rangle\langle a_\mathcal{L}|\otimes\rho_E^{F_\mathcal{L},a_\mathcal{L}}$, (b) holds by Lemma 9 in Appendix F with $\rho \triangleq \rho_{A_\mathcal{L}E}^{F_\mathcal{L}} - \rho_U\otimes\rho_E$ and $\sigma \triangleq I_{A_\mathcal{L}}\otimes\sigma_E$ for any $\sigma_E \in \mathcal{S}_\leqslant(\mathcal{H}_E)$, (c) holds by Jensen's inequality, (d) holds because

$$\begin{aligned}
&\text{Tr}[\left((\rho_{A_\mathcal{L}E}^{F_\mathcal{L}} - \rho_U\otimes\rho_E)(I_{A_\mathcal{L}}\otimes\sigma_E^{-1/2})\right)^2]\\
&= \text{Tr}\left[\left((I_{A_\mathcal{L}}\otimes\sigma_E^{-1/4})\right.\right.\\
&\quad\left.\left.\cdot\left[\sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}|a_\mathcal{L}\rangle\langle a_\mathcal{L}|\otimes\left(\rho_E^{F_\mathcal{L},a_\mathcal{L}} - 2^{-r_\mathcal{L}}\rho_E\right)\right](I_{A_\mathcal{L}}\otimes\sigma_E^{-1/4})\right)^2\right],
\end{aligned}$$

(e) holds by expanding and simplifying the square inside the trace. Next, we have

$$\begin{aligned}
&\sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}\text{Tr}[\left(\sigma_E^{-1/4}\rho_E^{F_\mathcal{L},a_\mathcal{L}}\sigma_E^{-1/4}\right)^2]\\
&= \sum_{a_\mathcal{L}\in\mathcal{A}_\mathcal{L}}\text{Tr}\left[\sigma_E^{-1/4}\left(\sum_{x_\mathcal{L}\in F_\mathcal{L}^{-1}(a_\mathcal{L})}\rho_E^{x_\mathcal{L}}\right)\sigma_E^{-1/2}\right.\\
&\qquad\left.\cdot\left(\sum_{x'_\mathcal{L}\in F_\mathcal{L}^{-1}(a_\mathcal{L})}\rho_E^{x'_\mathcal{L}}\right)\sigma_E^{-1/4}\right]
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{a_{\mathcal{L}}\in\mathcal{A}_{\mathcal{L}}} \sum_{x_{\mathcal{L}},x'_{\mathcal{L}}\in F_{\mathcal{L}}^{-1}(a_{\mathcal{L}})} \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}] \\
&\overset{(a)}{=} \sum_{a_{\mathcal{L}}\in\mathcal{A}_{\mathcal{L}}} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in F_{\mathcal{L}}^{-1}(a_{\mathcal{L}})} \sum_{\substack{x'_{\mathcal{L}}\in F_{\mathcal{L}}^{-1}(a_{\mathcal{L}}) \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} 1 \\
&\qquad \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}] \\
&= \sum_{a_{\mathcal{L}}\in\mathcal{A}_{\mathcal{L}}} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \mathbb{1}\{x_{\mathcal{L}}\in F_{\mathcal{L}}^{-1}(a_{\mathcal{L}})\} \\
&\qquad \times \mathbb{1}\{x'_{\mathcal{S}}\in F_{\mathcal{S}}^{-1}(a_{\mathcal{S}})\}\,\mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}] \\
&\overset{(b)}{=} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{a_{\mathcal{S}}\in\mathcal{A}_{\mathcal{S}}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \mathbb{1}\{x_{\mathcal{S}},x'_{\mathcal{S}}\in F_{\mathcal{S}}^{-1}(a_{\mathcal{S}})\} \\
&\qquad \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}] \\
&\overset{(c)}{=} \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \mathbb{1}\{F_{\mathcal{S}}(x_{\mathcal{S}})=F_{\mathcal{S}}(x'_{\mathcal{S}})\} \\
&\qquad \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}], \qquad (25)
\end{aligned}
$$

where in (a) the notation $x'_{\mathcal{S}}\neq x_{\mathcal{S}}$ means $\forall l\in\mathcal{S}$, $x'_l\neq x_l$, (b) holds because $\sum_{a_{\mathcal{S}^c}\in\mathcal{A}_{\mathcal{S}^c}}\mathbb{1}\{x_{\mathcal{S}^c}\in F_{\mathcal{L}}^{-1}(a_{\mathcal{S}^c})\}=1$, and (c) holds because $\sum_{a_{\mathcal{S}}\in\mathcal{A}_{\mathcal{S}}}\mathbb{1}\{x_{\mathcal{S}},x'_{\mathcal{S}}\in F_{\mathcal{S}}^{-1}(a_{\mathcal{S}})\}=\mathbb{1}\{F_{\mathcal{S}}(x_{\mathcal{S}})=F_{\mathcal{S}}(x'_{\mathcal{S}})\}$. Then, taking the expectation over $F_{\mathcal{L}}$ in (25), we obtain

$$
\begin{aligned}
&\mathbb{E}_{F_{\mathcal{L}}} \sum_{a_{\mathcal{L}}\in\mathcal{A}_{\mathcal{L}}} \mathrm{Tr}[\Big(\sigma_E^{-1/4}\rho_E^{F_{\mathcal{L}},a_{\mathcal{L}}}\sigma_E^{-1/4}\Big)^2] \\
&= \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \mathbb{E}_{F_{\mathcal{L}}}\mathbb{1}\{F_{\mathcal{S}}(x_{\mathcal{S}})=F_{\mathcal{S}}(x'_{\mathcal{S}})\} \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}] \\
&\leqslant \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} 2^{-r_{\mathcal{S}}}\,\mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}],
\end{aligned} \qquad (26)
$$

where the inequality holds because $\mathbb{E}_{F_{\mathcal{L}}}\mathbb{1}\{F_{\mathcal{S}}(x_{\mathcal{S}})=F_{\mathcal{S}}(x'_{\mathcal{S}})\}=\mathbb{E}_{F_{\mathcal{S}}}\mathbb{1}\{F_{\mathcal{S}}(x_{\mathcal{S}})=F_{\mathcal{S}}(x'_{\mathcal{S}})\}=\prod_{l\in\mathcal{S}}\mathbb{E}_{F_l}\mathbb{1}\{F_l(x_l)=F_l(x'_l)\}\leqslant\prod_{l\in\mathcal{S}}2^{-r_l}$ by two-universality of the hash functions $F_{\mathcal{S}}$. Note that we also have

$$
\begin{aligned}
&\mathrm{Tr}[\Big(\sigma_E^{-1/4}\rho_E\sigma_E^{-1/4}\Big)^2] \\
&= \sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}]. \qquad (27)
\end{aligned}
$$

Hence, by combining (24), (26), and (27), we have

$$
\begin{aligned}
&\|\rho_{A_{\mathcal{L}}EF_{\mathcal{L}}}-\rho_U\otimes\rho_{EF_{\mathcal{L}}}\|_1 \\
&\leqslant \sqrt{2^{r_{\mathcal{L}}}}\Big(\sum_{\mathcal{S}\subseteq\mathcal{L}} \sum_{x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}} \sum_{\substack{x'_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}} \\ x'_{\mathcal{S}^c}=x_{\mathcal{S}^c}}} (2^{-r_{\mathcal{S}}}-2^{-r_{\mathcal{L}}}) \\
&\qquad \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{L}}}\sigma_E^{-1/2}\rho_E^{x'_{\mathcal{L}}}\sigma_E^{-1/4}]\Big)^{1/2} \\
&= \Big(\sum_{\mathcal{S}\subsetneq\mathcal{L}} \sum_{x_{\mathcal{S}}\in\mathcal{X}_{\mathcal{S}}} \sum_{x_{\mathcal{S}^c}\in\mathcal{X}_{\mathcal{S}^c}} \sum_{\substack{x'_{\mathcal{S}}\in\mathcal{X}_{\mathcal{S}} \\ \text{s.t } x'_{\mathcal{S}}\neq x_{\mathcal{S}}}} (2^{r_{\mathcal{S}^c}}-1) \\
&\qquad \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{(x_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/2}\rho_E^{(x'_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/4}]\Big)^{1/2} \\
&\overset{(a)}{\leqslant} \Big(\sum_{\mathcal{S}\subsetneq\mathcal{L}} \sum_{x_{\mathcal{S}}\in\mathcal{X}_{\mathcal{S}}} \sum_{x_{\mathcal{S}^c}\in\mathcal{X}_{\mathcal{S}^c}} \sum_{x'_{\mathcal{S}}\in\mathcal{X}_{\mathcal{S}}} 2^{r_{\mathcal{S}^c}} \\
&\qquad \times \mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{(x_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/2}\rho_E^{(x'_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/4}]\Big)^{1/2} \\
&\overset{(b)}{=} \sqrt{\sum_{\mathcal{S}\subsetneq\mathcal{L}} \sum_{x_{\mathcal{S}^c}\in\mathcal{X}_{\mathcal{S}^c}} 2^{r_{\mathcal{S}^c}}\,\mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{x_{\mathcal{S}^c}}\sigma_E^{-1/2}\rho_E^{x_{\mathcal{S}^c}}\sigma_E^{-1/4}]} \\
&= \sqrt{\sum_{\mathcal{S}\subsetneq\mathcal{L}} 2^{r_{\mathcal{S}^c}}\,\mathrm{Tr}[\sum_{x_{\mathcal{S}^c}\in\mathcal{X}_{\mathcal{S}^c}} |x_{\mathcal{S}^c}\rangle\langle x_{\mathcal{S}^c}|\otimes\Big(\rho_E^{x_{\mathcal{S}^c}}\sigma_E^{-1/2}\Big)^2]} \\
&\overset{(c)}{=} \sqrt{\sum_{\mathcal{S}\subsetneq\mathcal{L}} 2^{r_{\mathcal{S}^c}}\,\mathrm{Tr}[\rho_{X_{\mathcal{S}^c}E}]2^{-H_2(\rho_{X_{\mathcal{S}^c}E}|\sigma_E)}} \\
&\overset{(d)}{\leqslant} \sqrt{\sum_{\mathcal{S}\subsetneq\mathcal{L}} 2^{r_{\mathcal{S}^c}}2^{-H_{\min}(\rho_{X_{\mathcal{S}^c}E}|\sigma_E)}} \\
&= \sqrt{\sum_{\substack{\mathcal{S}\subseteq\mathcal{L} \\ \mathcal{S}\neq\emptyset}} 2^{r_{\mathcal{S}}-H_{\min}(\rho_{X_{\mathcal{S}}E}|\sigma_E)}},
\end{aligned}
$$

where (a) holds because for any $x_{\mathcal{L}}\in\mathcal{X}_{\mathcal{L}}$, $x'_{\mathcal{S}}\in\mathcal{X}_{\mathcal{S}}$, $\mathrm{Tr}[\sigma_E^{-1/4}\rho_E^{(x_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/2}\rho_E^{(x'_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/4}]=\mathrm{Tr}[\Big(\sigma_E^{-1/4}\rho_E^{(x_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/4}\Big)\Big(\sigma_E^{-1/4}\rho_E^{(x'_{\mathcal{S}},x_{\mathcal{S}^c})}\sigma_E^{-1/4}\Big)]\geqslant 0$ since the trace of the product of two non-negative operators defined on the same Hilbert space is non-negative, (b) holds with $\forall\mathcal{S}\subseteq\mathcal{L}$, $\forall x_{\mathcal{S}}\in\mathcal{X}_{\mathcal{S}}$, $\rho_E^{x_{\mathcal{S}}}\triangleq\sum_{x_{\mathcal{S}^c}\in\mathcal{X}_{\mathcal{S}^c}}\rho_E^{x_{\mathcal{L}}}=p_{X_{\mathcal{S}}}(x_{\mathcal{S}})\sum_{x_{\mathcal{S}^c}\in\mathcal{X}_{\mathcal{S}^c}}p_{X_{\mathcal{S}^c}|X_{\mathcal{S}}}(x_{\mathcal{S}^c}|x_{\mathcal{S}})\bar{\rho}_E^{x_{\mathcal{L}}}$, (c) holds by definition of the collision entropy in (23), (d) holds by Lemma 10 in Appendix F.

Appendix B
Proof of Lemma 2

Define

$$
\begin{aligned}
\mathcal{A} &\triangleq \{(x_{\mathcal{L}}^n,y^n)\in\mathcal{X}_{\mathcal{L}}^n\times\mathcal{Y}^n:\forall\mathcal{S}\subseteq\mathcal{L}, \\
&\qquad -\log p_{X_{\mathcal{S}}^nY^n}(x_{\mathcal{S}}^n,y^n)\geqslant H(X_{\mathcal{S}}^nY^n)-n\delta_{\mathcal{S}}(n)\}, \\
\mathcal{B} &\triangleq \{y^n\in\mathcal{Y}^n:-\log p_{Y^n}(y^n)\leqslant H(Y^n)+n\delta(n)\},
\end{aligned}
$$

and for $\mathcal{S}\subseteq\mathcal{L}$,

$$
\begin{aligned}
\mathcal{A}_{\mathcal{S}} &\triangleq \{(x_{\mathcal{S}}^n,y^n)\in\mathcal{X}_{\mathcal{S}}^n\times\mathcal{Y}^n: \\
&\qquad -\log p_{X_{\mathcal{S}}^nY^n}(x_{\mathcal{S}}^n,y^n)\geqslant H(X_{\mathcal{S}}^nY^n)-n\delta_{\mathcal{S}}(n)\}.
\end{aligned}
$$

Next, define for $(x_{\mathcal{L}}^n,y^n)\in\mathcal{X}_{\mathcal{L}}^n\times\mathcal{Y}^n$,

$$
\begin{aligned}
&q_{X_{\mathcal{L}}^nY^n}(x_{\mathcal{L}}^n,y^n) \\
&\quad \triangleq \mathbb{1}\{(x_{\mathcal{L}}^n,y^n)\in\mathcal{A}\}\mathbb{1}\{y^n\in\mathcal{B}\}p_{X_{\mathcal{L}}^nY^n}(x_{\mathcal{L}}^n,y^n), \qquad (28)
\end{aligned}
$$

and for $\mathcal{S} \subseteq \mathcal{L}$,

$$q_{X_{\mathcal{S}}^n Y^n}(x_{\mathcal{S}}^n, y^n) \triangleq \sum_{x_{\mathcal{S}^c}^n \in \mathcal{X}_{\mathcal{S}^c}^n} q_{X_{\mathcal{L}}^n Y^n}(x_{\mathcal{L}}^n, y^n). \tag{29}$$

We first show that $\mathbb{V}(p_{X_{\mathcal{L}}^n Y^n}, q_{X_{\mathcal{L}}^n Y^n}) \leqslant \epsilon$. We have

$$\begin{aligned}
&\mathbb{V}(p_{X_{\mathcal{L}}^n Y^n}, q_{X_{\mathcal{L}}^n Y^n}) \\
&= \sum_{x_{\mathcal{L}}^n, y^n} |p_{X_{\mathcal{L}}^n Y^n}(x_{\mathcal{L}}^n, y^n) - q_{X_{\mathcal{L}}^n Y^n}(x_{\mathcal{L}}^n, y^n)| \\
&\leqslant \sum_{x_{\mathcal{L}}^n, y^n} p_{X_{\mathcal{L}}^n Y^n}(x_{\mathcal{L}}^n, y^n)(\mathbb{1}\{(x_{\mathcal{L}}^n, y^n) \notin \mathcal{A}\} + \mathbb{1}\{y^n \notin \mathcal{B}\}) \\
&= \mathbb{P}\left[(X_{\mathcal{L}}^n, Y^n) \notin \mathcal{A}\right] + \mathbb{P}\left[Y^n \notin \mathcal{B}\right] \\
&= \mathbb{P}\left[\exists \mathcal{S} \subseteq \mathcal{L}, (X_{\mathcal{S}}^n, Y^n) \notin \mathcal{A}_{\mathcal{S}}\right] + \mathbb{P}\left[Y^n \notin \mathcal{B}\right] \\
&\overset{(a)}{\leqslant} \sum_{\mathcal{S} \subseteq \mathcal{L}} \mathbb{P}\left[(X_{\mathcal{S}}^n, Y^n) \notin \mathcal{A}_{\mathcal{S}}\right] + \mathbb{P}\left[Y^n \notin \mathcal{B}\right] \\
&\overset{(b)}{\leqslant} \sum_{\mathcal{S} \subseteq \mathcal{L}} 2^{-\frac{n\delta_{\mathcal{S}}^2(n)}{2\log(|\mathcal{X}_{\mathcal{S}}||\mathcal{Y}|+3)^2}} + 2^{-\frac{n\delta^2(n)}{2\log(|\mathcal{Y}|+3)^2}} \\
&\overset{(c)}{=} \sum_{\mathcal{S} \subseteq \mathcal{L}} 2^{-L}\epsilon/2 + \epsilon/2 \\
&= \epsilon,
\end{aligned}$$

where (a) holds by the union bound, (b) holds by Lemma 11 in Appendix F, (c) holds by definitions of $\delta_{\mathcal{S}}(n)$ and $\delta(n)$. Next, for $\mathcal{S} \subseteq \mathcal{L}$, we have

$$\begin{aligned}
&H_{\min}(q_{X_{\mathcal{S}}^n Y^n}) \\
&= -\max_{(x_{\mathcal{S}}^n, y^n) \in \mathcal{X}_{\mathcal{S}}^n \times \mathcal{Y}^n} \log q_{X_{\mathcal{S}}^n Y^n}(x_{\mathcal{S}}^n, y^n) \\
&\overset{(a)}{=} -\max_{(x_{\mathcal{S}}^n, y^n) \in \mathcal{X}_{\mathcal{S}}^n \times \mathcal{Y}^n} \log \Big(\textstyle\sum_{x_{\mathcal{S}^c}^n \in \mathcal{X}_{\mathcal{S}^c}^n} \mathbb{1}\{(x_{\mathcal{L}}^n, y^n) \in \mathcal{A}\} \\
&\qquad\qquad \times \mathbb{1}\{y^n \in \mathcal{B}\} p_{X_{\mathcal{L}}^n Y^n}(x_{\mathcal{L}}^n, y^n)\Big) \\
&\overset{(b)}{\geqslant} -\max_{(x_{\mathcal{S}}^n, y^n) \in \mathcal{X}_{\mathcal{S}}^n \times \mathcal{Y}^n} \log(\mathbb{1}\{(x_{\mathcal{S}}^n, y^n) \in \mathcal{A}_{\mathcal{S}}\} p_{X_{\mathcal{S}}^n Y^n}(x_{\mathcal{S}}^n, y^n)) \\
&\overset{(c)}{\geqslant} H(X_{\mathcal{S}}^n Y^n) - n\delta_{\mathcal{S}}(n),
\end{aligned}$$

where (a) holds by (28) and (29), (b) holds because for any $(x_{\mathcal{L}}^n, y^n) \in \mathcal{X}_{\mathcal{L}}^n \times \mathcal{Y}^n$, $\mathbb{1}\{(x_{\mathcal{S}}^n, y^n) \in \mathcal{A}_{\mathcal{S}}\} \geqslant \mathbb{1}\{(x_{\mathcal{L}}^n, y^n) \in \mathcal{A}\}\mathbb{1}\{y^n \in \mathcal{B}\}$ and by marginalization over $X_{\mathcal{S}^c}^n$, (c) holds by definition of $\mathcal{A}_{\mathcal{S}}$. Then, we also have

$$\begin{aligned}
H_{\max}(q_{Y^n}) &= \log \operatorname{supp}(q_{Y^n}) \\
&\overset{(a)}{\leqslant} \log |\mathcal{B}| \\
&\overset{(b)}{\leqslant} nH(Y) + n\delta(n),
\end{aligned}$$

where (a) holds by (28) and (29), and (b) holds because $1 \geqslant \sum_{y^n \in \mathcal{B}} p_{Y^n}(y^n) \geqslant |\mathcal{B}| 2^{-H(Y^n) - n\delta(n)}$ by definition of $\mathcal{B}$.

Appendix C
Proof of Lemma 3

Consider a spectral decomposition of the product state $\rho_{X_{\mathcal{L}}^n E^n}$ given by

$$\rho_{X_{\mathcal{L}}^n E^n} = \sum_{x_{\mathcal{L}}^n, e^n} p_{X_{\mathcal{L}}^n E^n}(x_{\mathcal{L}}^n, e^n) |\phi_{x_{\mathcal{L}}^n, e^n}\rangle\langle\phi_{x_{\mathcal{L}}^n, e^n}|.$$

By Lemma 2, there exists a subnormalized non-negative function $q_{X_{\mathcal{L}}^n E^n}$ such that $\mathbb{V}(p_{X_{\mathcal{L}}^n E^n}, q_{X_{\mathcal{L}}^n E^n}) \leqslant \epsilon$ and

$$\forall \mathcal{S} \subseteq \mathcal{L}, H_{\min}(q_{X_{\mathcal{S}}^n E^n}) \geqslant nH(X_{\mathcal{S}}E) - n\delta_{\mathcal{S}}(n), \tag{30}$$

$$H_{\max}(q_{E^n}) \leqslant nH(E) + n\delta(n). \tag{31}$$

Next, define the state

$$\bar{\rho}_{X_{\mathcal{L}}^n E^n} = \sum_{x_{\mathcal{L}}^n, e^n} q_{X_{\mathcal{L}}^n E^n}(x_{\mathcal{L}}^n, e^n) |\phi_{x_{\mathcal{L}}^n, e^n}\rangle\langle\phi_{x_{\mathcal{L}}^n, e^n}|, \tag{32}$$

and for $\mathcal{S} \subseteq \mathcal{L}$

$$\begin{aligned}
\bar{\rho}_{X_{\mathcal{S}}^n E^n} &= \operatorname{Tr}_{X_{\mathcal{S}^c}^n}[\bar{\rho}_{X_{\mathcal{L}}^n E^n}] \\
&= \sum_{x_{\mathcal{S}}^n, e^n} q_{X_{\mathcal{S}}^n E^n}(x_{\mathcal{S}}^n, e^n) |\phi_{x_{\mathcal{S}}^n, e^n}\rangle\langle\phi_{x_{\mathcal{S}}^n, e^n}|,
\end{aligned} \tag{33}$$

where for any $(x_{\mathcal{S}}^n, e^n)$, $q_{X_{\mathcal{S}}^n E^n}(x_{\mathcal{S}}^n, e^n) \triangleq \sum_{x_{\mathcal{S}^c}^n} q_{X_{\mathcal{L}}^n E^n}(x_{\mathcal{L}}^n, e^n)$. Hence, we have

$$\begin{aligned}
&\|\rho_{X_{\mathcal{L}}^n E^n} - \bar{\rho}_{X_{\mathcal{L}}^n E^n}\|_1 \\
&\leqslant \sum_{x_{\mathcal{L}}^n, e^n} |q_{X_{\mathcal{L}}^n E^n}(x_{\mathcal{L}}^n, e^n) - p_{X_{\mathcal{L}}^n E^n}(x_{\mathcal{L}}^n, e^n)| \\
&= \mathbb{V}(p_{X_{\mathcal{L}}^n E^n}, q_{X_{\mathcal{L}}^n E^n}) \\
&\leqslant \epsilon.
\end{aligned} \tag{34}$$

Then, let ρ_U be the fully mixed state on $\mathcal{H}_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)}$, and define the operator $\bar{\rho}_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}}$ as in (6) using $\bar{\rho}_{X_{\mathcal{L}}^n E^n}$ in place of $\rho_{X_{\mathcal{L}}^n E^n}$. We have

$$\begin{aligned}
&\|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1 \\
&\overset{(a)}{\leqslant} \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \bar{\rho}_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}}\|_1 \\
&\quad + \|\bar{\rho}_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \bar{\rho}_{E^n F_{\mathcal{L}}}\|_1 \\
&\quad + \|\rho_U \otimes \bar{\rho}_{E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1 \\
&\overset{(b)}{\leqslant} 2\epsilon + \|\bar{\rho}_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \bar{\rho}_{E^n F_{\mathcal{L}}}\|_1 \\
&\overset{(c)}{\leqslant} 2\epsilon + \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{L}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} - H_{\min}(\bar{\rho}_{X_{\mathcal{S}}^n E^n}|\sigma_{E^n})}} \\
&\overset{(d)}{=} 2\epsilon + \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{L}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} - H_{\min}(\bar{\rho}_{X_{\mathcal{S}}^n E^n}) + H_{\max}(\bar{\rho}_{E^n})}} \\
&\overset{(e)}{=} 2\epsilon + \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{L}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} + \log(\lambda_{\max}(\bar{\rho}_{X_{\mathcal{S}}^n E^n})) + \log(\operatorname{rank}(\bar{\rho}_{E^n}))}} \\
&\overset{(f)}{=} 2\epsilon + \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{L}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} - H_{\min}(q_{X_{\mathcal{S}}^n E^n}) + H_{\max}(q_{E^n})}} \\
&\overset{(g)}{\leqslant} 2\epsilon + \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{L}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} - n(H(X_{\mathcal{S}}E) - H(E) - \delta_{\mathcal{S}}(n) - \delta(n))}} \\
&\overset{(i)}{=} 2\epsilon + \sqrt{\sum_{\mathcal{S} \subseteq \mathcal{L}, \mathcal{S} \neq \emptyset} 2^{r_{\mathcal{S}} - nH(X_{\mathcal{S}}|E)_\rho + n(\delta_{\mathcal{S}}(n) + \delta(n))}},
\end{aligned}$$

where (a) holds by the triangle inequality, (b) holds by the data processing inequality, e.g., [32, Lemma A.2.1], and (34), (c) holds by Lemma 1 where σ_{E^n} is the fully mixed state on the support of $\bar{\rho}_{E^n}$, (d) holds by Lemma 12 in Appendix F, (e) follows from the definitions of $H_{\min}$ and $H_{\max}$, where $\lambda_{\max}(\bar{\rho}_{X_{\mathcal{S}}^n E^n})$ is the maximum eigenvalue of

$\bar{\rho}_{X_{\mathcal{S}}^n E^n}$, (f) holds by (32) and (33), (g) holds by (30), (31), (i) holds because the von Neumann entropy of an operator with eigenvalues (p_i) is equal to the Shannon entropy of a random variable distributed according to (p_i).

Appendix D
Proof of Lemma 5

Assume that a $(2^{nR_l^{\mathrm{DC}}})_{l\in\mathcal{L}}$ distributed source code is given and that the corresponding encoding and decoding functions are $(g_l)_{l\in\mathcal{L}}$ and h, respectively. We use the same notation as in Definition 4. To simplify notation, we define $\mathbf{u}_{\mathcal{L}} \triangleq u_{\mathcal{L}}^n$, for $u_{\mathcal{L}}^n \in \mathcal{U}_{\mathcal{L}}^n$. By definition, we have $\lim_{n\to\infty} P_e(n) = 0$ and

$$
\begin{aligned}
&P_e(n)\\
&\triangleq \frac{1}{|\mathcal{U}_{\mathcal{L}}^n|}\sum_{\mathbf{u}_{\mathcal{L}}\in\mathcal{U}_{\mathcal{L}}^n}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]\\
&= \frac{1}{|\mathcal{U}_{\mathcal{L}}^n|}\sum_{c_{\mathcal{L}}\in\mathcal{C}_{\mathcal{L}}}\sum_{\mathbf{u}_{\mathcal{L}}\in g_{\mathcal{L}}^{-1}(c_{\mathcal{L}})}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]\\
&= \frac{1}{|\mathcal{C}_{\mathcal{L}}|}\sum_{c_{\mathcal{L}}\in\mathcal{C}_{\mathcal{L}}}\sum_{\mathbf{u}_{\mathcal{L}}\in g_{\mathcal{L}}^{-1}(c_{\mathcal{L}})}\prod_{l\in\mathcal{L}}\frac{\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]}{|\mathcal{U}_l^n|/|\mathcal{C}_l|}\\
&\overset{(a)}{\geqslant} \frac{1}{|\mathcal{C}_{\mathcal{L}}|}\sum_{c_{\mathcal{L}}\in\mathcal{C}'_{\mathcal{L}}}\sum_{\mathbf{u}_{\mathcal{L}}\in g_{\mathcal{L}}^{-1}(c_{\mathcal{L}})}\prod_{l\in\mathcal{L}}\frac{\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]}{|\mathcal{U}_l^n|/|\mathcal{C}_l|}\\
&\overset{(b)}{\geqslant} \frac{1}{|\mathcal{C}_{\mathcal{L}}|}\sum_{c_{\mathcal{L}}\in\mathcal{C}'_{\mathcal{L}}}\sum_{\mathbf{u}_{\mathcal{L}}\in g_{\mathcal{L}}^{-1}(c_{\mathcal{L}})}\prod_{l\in\mathcal{L}}\frac{\epsilon\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]}{|g_l^{-1}(c_l)|}\\
&\overset{(c)}{=} \frac{\epsilon}{|\mathcal{C}_{\mathcal{L}}|}\sum_{c_{\mathcal{L}}\in\mathcal{C}'_{\mathcal{L}}}\mathbb{E}_{p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}}}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]\\
&\overset{(d)}{\geqslant} \epsilon\mathbb{E}_{p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}^*}}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]\sum_{c_{\mathcal{L}}\in\mathcal{C}'_{\mathcal{L}}}\frac{1}{|\mathcal{C}_{\mathcal{L}}|}\\
&= \epsilon\mathbb{E}_{p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}^*}}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]\\
&\qquad\times\sum_{c_{\mathcal{L}}\in\mathcal{C}_{\mathcal{L}}}\frac{1}{|\mathcal{C}_{\mathcal{L}}|}\mathbb{1}\{|g_l^{-1}(c_l)| \geqslant \epsilon|\mathcal{U}_l^n|/|\mathcal{C}_l|, \forall l\in\mathcal{L}\}\\
&\overset{(e)}{\geqslant} \epsilon(1-\epsilon)^L\mathbb{E}_{p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}^*}}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right], \qquad (35)
\end{aligned}
$$

where in (a) we have defined $\mathcal{C}'_{\mathcal{L}} \triangleq \{c_{\mathcal{L}} \in \mathcal{C}_{\mathcal{L}} : |g_l^{-1}(c_l)| \geqslant \epsilon|\mathcal{U}_l^n|/|\mathcal{C}_l|, \forall l \in \mathcal{L}\}$, (b) holds by definition of $\mathcal{C}'_{\mathcal{L}}$, in (c) we have defined $p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}} \triangleq \prod_{l\in\mathcal{L}} p_{\mathbf{U}_l|C_l=c_l}$ and $p_{\mathbf{U}_l|C_l=c_l}$ is the uniform distribution over $g_l^{-1}(c_l)$, $l \in \mathcal{L}$, in (d) we have chosen $c_{\mathcal{L}}^* \in \arg\min_{c_{\mathcal{L}}} \mathbb{E}_{p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}}}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right]$, (e) holds by Lemma 13 in Appendix F.

From (35), we conclude that

$$
\lim_{n\to\infty}\mathbb{E}_{p_{\mathbf{U}_{\mathcal{L}}|C_{\mathcal{L}}=c_{\mathcal{L}}^*}}\mathbb{P}\left[\mathbf{u}_{\mathcal{L}} \neq h\left(\bar{\rho}_{B^n}^{\mathbf{u}_{\mathcal{L}}}, g_{\mathcal{L}}(\mathbf{u}_{\mathcal{L}})\right)\right] = 0. \qquad (36)
$$

For $l \in \mathcal{L}$, let $\mathcal{M}_l$ be such that $|\mathcal{M}_l| = |g_l^{-1}(c_l^*)|$, and let the encoder e_l be a bijection between $\mathcal{M}_l$ and $g_l^{-1}(c_l^*)$. Hence, for any $m_{\mathcal{L}} \in \mathcal{M}_{\mathcal{L}}$, we have $g_{\mathcal{L}}(e_{\mathcal{L}}(m_{\mathcal{L}})) = c_{\mathcal{L}}^*$. Then, define the decoder as $d(\bar{\rho}_{B^n}^{e_{\mathcal{L}}(M_{\mathcal{L}})}) \triangleq e_{\mathcal{L}}^{-1}\left(h(\bar{\rho}_{B^n}^{e_{\mathcal{L}}(M_{\mathcal{L}})}, c_{\mathcal{L}}^*)\right)$. Hence, by (36), we have $\lim_{n\to\infty}\mathbb{P}[d(\bar{\rho}_{B^n}^{e_{\mathcal{L}}(M_{\mathcal{L}})}) \neq M_{\mathcal{L}}] = 0$. Finally, for $l \in \mathcal{L}$, we have $2^{nR_l} = |\mathcal{M}_l| \geqslant \epsilon|\mathcal{U}_l^n|/|\mathcal{C}_l| = \epsilon 2^{n(R_l^{\mathrm{U}} - R_l^{\mathrm{DC}})}$, which yields $R_l \geqslant R_l^{\mathrm{U}} - R_l^{\mathrm{DC}}$ as $n \to \infty$.

Appendix E
Proof of Lemma 7

The arguments closely follow the proof for the special case $L = 1$, e.g., [43, Th. 13.6.2]. We first prove $P_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N}) \leqslant Q_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N})$. Consider a state $\rho_{X_{\mathcal{L}}EB} \triangleq \mathcal{U}_{A'_{\mathcal{L}}\to BE}^{\mathcal{N}}(\rho_{X_{\mathcal{L}}A'_{\mathcal{L}}})$ that achieves $P_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N})$, i.e., maximizes the right-hand side in (3). For $l \in \mathcal{L}$, consider a spectral decomposition for $\rho_{A'_l}^{x_l} = \sum_{y_l} p(y_l|x_l)\psi_{A'_l}^{x_l,y_l}$, where each state $\psi_{A'_l}^{x_l,y}$ is pure. Next, consider $\sigma_{X_{\mathcal{L}}Y_{\mathcal{L}}BE}$ such that $\mathrm{Tr}_{Y_{\mathcal{L}}}[\sigma_{X_{\mathcal{L}}Y_{\mathcal{L}}BE}] = \rho_{X_{\mathcal{L}}BE}$ with

$$
\begin{aligned}
\sigma_{X_{\mathcal{L}}Y_{\mathcal{L}}BE} \triangleq \sum_{x_{\mathcal{L}}}\sum_{y_{\mathcal{L}}} & p_{X_{\mathcal{L}}}(x_{\mathcal{L}})p_{Y_{\mathcal{L}}|X_{\mathcal{L}}}(y_{\mathcal{L}}|x_{\mathcal{L}})\\
& |x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \otimes |y_{\mathcal{L}}\rangle\langle y_{\mathcal{L}}| \otimes \mathcal{U}_{A'_{\mathcal{L}}\to BE}^{\mathcal{N}}\Big(\bigotimes_{l\in\mathcal{L}}\psi_{A'_l}^{x_l,y_l}\Big),
\end{aligned}
$$

where $p_{X_{\mathcal{L}}}(x_{\mathcal{L}}) \triangleq \prod_{l\in\mathcal{L}} p(x_l)$, $p_{Y_{\mathcal{L}}|X_{\mathcal{L}}}(y_{\mathcal{L}}|x_{\mathcal{L}}) \triangleq \prod_{l\in\mathcal{L}} p(y_l|x_l)$, $x_{\mathcal{L}} \triangleq (x_l)_{l\in\mathcal{L}}$, $y_{\mathcal{L}} \triangleq (y_l)_{l\in\mathcal{L}}$, $|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}} |x_l\rangle\langle x_l|$, and $|y_{\mathcal{L}}\rangle\langle y_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}} |y_l\rangle\langle y_l|$. Then, we have

$$
\begin{aligned}
&P_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N})\\
&= I(X_{\mathcal{L}};B)_\rho - I(X_{\mathcal{L}};E)_\rho\\
&= I(X_{\mathcal{L}};B)_\sigma - I(X_{\mathcal{L}};E)_\sigma\\
&= I(X_{\mathcal{L}}Y_{\mathcal{L}};B)_\sigma - I(X_{\mathcal{L}}Y_{\mathcal{L}};E)_\sigma\\
&\quad - I(Y_{\mathcal{L}};B|X_{\mathcal{L}})_\sigma + I(Y_{\mathcal{L}};E|X_{\mathcal{L}})_\sigma\\
&\overset{(a)}{\leqslant} I(X_{\mathcal{L}}Y_{\mathcal{L}};B)_\sigma - I(X_{\mathcal{L}}Y_{\mathcal{L}};E)_\sigma\\
&= H(B)_\sigma - H(E)_\sigma + H(E|X_{\mathcal{L}}Y_{\mathcal{L}})_\sigma - H(B|X_{\mathcal{L}}Y_{\mathcal{L}})_\sigma\\
&\overset{(b)}{=} H(B)_\sigma - H(E)_\sigma\\
&\overset{(c)}{=} H(B)_\phi - H(A_{\mathcal{L}}B)_\phi\\
&= I(A_{\mathcal{L}}\rangle B)_\phi\\
&\overset{(d)}{\leqslant} Q_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N}),
\end{aligned}
$$

where (a) holds by the quantum data processing inequality because $\mathcal{N}$ is degradable, (b) holds because $\sigma_{BE}^{x_{\mathcal{L}},y_{\mathcal{L}}}$ is pure by purity of $\bigotimes_{l\in\mathcal{L}}\psi_{A'_l}^{x_l,y_l}$, in (c), for $l \in \mathcal{L}$, we consider $\phi_{A_lA'_l}$ a purification of $\rho_{A'_l}$ and define $\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}} \triangleq \bigotimes_{l\in\mathcal{L}}\phi_{A_lA'_l}$ and $\phi_{A_{\mathcal{L}}BE} \triangleq \mathcal{U}_{A'_{\mathcal{L}}\to BE}^{\mathcal{N}}(\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}})$ such that $\phi_{A_{\mathcal{L}}BE}$ is pure and $\mathrm{Tr}_{A_{\mathcal{L}}}[\phi_{A_{\mathcal{L}}BE}] = \rho_{BE} = \sigma_{BE}$, (d) holds by definition of $Q_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N})$.

Next, we show $P_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N}) \geqslant Q_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N})$. Consider a state $\phi_{A_{\mathcal{L}}BE} \triangleq \mathcal{U}_{A'_{\mathcal{L}}\to BE}^{\mathcal{N}}(\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}})$ that achieves $Q_{\mathrm{MAC}}^{\mathrm{sum}}(\mathcal{N})$, i.e., maximizes the right-hand side of (4). Consider for $l \in \mathcal{L}$ a spectral decomposition of $\phi_{A'_l}$ such that $\phi_{A'_l} = \sum_{x_l} p_{X_l}(x_l)\phi_{A'_l}^{x_l}$, where each state $\phi_{A'_l}^{x_l}$ is pure. Then, define

$$
\sigma_{X_{\mathcal{L}}A'_{\mathcal{L}}} \triangleq \sum_{x_{\mathcal{L}}} p_{X_{\mathcal{L}}}(x_{\mathcal{L}})|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \otimes \bigotimes_{l\in\mathcal{L}}\phi_{A'_l}^{x_l},
$$

where $|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \triangleq \bigotimes_{\in\mathcal{L}} |x_l\rangle\langle x_l|$, $x_{\mathcal{L}} \triangleq (x_l)_{l\in\mathcal{L}}$, and $p_{X_{\mathcal{L}}}(x_{\mathcal{L}}) \triangleq \prod_{\in\mathcal{L}} p_{X_l}(x_l)$. Define also $\sigma_{X_{\mathcal{L}}BE} \triangleq$

$\mathcal{U}^{\mathcal{N}}_{A'_{\mathcal{L}}\to BE}(\sigma_{X_{\mathcal{L}}A'_{\mathcal{L}}})$. Then, we have

$$\begin{aligned} Q^{\text{sum}}_{\text{MAC}}(\mathcal{N}) &= I(A_{\mathcal{L}}\rangle B)_{\phi} \\ &\overset{(a)}{=} H(B)_{\phi} - H(E)_{\phi} \\ &= H(B)_{\sigma} - H(E)_{\sigma} \\ &\overset{(b)}{=} I(X_{\mathcal{L}};B)_{\sigma} - I(X_{\mathcal{L}};E)_{\sigma} \\ &\overset{(c)}{\leqslant} P^{\text{sum}}_{\text{MAC}}(\mathcal{N}), \end{aligned}$$

where (a) holds because $H(A_{\mathcal{L}}B)_{\rho} = H(E)_{\rho}$ by purity of $\phi_{A_{\mathcal{L}}BE}$, (b) holds because $H(E|X_{\mathcal{L}})_{\sigma} = H(B|X_{\mathcal{L}})_{\sigma}$ by purity of $\sigma^{x_{\mathcal{L}}}_{BE}$, (c) holds by definition of $P^{\text{sum}}_{\text{MAC}}(\mathcal{N})$.

Appendix F
Supporting Lemmas

Lemma 9 ([32, Lemma 5.1.3]): Let ρ be a Hermitian operator and σ be a nonnegative operator on the same Hilbert space. Then, $\|\rho\|_1 \leqslant \sqrt{\text{Tr}[\sigma]\,\text{Tr}[(\rho\sigma^{-1/2})^2]}$.

Lemma 10 ([32, Lemma B.5.3]): For any $\rho_{XE} \in \mathcal{S}_{\leqslant}(\mathcal{H}_X \otimes \mathcal{H}_E)$ and $\sigma_E \in \mathcal{S}_{=}(\mathcal{H}_E)$, we have $H_2(\rho_{XE}|\sigma_E) \geqslant H_{\min}(\rho_{XE}|\sigma_E)$.

Lemma 11 ([45, Theorem 2]): Consider a probability distribution $p_{X^n} \triangleq \prod_{i=1}^n p_{X_i}$ over $\mathcal{X}^n$. For any $\delta \in [0, \log|\mathcal{X}|]$, we have

$$\mathbb{P}[-\log p_{X^n}(X^n) \leqslant H(X^n) - n\delta] \leqslant 2^{-\frac{n\delta^2}{2\log(|\mathcal{X}|+3)^2}},$$

$$\mathbb{P}[-\log p_{X^n}(X^n) \geqslant H(X^n) + n\delta] \leqslant 2^{-\frac{n\delta^2}{2\log(|\mathcal{X}|+3)^2}}.$$

Lemma 12 ([32, Lemma 3.1.10]): For any $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$, the fully mixed state on the support of ρ_B, we have $H_{\min}(\rho_{AB}) = H_{\min}(\rho_{AB}|\sigma_B) + H_{\max}(\rho_B)$.

Lemma 13 ([20, Lemma 4]): Consider a function $f : \mathcal{X} \to \mathcal{Y}$ and $\epsilon > 0$. We have $\mathbb{P}[|f^{-1}(Y)| \geqslant \epsilon|\mathcal{X}|/|\mathcal{Y}|] \geqslant 1-\epsilon$, where the probability is taken over Y uniformly distributed in $\mathcal{Y}$.

We next review some definitions and results related to submodular functions.

Definition 5 ([42], [46]): Let $f : 2^{\mathcal{L}} \to \mathbb{R}$. $\mathcal{P}(f) \triangleq \left\{(R_l)_{l\in\mathcal{L}} \in \mathbb{R}^L_+ : R_{\mathcal{S}} \leqslant f(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L}\right\}$ associated with the function f, is a polymatroid if

i) f is normalized, i.e., $f(\emptyset) = 0$,
ii) f is non-decreasing, i.e., $\forall \mathcal{S},\mathcal{T} \subset \mathcal{L}, \mathcal{S} \subset \mathcal{T} \implies f(\mathcal{S}) \leqslant f(\mathcal{T})$,
iii) f is submodular, i.e., $\forall \mathcal{S},\mathcal{T} \subset \mathcal{L}, f(\mathcal{S}\cup\mathcal{T}) + f(\mathcal{S}\cap\mathcal{T}) \leqslant f(\mathcal{S}) + f(\mathcal{T})$.

Lemma 14: Let $\rho_{X_{\mathcal{L}}BE}$ be as defined in Theorem 1.

i) The set function $h_{\rho} : 2^{\mathcal{L}} \to \mathbb{R}, \mathcal{S} \mapsto H(X_{\mathcal{S}}|E)_{\rho}$ is submodular.
ii) The set function $g_{\rho} : 2^{\mathcal{L}} \to \mathbb{R}, \mathcal{S} \mapsto -H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_{\rho}$ is submodular.
iii) The set function $f_{\rho} : 2^{\mathcal{L}} \to \mathbb{R}, \mathcal{S} \mapsto I(X_{\mathcal{S}};B|X_{\mathcal{S}^c})_{\rho} - I(X_{\mathcal{S}};E)_{\rho}$ is submodular.

Proof: We first prove (i). For $\mathcal{S},\mathcal{T} \subseteq \mathcal{L}$, we have

$$\begin{aligned} &h_{\rho}(\mathcal{S}\cup\mathcal{T}) + h_{\rho}(\mathcal{S}\cap\mathcal{T}) \\ &= H(X_{\mathcal{S}\cup\mathcal{T}}|E)_{\rho} + H(X_{\mathcal{S}\cap\mathcal{T}}|E)_{\rho} \\ &= H(X_{\mathcal{S}}|E)_{\rho} + H(X_{\mathcal{T}\setminus\mathcal{S}}|X_{\mathcal{S}}E)_{\rho} + H(X_{\mathcal{S}\cap\mathcal{T}}|E)_{\rho} \\ &\leqslant H(X_{\mathcal{S}}|E)_{\rho} + H(X_{\mathcal{T}\setminus\mathcal{S}}|X_{\mathcal{S}\cap\mathcal{T}}E)_{\rho} + H(X_{\mathcal{S}\cap\mathcal{T}}|E)_{\rho} \\ &= h_{\rho}(\mathcal{S}) + h_{\rho}(\mathcal{T}), \end{aligned}$$

where the inequality holds because conditioning does not increase entropy.

Next, we prove (ii). Remark that for any $\mathcal{S} \subseteq \mathcal{L}$, we have $g_{\rho}(\mathcal{S}) = -H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_{\rho} = H(BX_{\mathcal{S}^c})_{\rho} - H(X_{\mathcal{L}}B)_{\rho} = H(X_{\mathcal{S}^c}|B)_{\rho} - H(X_{\mathcal{L}}|B)_{\rho}$, and $\mathcal{S} \mapsto H(X_{\mathcal{S}^c}|B)_{\rho}$ is submodular by (i) since $\mathcal{S} \mapsto f(\mathcal{S})$ submodular implies $\mathcal{S} \mapsto f(\mathcal{S}^c)$ submodular. Hence, g_{ρ} is submodular.

Finally, we prove (iii). Remark that we have $f_{\rho} = g_{\rho} + h_{\rho}$. Hence, since the sum of two submodular functions is submodular, f_{ρ} is submodular. ∎

Lemma 15 ([47, Lemma 2]): Consider two submodular functions $f : 2^{\mathcal{L}} \to \mathbb{R}$ and $g : 2^{\mathcal{L}} \to \mathbb{R}$. Then, the following system of equations for $(x_l)_{l\in\mathcal{L}} \in \mathbb{R}^L_+$

$$-g(\mathcal{S}) \leqslant \sum_{s\in\mathcal{S}} x_s \leqslant f(\mathcal{S}), \forall \mathcal{S} \subseteq \mathcal{L},$$

has a solution if and only if $-g(\mathcal{S}) \leqslant f(\mathcal{S}), \forall \mathcal{S} \subseteq \mathcal{L}$.

Lemma 16 ([15, Lemma 9]): Let $f : 2^{\mathcal{L}} \to \mathbb{R}$ be a positive, normalized, and submodular function. Then,

$$f^* : 2^{\mathcal{L}} \to \mathbb{R}_+, \mathcal{S} \mapsto \min_{\substack{\mathcal{A}\subseteq\mathcal{L} \\ \text{s.t. } \mathcal{A}\supseteq\mathcal{S}}} f(\mathcal{A}).$$

is normalized, non-decreasing, and submodular.

References

[1] R. A. Chou, "Private classical communication over quantum multiple-access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 617–622.
[2] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems Inf. Transmiss.*, vol. 40, no. 4, pp. 318–336, 2004.
[3] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.
[4] G. Smith, "Private classical capacity with a symmetric side channel and its application to quantum cryptography," *Phys. Rev. A, Gen. Phys.*, vol. 78, Aug. 2008, Art. no. 022306.
[5] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[6] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Aug. 2010, pp. 1–5.
[7] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 595–605, Sep. 2011.
[8] M. Wiese and H. Boche, "Strong secrecy for multiple access channels," in *Information Theory, Combinatorics, Search Theory*. Springer, 2013, pp. 71–122.
[9] Y. Chen, O. O. Koyluoglu, and A. H. Vinck, "Collective secrecy over the k-transmitter multiple access channel," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2279–2293, Mar. 2018.
[10] M. Hayashi and Y. Chen, "Secrecy and error exponents of k-transmitter multiple access wire-tap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2019, pp. 1–5.
[11] A. Winter, "The capacity of the quantum multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3059–3065, Nov. 2001.
[12] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 364–375, Mar. 1996.
[13] A. J. Grant, B. Rimoldi, R. L. Urbanke, and P. A. Whiting, "Rate-splitting multiple access for discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 873–890, Mar. 2001.

[14] R. A. Chou and A. Yener, "The Gaussian multiple access wiretap channel when the eavesdropper can arbitrarily jam," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1958–1962.
[15] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, Dec. 2018.
[16] I. Csiszár, "Almost independence and secrecy capacity," *Problems Inf. Transmiss.*, vol. 32, no. 1, pp. 40–47, 1996.
[17] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.
[18] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[19] T. S. Han, *Information-Spectrum Methods in Information Theory*, vol. 50. Berlin, Germany: Springer, 2002.
[20] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7377–7385, Nov. 2011.
[21] I. Devetak and A. Winter, "Classical data compression with quantum side information," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 4, Oct. 2003, Art. no. 042301.
[22] M. Tomamichel and M. Hayashi, "A hierarchy of information quantities for finite block length analysis of quantum tasks," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7693–7710, Nov. 2013.
[23] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.
[24] R. A. Chou, "Unified framework for polynomial-time wiretap channel codes," 2020, *arXiv:2002.01924*.
[25] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.
[26] R. A. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 476–480.
[27] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.
[28] M. Hayashi, "Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5595–5622, Oct. 2015.
[29] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.
[30] L. Drescher and O. Fawzi, "On simultaneous min-entropy smoothing," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 161–165.
[31] S. Chakraborty, A. Nema, and P. Sen, "One-shot inner bounds for sending private classical information over a quantum MAC," 2021, *arXiv:2105.06100*.
[32] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.* vol. 6, no. 1, pp. 1–127, Feb. 2008.
[33] J. Yard, P. Hayden, and I. Devetak, "Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3091–3113, Jul. 2008.
[34] J. Wullschleger, "Oblivious-transfer amplification," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2007, pp. 555–572.
[35] A. C. A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2572–2581, Jun. 2008.
[36] R. A. Chou, "Pairwise oblivious transfer," in *IEEE Inf. Theory Workshop (ITW)*, Apr. 2021, pp. 1–5.
[37] R. A. Chou and A. Yener, "Secret-key generation in many-to-one networks: An integrated game-theoretic and information-theoretic approach," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5144–5159, Aug. 2019.
[38] R. A. Chou, "Biometric systems with multiuser access structures," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 807–811.
[39] R. A. Chou, "Secret sharing over a public channel from correlated random variables," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 991–995.
[40] R. Sultana and R. A. Chou, "Explicit construction of multiple access channel resolvability codes from source resolvability codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 1576–1580.
[41] A. Winter, "Coding theorems of quantum information theory," Ph.D. dissertation, Dept. Mathematik, Univ. Bielefeld, Bielefeld, Germany, 1999.
[42] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," *Combinat. Struct. Appl.*, vol. 14, pp. 69–87, Jan. 1970.
[43] M. M. Wilde, *Quantum Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[44] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, Aug. 2011.
[45] T. Holenstein and R. Renner, "On the randomness of independent experiments," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1865–1871, Apr. 2011.
[46] D. N. C. Tse and S. V. Hanly, "Multiaccess fading channels. I. Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, Nov. 1998.
[47] H. Zhang, Y. Liang, L. Lai, and S. Shamai (Shitz), "Multi-key generation over a cellular model with a helper," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3804–3822, Jun. 2017.

Rémi A. Chou (Member, IEEE) received the degree in engineering from Supélec, Gif-sur-Yvette, France, in 2011, and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2015. From 2015 to 2017, he was a Post-Doctoral Scholar at The Pennsylvania State University, University Park, PA, USA. He is currently an Assistant Professor with the Electrical Engineering and Computer Science Department, Wichita State University, Wichita, KS, USA.