Private Classical Communication over Quantum Multiple-Access Channels

Rémi A. Chou
Department of Electrical Engineering & Computer Science
Wichita State University, Wichita, KS 67260
remi.chou@wichita.edu

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9517802

***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. 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. 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.**

I. Introduction

The capacity of private classical communication over point-to-point quantum channels has been characterized in [1], [2]. Moreover, in the case of degradable quantum channels, a single-letter expression of the capacity is known [3], and coincides with the coherent information of the channel. In this paper, we define private classical communication over quantum multiple-access channels, and determine 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 generalization of the classical multiple-access wiretap channel [4]. Note also that the capacity region of classical communication over multiple-access quantum channels without privacy constraint is characterized in [5].

Often, for simplicity and to facilitate the design of codes, coding for multiple-access channels is reduced to single-user coding, for instance, with successive decoding or rate-splitting [6]. 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 [5] 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 [7], 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 [8]. Instead, our approach relies on ideas from random binning techniques, first developped in [9] for classical point-to-point wiretap channels and that have been succesfully applied to point-to-point classical-quantum wiretap channels [10] and several other point-to-point wiretap channel models [11]–[14]. In our approach, reliability and privacy constraints are decoupled. It allows us to handle the reliability via distributed source coding with quantum side information at the receiver, and to handle the privacy constraint via distributed hashing.

This work was supported in part by NSF grants CCF-1850227 and CCF-2047913.

We summarize our main contributions as follows. We derive (i) a regularized expression for the private classical capacity region of quantum multiple-access channels *for an arbitrary number of transmitters*, and (ii) a single-letter expression of the best achievable sum-rate for degradable channels. (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.

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. Finally, we provide concluding remarks in Section VII.

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 definite operators on $\mathcal{H}$. Then, let $\mathcal{S}_=(\mathcal{H}) \triangleq \{\rho \in \mathcal{P}(\mathcal{H}) : \operatorname{Tr}\rho = 1\}$ and $\mathcal{S}_\leqslant(\mathcal{H}) \triangleq \{\rho \in \mathcal{P}(\mathcal{H}) : \operatorname{Tr}\rho \leqslant 1\}$ 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 [15] is defined as $H_{\min}(\rho_{XE}|\sigma_E) \triangleq \inf\left\{\lambda \in \mathbb{R} : \rho_{XE} \leqslant 2^{-\lambda} I_X \otimes \sigma_E\right\}$, where I_X denotes the identity operator on $\mathcal{H}_X$, and the max-entropy of ρ_E [15] is defined as $H_{\max}(\rho_E) \triangleq \log \operatorname{rank}(\rho_E)$. For two probability

distributions p and q defined over the same finite alphabet $\mathcal{X}$, define the variational distance between p and q as $\mathbb{V}(p,q) \triangleq \sum_{x\in\mathcal{X}}|p(x)-q(x)|$. 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 $\mathcal{N}^c_{A'_{\mathcal{L}}\to E}(\rho) = \mathrm{Tr}_B[\mathcal{U}^{\mathcal{N}}_{A'_{\mathcal{L}}\to BE}(\rho)]$ 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*

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

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

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*

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

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

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

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

Proof. The achievability is proved in Section VI. The proof of the converse is omitted due to space constraints. ∎

Remark 1. *In the absence of the privacy constraint (2), one easily has a regularized expression for the best achievable sum-rate from Theorem 1 because $\{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{S}} \leqslant I(X_{\mathcal{S}};B|X_{\mathcal{S}^c})_\rho, \forall\mathcal{S}\subseteq\mathcal{L}\}$ defines a polymatroid [16], [17]. However, for general (or even degradable) channels, it is non-trivial to obtain a simple regularized expression for the best achievable sum-rate in $C_{\text{P-MAC}}$, because $\{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{S}} \leqslant [I(X_{\mathcal{S}};B|X_{\mathcal{S}^c})_\rho - I(X_{\mathcal{S}};E)_\rho]^+, \forall\mathcal{S}\subseteq\mathcal{L}\}$ does not describe a polymatroid in general.*

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*

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

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

We now propose another 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 $Q^{\text{sum}}_{\text{MAC}}(\mathcal{N}) \triangleq \max_{\phi_{A_{\mathcal{L}}A'_{\mathcal{L}}}} I(A_{\mathcal{L}}\rangle B)_\rho$, 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 [18], $\lim_{n\to\infty} \frac{1}{n} Q^{\text{sum}}_{\text{MAC}}(\mathcal{N}^{\otimes n})$ 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*

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

The proofs of Theorems 2 and 3 are omitted due to space constraints. Note that in the case of point-to-point channels Theorem 3 recovers the result in [3, 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:

$$\rho_{X_{\mathcal{L}}E} \triangleq \sum_{x_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}} |x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \otimes \rho_E^{x_{\mathcal{L}}}, \tag{4}$$

where $\rho_E^{x_{\mathcal{L}}} \triangleq p_{X_{\mathcal{L}}}(x_{\mathcal{L}})\bar{\rho}_E^{x_{\mathcal{L}}}$ with $\bar{\rho}_E^{x_{\mathcal{L}}}$ the state of the system E conditioned on the realization $x_{\mathcal{L}}$, and $|x_{\mathcal{L}}\rangle\langle x_{\mathcal{L}}| \triangleq \bigotimes_{l\in\mathcal{L}} |x_l\rangle\langle x_l|$. 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 [19], 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 $a_{\mathcal{S}} \in \mathcal{A}_{\mathcal{S}}$, $f_{\mathcal{S}} \in \mathcal{F}_{\mathcal{S}}$, $f_{\mathcal{S}}^{-1}(a_{\mathcal{S}}) \triangleq \{x_{\mathcal{S}} \in \mathcal{X}_{\mathcal{S}} : f(x_l) = a_l, \forall l \in \mathcal{S}\}$. The hash functions outputs $f_{\mathcal{L}}(x_{\mathcal{L}})$, the state of the quantum system, and the choice of the functions $f_{\mathcal{L}}$ are described by

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

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

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*

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

Note that a similar lemma is known in the classical case, e.g., [20], and has found a wide range of applications including oblivious transfer [20]–[22], many-to-one secret-key generation [23], biometric authentication with access structures [24], multiple-access channel resolvability [25], and distributed secret sharing [26]. We will also need the following version of the distributed leftover hash lemma for product states. The proof of Lemmas 1, 2 are omitted due to space constraints.

Lemma 2 (Distributed leftover hash lemma for product states)**.** *Consider the product state $\rho_{X_{\mathcal{L}}^n E^n} \triangleq \rho_{X_{\mathcal{L}}E}^{\otimes n}$, where $\rho_{X_{\mathcal{L}}E}$ is defined in* (4)*. 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* $d_E \triangleq \dim \mathcal{H}_E$.

B. Distributed classical data compression 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 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 compression 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 $h : \mathcal{S}_=(\mathcal{H}_{B^n}) \times \bigtimes_{l\in\mathcal{L}} \mathcal{C}_l$.*

A rate-tuple $(R_l)_{l\in\mathcal{L}}$ is said to be achievable when the average error probability satisfies

$$P_e(n) \triangleq \sum_{x_{\mathcal{L}}^n \in \mathcal{X}_{\mathcal{L}}^n} p_{X_{\mathcal{L}}^n}(x_{\mathcal{L}}^n)\mathbb{P}\Big[h(\bar{\rho}_{B^n}^{x_{\mathcal{L}}^n}, g_{\mathcal{L}}(x_{\mathcal{L}}^n)) \neq x_{\mathcal{L}}^n\Big] \xrightarrow{n\to\infty} 0,$$

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 3 ([27])**.** *We have*

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

C. MAC 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 4 (MAC coding from distributed compression)**.** *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 compression code (as in Definition 4) for the classical-quantum product state $\rho_{U_{\mathcal{L}}B}^{\otimes n}$, then there exist $(R_l)_{l\in\mathcal{L}} \in \mathbb{R}_+^L$, 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 $R_l = R_l^{\mathrm{U}} - R_l^{\mathrm{DC}}$ as $n \to \infty$, $l \in \mathcal{L}$, and $\mathbb{P}[d(\bar{\rho}_{B^n}^{e_{\mathcal{L}}(M_{\mathcal{L}})}) \neq M_{\mathcal{L}}] \xrightarrow{n\to\infty} 0$, where $e_{\mathcal{L}}(M_{\mathcal{L}}) \triangleq (e_l(M_l))_{l\in\mathcal{L}}$.*

The proof of Lemma 4 is omitted due to space constraints. Note that this lemma generalizes [10, 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 follows from 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

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

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 this region 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.

Step 1: We create a stochastic channel that simulates the inversion of multiple hash functions while preserving the joint distribution of the inputs and outputs of the hash functions. Preserving 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 [10] and distribution approximation in [12].

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 $(nR_l^{\mathrm{U}})_{l\in\mathcal{L}}$ of the hash functions 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 $\mathcal{U}_l^n \triangleq [2^{nR_l^{\mathrm{U}}}]$ for some $R_l^{\mathrm{U}} \in \mathbb{R}_+$ to be defined later, and define

$$\widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}} \triangleq p_{X_{\mathcal{L}}^n|F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}} p_{U_{\mathcal{L}}^n} p_{F_{\mathcal{L}}}, \tag{5}$$

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, $\widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}}$ 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 $\widetilde{W}_{\mathcal{L}}$. Note that $F_{\mathcal{L}}$ is uniformly distributed over $\mathcal{F}_{\mathcal{L}}$ and is interpreted as local randomness. 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 the local randomness $F_{\mathcal{L}}$ in its definition.

Step 2: Using Lemma 4, 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 3, there exists a $(2^{mnR_l^{\mathrm{DC}}})_{l\in\mathcal{L}}$ distributed compression code (as defined in Definition 4) for the classical-quantum product state $\widetilde{\rho}_{U_{\mathcal{L}}^n B^n}^{\otimes m}$, where

$$\widetilde{\rho}_{U_{\mathcal{L}}^n B^n} \triangleq \frac{1}{|\mathcal{U}_{\mathcal{L}}^n|} \sum_{u_{\mathcal{L}}^n \in \mathcal{U}_{\mathcal{L}}^n} |u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes \bar{\rho}_{B^n}^{\widetilde{W}_{\mathcal{L}}(u_{\mathcal{L}}^n)}, \tag{6}$$

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 4, there exist $e_l : \mathcal{M}_l^m \to \mathcal{U}_l^{mn}, l \in \mathcal{L}$, and $d : \mathcal{S}_=(\mathcal{H}_{B^{mn}}) \to \mathcal{M}_{\mathcal{L}}^m$, 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

$$\lim_{m\to\infty} \mathbb{P}\left[d\left(\bar{\rho}_{B^{mn}}^{\widetilde{W}_{\mathcal{L}}^{\otimes m}(e_{\mathcal{L}}(M_{\mathcal{L}}^m))} \right) \neq M_{\mathcal{L}}^m \right] = 0, \tag{7}$$

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

$$\phi_l : M_l^m \mapsto \widetilde{W}_l^{\otimes m}(e_l(M_l^m)), l \in \mathcal{L}, \tag{8}$$

and the decoder is defined as

$$\psi : \bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)} \mapsto d(\bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)}), \tag{9}$$

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

Remark 2. *In Step 2, Lemma 3 cannot be directly applied to $\widetilde{\rho}_{U_{\mathcal{L}}^n Y^n}$ as it is not a product state.*

B. Coding scheme analysis

1) Average reliability: We have

$$\begin{aligned}\mathbb{P}\left[\psi(\bar{\rho}_{B^{mn}}^{\phi_{\mathcal{L}}(M_{\mathcal{L}}^m)}) \neq M_{\mathcal{L}}^m\right] &= \mathbb{P}\left[d(\bar{\rho}_{B^{mn}}^{\widetilde{W}_{\mathcal{L}}^{\otimes m}(e_{\mathcal{L}}(M_{\mathcal{L}}^m))}) \neq M_{\mathcal{L}}^m \right] \\ &\xrightarrow{m\to\infty} 0, \end{aligned} \tag{10}$$

where the equality holds by definition of ψ and $(\phi_l)_{l\in\mathcal{L}}$ in (8), (9), and the limit holds by (7).

2) Average message indistinguishability: To simplify notation, we use the notation $\mathbf{x}_{\mathcal{L}} \triangleq x_{\mathcal{L}}^{nm}$, $\mathbf{u}_{\mathcal{L}} \triangleq u_{\mathcal{L}}^{nm}$, $\mathbf{f}_{\mathcal{L}} \triangleq f_{\mathcal{L}}^m$, for $u_{\mathcal{L}}^{nm} \in \mathcal{U}_{\mathcal{L}}^{mn}$, $x_{\mathcal{L}}^{mn} \in \mathcal{X}_{\mathcal{L}}^{mn}$, $f_{\mathcal{L}}^m \in \mathcal{F}_{\mathcal{F}}^m$. According to Step 3 in Section VI-A, the messages $M_{\mathcal{L}}^m$ and the output of the channel between the transmitters and the eavesdropper are described by the classical-quantum state $\widetilde{\rho}_{M_{\mathcal{L}}^m E^{nm} F_{\mathcal{L}}^m}$ with

$$\begin{aligned}\widetilde{\rho}_{M_{\mathcal{L}}^m E^{mn} F_{\mathcal{L}}^m} \triangleq \sum_{\mathbf{f}_{\mathcal{L}},\mathbf{u}_{\mathcal{L}},\mathbf{x}_{\mathcal{L}}} \widetilde{p}_{X_{\mathcal{L}}^{mn} M_{\mathcal{L}}^m F_{\mathcal{L}}^m}(\mathbf{x}_{\mathcal{L}}, \mathbf{u}_{\mathcal{L}}, \mathbf{f}_{\mathcal{L}}) \\ \times |\mathbf{u}_{\mathcal{L}}\rangle\langle\mathbf{u}_{\mathcal{L}}| \otimes \bar{\rho}_{E^{mn}}^{\mathbf{x}_{\mathcal{L}}} \otimes |\mathbf{f}_{\mathcal{L}}\rangle\langle\mathbf{f}_{\mathcal{L}}|, \end{aligned}$$

where $\widetilde{p}_{X_{\mathcal{L}}^{mn} M_{\mathcal{L}}^m F_{\mathcal{L}}^m} \triangleq \prod_{i=1}^m \widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}}$. Note that $M_{\mathcal{L}}$ is uniformly distributed over $\mathcal{U}_{\mathcal{L}}^n$ and, by Lemma 4, $e_{\mathcal{L}}(M_{\mathcal{L}}^m)$ is uniformly distributed over $\mathcal{U}_{\mathcal{L}}^{mn}$. Hence, $\widetilde{W}_{\mathcal{L}}^{\otimes m}(e_{\mathcal{L}}(M_{\mathcal{L}}^m))$ is distributed according to a product distribution, and $\widetilde{\rho}_{M_{\mathcal{L}}^m E^{mn} F_{\mathcal{L}}^m}$ is thus a product state, which we can write $\widetilde{\rho}_{M_{\mathcal{L}}^m E^{mn} F_{\mathcal{L}}^m} = \widetilde{\rho}_{M_{\mathcal{L}} E^n F_{\mathcal{L}}}^{\otimes m}$, where

$$\begin{aligned}\widetilde{\rho}_{M_{\mathcal{L}} E^n F_{\mathcal{L}}} \triangleq \sum_{f_{\mathcal{L}},u_{\mathcal{L}}^n,x_{\mathcal{L}}^n} \widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}}(x_{\mathcal{L}}^n, u_{\mathcal{L}}^n, f_{\mathcal{L}}) \\ \times |u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes \bar{\rho}_{E^n}^{x_{\mathcal{L}}^n} \otimes |f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|. \end{aligned} \tag{11}$$

Next, define the following classical-quantum state

$$\begin{aligned}\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n)E^n F_{\mathcal{L}}} \triangleq \sum_{f_{\mathcal{L}},u_{\mathcal{L}}^n,x_{\mathcal{L}}^n} p_{X_{\mathcal{L}}^n F_{\mathcal{L}}(X_{\mathcal{L}}^n)F_{\mathcal{L}}}(x_{\mathcal{L}}^n, u_{\mathcal{L}}^n, f_{\mathcal{L}}) \\ \times |u_{\mathcal{L}}^n\rangle\langle u_{\mathcal{L}}^n| \otimes \bar{\rho}_{E^n}^{x_{\mathcal{L}}^n} \otimes |f_{\mathcal{L}}\rangle\langle f_{\mathcal{L}}|. \end{aligned} \tag{12}$$

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

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

$$
\begin{aligned}
&\quad + \|\rho_U \otimes \rho_{E^n F_{\mathcal{L}}} - \rho_U \otimes \widetilde{\rho}_{E^n F_{\mathcal{L}}}\|_1) \\
&\leqslant m(2\|\widetilde{\rho}_{M_{\mathcal{L}} E^n F_{\mathcal{L}}} - \rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}}\|_1 \\
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1) \\
&\overset{(c)}{\leqslant} m(2\mathbb{V}(\widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}}, p_{X_{\mathcal{L}}^n F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}}) \\
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1) \\
&\overset{(d)}{=} m(2\mathbb{V}(p_{U_{\mathcal{L}}^n} p_{F_{\mathcal{L}}}, p_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}}) \\
&\quad + \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1) \\
&\overset{(e)}{\leqslant} 3m\|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1 \\
&\xrightarrow{n\to\infty} 0, \qquad (13)
\end{aligned}
$$

where (a) and (b) hold by the triangle inequality, (c) holds by strong convexity of the trace distance and the definitions of $\widetilde{\rho}_{M_{\mathcal{L}} E^n F_{\mathcal{L}}}$ and $\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}}$ in (11) and (12), (d) holds by the definition of $\widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}}$ in (5), (e) holds because $\mathbb{V}(p_{U_{\mathcal{L}}^n} p_{F_{\mathcal{L}}}, p_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}}) \leqslant \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}} - \rho_U \otimes \rho_{F_{\mathcal{L}}}\|_1$, and the limit holds by Lemma 2 provided that $R_{\mathcal{S}}^{\mathrm{U}} \leqslant H(X_{\mathcal{S}}|E)_\rho$, $\forall \mathcal{S} \subseteq \mathcal{L}$ as $n \to \infty$.

3) Achievable rate-tuples: Consider the following extension of the state described in (6)

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

Define also the state

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

Then, we have

$$
\begin{aligned}
&\max\left(\|\widetilde{\rho}_{X_{\mathcal{L}}^n B^n} - \rho_{X_{\mathcal{L}}^n B^n}\|_1, \max_{\mathcal{S}\subseteq\mathcal{L}} \|\widetilde{\rho}_{U_{\mathcal{S}}^n B^n} - \rho_{U_{\mathcal{S}}^n B^n}\|_1\right) \\
&\leqslant \|\widetilde{\rho}_{U_{\mathcal{L}}^n X_{\mathcal{L}}^n B^n F_{\mathcal{L}}} - \rho_{U_{\mathcal{L}}^n X_{\mathcal{L}}^n B^n F_{\mathcal{L}}}\|_1 \\
&\overset{(a)}{\leqslant} \mathbb{V}(\widetilde{p}_{X_{\mathcal{L}}^n M_{\mathcal{L}} F_{\mathcal{L}}}, p_{X_{\mathcal{L}}^n F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}}) \\
&\overset{(b)}{=} \mathbb{V}(p_{U_{\mathcal{L}}^n} p_{F_{\mathcal{L}}}, p_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}}) \\
&\leqslant \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) F_{\mathcal{L}}} - \rho_U \otimes \rho_{F_{\mathcal{L}}}\|_1 \\
&\leqslant \|\rho_{F_{\mathcal{L}}(X_{\mathcal{L}}^n) E^n F_{\mathcal{L}}} - \rho_U \otimes \rho_{E^n F_{\mathcal{L}}}\|_1 \\
&\xrightarrow{n\to\infty} 0 \qquad (14)
\end{aligned}
$$

where (a) holds by strong convexity of the trace distance, (b) holds by (5), and the limit holds by (13).

Next, by Step 2 in Section VI-A, $(nR_l^{\mathrm{DC}})_{l\in\mathcal{L}}$ must belong to $\mathcal{C}(\widetilde{\rho}_{U_{\mathcal{L}}^n B^n})$. We 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

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

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 2 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 (14), (e) holds by the quantum data processing inequality because, by definition of $\widetilde{\rho}$, $\widetilde{X}_{\mathcal{L}}^n$ 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 $R_{\mathcal{S}}^{\mathrm{U}} \leqslant H(X_{\mathcal{S}}|E)_\rho$, $\forall \mathcal{S} \subseteq \mathcal{L}$ in (13), and by using Step 3 in Section VI-A, we have the system

$$
\begin{pmatrix} R_{\mathcal{S}}^{\mathrm{DC}} \geqslant H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho, \forall \mathcal{S} \subseteq \mathcal{L} \\ R_{\mathcal{S}} + R_{\mathcal{S}}^{\mathrm{DC}} \leqslant H(X_{\mathcal{S}}|E)_\rho, \forall \mathcal{S} \subseteq \mathcal{L} \end{pmatrix}. \qquad (15)
$$

Next, one can show that the set function $\mathcal{S} \mapsto H(X_{\mathcal{S}}|E)_\rho - H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho$ is submodular. Using this fact and Fourier-Motzkin elimination, one can then show that the system (15) reduces to

$$
R_{\mathcal{S}} \leqslant H(X_{\mathcal{S}}|E)_\rho - H(X_{\mathcal{S}}|BX_{\mathcal{S}^c})_\rho, \forall \mathcal{S} \subseteq \mathcal{L}. \qquad (16)
$$

4) Expurgation: With an expurgation argument that has a negligible impact on the asymptotic communication rates, one can show the existence of a code such that for any codeword $\mathbf{m}_{\mathcal{L}}$, we have $\|\bar{\rho}_{E^{nm} F_{\mathcal{L}}^m}^{\mathbf{m}_{\mathcal{L}}} - \widetilde{\rho}_{E^{nm} F_{\mathcal{L}}^m}\|_1 \xrightarrow{n\to\infty} 0$ and $\mathbb{P}\left[\psi(\bar{\rho}_{Y^{mn}}^{\phi_{\mathcal{L}}(\mathbf{M}_{\mathcal{L}})}) \neq \mathbf{M}_{\mathcal{L}} | \mathbf{M}_{\mathcal{L}} = \mathbf{m}_{\mathcal{L}}\right] \xrightarrow{n\to\infty} 0$.

VII. Concluding remarks

We defined the private capacity region for quantum multiple-access channels and established a regularized expression for this capacity region. In the case of degradable channels, we also derived two single-letter expressions for the best achievable sum-rate.

Our proof technique for the achievability part emulates 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, our proof reduces 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 (for instance, via time-sharing), and distributed hashing is, by construction, performed independently at each transmitter.

REFERENCES

[1] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, no. 4, pp. 318–336, 2004.

[2] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[3] G. Smith, "Private classical capacity with a symmetric side channel and its application to quantum cryptography," *Physical Review A*, vol. 78, no. 2, p. 022306, 2008.

[4] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[5] A. Winter, "The capacity of the quantum multiple-access channel," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3059–3065, 2001.

[6] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 364–375, 1996.

[7] R. Chou and A. Yener, "The Gaussian multiple access wiretap channel when the eavesdropper can arbitrarily jam," in *IEEE International Symposium on Information Theory (ISIT)*, 2017, pp. 1958–1962.

[8] ——, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7903–7921, 2018.

[9] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, 1996.

[10] J. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7377–7385, 2011.

[11] R. Chou, "Unified framework for polynomial-time wiretap channel codes," *arXiv preprint arXiv:2002.01924*, 2020.

[12] R. Chou and M. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, 2016.

[13] M. Yassaee, M. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6760–6786, 2014.

[14] R. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 476–480.

[15] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[16] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," *Combinatorial structures and their applications*, pp. 69–87, 1970.

[17] D. Tse and S. Hanly, "Multiaccess fading channels-Part I: Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 2796–2815, 1998.

[18] J. Yard, P. Hayden, and I. Devetak, "Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3091–3113, 2008.

[19] C. Bennett, G. Brassard, and U. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, pp. 1915–1923, 1995.

[20] J. Wullschleger, "Oblivious-transfer amplification," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2007, pp. 555–572.

[21] A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2572–2581, 2008.

[22] R. Chou, "Pairwise oblivious transfer," in *IEEE Information Theory Workshop (ITW)*, 2021.

[23] R. Chou and A. Yener, "Secret-key generation in many-to-one networks: An integrated game-theoretic and information-theoretic approach," *IEEE Transactions on Information Theory*, vol. 65, no. 8, pp. 5144–5159, 2019.

[24] R. Chou, "Biometric systems with multiuser access structures," in *IEEE International Symposium on Information Theory (ISIT)*, 2019, pp. 807–811.

[25] R. Sultana and R. Chou, "Explicit construction of multiple access channel resolvability codes from source resolvability codes," in *IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 1576–1580.

[26] R. Chou, "Secret sharing over a public channel from correlated random variables," in *IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 991–995.

[27] A. Winter, "Coding theorems of quantum information theory," *Ph.D. dissertation, Univ. Bielefeld, Bielefeld, Germany*, 1999.