Single-Serving Quantum Broadcast Channel with Common, Individualized and Confidential Messages

Farzin Salek, *Student Member, IEEE,* Min-Hsiu Hsieh, *Senior Member, IEEE,* Javier R. Fonollosa, *Senior Member, IEEE,*

***Abstract*—The two-receiver broadcast channel with primary and third party receivers is studied. The sender wishes to reliably communicate a common (or public) message to both receivers as well as individualized and confidential messages to the primary receiver only. The third party receiver must be kept completely ignorant of the confidential message but there are no secrecy requirements associated to the individualized message. A trade-off arises between the rates of the three messages: when one of the rates is high, the other rates may need to back off to guarantee the reliable transmission of all three messages. In addition, the confidentiality requirement implies availability of local randomness at the transmitter in order to implement a stochastic encoding. This paper studies the trade-off between the rates of the common, individualized and confidential messages as well as that of the local randomness in the one-shot regime of a quantum broadcast channel. We provide an achievability region, by proving a conditional version of the convex-split lemma combined with the position-based decoding, as well as a (weak) converse region. We study the asymptotic behaviour of our bounds and recover several well-known asymptotic results in the literature, including simultaneous transmission of classical and quantum information.**

***Index Terms*—One-shot coding, channel coding, private capacity, quantum capacity**

I. Introduction

Consider a communication system in which a sender aims to transmit a message reliably to a receiver while hiding it from an eavesdropper. This model was introduced by Wyner under the name "wiretap channel" [1]. The basic idea underlying Wyner's coding scheme is to generate a sufficiently large number of random sequences and position them into bins labeled with the messages to be transmitted. To send a message, a sequence from the message bin is randomly selected and transmitted. In the original model of Wyner, the eavesdropper is assumed to be at a physical disadvantage with respect to the legitimate receiver, meaning that, upon transmission over the channel, the eavesdropper only receives what can be regarded as a noisy version of the information received by the legitimate receiver. This model is usually referred to as the physically degraded wiretap channel. This channel description was later enhanced by Csiszár and Körner [2] by introducing a public message that is piggybacked on top of the confidential message and that is to be reliably decoded by both receivers. Furthermore, in this new model called broadcast channel with confidential messages (BCC), the legitimate receiver has no specific physical advantage over the eavesdropper. The coding scheme of the BCC consists of superposition coding [3] to encode the confidential message on top of the common message in combination with Wyner's codebook structure with local randomness for equivocation. The most important contribution of Csiszár and Körner consists of prepending a prefixing stochastic map to the channel and using a then-new single-letterization trick in the converse proof.

The implementation of the prefixing stochastic map is performed from random numbers using a method such as channel simulation [4]. This means that two sources of randomness are required for BCC coding, one for random codeword selection and another for channel simulation. Traditionally randomness has been assumed to be an unlimited resource. In practice, however, a limited randomness rate is reasonable, potentially compromising the simultaneous reliability and secrecy criteria. Csiszár and Körner [5] later proposed an alternative description of the BCC where the message to be transmitted consists of two *independent* parts, a confidential part defined in the same sense as the original BCC and a non-secret or individualized part, i.e. a message without any secrecy requirement placed on it, potentially and partially playing the role of a source of randomness.

The degraded wiretap channel when the randomness is constrained and not necessarily uniform was studied in [6]. The general BCC model with rate-constrained randomness was studied in [7] where the optimal rate region of the common, individualized, confidential and dummy randomness was determined for classical channels[1]. The achievability is based on superposition coding and building a deterministic codebook to replace the prefixing stochastic map. The idea of using a deterministic encoder in the wiretap channel was originally proposed in [8] in the contex of three-receiver broadcast channel . It was shown in [7] that the randomness

This work was presented in part at ISIT2019.

F. Salek is jointly affiliated with the Quantum Information Group (GIQ), Department of Physics at the Universitat Autònoma de Barcelona, Barcelona, Spain and with the Department of Signal Theory and Communications, Universitat Politècnica de Catalunya, Barcelona, Spain, e-mail: (farzin.salek@gmail.com).

J. R. Fonollosa is with the Department of Signal Theory and Communications, Universitat Politècnica de Catalunya, Barcelona, Spain, e-mail: (javier.fonollosa@upc.edu).

Min-Hsiu Hsieh is with the Center for Quantum Software and Information, Sydney University of Technology, Sydney, Australia, e-mail: (min-hsiu.hsieh@uts.edu.au).

[1]In [7], the non-secret or individualized message is referred to as private message. We find the nomenclature "private message" to be rather inconsistent for a message that need not be kept private and we instead use the word "individualized".

 DOI 10.1109/TIT.2020.3013098

needed to select a codeword following the scheme of [8] is smaller than the randomness rate needed to simulate the prefixing map. This shows that the direct concatenation of the ordinary random encoding and channel prefixing with channel simulation is in general suboptimal.

The quantum generalisation of the wiretap channel was studied in [9] and [10], where the capacity for the transmission of confidential classical information was given by a regularized formula. The ability of the quantum channels to preserve quantum superpositions gives rise to purely quantum information processing tasks with no classical counterparts. The quantum capacity, i.e., the ability of a quantum channel to transmit qubits, is one such example. The unified task of transmission of the classical and quantum information was studied in [11] and simultaneously achievable rates were proven. The protocol of [11] is conceptually related to the superposition coding, where, for each classical message a different quantum code is used and the capacity region is given in the form of a regularized rate region. Subsequently, general trade-off capacity theorems for three or more resources were proved [12], [13], [14], [15], [16], [17], [18], [19], [20], [21].

The unavailability of unlimited resources such as many instances of channels or many copies of certain states in nature, triggered a new area of research known as the information theory with finite resources. This area has drawn significant attention over the past years; see [22] for a survey. The extreme scenario where only one instance of a certain resource such as a channel use or a source state is available, is generally called the *one-shot* regime and such a channel (res. source) is called a *single-serving* channel (res. source). The one-shot channel model is the most general model and its capacity to accomplish several information-processing tasks has been studied. The question of the number of bits that can be transmitted with an error of at most $\varepsilon > 0$ by a single use of a classical channel was answered in [23] where the capacity was characterized in terms of smooth min- and max-entropies. The same question for the quantum channels was studied in [24] following a hypothesis-testing approach and the capacity was characterized in terms of the general Rényi entropies. In this context, a reformulation of a novel positive operator-valued measurement (POVM) originally introduced in [25] (see also [26]), was employed in [27] yielding an achievability bound for the capacity of the classical-quantum channels. The POVM construction as well as the converse proof followed a hypothesis-testing procedure and the result was governed by a smooth relative entropy quantity. This result was rederived in [28] by deploying a coding scheme known as position-based decoding [29]. While the position-based decoding ensures the reliability of the transmitted messages, the so-called convex-split lemma [30] also employed in [28] guarantees confidentiality resulting in a capacity theorem for the one-shot wiretap quantum channel.

Position-based decoding and the convex-split lemma are governed by the quantities known as the smooth relative entropies and can be regarded as generalizations of the packing and covering lemmas, respectively. Another result on the one-shot capacity of the quantum wiretap channel was given by [31] where the reliability of the messages is ensured by employing the POVMs introduced in [27] and the confidentiality of the messages is established by proving a novel one-shot covering lemma analogous in approach to [32].

From a different perspective, [33] showed that two primitive information-theoretic protocols, namely information reconciliation and privacy amplification, can be used to directly construct optimal two-terminal protocols for noisy channels without being concerned about the internal workings of the primitives. This approach yields achievability bounds for the public and confidential capacities of classical-quantum channels and their tightness also established by proving corresponding converse bounds. The quantum capacity of a quantum channel for one or a finite number of uses is studied in [34]. The authors of the current paper with their colleagues in a former work [35], unified the problems of one-shot transmission of public and confidential information over quantum channels and proposed a protocol for simultaneously achieviable public and confidential rates as well as tight converse bounds. Later, following the proof of the quantum capacity in [10], they proved a one-shot result for the simultaneous transmission of classical and quantum information [36], contributing to the literature of the one-shot trade-off capacities [37], [38], [39], [40]. Another coding scheme known as Marton coding is known to yield tight achievability and converse regions for the broadcast channel. However, since our scheme is based on superposition coding, we do not use the ideas from Marton coding. The interested reader may refer to [41], [42], [43].

This work grew out of an interest to understand the amount of dummy randomness that is needed to accomplish the task of secret message transmission in the most general channel model. As mentioned earlier, in the asymptotic limit of a memoryless classical channel, it is shown that non-secret messages may compensate for the lack of enough dummy randomness to secure certain confidential messages. This was our main motivation: to understand the price of the dummy randomness and how (much) it can be traded off for a non-secret message. In this work, we consider a broader question featuring our main goal, we study the problem of the transmission of common, individualized and confidential messages with randomness constrained encoder over a single use of a two-receiver quantum broadcast channel. This problem in the asymptotic setting of a memoryless classical channel was studied in [7]. One additional contribution of [7] is the study of the channel resolvability problem via superposition of classical codewords. The quantum channel resolvability via superpositions in the one-shot regime was studied in [44] in the context of the Gelfand-Pinsker quantum wiretap channel. We leverage these results to derive achievability bounds based on position-based decoding and the convex-split lemma. The setup of our problem, however, requires an extension of the position-based decoding and convex-split lemma, which we refer to as the conditional position-based decoding and conditional convex-split lemma. The former leads to an operational interpretation of a recently-defined mutual information-like quantity [45] whereas the latter gives rise to another novel mutual-information like quantity and its operational interpretation. The broad scope of the rate region developed in this paper enables us to recover not only the classical result of [7], but also

the case of simultaneous transmission of public and private information [35], the simultaneous transmission of classical and quantum information [11], [36] and the capacity region of the quantum broadcast channel derived in [46].

The rest of the paper is organized as follows. We start with definitions in Section II. Section III is devoted to the description of the information-processing task, the definition of the code for the task and our main results. We prove an achievability region in Section IV and a converse region in Section V. We give asymptotic analysis in Section VI. We finally conclude the paper in Section VII. The proof of the conditional convex-split lemma as well as several other lemmas are given in the appendix.

II. Miscellaneous Definitions

We use the following conventions throughout the paper. The capital letters X, Y, etc. denote random variables whose realizations and the alphabets are shown by the corresponding small and calligraphic letters, respectively. The classical systems associated to the random variables are denoted by the same capital letters. Quantum systems A, B, etc. are associated with (finite dimensional) Hilbert spaces $\mathcal{H}^A, \mathcal{H}^B$, etc. The set of linear operators on $\mathcal{H}$ are denoted by $\mathcal{L}(\mathcal{H})$, the set of positive semi-definite operators acting on $\mathcal{H}$ is denoted by $\mathcal{P}(\mathcal{H})$, the set of normalized and subnormalized quantum states is given by $\mathcal{D}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) | \mathrm{Tr}\rho = 1\}$ and $\mathcal{D}_{\leq}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) | \mathrm{Tr}\rho \leq 1\}$, respectively, where Tr indicates the trace operator. Multipartite systems are described by tensor product Hilbert space $\mathcal{H}^{AB\ldots D} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes \ldots \otimes \mathcal{H}^D$. We identify states with their density operators and use superscripts to denote the systems on which the mathematical objects are defined. For example if $\rho^{AB} \in \mathcal{D}(\mathcal{H}^{AB})$, then $\rho^A = \mathrm{Tr}_B \rho^{AB} \in \mathcal{D}(\mathcal{H}^A)$ is implicitly defined as its marginal on A, where Tr_B is the partial trace operator. The identity operator in $\mathcal{L}(\mathcal{H}^A)$ is denoted by $\mathbb{1}^A$. For a pair of integers $i \leq j$, we define the discrete interval $[i:j] := \{i, i+1, ..., j\}$. For Hermitian operators M and N, $M \leq N$ means that $(N - M) \in \mathcal{P}(\mathcal{H})$.

Denoted by $\mathcal{N}^{A\to B}$, a quantum channel is a completely positive trace-preserving (CPTP) linear map taking input states from $\mathcal{D}(\mathcal{H}^A)$ to output states belonging to $\mathcal{D}(\mathcal{H}^B)$. A quantum broadcast channel $\mathcal{N}^{A\to BC}$, refers to a quantum channel with a single input and two outputs such that when the transmitter inputs a quantum state in $\mathcal{D}(\mathcal{H}^A)$, one receiver obtains a state in $\mathcal{D}(\mathcal{H}^B)$ while the other receiver obtains system C in $\mathcal{D}(\mathcal{H}^C)$. Throughout we assume the receiver obtaining B system is the primary receiver and the receiver obtaining C is a third party. It is also useful to personify the users of the channel such that Alice is the user controlling the input and Bob and Charlie are the recipients of the systems B and C, respectively. According to the Stinespring dilation of the CPTP map $\mathcal{N}^{A\to BC}$ (see for example [47]), there exists an *inaccessible environment* F in $\mathcal{H}^F$ and a unitary operator U acting on A, C and F systems such that

$$\mathcal{N}^{A\to BC}(\rho^A) = \mathrm{Tr}_F\{U(\rho^A \otimes \sigma^C \otimes \omega^F)U^\dagger\}, \qquad (1)$$

where ρ^A is the input state and σ^C and ω^F are some constant states on systems C and F, respectively[2]. An additional trace over C system gives the quantum channel from Alice to Bob $\mathcal{N}^{A\to B}$ implying that the composite system $E := CF$ plays the role of an inaccessible environment for $\mathcal{N}^{A\to B}$.

The von Neumann entropy and the quantum relative entropy are defined as:

$$H(A)_\rho := H(\rho^A) := -\mathrm{Tr}\rho^A \log \rho^A.$$

$$D(\rho\|\sigma) := \mathrm{Tr}(\rho\log\rho - \rho\log\sigma),$$
$$\text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \text{ and } +\infty \text{ otherwise},$$

respectively, where $\mathrm{supp}(\rho)$ is the support of ρ. Throughout this paper, log denotes by default the binary logarithm. Conditional entropy, mutual information and conditional mutual information, $H(A|B)_\rho$, $I(A;B)_\rho$ and $I(A;B|C)_\rho$, are defined as:

$$\begin{aligned} H(A|B)_\rho &:= H(AB)_\rho - H(B)_\rho, \\ I(A;B)_\rho &:= H(A)_\rho + H(B)_\rho - H(AB)_\rho, \\ I(A;B|C)_\rho &:= H(A|C)_\rho - H(A|BC)_\rho \\ &= H(AC)_\rho + H(BC)_\rho - H(ABC)_\rho - H(C)_\rho. \end{aligned}$$

The von Neumann entropy and the mutual information can be defined as special cases of the quantum relative entropy; for instance it can be seen that $D(\rho^{AB}\|\rho^A \otimes \rho^B) = I(A;B)_\rho$.

The normalized trace distance between two states ρ and σ is given as $\frac{1}{2}\|\rho - \sigma\|_1$ and the fidelity between them is defined as:

$$F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$$

The fidelity relates to the quantum relative entropy in the following way [48]:

$$F^2(\rho,\sigma) \geq 2^{-D(\rho\|\sigma)}. \qquad (2)$$

The (normalized) trace distance (res. fidelity) is a convex (res. concave) function. Notice the following, for classical-quantum states $\rho^{XA} = \sum_x p(x)\,|x\rangle\langle x| \otimes \rho_x^A$ and $\sigma^{XA} = \sum_x p(x)\,|x\rangle\langle x| \otimes \sigma_x^A$, we have:

$$\frac{1}{2}\left\|\rho^A - \sigma^A\right\|_1 \leq \frac{1}{2}\left\|\rho^{XA} - \sigma^{XA}\right\|_1 = \sum_x p(x)\frac{1}{2}\left\|\rho_x^A - \sigma_x^A\right\|_1. \qquad (3)$$

The definition of the fidelity can be extended to subnormalized states, where the generalized fidelity is defined for subnormalized states $\tau, \nu \in \mathcal{D}_{\leq}(\mathcal{H})$ as follows [49]

$$\bar{F}(\tau,\nu) = F(\tau,\nu) + \sqrt{(1-\mathrm{Tr}\tau)(1-\mathrm{Tr}\nu)}.$$

It is easily seen that the generalized fidelity reduces to the fidelity if at least one of the states is normalized. The generalized fidelity is used to define the purified distance as follows:

$$\mathrm{P}(\rho,\sigma) := \sqrt{1 - \bar{F}^2(\rho,\sigma)}.$$

[2]This can be equivalently shown via an isometric extension of the channel $V_{\mathcal{N}}^{A\to BCF}$ defined as $\mathcal{N}^{A\to BC}(\rho^A) = \mathrm{Tr}_F\{V\rho^A V^\dagger\}$ with $V^\dagger V = \mathbb{1}^A$, $VV^\dagger = \Pi_{BCF}$ where Π_{BCF} is a projection on the product Hilbert space $\mathcal{H}^B \otimes \mathcal{H}^C \otimes \mathcal{H}^F$.

It relates to the trace distance in the following way:

$$\frac{1}{2}\|\rho-\sigma\|_1 \leq \mathrm{P}(\rho,\sigma) \leq \sqrt{\|\rho-\sigma\|_1}.$$

The purified distance satisfies several properties similar to those of the trace distance, we list some of them below[3].

Lemma 1 (see for example [50]):

- Monotonicity: For quantum states ρ,σ and any completely positive trace-preserving map $\mathcal{E}$,

$$\mathrm{P}(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq \mathrm{P}(\rho,\sigma).$$

- Triangle inequality: For quantum states ρ,σ and ω, it holds that

$$\mathrm{P}(\rho,\sigma) \leq \mathrm{P}(\rho,\omega)+\mathrm{P}(\omega,\sigma).$$

- Invariance with respect to tensor product states: For quantum states ρ,σ and ω, it holds that:

$$\mathrm{P}(\rho\otimes\omega,\sigma\otimes\omega) = \mathrm{P}(\rho,\sigma).$$

The following can also be easily verified:

$$\mathrm{P}\big(\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\omega_x^B, \sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes\omega_x^B\big) = \mathrm{P}\big(\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A, \sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\big).$$

Lemma 2 (Lemma 17 in [51]): Let $\rho\in\mathcal{H}$ and Π a projector on $\mathcal{H}$, then

$$\mathrm{P}(\rho,\Pi\rho\Pi) \leq \sqrt{2\mathrm{Tr}\rho\Pi_\perp - (\mathrm{Tr}\rho\Pi_\perp)^2},$$

where $\Pi_\perp = \mathbb{1}-\Pi$.

Lemma 3 (corollary 16 in [51]): Let $\rho^{AB} = |\varphi\rangle\langle\varphi|^{AB} \in \mathcal{P}(\mathcal{H}^{AB})$ be a pure state, $\rho^A = \mathrm{Tr}_B\rho^{AB}$, $\rho^B = \mathrm{Tr}_A\rho^{AB}$ and let $\Pi^A\in\mathcal{P}(\mathcal{H}^A)$ be a projector in $\mathrm{supp}(\rho^A)$. Then, there exists a dual projector Π^B on $\mathcal{H}^B$ such that

$$(\Pi^A\otimes(\rho^B)^{-\frac{1}{2}})\,|\varphi\rangle^{AB} = ((\rho^A)^{-\frac{1}{2}}\otimes\Pi^B)\,|\varphi\rangle^{AB}.$$

Lemma 4 ([50]): Let $\rho,\sigma\in\mathcal{P}(\mathcal{H})$, then

- For any $\omega\geq\rho$,

$$\big\|\sqrt{\omega}\sqrt{\sigma}\big\|_1 \geq \big\|\sqrt{\rho}\sqrt{\sigma}\big\|_1.$$

- For any projector $\Pi\in\mathcal{P}(\mathcal{H})$,

$$\big\|\sqrt{\Pi\rho\Pi}\sqrt{\sigma}\big\|_1 = \big\|\sqrt{\rho}\sqrt{\Pi\sigma\Pi}\big\|_1 = \big\|\sqrt{\Pi\rho\Pi}\sqrt{\Pi\sigma\Pi}\big\|_1.$$

Definition 1 (Hypothesis testing relative entropy [27],[34]): Let $\{\Lambda,\mathbb{1}-\Lambda\}$ be the elements of a POVM that distinguishes between quantum states ρ and σ such that the probability of a correct guess on input ρ equals $\mathrm{Tr}\Lambda\rho$ and a wrong guess on σ is made with probability $\mathrm{Tr}\Lambda\sigma$. Let $\varepsilon\in(0,1)$. Then, the hypothesis testing relative entropy is defined as follows:

$$D_{\mathrm{H}}^{\varepsilon}(\rho\|\sigma) \coloneqq \max\{-\log_2\mathrm{Tr}\Lambda\sigma : 0\leq\Lambda\leq\mathbb{1}\wedge\mathrm{Tr}\Lambda\rho\geq1-\varepsilon\}.$$

[3]In this paper, without loss of generality, we work with normalized quantum states and the definition of the generalized fidelity is mentioned for completeness.

From the definition above, the hypothesis testing mutual information for a bipartite state ρ^{AB} is defined as follows:

$$I_{\mathrm{H}}^{\varepsilon}(A;B)_\rho \coloneqq D_{\mathrm{H}}^{\varepsilon}(\rho^{AB}\|\rho^A\otimes\rho^B).$$

Lemma 5 (Relation between the relative entropy and the hypothesis testing relative entropy): For quantum states ρ and σ and a parameter $\varepsilon\in(0,1)$, the following relation exists between the hypothesis testing relative entropy and the quantum relative entropy [27]:

$$D_{\mathrm{H}}^{\varepsilon}(\rho\|\sigma) \leq \frac{1}{1-\varepsilon}(D(\rho\|\sigma)+h_b(\varepsilon)),$$

where $h_b(\varepsilon) \coloneqq -\varepsilon\log\varepsilon-(1-\varepsilon)\log(1-\varepsilon)$ is the binary entropy function. Another connection between the two relative entropies is due to the quantum Stein's lemma as given below [52], [53]:

$$\lim_{n\to\infty}\frac{1}{n}D_{\mathrm{H}}^{\varepsilon}(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma).$$

The followings are simple consequences of this lemma. For a bipartite state $\rho^{AB}\in D(\mathcal{H}^{AB})$, we have

$$I_{\mathrm{H}}^{\varepsilon}(A;B)_\rho \leq \frac{1}{1-\varepsilon}(I(A;B)_\rho+h_b(\varepsilon)), \tag{4}$$

$$\lim_{n\to\infty}\frac{1}{n}I_{\mathrm{H}}^{\varepsilon}(A^n;B^n)_{\rho^{\otimes n}} = D(\rho^{AB}\|\rho^A\otimes\rho^B) = I(A;B)_\rho. \tag{5}$$

Definition 2 (Hypothesis testing conditional mutual information [45]): Let $\rho^{XAB} \coloneqq \sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB}$, $\rho^{A-X-B} \coloneqq \sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\rho_x^B$ be two tripartite states classical on X system. Let $\varepsilon\in(0,1)$. Then, the hypothesis testing conditional mutual information is defined as:

$$I_{\mathrm{H}}^{\varepsilon}(A;B|X)_\rho \coloneqq D_{\mathrm{H}}^{\varepsilon}(\rho^{XAB}\|\rho^{A-X-B}).$$

From Lemma 5, the following relations can be obtained:

$$I_{\mathrm{H}}^{\varepsilon}(A;B|X)_\rho \leq \frac{1}{1-\varepsilon}(I(A;B|X)_\rho+h_b(\varepsilon)), \tag{6}$$

$$\lim_{n\to\infty}\frac{1}{n}I_{\mathrm{H}}^{\varepsilon}(A^n;B^n|X^n)_{\rho^{\otimes n}} = I(A;B|X)_\rho. \tag{7}$$

Notice that for states $\rho^{XAB} \coloneqq \sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB}$ and $\rho^{A-X-B} \coloneqq \sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\rho_x^B$, we have $D(\rho^{XAB}\|\rho^{A-X-B}) = I(A;B|X)_\rho$.

Definition 3 (Max-relative entropy [54]): For quantum states ρ and σ, the max-relative entropy is defined as follows:

$$D_{\max}(\rho\|\sigma) \coloneqq \inf\left\{\lambda\in\mathbb{R} : \rho\leq2^\lambda\sigma\right\}, \tag{8}$$

where it is well-defined if $\mathrm{supp}(\rho)\subseteq\mathrm{supp}(\sigma)$.

Lemma 6 ([54]): The max-relative entropy is monotonically non-increasing with CPTP maps, i.e., for quantum states ρ,σ and any CPTP map $\mathcal{E}$, the following holds:

$$D_{\max}(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) \leq D_{\max}(\rho\|\sigma).$$

Definition 4 (Smooth max-relative entropy [54]): For a parameter $\epsilon\in(0,1)$ and quantum states ρ and σ, the smooth max-relative entropy is defined as:

$$D_{\max}^{\varepsilon}(\rho\|\sigma) \coloneqq \min_{\rho'\in\mathcal{B}^{\varepsilon}(\rho)} D_{\max}(\rho'\|\sigma).$$

From the smooth max-relative entropy, one can define a mutual information-like quantity for a bipartite state ρ^{AB} as follows:

$$D^{\varepsilon}_{\max}(A;B)_{\rho} \coloneqq D^{\varepsilon}_{\max}(\rho^{AB}\|\rho^{A}\otimes\rho^{B}) = \min_{\rho'\in\mathcal{B}^{\varepsilon}(\rho)} D_{\max}(\rho'^{AB}\|\rho^{A}\otimes\rho^{B}). \quad (9)$$

Lemma 7: For quantum states ρ and σ and a parameter $\varepsilon\in(0,1)$, the following indicates the relation between the smooth max-relative entropy and quantum relative entropy.

$$D^{\sqrt{2\varepsilon}}_{\max}(\rho\|\sigma)\leq\frac{1}{1-\varepsilon}(D(\rho\|\sigma)+h_b(\varepsilon)),$$

where $h_b(\varepsilon)\coloneqq-\varepsilon\log\varepsilon-(1-\varepsilon)\log(1-\varepsilon)$ is the binary entropy function. Further relation between the two entropies is given by the quantum Stein's lemma [55]:

$$\lim_{n\to\infty}\frac{1}{n}D^{\varepsilon}_{\max}(\rho^{\otimes n}\|\sigma^{\otimes n})=D(\rho\|\sigma),$$

and consequently we have

$$\lim_{n\to\infty}\frac{1}{n}D^{\varepsilon}_{\max}(A^n;B^n)_{\rho^{\otimes n}}=D(\rho^{AB}\|\rho^{A}\otimes\rho^{B})=I(A;B)_{\rho}.$$

Proof: The first inequality, the upper bound on the smooth max-relative entropy, follows by a straightforward manipulation of Proposition 4.1 in [56] and Lemma 5. □

Definition 5: Let $\rho^{XAB}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{AB}_x$ and $\rho^{A-X-B}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{A}_x\otimes\rho^{B}_x$ be quantum states classical on X and $\varepsilon\in(0,1)$, then

$$D^{\varepsilon}_{\max}(A;B|X)_{\rho}\coloneqq D^{\varepsilon}_{\max}(\rho^{XAB}\|\rho^{A-X-B})_{\rho}.$$

From Lemma 7, the following relations can be seen:

$$D^{\sqrt{2\varepsilon}}_{\max}(A;B|X)_{\rho}\leq\frac{1}{1-\varepsilon}(I(A;B|X)+h_b(\varepsilon)), \quad (10)$$

and

$$\lim_{n\to\infty}\frac{1}{n}D^{\varepsilon}_{\max}(A^n;B^n|X^n)_{\rho^{\otimes n}}=D(\rho^{XAB}\|\rho^{A-X-B})=I(A;B|X)_{\rho}. \quad (11)$$

Definition 6 ([29]): For a bipartite state ρ^{AB} and a parameter $\varepsilon\in(0,1)$, a mutual information-like quantity can be defined as follows:

$$\widetilde{I}^{\varepsilon}_{\max}(A;B)_{\rho}\coloneqq\inf_{\rho'^{AB}\in\mathcal{B}^{\varepsilon}(\rho^{AB})}D_{\max}(\rho'^{AB}\|\rho'^{A}\otimes\rho^{B}).$$

The following lemmas relate the aforementioned mutual information-like quantity and the quantity defined in (9).

Lemma 8 ([29]): For a bipartite state ρ^{AB} and a parameter $\varepsilon\in(0,1)$, the following relation holds:

$$\widetilde{I}^{2\varepsilon}_{\max}(A;B)_{\rho}\leq D^{\varepsilon}_{\max}(A;B)_{\rho}+\log_2\left(\frac{3}{\varepsilon^2}\right).$$

Lemma 9: For a bipartite state ρ^{AB} and a parameter $\varepsilon\in(0,1)$, the following relation holds:

$$D^{\varepsilon}_{\max}(A;B)_{\rho}\leq\widetilde{I}^{\varepsilon}_{\max}(A;B)_{\rho}.$$

Proof: The proof is given in the appendix. □

We define another mutual information-like quantity similar to the one given by Definition 5.

Definition 7: Let $\rho^{XAB}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{AB}_x$ and $\rho^{A-X-B}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{A}_x\otimes\rho^{B}_x$ be quantum states classical on X and $\varepsilon\in(0,1)$, then

$$\widetilde{I}^{\varepsilon}_{\max}(A;B|X)_{\rho}\coloneqq\min_{\rho'\in\mathcal{B}^{\varepsilon}(\rho)}D_{\max}(\rho'^{XAB}\|\sum_x p'(x)|x\rangle\langle x|^X\otimes\rho'^{A}_x\otimes\rho^{B}_x),$$

where $\mathrm{Tr}_B\rho'^{XAB}=\sum_x p'(x)|x\rangle\langle x|^X\otimes\rho'^{A}_x$.

Remark 1: In the definition above, it is implied that the minimization is in fact being performed over states which are classical on subsystem X, leading to the conclusion that the optimal state attaining the minimum is classical on X. Lemma 6.6 in [22] studied two important entropic quantities, namely smooth conditional min- and max-entropies, and concluded that smoothing respects the structure of the state ρ^{XAB}, meaning that the optimal state $\rho'^{XAB}\in\mathcal{B}^{\varepsilon}(\rho^{XAB})$ will be classical on subsystem X. Here we make an argument showing that our definition is indeed a legitimate definition. Let $\bar{\rho}^{XAB}\in\mathcal{B}^{\varepsilon}(\rho^{XAB})$ be the state attaining the minimum in the quantity $\widetilde{I}^{\varepsilon}_{\max}(A;B|X)_{\rho}$ if we do not restrict X system to be classical. Let the *pinching map* be defined as $\mathcal{P}^X(.)=\sum_x|x\rangle\langle x|(.)|x\rangle\langle x|$ and define $\rho'^{XAB}=\mathcal{P}^X(\bar{\rho}^{XAB})$. Note that the pinching map does not affect ρ^{XAB}, and since such maps are CPTP and unital, from the monotonicity of the purified distance and also smooth max-relative entropy, we will have $\rho'^{XAB}\in\mathcal{B}^{\varepsilon}(\rho^{XAB})$ and $\widetilde{I}^{\varepsilon}_{\max}(A;B|X)_{\rho'^{XAB}}\leq\widetilde{I}^{\varepsilon}_{\max}(A;B|X)_{\bar{\rho}^{XAB}}$, respectively.

Lemma 10: For quantum states $\rho^{XAB}=\sum_x p(x)|x\rangle\langle x|\otimes\rho^{AB}_x$ and $\rho^{A-X-B}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{A}_x\otimes\rho^{B}_x$ and a parameter $\varepsilon\in(0,1)$, we have:

$$\widetilde{I}^{2\varepsilon}_{\max}(A;B|X)_{\rho}\leq D^{\varepsilon}_{\max}(A;B|X)_{\rho}+\log\left(\frac{1}{1-\sqrt{1-\varepsilon^2}}+1\right).$$

Proof: The proof is relegated to the appendix. □

Lemma 11: [4] For quantum states $\rho^{XAB}=\sum_x p(x)|x\rangle\langle x|\otimes\rho^{AB}_x$ and $\rho^{A-X-B}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{A}_x\otimes\rho^{B}_x$ and a parameter $\varepsilon\in(0,1)$, the following stands:

$$D^{\varepsilon}_{\max}(A;B|X)_{\rho}\leq\widetilde{I}^{\varepsilon}_{\max}(A;B|X)_{\rho}.$$

Proof: The proof is provided in the appendix. □

Lemma 12: For quantum states $\rho^{XAB}=\sum_x p(x)|x\rangle\langle x|\otimes\rho^{AB}_x$ and $\rho^{A-X-B}\coloneqq\sum_x p(x)|x\rangle\langle x|^X\otimes\rho^{A}_x\otimes\rho^{B}_x$ and a parameter $\varepsilon\in(0,1)$, it holds that:

$$\lim_{n\to\infty}\frac{1}{n}\widetilde{I}^{\varepsilon}_{\max}(A^n;B^n|X^n)_{\rho^{\otimes n}}=I(A;B|X)_{\rho}.$$

Proof: The proof follows from Lemma 10 and Lemma 11 as well as the fact given by (11). □

The following lemma comes in handy in the proof of the conditional convex-split lemma.

Lemma 13: For an ensemble of classical-quantum states $\{\rho^{XA}_1,...,\rho^{XA}_n\}$ and a probability mass function $\{p(i)\}_{i=1}^n$,

[4]Note that for our purposes in this paper, the upper bound given by Lemma 10 is enough; we prove this lemma further for sake of completeness of our study.

let $\rho^{XA}=\sum_i p(i)\rho_i^{XA}$ be the average state. Then for a state θ^{XA} we have the following equality:

$$D(\rho^{XA}\|\theta^{XA})=\sum_{i=1}^{n}p(i)\left(D(\rho_i^{XA}\|\theta^{XA})-D(\rho_i^{XA}\|\rho^{XA})\right).$$

Proof: Proof is presented in the appendix. □

Lemma 14 (Conditional convex-split lemma): Consider the classical-quantum state $\rho^{XAB}:=\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB}$, define $\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^B$ such that $\text{supp}(\rho_x^B)\subseteq\text{supp}(\sigma_x^B)$ for all x. Let $k:=D_{\max}(\rho^{XAB}\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^B)$. Define the following state:

$$\tau^{XAB_1\ldots B_n}:=\sum_x p(x)|x\rangle\langle x|^X\otimes\left(\frac{1}{n}\sum_{j=1}^{n}\rho_x^{AB_j}\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_{j-1}}\otimes\sigma_x^{B_{j+1}}\otimes\ldots\otimes\sigma_x^{B_n}\right),$$

on $n+2$ systems $X,A,B_1,\ldots,B_n$, where for $\forall j\in[1:n]$ and $x\in\text{supp}(p(x)):\rho_x^{AB_j}=\rho_x^{AB}$ and $\sigma_x^{B_j}=\sigma_x^B$. We have the following:

$$D\big(\tau^{XAB_1\ldots B_n}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_n}\big)\leq\log\left(1+\frac{2^k}{n}\right).$$

In particular, for some $\delta\in(0,1)$ and $n=\lceil\frac{2^k}{\delta^2}\rceil$ the following holds:

$$P(\tau^{XAB_1\ldots B_n},\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_n})\leq\delta.$$

Proof: The proof is presented in the appendix. □

In the following, we present a variation of the conditional convex-split lemma which involves smooth conditional max-relative entropy.

Corollary 1: Fix a $\varepsilon>0$. Let $\rho^{XAB}=\sum_x p(x)\,|x\rangle\langle x|^X\otimes\rho_x^{AB}$ and $\sum_x p(x)\,|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^B$ be quantum states such that $\text{supp}(\rho_x^B)\subseteq\text{supp}(\sigma_x^B)$ for all x. Define $k:=\min_{\rho'\in\mathcal{B}^\varepsilon(\rho)}D_{\max}(\rho'^{XAB}\|\sum_x p'(x)|x\rangle\langle x|^X\otimes\rho_x'^A\otimes\sigma_x^B)$ where the optimization takes place over states classical on X. Further define the following state

$$\tau^{XAB_1\ldots B_n}:=\sum_x p(x)|x\rangle\langle x|^X\otimes\left(\frac{1}{n}\sum_{j=1}^{n}\rho_x^{AB_j}\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_{j-1}}\otimes\sigma_x^{B_{j+1}}\otimes\ldots\otimes\sigma_x^{B_n}\right),$$

on $n+2$ systems $X,A,B_1,\ldots,B_n$, where $\forall j\in[1:n]$ and $x\in\text{supp}(p(x)):\rho_x^{AB_j}=\rho_x^{AB}$ and $\sigma_x^{B_j}=\sigma_x^B$. For $\delta\in(0,1)$ and $n=\lceil\frac{2^k}{\delta^2}\rceil$, the following holds true:

$$P(\tau^{XAB_1\ldots B_n},\sum_x p(x)\,|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_n})\leq 2\varepsilon+\delta.$$

Proof: Proof is presented in the appendix. □

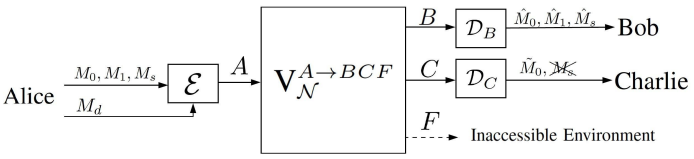

Fig. 1: Single-serving quantum broadcast channel with isometric extension $V_{\mathcal{N}}^{A\to BCF}$. Alice attempts to transmit a common message M_0 to Bob and Charlie and a private message M_1 and a confidential message M_s to Bob only such that the confidential message must be kept secret from Charlie. The dummy randomness used by Alice for encryption is modeled by a message M_d.

Lemma 15 (Hayashi-Nagaoka operator inequality [25]): Let $T,S\in\mathcal{P}(\mathcal{H}^A)$ such that $(\mathbb{1}-S)\in\mathcal{P}(\mathcal{H}^A)$. Then for all constants $c>0$, the following inequality holds:

$$\mathbb{1}-(S+T)^{-\frac{1}{2}}S(S+T)^{-\frac{1}{2}}\leq(1+c)(\mathbb{1}-S)+(2+c+c^{-1})T.$$

III. Information-Processing Task, Code Definition and Main Results

Consider the quantum broadcast communication system model depicted in Fig. 1. A quantum broadcast channel $\mathcal{N}^{A\to BC}$ with isometric extension $\mathrm{V}_{\mathcal{N}}^{A\to BCF}$ connects a sender in possession of A system (Alice) to two receivers, a primary receiver (Bob) in possession of B and a third-party receiver (Charlie) possessing C system and the communication is surrounded by an inaccessible environment modeled as F system. Alice attempts to send three messages simultaneously: a common message M_0 that is to be decoded by Bob and Charlie, a private message M_1 addressed to Bob with no secrecy requirement and a confidential message M_s to Bob that must not be leaked to Charlie. The obfuscation of the confidential message is done by virtue of stochastic encoding, i.e., introducing local randomness into codewords in the encoding process. It is convenient to represent this local randomness as a *dummy message* M_d taking its values according to some distribution.

The encoder encodes the message triple (M_0,M_1,M_s) as well as the dummy message M_d into a quantum codeword ρ^A and transmits it over the quantum channel. Upon receiving ρ^B and ρ^C, Bob finds the estimates $\hat{M}_0,\hat{M}_1,\hat{M}_s$ of the common, individualized and confidential messages, respectively, while Charlie finds the estimate $\tilde{M}_0$ of the common message. To ensure reliability and security, a tradeoff arises between the rates of the messages. We study the one-shot limit on this tradeoff.

Definition 8: A $(2^{R_0},2^{R_1},2^{R_s})$ one-shot code $\mathcal{C}$ for the quantum broadcast channel $\mathcal{N}^{A\to BC}$ consists of

- Three message sets $[1:2^{R_0}]$, $[1:2^{R_1}]$ and $[1:2^{R_s}]$ (common, individualized and confidential, respectively),
- A source of local randomness $[1:2^{R_d}]$,
- An encoding operator $\mathcal{E}:M_0\times M_1\times M_s\times M_d\to A$, which maps a message triple $(m_0,m_1,m_s)\in[1:2^{R_0}]\times$

$[1:2^{R_1}]\times[1:2^{R_s}]$ and a realization of the local source of randomness $m_d \in [1:2^{R_d}]$ to a codeword $\rho^A_{m_0,m_1,m_s}$,
- A decoding POVM $\mathcal{D}_B : B \to (M_0 \times M_1 \times M_s) \cup \{?\}$, which assigns an estimate $(\hat{m}_0, \hat{m}_1, \hat{m}_s) \in [1:2^{R_0}]\times[1:2^{R_1}]\times[1:2^{R_s}]$ or an error message $\{?\}$ to each received state $\rho^B_{m_0,m_1,m_s}$,
- A decoding POVM $\mathcal{D}_C : C \to M_0 \cup \{?\}$ that assigns an estimate $\tilde{m}_0 \in [1:2^{R_0}]$ or an error message $\{?\}$ to each received state $\rho^C_{m_0,m_1,m_s}$.

The $(2^{R_0}, 2^{R_1}, 2^{R_s})$ one-shot code is assumed to be known by all parties beforehand; likewise, the distribution of the local randomness is assumed known to all parties, however, its realization m_d is only accessible to Alice. Note that we have included the source of local randomness in the definition of the code to imply that it can be optimized over as part of the code design. Nevertheless, we do not consider the effect of non-uniform randomness in our analysis [6] and throughout we assume that the dummy message M_d is uniformly distributed over $[1:2^{R_d}]$. We further assume that the message triple (M_0, M_1, M_s) is uniformly distributed over $[1:2^{R_0}]\times[1:2^{R_1}]\times[1:2^{R_s}]$ so that the rates of the common, individualized and confidential messages are $H(M_0) = R_0, H(M_1) = R_1$ and $H(M_s) = R_s$, respectively. The reliability performance of the code $\mathcal{C}$ is measured by its average probability of error defined as follows:

$$P^1_{\text{error}} \coloneqq \Pr\{(\hat{M}_0, \hat{M}_1, \hat{M}_s) \neq (M_0, M_1, M_s) \text{ or } \tilde{M}_0 \neq M_0\}, \tag{12}$$

while its secrecy level, i.e., an indication of Charlie's ignorance about the confidential message, is measured in terms of the trace distance between Charlie's received state and some constant state as follows:

$$P^1_{\text{secrecy}}(m_0) \coloneqq \frac{1}{2^{R_s}} \sum_{m_s} \frac{1}{2} \|\rho^C_{m_0,m_s} - \sigma^C_{m_0}\|_1, \tag{13}$$

where $\rho^C_{m_0,m_s}$ and $\sigma^C_{m_0}$ are the average states at C when m_0 and m_s are transmitted. Note that the secrecy requirement indicates Charlie's ignorance about the confidential message m_s on average conditioned on the fact that he has decoded the common message m_0 correctly.

A rate quadruple (R_0, R_1, R_s, R_d) is said to be ε-achievable if there exist a one-shot code $\mathcal{C}$ satisfying the following conditions:

$$P^1_{\text{error}} \leq \varepsilon, \tag{14}$$

$$\forall m_0 : \quad P^1_{\text{secrecy}}(m_0) \leq \varepsilon, \tag{15}$$

where $\varepsilon \in (0,1)$ characterizes both the reliability and secrecy of the code. Then the ε-achievable rate region $\mathcal{R}^\varepsilon(\mathcal{N})$ is defined to consist of the closure of the set of all ε-achievable rate quadruples. In this paper, our main goal is to bound the optimal rate region $\mathcal{R}^\varepsilon(\mathcal{N})$ by establishing achievability and converse regions.

The following theorem presents our achievability region on $\mathcal{R}^\epsilon(\mathcal{N})$.

Theorem 1 (Achievability Region): Fix $\varepsilon', \varepsilon'', \delta_1, \delta_2, \delta_3$ and η such that $0 < 3\varepsilon' + 2\sqrt{\varepsilon'} < 1, 0 < \delta_1, \delta_2, \delta_3 < \varepsilon'$, $0 < \varepsilon'' < \sqrt{2} - 1$, $0 < \eta < \varepsilon''^2$. Consider a quantum broadcast channel $\mathcal{N}^{A\to BC}$. Let the random variables U,V and X be distributed such that $U \to V \to X$ forms a Markov chain and define classical-quantum state $\rho^{UVXA} = \sum_{u,v,x} p(u,v,x) \left|u\right\rangle\!\left\langle u\right|^U \otimes \left|v\right\rangle\!\left\langle v\right|^V \otimes \left|x\right\rangle\!\left\langle x\right|^X \otimes \rho^A_x$. Let $\mathcal{R}^{(\text{in})}(\rho)$ be the set of those quadruples (R_0, R_1, R_s, R_d) satisfying the conditions given by equations (16)-(20) on $\rho^{UVXBC} = \mathcal{N}^{A\to BC}(\rho^{UVXA})$. Let $\varepsilon \coloneqq \max\{\sqrt[4]{\varepsilon'}, \sqrt[4]{\varepsilon''}\}$. Then $\bigcup \mathcal{R}^{(\text{in})}(\rho) \subseteq \mathcal{R}^\varepsilon(\mathcal{N})$ where the union is over all ρ^{UVXBC} arising from the channel.

Proof: See Section IV. □

Theorem 2 (Converse Region): Fix $\varepsilon \in (0,1)$. Let the random variables U,V and X be distributed such that $U \to V \to X$ forms a Markov chain and define classical-quantum state $\rho^{UVXA} = \sum_{u,v,x} p(u,v,x) \left|u\right\rangle\!\left\langle u\right|^U \otimes \left|v\right\rangle\!\left\langle v\right|^V \otimes \left|x\right\rangle\!\left\langle x\right|^X \otimes \rho^A_x$. Let the state ρ^{UVXBC} be the result of the action of the quantum broadcast channel $\mathcal{N}^{A\to BC}$ on the state ρ^{UVXA}. Let $\mathcal{R}^{(\text{co})}(\rho)$ be the set of those quadruples (R_0, R_1, R_s, R_d) satisfying the following conditions:

$$R_0 \leq \min\left[I^\varepsilon_{\text{H}}(U;B)_\rho, I^\varepsilon_{\text{H}}(U;C)_\rho\right], \tag{21}$$

$$R_0 + R_1 + R_s \leq I^\varepsilon_{\text{H}}(V;B|U)_\rho + \min\left[I^\varepsilon_{\text{H}}(U;B)_\rho, I^\varepsilon_{\text{H}}(U;C)_\rho\right], \tag{22}$$

$$R_s \leq I^\varepsilon_{\text{H}}(V;B|U)_\rho - D^{\sqrt{2\varepsilon}}_{\max}(V;C|U)_\rho, \tag{23}$$

$$R_1 + R_d \geq D^{\sqrt{2\varepsilon}}_{\max}(V;C|U)_\rho + D^{\sqrt{2\varepsilon}}_{\max}(X;C|V)_\rho, \tag{24}$$

$$R_d \geq D^{\sqrt{2\varepsilon}}_{\max}(X;C|V)_\rho. \tag{25}$$

Then $\mathcal{R}^\varepsilon(\mathcal{N}) \subseteq \bigcup \mathcal{R}^{(\text{co})}(\rho)$ and the union is over all ρ^{UVXBC} arising from the channel.

Proof: See Section V. □

From the theorems above, the recent result by the same authors on the simultaneous transmission of classical and quantum information can be obtained. The slight difference between the results stems from the fact that in [36], there is a single criterion for the error probability and secrecy while in this work separate criteria are considered.

Corollary 2 ([36]): Fix $\varepsilon', \varepsilon'', \delta_1, \delta_3$ and η such that $0 < 3\varepsilon' + 2\sqrt{\varepsilon'} < 1, 0 < \delta_1, \delta_3 < \varepsilon'$, $0 < \varepsilon'' < \sqrt{2} - 1$, $0 < \eta < \varepsilon''^2$. Define $\varepsilon \coloneqq \max\{\sqrt[4]{\varepsilon'}, \sqrt[4]{\varepsilon''}\}$. Let C^ε denote the one-shot capacity region of the channel $\mathcal{N}^{A\to BE}$ for simultaneous transmission of classical and quantum information. For a classical-quantum state $\rho^{UVA} = \sum_{u,v} p(u,v) \left|u\right\rangle\!\left\langle u\right| \otimes \left|v\right\rangle\!\left\langle v\right| \otimes \left|\psi_v\right\rangle\!\left\langle \psi_v\right|^A$, the following achievability bound holds:

$$C^{(\text{in})} \subseteq C^\varepsilon,$$

where, denoting the one-shot rates of the classical and quantum information by R^1_c and R^1_q, respectively, $C^{(\text{in})}$ is the union over all states ρ^{UVBE} arising from the channel, of rate pairs (R^1_c, R^1_q) obeying:

$$R^1_c \leq I^{\varepsilon'-\delta_1}_{\text{H}}(U;B)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right),$$

$$R^1_q \leq I^{\varepsilon'-\delta_3}_{\text{H}}(V;B|U)_\rho - \widetilde{I}^{\varepsilon''}_{\max}(V;E|U)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_3^2}\right) - 2\log_2\left(\frac{1}{\eta}\right).$$

Let $\varepsilon \in (0,1)$. Then the following converse holds:

$$C^\varepsilon \subseteq C^{(\text{co})},$$

$$R_0 \leq \min\left[I_{\mathrm{H}}^{\varepsilon'-\delta_1}(U;B)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right), I_{\mathrm{H}}^{\varepsilon'-\delta_2}(U;C)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_2^2}\right)\right], \tag{16}$$

$$R_0 + R_1 + R_s \leq I_{\mathrm{H}}^{\varepsilon'-\delta_3}(V;B|U)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_3^2}\right) + \min\left[I_{\mathrm{H}}^{\varepsilon'-\delta_1}(U;B)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right), I_{\mathrm{H}}^{\varepsilon'-\delta_2}(U;C)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_2^2}\right)\right], \tag{17}$$

$$R_s \leq I_{\mathrm{H}}^{\varepsilon'-\delta_3}(V;B|U)_\rho - \widetilde{I}_{\max}^{\varepsilon''}(V;C|U)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_3^2}\right) - 2\log_2\left(\frac{1}{\eta}\right), \tag{18}$$

$$R_1 + R_d \geq \widetilde{I}_{\max}^{\varepsilon''}(V;C|U)_\rho + \widetilde{I}_{\max}^{\varepsilon''}(X;C|V)_\rho + 4\log_2\left(\frac{1}{\eta}\right), \tag{19}$$

$$R_d \geq \widetilde{I}_{\max}^{\varepsilon''}(X;C|V)_\rho + 2\log_2\left(\frac{1}{\eta}\right). \tag{20}$$

where $C^{(\mathrm{co})}$ is the union over all states ρ^{UVBE} arising from the channel, of rate pairs (R_c^1, R_q^1) obeying

$$R_c^1 \leq I_{\mathrm{H}}^{\varepsilon}(U;B)_\rho,$$
$$R_q^1 \leq I_{\mathrm{H}}^{\varepsilon}(V;B|U)_\rho - D_{\max}^{\sqrt{2\varepsilon}}(V;E|U)_\rho.$$

Proof: The approach for the simultaneous transmission of classical and quantum information is through finding the limits on the simultaneous transmission of common and confidential messages. From [10] it is well-known that the rate of the confidential message can be translated into the rate of quantum information. As hinted in the introductory part, when it comes to transmission of quantum information, there is zero-tolerance condition of copying quantum information; therefore the confidential messages must be kept secret from the entire universe but Bob, meaning that the output of the channel consists of a system received by Bob and another inaccessible environment E (which includes Charlie's system). From Theorem 1 and Theorem 2 onward, since there is no concern regarding the rate of the dummy randomness, the last two inequalities in both regions will be trivial. And the achievability part can be seen from (16) and (18) and the converse part from (21) and (23). □

IV. Achievability

The achievability proof of the reliability condition (14) is based on a combination of classical superposition coding and position-based decoding whereas the secrecy condition (15) is handled by a version of the convex-split lemma which relies on superposition of codewords. This result is reminiscent of the channel resolvability problem via superposition studied for classical [7] and quantum [44] channels.

The proof of Theorem 1 follows from Lemma 16 and Lemma 17 where the former proves an alternative rate region and the latter shows the equivalence of the two regions.

Lemma 16: Fix $\varepsilon', \varepsilon'', \delta_1, \delta_2, \delta_3$ and η such that $0 < 3\varepsilon' + 2\sqrt{\varepsilon'} < 1, 0 < \delta_1, \delta_2, \delta_3 < \varepsilon'$, $0 < \varepsilon'' < \sqrt{2} - 1$, $0 < \eta < \varepsilon''^2$ and define $\varepsilon := \max\{\sqrt[4]{\varepsilon'}, \sqrt[4]{\varepsilon''}\}$. Let the random variables U,V and X be distributed such that $U \to V \to X$ forms a Markov chain. We further define classical-quantum state $\rho^{UVXA} = \sum_{u,v,x} p(u,v,x)|u\rangle\langle u|^U \otimes |v\rangle\langle v|^V \otimes |x\rangle\langle x|^X \otimes \rho_x^A$. Let $\mathcal{R}^*(\rho)$ be the set of those quadruples (R_0, R_1, R_s, R_d) satisfying the following conditions on $\rho^{UVXBC} = \mathcal{N}^{A\to BC}(\rho^{UVXA})$:

$$R_0 \leq \min[I_{\mathrm{H}}^{\varepsilon'-\delta_1}(U;B)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right), \tag{26}$$
$$I_{\mathrm{H}}^{\varepsilon'-\delta_2}(U;C)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_2^2}\right)],$$

$$R_1 + R_s \leq I_{\mathrm{H}}^{\varepsilon'-\delta_3}(V;B|U)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_3^2}\right), \tag{27}$$

$$R_1 \geq \widetilde{I}_{\max}^{\varepsilon''}(V;C|U)_\rho + 2\log_2\left(\frac{1}{\eta}\right), \tag{28}$$

$$R_d \geq \widetilde{I}_{\max}^{\varepsilon''}(X;C|V)_\rho + 2\log_2\left(\frac{1}{\eta}\right), \tag{29}$$

Then $\bigcup \mathcal{R}^*(\rho) \subseteq \mathcal{R}^\varepsilon(\mathcal{N})$ and the union is over all ρ^{UVXBC} arising from the channel.

Proof: Let $\varepsilon', \varepsilon'', \delta_1, \delta_2, \delta_3$ and η be such that $0 < 3\varepsilon' + 2\sqrt{\varepsilon'} < 1, 0 < \delta_1, \delta_2, \delta_3 < \varepsilon'$, $0 < \varepsilon'' < \sqrt{2} - 1$, $0 < \eta < \varepsilon''^2$ and $\varepsilon := \max\{\sqrt[4]{\varepsilon'}, \sqrt[4]{\varepsilon''}\}$.

Codebook generation: Fix a distribution $p(u,v,x)$ such that $U \to V \to X$. Alice, Bob and Charlie share randomness in the form of 2^{R_0} copies of the classical state $\rho^{U^A U^B U^C} := \sum_u p(u)|u\rangle\langle u|^{U^A} \otimes |u\rangle\langle u|^{U^B} \otimes |u\rangle\langle u|^{U^C} = \sum_u p(u)|uuu\rangle\langle uuu|^{U^A U^B U^C}$ as follows:

$$(\rho^{U^A U^B U^C})^{\otimes 2^{R_0}} = \rho^{U_1^A U_1^B U_1^C} \otimes \ldots \otimes \rho^{U_{2^{R_0}}^A U_{2^{R_0}}^B U_{2^{R_0}}^C},$$

where Alice possesses U^A systems, Bob U^B systems and Charlie has U^C systems (the superscripts should not be confused with the input A or output systems B and C of the channel, here they indicate the party to whom the underlying state belongs). We consider the shared state above to construct the first layer of our code. Conditioned on each of the 2^{R_0} states above, the parties are assumed to share $2^{R_s+R_1}$ copies of the state $\rho_u^{V^A V^B V^C} = \sum_v p(v|u)|vvv\rangle\langle vvv|^{V^A V^B V^C}$, as given below for the i-th state $\rho^{U_i^A U_i^B U_i^C}$:

$$\sum_u p(u)|uuu\rangle\langle uuu|^{U_i^A U_i^B U_i^C} \otimes (\rho_u^{V^A V^B V^C})^{\otimes 2^{R_s+R_1}},$$

where Alice, Bob and Charlie are in possession of the V^A, V^B and V^C systems, respectively. The set $[1 : 2^{R_s+R_1}]$ is partitioned into 2^{R_s} equal size bins. This constitutes the second

layer of the code. Finally, conditioned on each of the $2^{R_s+R_1}$ states above the parties will share 2^{R_d} copies of the state $\rho_v^{X^AX^BX^C} := \sum_x p(x|v)|xxx\rangle\langle xxx|^{X^AX^BX^C}$, as illustrated below for the i-th state $\rho^{V_i^AV_i^BV_i^C}$:

$$\sum_{u,v} p(u,v)|vvv\rangle\langle vvv|^{V_i^AV_i^BV_i^C} \otimes (\rho_v^{X^AX^BX^C})^{\otimes 2^{R_d}},$$

where X^A, X^B and X^C systems are owned by Alice, Bob and Charlie, respectively. These states build the third layer of the code. All states above are assumed to be available to all parties before communication begins. In the following, to avoid inefficient notation we may drop the superscripts if it does not lead to ambiguity; for instance when we analyze Bob's error probability, it is obvious that we are dealing with Bob's systems or in the secrecy analysis those of Charlie are dealt with.

Encoding: To send a message triple (m_0, m_1, m_s), the encoder first chooses a dummy message $m_d \in [1 : 2^{R_d}]$. In the first layer, the encoder finds the m_0-th state, i.e. $\rho^{U^A_{m_0}}$, then it looks for the m_s-th bin, inside which it selects the state associated to the individualized message m_1; finally, the encoder picks the m_d-th state $\rho^{X^A_{m_d}}$ among those tied to the state found in the preceding step. The encoder sends the selected classical system through a modulator (a linear operator $\mathcal{V} : \mathcal{X} \to \mathcal{D}(\mathcal{H}^A)$ which maps the classical control variable $x \in \mathcal{X}$ to a quantum state in the input Hilbert space) resulting in a quantum codeword ρ_x^A which will be then transmitted over the channel[5].

Decoding: Bob performs a two-phase decoding strategy such that he finds the common message in the first phase and then confidential and individualized messages in the subsequent phase. The transmission of the m_0-th common message induces the following state on Bob's side:

$$\rho^{U_1} \otimes ... \otimes \rho^{U_{m_0}B} \otimes ... \otimes \rho^{U_{2^{R_0}}}, \tag{30}$$

where $\rho^{U_{m_0}B} = \sum_u p(u)\,|u\rangle\langle u|^{U_{m_0}} \otimes \rho_u^B$. Apparently Bob has to be able to spot the location where the received system B is tied to his U system. In other words, he should be able to distinguish between states induced for different values of the common message. Bob employs a position-based decoding to solve the raised 2^{R_0}-ary hypothesis testing problem. Moreover, for the common message m_0, the selection of the pair (m_s, m_1) will induce the following state on Bob's side:

$$\rho^{V_{(m_0,1,1)}} \otimes ... \otimes \rho^{V_{(m_0,m_s,m_1)}B} \otimes ... \otimes \rho^{V_{(m_0,2^{R_s},2^{R_1})}}, \tag{31}$$

where $\rho^{V_{(m_0,m_s,m_1)}B} = \sum_v p(v)\,|v\rangle\langle v|^{V_{(m_0,m_s,m_1)}} \otimes \rho_v^B$. Bob runs the second position-based POVM to solve the $2^{R_s+R_1}$-ary hypothesis testing problem. Charlie also runs the position-based decoding POVM to find out the transmitted common message. The state induced at Charlie side comes about by replacing B with C in (30).

Analysis of the probability of error: We first analyze the error probability of the common message by studying Bob's first decoder and the error analysis of Charlie can be carried out along the same lines. It is worth pointing out that although the messages encoded in the second layer might include dummy randomness, Bob will still decode them. The dummy messages in the third layer will not be decoded.

Reconsider the state in (30). To find out the transmitted common message, Bob has to distinguish between 2^{R_0} different states. As hinted before, this puts forward a 2^{R_0}-ary hypothesis testing problem. Let $\{T^{UB}, I - T^{UB}\}$ be the elements of a POVM that is chosen for discriminating between two states ρ^{UB} and $\rho^U \otimes \rho^B$. Further, we assume that the test operator T^{UB} decides correctly in favor of ρ^{UB} with probability at least[6] $1 - (\varepsilon' - \delta_1)$. Bob will use the following square-root measurement to detect the common message:

$$\Omega_{m_0} := \left(\sum_{m_0'=1}^{2^{R_0}} \Pi_{m_0'}\right)^{-\frac{1}{2}} \Pi_{m_0} \left(\sum_{m_0'=1}^{2^{R_0}} \Pi_{m_0'}\right)^{-\frac{1}{2}},$$

where $\Pi_{m_0} := \mathbb{1}^{U_1} \otimes ... \otimes T^{U_{m_0}B} \otimes ... \otimes \mathbb{1}^{U_{2^{R_0}}}$ and $T^{U_{m_0}B}$ is the test operator. It can be easily checked that the set $\{\Omega_{m_0}\}_{m_0}$ constitutes a valid POVM, i.e. $\sum_{m_0} \Omega_{m_0} = \mathbb{1}$. Besides, direct calculation shows that $\mathrm{Tr}\{\Pi_{m_0}(\rho^{U_1} \otimes ... \otimes \rho^{U_{m_0}B} \otimes ... \otimes \rho^{U_{2^{R_0}}})\} = \mathrm{Tr}\{T^{U_{m_0}B}\rho^{U_{m_0}B}\}$ and for any $m_0' \neq m_0$, $\mathrm{Tr}\{\Pi_{m_0}(\rho^{U_1} \otimes ... \otimes \rho^{U_{m_0'}B} \otimes ... \otimes \rho^{U_{2^{R_0}}})\} = \mathrm{Tr}\{\Pi_{m_0}(\rho^{U_{m_0}} \otimes \rho^B)\}$.

Observe that the symmetric structure of the codebook generation and decoding leads to an average error probability that is equal to the individual error probabilities. Therefore, we might assume $m_0 = 1$ was transmitted. Hence,

$$\begin{aligned}
&\Pr(\hat{M}_0 \neq 1 | M_0 = 1) \\
&\quad = \mathrm{Tr}\{(\mathbb{1} - \Omega_1)(\rho^{U_1B} \otimes ... \otimes \rho^{U_{2^{R_0}}})\} \\
&\quad \leq (1+c)\mathrm{Tr}\{(\mathbb{1} - \Pi_1)(\rho^{U_1B} \otimes ... \otimes \rho^{U_{2^{R_0}}})\} \\
&\qquad + (2 + c + c^{-1}) \sum_{m_0 \neq 1} \mathrm{Tr}\{\Pi_{m_0}(\rho^{U_1B} \otimes ... \otimes \rho^{U_{2^{R_0}}})\} \\
&\quad \leq (1+c)(\varepsilon' - \delta_1) + (2 + c + c^{-1})2^{R_0 - I_H^{\varepsilon'-\delta_1}(U;B)_\rho},
\end{aligned}$$

where the first inequality follows from Lemma 15 and in the second inequality, the first term is based on the assumption and the second term follows from the definition of the hypothesis testing mutual information (see Definition 1). The last expression is set equal to ε' and the optimal value of c is derived as $c = \frac{\delta_1}{2\varepsilon' - \delta_1}$. Then, we will have

$$R_0 = I_H^{\varepsilon'-\delta_1}(U;B)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right).$$

In the same manner, it can be shown that the achievable rate of the common message to Charlie equals $R_0 = I_H^{\varepsilon'-\delta_2}(U;C)_{\rho^{UC}} - \log_2(\frac{4\epsilon'}{\delta_2^2})$.

In an analogous way, the reliability analysis of the confidential and the individualized messages goes as follows. Before we delve into the error analysis of the confidential and individualized messages, note from the gentle measurement

[5]Note that we have included the modulator in the definition of the code meaning that it needs to be optimized over to get our capacity results.

[6]For the sake of clarity, we choose to specify the error probability of the test operator to be $\varepsilon' - \delta_1$ to ensure that the error probability of the code will be larger than this and at most ε'.

lemma [57] that the disturbed state fed into the second decoder of Bob is impaired by at most $2\sqrt{\varepsilon'}$; this should be taken into account in final assessment of the error probability. Consider a binary POVM with elements $\{Q^{UVB}, \mathbb{1}-Q^{UVB}\}$. The POVM is to discriminate the states $\rho^{UVB} = \sum_u p(u)|u\rangle\langle u|^U \otimes \rho_u^{VB}$ and $\rho^{V-U-B} \coloneqq \sum_u p(u)|u\rangle\langle u|^U \otimes \rho_u^V \otimes \rho_u^B$ such that the value of Q^{UVB} estimates the state to be ρ^{UVB}. Assume the probability of failure to make a correct decision on ρ^{UVB} is at most $\varepsilon' - \delta_3$, i.e., $\mathrm{Tr}\{(\mathbb{1}-Q)\rho^{UVB}\} \leq \varepsilon' - \delta_3$. Bob will take the following square-root measurement POVM :

$$\Theta_{m_s,m_1} \coloneqq$$
$$\left(\sum_{m'_s=1}^{2^{R_s}}\sum_{m'_1=1}^{2^{R_1}} \Gamma_{m'_s,m'_1}\right)^{-\frac{1}{2}} \Gamma_{m_s,m_1} \left(\sum_{m'_s=1}^{2^{R_s}}\sum_{m'_1=1}^{2^{R_0}} \Gamma_{m'_s,m'_1}\right)^{-\frac{1}{2}},$$

where $\Gamma_{m_s,m_1} \coloneqq \mathbb{1}^{V_{1,1}} \otimes ... \otimes Q^{UV_{m_s,m_1}B} \otimes ... \otimes \mathbb{1}^{V_{2^{R_s},2^{R_1}}}$ and $Q^{UV_{m_s,m_1}B}$ is the binary test operator. Observe that $\sum_{m_s,m_1} \Theta_{m_s,m_1} = \mathbb{1}$. It is easy to show that for all m_s, m_1, we have $\mathrm{Tr}\{\Gamma_{m_s,m_1}(\sum_u p(u)|u\rangle\langle u|^U \otimes \rho_u^{V_{1,1}} \otimes ... \otimes \rho_u^{V_{m_s,m_1}B} \otimes ... \otimes \rho_u^{V^B_{2^{R_s},2^{R_1}}})\} = \mathrm{Tr}\{Q\rho^{UVB}\}$. On the other hand, for any $m'_s \neq m_s$ or $m'_1 \neq m_1$, $\mathrm{Tr}\{\Gamma_{m_s,m_1}(\sum_u p(u)|u\rangle\langle u|^U \otimes \rho_u^{V_{1,1}} \otimes ... \otimes \rho_u^{V_{m'_s,m'_1}B} \otimes ... \otimes \rho_u^{V_{2^{R_s},2^{R_1}}})\} = \mathrm{Tr}\{Q\rho^{V-U-B}\}$. By the symmetry of the random codebook construction, the average error probability is the same as the error probability of any pair (m_s, m_1), hence it suffices to find the error probability if $(m_s = 1, m_1 = 1)$ was sent. The analysis continues as shown at the top of the next page.

where the first inequality is due to Lemma 15 and in the second inequality, the first term comes from the assumption about the accuracy of the test operator Q and the second term uses the definition of the hypothesis testing conditional mutual information, Definition 2. We choose the error probability be less that or equal to ε', so the optimal value of the constant is set to $c = \frac{\delta_3}{2\varepsilon'-\delta_3}$ and eventually we will get the following sum rate:

$$R_s + R_1 = I_H^{\varepsilon'-\delta_3}(V;B|U)_\rho - \log_2\left(\frac{4\varepsilon'}{\delta_3^2}\right).$$

Analysis of the secrecy: Our tool to study secrecy is the conditional convex-split lemma. The dummy message and perhaps the individualized message which take care of confidentiality are encoded in the second and third layers as superposition of shared states. The quantum channel resolvability via superposition coding was studied in [44]. Given the setup of our problem, here we should try to prove the resolvability problem using convex-split lemma. We gave the analysis for Charlie's successful detection of the common message; in the secrecy analysis we assume Charlie knows the common message and the correct copy of the ρ^U used in the first layer. The idea for secrecy is that Charlie's systems have to remain close to some constant state, no matter which confidential message was transmitted.

For a given confidential message, the choice of the individualized message will induce an average state on Charlie's V systems in the second layer where the dummy message induces an average state on his X systems in the third layer. Since the states in the second layer are superposed to those in the third layer, both the individualized message and the dummy message will help to induce a state at Charlie's side that should be close enough to a target state. We first sketch the state induced by the chosen individualized and dummy messages. For a choice of the confidential message $m_s \in [1 : 2^{R_s}]$, the induced state is as given by Eq. (32) (the subscripts of variable V should be understood as the ordered pairs $(1,1), ..., (1,2^{R_1}), (2,1), ..., (2,2^{R_1}), ..., (m_s,m_1), ..., (2^{R_s},2^{R_1})$ where the first component belongs to $[1 : 2^{R_s}]$ and the second component is in $[1 : 2^{R_1}]$):

In order to get an intuitive understanding of the equations above, first we should think of the sources of the randomness available in the protocol. Since the common message is already known, the remaining sources of the randomness with respect to the confidential message are the individualized and dummy messages. Second, we should note where each source of the randomness is being consumed. Equation (32) indicates that the chosen confidential message is m_s, equation (33) represents the uniform randomness imposed by the individualized message (see the range of the variable j) and finally, equation (34) reflects the randomness introduced by the dummy message (see the range of the variable i). All the messages available to the encoder are potential sources of randomness that can be used for secrecy purposes, i.e., to confuse a receiver about other messages. In our setting, the common message is decoded by Charlie and to hide the confidential message, there is randomness coming from the individualized and dummy messages. Note that with regard to the individualized message, neither Alice's encoding nor Bob's decoding influence the role it plays as a source of randomness. Moreover, as discussed before, the individualized message may or may not contain useful information for Bob; however, Bob will decode the individualized message and then he can throw away its content. In case the individualized message contains useful information for Bob, by definition, we do not care if information about the individualized message is leaked to Charlie.

Charlie not being able to detect the confidential message amounts to his state being sufficiently close to the state given by Eq. (35), where $\rho_u^C = \sum_{v,x} p(v,x|u)\rho_x^C$ is considered the constant state independent of the chosen confidential message. Concerning the trace distance between the aforementioned states, since the trace distance is invariant with respect to tensor product states, we can remove the same terms from both states. Eventually the expression given by Eq. (36) is the distance required to be small enough. Note that in Eq. (36) the expression being subtracted refers to the state associated to the chosen confidential message given inside the brackets in (35). We proceed to bound equation (36) from above by envisioning an intermediate state which is, intuitively, closer to either of the states involved in (36) than the two states themselves. We define such an intermediate state as $\sum_u p(u)|u\rangle\langle u|^U \otimes \Xi_u^C$ where Ξ_u^C is giveb by Eq. (37). Next, we have to bring in the intermediate state. We do so by the triangle inequality as shown by Eq. (38).

We now try to upper bound each term appearing on the right-hand side. For the first term, simply by expanding the

$$
\begin{aligned}
&\Pr((\hat{M}_s,\hat{M}_1)\neq(1,1)|(M_s,M_1)=(1,1))\\
&=\mathrm{Tr}\{(\mathbb{1}-\Theta_{1,1})(\sum_u p(u)|u\rangle\langle u|^U\otimes\rho_u^{V_{1,1}B}\otimes...\otimes\rho_u^{V_{2^{R_s},2^{R_1}}})\}\\
&\leq(1+c)\mathrm{Tr}\{(\mathbb{1}-\Gamma_{1,1})(\sum_u p(u)|u\rangle\langle u|^U\otimes\rho_u^{V_{1,1}B}\otimes...\otimes\rho_u^{V_{2^{R_s},2^{R_1}}})\}\\
&\qquad+(2+c+c^{-1})\sum_{(m_s,m_1)\neq(1,1)}\mathrm{Tr}\{\Gamma_{m_s,m_1}(\sum_u p(u)|u\rangle\langle u|^U\otimes\rho_u^{V_{1,1}B}\otimes...\otimes\rho_u^{V_{2^{R_s},2^{R_1}}})\}\\
&\leq(1+c)(\varepsilon'-\delta_3)+(2+c+c^{-1})2^{R_1+R_s-I_H^{\varepsilon'-\delta_3}(V;B|U)_{\rho^{UVB}}},
\end{aligned}
$$

$$
\begin{aligned}
&\sum_u p(u)|u\rangle\langle u|^U\otimes\Big(\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{1,1}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big]\otimes...\otimes\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s-1,2^{R_1}}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big]\otimes\\
&\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j}\otimes\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s+1,1}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big]\otimes...\otimes\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{2^{R_s},2^{R_1}}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big]\Big).
\end{aligned}
\tag{32}
$$

where

$$
\Upsilon_u^{C,j}\coloneqq\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s,1}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\otimes...\otimes\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s,j}}\otimes\Psi_v^C\otimes...\otimes\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s,2^{R_1}}}\otimes(\rho_v^X)^{\otimes 2^{R_d}},
\tag{33}
$$

and

$$
\Psi_v^C\coloneqq\frac{1}{2^{R_d}}\sum_{i=1}^{2^{R_d}}\rho_v^{X_1^C}\otimes...\otimes\rho_v^{X_i^CC}\otimes...\otimes\rho_v^{X_{2^{R_d}}^C}.
\tag{34}
$$

$$
\begin{aligned}
&\sum_u p(u)|u\rangle\langle u|^U\otimes\Big(\big(\sum_v p(v|u)|v\rangle\langle v|^{V_{1,1}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big)\otimes...\otimes\big(\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s-1,2^{R_1}}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big)\\
&\qquad\otimes\Big[\big(\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s}}\otimes(\rho_v^{X^C})^{\otimes 2^{R_d}}\big)^{\otimes 2^{R_1}}\otimes\rho_u^C\Big]\otimes...\otimes\big(\sum_v p(v|u)|v\rangle\langle v|^{V_{R_s,R_1}}\otimes(\rho_v^X)^{2^{R_d}}\big)\Big).
\end{aligned}
\tag{35}
$$

$$
\frac{1}{2}\Big\|\sum_u p(u)|u\rangle\langle u|^U\otimes\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j}-\sum_u p(u)|u\rangle\langle u|^U\otimes\big(\sum_v p(v|u)|v\rangle\langle v|^V\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big)^{\otimes 2^{R_1}}\otimes\rho_u^C\Big\|_1,
\tag{36}
$$

$$
\begin{aligned}
\Xi_u^C\coloneqq\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Big(&\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s,1}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big]\otimes...\\
&\otimes\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s,j}}\otimes(\rho_v^{X_1}\otimes...\otimes\rho_v^{X_{R_d}}\otimes\rho_v^C)\big]\otimes...\otimes\big[\sum_v p(v|u)|v\rangle\langle v|^{V_{m_s,2^{R_1}}}\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big]\Big).
\end{aligned}
\tag{37}
$$

---

summation and subtracting equal terms from both side, the argument follows as given by Eq. (39). Then immediately by noting the Markov chain, the conditional convex-split lemma asserts that if $R_d=\widetilde{I}_{\max}^{\varepsilon''}(X;C|V)_\rho+2\log_2(\frac{1}{\eta})$, then

$$
\begin{aligned}
&P(\sum_u p(u)|u\rangle\langle u|^U\otimes\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j},\sum_u p(u)|u\rangle\langle u|^U\otimes\Xi_u^C)\\
&\qquad\leq 2\varepsilon''+\eta.
\end{aligned}
$$

and from the relation between the purified distance and the

$$\frac{1}{2}\Big\|\sum_u p(u)|u\rangle\langle u|^U\otimes\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j}-\sum_u p(u)|u\rangle\langle u|^U\otimes\big(\sum_v p(v|u)|v\rangle\langle v|^V\otimes(\rho_v^X)^{\otimes 2^{R_d}}\big)^{\otimes 2^{R_1}}\otimes\rho_u^C\Big\|_1 \tag{38}$$
$$\leq\frac{1}{2}\Big\|\sum_u p(u)|u\rangle\langle u|^U\otimes\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j}-\sum_u p(u)|u\rangle\langle u|^U\otimes\Xi_u^C\Big\|_1$$
$$+\frac{1}{2}\Big\|\sum_u p(u)|u\rangle\langle u|^U\otimes\Xi_u^C-\sum_u p(u)|u\rangle\langle u|^U\otimes\big(\rho_u^{V^C}\otimes(\rho_v^{X^C})^{\otimes 2^{R_d}}\big)^{\otimes 2^{R_1}}\otimes\rho_u^C\Big\|_1.$$

$$\frac{1}{2}\Big\|\sum_u p(u)|u\rangle\langle u|^U\otimes(\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j}-\Xi_u^C)\Big\|_1$$
$$=\frac{1}{2}\sum_u p(u)\Big\|\sum_v p(v|u)|v\rangle\langle v|^V\otimes\big(\frac{1}{2^{R_d}}\sum_{i=1}^{2^{R_d}}\rho_v^X\otimes...\otimes\rho_v^{X_iC}\otimes...\otimes\rho_v^{X_{2^{R_d}}}-\rho_v^{X_1}\otimes...\otimes\rho_v^{X_{2^{R_d}}}\otimes\rho_v^C\big)\Big\|_1. \tag{39}$$

trace distance, we have

$$\frac{1}{2}\Big\|\sum_u p(u)|u\rangle\langle u|^U\otimes(\frac{1}{2^{R_1}}\sum_{j=1}^{2^{R_1}}\Upsilon_u^{C,j}-\Xi_u^C)\Big\|_1\leq 2\varepsilon''+\eta,$$

For the second term, from the invariance of the trace distance with respect to tensor product states, we can trace out X systems from both expressions leading to the expression shown by Eq. (40). Then the conditional convex-split lemma guarantees the purified distance between states to be less than or equal to $(2\varepsilon''+\eta)$ if we choose $R_1=\widetilde{I}^{\varepsilon''}_{\max}(V;C|U)_\rho+2\log_2(\frac{1}{\eta})$, which in turn, implies that the trace distance between the states is also less than or equal to $(2\varepsilon''+\eta)$.

Derandomization: The proposed protocol relies upon shared randomness among parties. In order to show that the results also hold without assistance of shared randomness, the code needs to be derandomized. Derandomization is a standard procedure which can be done by expanding the states and corresponding POVM's and using a property of the trace distance given by the equality in (3) (see [36], [28], [58]). The only point that might be needed to be made here is the structure of the test operators in Bob's decoders (as well as that of Charlie). Note than the test operators were described generally as T^{UB} and Q^{UVB} without specifying the nature of the subsystems, i.e., whether each of U,V or B systems are classical or quantum. For our purposes, it is sufficient to consider the test operators as $T^{UB}:=\sum_u|u\rangle\langle u|^U\otimes\overline{T}_u^B$ where $\overline{T}_u^B:=\langle u|T^{UB}|u\rangle$. Likewise, we only need to have $Q^{UVB}:=\sum_{u,v}|u\rangle\langle u|^U\otimes|v\rangle\langle v|^V\otimes\overline{Q}_{u,v}^B$ where $\overline{Q}_{u,v}^B:=\langle u,v|Q^{UVB}|v,u\rangle$.

Expurgation: So far we have come to know that there exists at least one code that satisfies the reliability criterion in (14) and at least one codebook that satisfies the secrecy requirement (15). We should use Markov inequality to find a good code that satisfies both the reliability (14) and secrecy (15) simultaneously. We have the average error probability over all codes $P^1_{\text{error}}\leq 3\varepsilon'+2\sqrt{\varepsilon'}$ (with $2\sqrt{\varepsilon'}$ coming from the gentle measurement lemma) and the secrecy over all code $P^1_{\text{secrecy}}\leq 4\varepsilon''+2\eta$. From Markov inequality we know that $\Pr(P^1_{\text{error}}\geq\sqrt[4]{\varepsilon'})\leq 3(\varepsilon')^{3/4}+2\sqrt[4]{\varepsilon'}$ and $\Pr(P^1_{\text{secrecy}}\geq\sqrt[4]{\varepsilon''})\leq 4(\varepsilon'')^{3/4}+2(\varepsilon'')^{7/4}$. Then there is a good code for which, with high probability neither statement is true:

$$\Pr(P^1_{\text{error}}\leq\sqrt[4]{\varepsilon'},P^1_{\text{secrecy}}\leq\sqrt[4]{\varepsilon''})$$
$$\geq 1-(3(\varepsilon')^{3/4}+2\sqrt[4]{\varepsilon'})-(4(\varepsilon'')^{3/4}+2(\varepsilon'')^{7/4}).$$

Let $\varepsilon:=\max\{\sqrt[4]{\varepsilon'},\sqrt[4]{\varepsilon''}\}$. This parameter works for both requirements and the results is concluded.

□

Lemma 17: We have $\bigcup\mathcal{R}^{(in)}(\rho)\subseteq\mathcal{R}^\varepsilon(\mathcal{N})$ and the union is over all ρ^{UVXBC} arising from the channel.

Proof: To prove the lemma we need to show that for all ρ arising from the channel $\mathcal{R}^{\text{in}}(\rho)\subseteq\mathcal{R}^*(\rho)$. While this can be proven in a standard way by Fourier-Motzkin elimination (see for example appendix D of [59]), we follow the approach of [7] to show the lemma. Note that from the definition of $\mathcal{R}^\varepsilon(\mathcal{N})$, if a quadruple $(R_0+r_0,R_1-r_0-r_s+r_d,R_s+r_s,R_d-r_d)\in\mathcal{R}^\varepsilon(\mathcal{N})$ for some $r_0,r_s,r_d\geq 0$, then $(R_0,R_1,R_s,R_d)\in\mathcal{R}^\varepsilon(\mathcal{N})$ as well. Then one can find explicit values of (r_0,r_s,r_d) such that for any given $(R_0,R_1,R_s,R_d)\in\mathcal{R}^{(in)}(\rho)$ we have $(R_0+r_0,R_1-r_0-r_s+r_d,R_s+r_s,R_d-r_d)\in\mathcal{R}^*(\rho)$. In fact for $R_1<\widetilde{I}^{\varepsilon''}_{\max}(V;C|U)_\rho+2\log_2(\frac{1}{\eta})$, the values $(r_0,r_s,r_d):=(0,0,\widetilde{I}^{\varepsilon''}_{\max}(V;C|U)_\rho+2\log_2(\frac{1}{\eta})-R_1)$ can be seen to satisfy equations (26) to (29) and thus imply $(R_0+r_0,R_1-r_0-r_s+r_d,R_s+r_s,R_d-r_d)\in\mathcal{R}^*(\rho)$. This combined with Lemma 16 proves $\bigcup\mathcal{R}^{(\text{in})}(\rho)\subseteq\mathcal{R}^\varepsilon(\mathcal{N})$.

□

V. Converse

Consider the common message rate R_0 bound from (21). This bound was proved in [27] by relating the communication problem to a problem in binary hypothesis testing. We briefly explain the approach here. From the definition of the reliability given in (14) both $\Pr\{\tilde{M}_0\neq M_0\}\leq\varepsilon$

$$\frac{1}{2}\Big\| \sum_u p(u)|u\rangle\langle u|^U \otimes \big(\frac{1}{2^{R_1}}\sum_{j=1}^{R_1}(\rho_u^{V_1^C}\otimes ...\otimes \rho_u^{V_i^C C}\otimes ...\otimes \rho_u^{V_{R_1}^C}) - \rho_u^{V_1^C}\otimes ...\otimes \rho_u^{V_{2^{R_1}}^C}\otimes \rho_u^C\big)\Big\|_1 \tag{40}$$

and $\Pr\{(\hat{M}_0,\hat{M}_1,\hat{M}_s)\neq(M_0,M_1,M_s)\}\leq\varepsilon$ must be satisfied. We concentrate now on the fulfillment of the first condition, i.e., $\Pr\{\hat{M}_0\neq M_0\}\leq\varepsilon$. Consider the task of distinguishing between two quantum states $\rho^{\hat{M}_0 M_0}=\frac{1}{2^{R_0}}\sum_{m_0}|m_0\rangle\langle m_0|^{\hat{M}_0}\otimes|m_0\rangle\langle m_0|^{M_0}$ and $\rho^{\hat{M}_0}\otimes\rho^{M_0}$ where the former is the null hypothesis and the latter the alternative hypothesis. It can be easily verified that $\Pr\{\hat{M}_0\neq M_0\}\leq\varepsilon$ implies that the type I error is less that or equal to ε and the type II error equals 2^{-R_0}. Then from the definition of the hypothesis-testing mutual information and the monotonicty of the hypothesis testing relative entropy with CPTP maps, we have $R_0\leq I_{\mathrm{H}}^{\varepsilon}(M_0;B)_\rho$. Let $U:=M_0$, then the converse follows. The proof of $R_0\leq I_{\mathrm{H}}^{\varepsilon}(M_0;C)_\rho$ follows the same argument.

We now analyze the condition $\Pr\{(\hat{M}_0,\hat{M}_1,\hat{M}_s)\neq(M_0,M_1,M_s)\}\leq\varepsilon$. Following a procedure similar to [36], we expand this expression as follows:

$$\begin{aligned}
\varepsilon &\geq \Pr\{(\hat{M}_0,\hat{M}_1,\hat{M}_s)\neq(M_0,M_1,M_s)\}\\
&= \sum_{m_0,m_1,m_s} p(m_0)p(m_1)p(m_s)\times\\
&\qquad \Pr\{(\hat{M}_0,\hat{M}_1,\hat{M}_s)\neq(m_0,m_1,m_s)|m_0,m_1,m_s\}\\
&= \sum_{m_0,m_1,m_s} p(m_0)p(m_1)p(m_s)\times\\
&\qquad \sum_{(m_0',m_1',m_s')\neq(m_0,m_1,m_s)} p(m_0',m_1',m_s'|m_0,m_1,m_s)\\
&\geq \sum_{m_0,m_1,m_s} p(m_0)p(m_1)p(m_s)\times\\
&\qquad \sum_{\substack{m_0',\\(m_1',m_s')\neq(m_1,m_s)}} p(m_0',m_1',m_s'|m_0,m_1,m_s)\\
&= \sum_{m_0,m_1,m_s} p(m_0)p(m_1)p(m_s)\times\\
&\qquad \sum_{(m_1',m_s')\neq(m_1,m_s)} p(m_1',m_s'|m_0,m_1,m_s)\\
&= \sum_{m_0} p(m_0)\Pr\{(\hat{M}_1,\hat{M}_s)\neq(M_1,M_s)|M_0=m_0\}.
\end{aligned}$$

Notice that the final expression indicates the probability of erroneous detection of (M_s,M_1) when M_0 is transmitted. We find an upper bound on the sum rate of (M_s,M_1) by considering a binary hypothesis testing problem with null and alternative hypotheses given respectively as follows:

$$\rho^{M_0\hat{M}_s\hat{M}_1 M_s M_1}:=\frac{1}{2^{R_0}}\sum_{m_0}|m_0\rangle\langle m_0|^{M_0}\otimes\rho_{m_0}^{\hat{M}_s\hat{M}_1 M_s M_1},$$

$$\rho^{\hat{M}_s\hat{M}_1-M_0-M_s M_1}:=\frac{1}{2^{R_0}}\sum_{m_0}|m_0\rangle\langle m_0|^{M_0}\otimes\rho_{m_0}^{\hat{M}_s\hat{M}_1}\otimes\rho_{m_0}^{M_s M_1},$$

where $\rho_{m_0}^{\hat{M}_s\hat{M}_1 M_s M_1}=\frac{1}{2^{R_s+R_1}}\sum_{m_s m_1}|m_s m_1\rangle\langle m_s m_1|^{\hat{M}_s\hat{M}_1}\otimes|m_s m_1\rangle\langle m_s m_1|^{M_s M_1}$. It can be easily verified that type I error is equivalent to $\sum_{m_0}p(m_0)\Pr\{(\hat{M}_1,\hat{M}_s)\neq(M_1,M_s)|M_0=m_0\}$ which is assumed to be less that or equal to ε. On the other hand, the type II error can be written as follows:

$$\begin{aligned}
&\sum_{m_0,m_s,m_1} p_{M_0}(m_0)p_{M_s M_1}(m_s,m_1)p_{\hat{M}_s\hat{M}_1}(m_s,m_1)\\
&=\frac{1}{2^{R_s+R_1}}\sum_{m_0,m_s,m_1} p_{M_0}(m_0)p_{\hat{M}_s\hat{M}_1}(m_s,m_1)=\frac{1}{2^{R_s+R_1}}.
\end{aligned}$$

Then we have the following:

$$R_s+R_1\leq I_{\mathrm{H}}^{\varepsilon}(M_s,M_1;\hat{M}_s,\hat{M}_1|M_0)_\rho\leq I_{\mathrm{H}}^{\varepsilon}(M_s,M_1;B|M_0)_\rho,$$

where the first inequality stems from the definition of the conditional hypothesis testing mutual information and the second inequality is from monotonicity under CPTP maps. Identifying the random variables $V:=(M_s,M_1)$ and $U:=M_0$ concludes the intended bound. So far we have dealt with the reliability condition and have derived (21) and (22).

Next we turn our attention to the secrecy criterion. The secrecy condition (13) requires that the state of the Charlie and the confidential message become close to a product state for every transmitted common message. In converse proof, we consider a less strict criterion such that we demand the aforementioned states to be close on average over the common messages. i.e.

$$\begin{aligned}
&\frac{1}{2}\Big\|\rho^{CM_0M_s}-\frac{1}{2^{R_0}}\sum_{m_0}|m_0\rangle\langle m_0|^{M_0}\otimes\rho_{m_0}^{M_s}\otimes\sigma_{m_0}^C\Big\|_1\\
&\qquad=\frac{1}{2^{R_0+R_s}}\sum_{m_0,m_s}\frac{1}{2}\|\rho_{m_0,m_s}^C-\sigma_{m_0}^C\|_1\leq\varepsilon.
\end{aligned}$$

From the relation between the purified distance and the trace distance, the purified distance between the above-mentioned states is less that or equal to $\sqrt{2\varepsilon}$. Then from the definition of the smooth conditional relative entropy, it is easily checked that the following holds:

$$\begin{aligned}
&D_{\max}^{\sqrt{2\varepsilon}}(M_s;C|M_0)_\rho\\
&:=D_{\max}^{\sqrt{2\varepsilon}}\big(\rho^{M_0M_sC}\big\|\frac{1}{2^{R_0}}\sum_{m_0}|m_0\rangle\langle m_0|^{M_0}\otimes\rho_{m_0}^{M_s}\otimes\sigma_{m_0}^C\big)_\rho=0.
\end{aligned}$$

Therefore, in the quantity $D_{\max}^{\sqrt{2\varepsilon}}(M_s;C|M_0)_\rho=0$, we define $U:=M_0$ and $V:=M_s$ to get $D_{\max}^{\sqrt{2\varepsilon}}(V;C|U)_\rho=0$. Similarly, we let $V:=M_0$ and $X:=M_s$ to get $D_{\max}^{\sqrt{2\varepsilon}}(X;C|V)_\rho=0$. Finally the bound on the rate of the confidential message (23) can be seen from the bound derived on R_s+R_1 and the preceding discussion.

VI. Asymptotic Analysis

So far we have studied the scenario in which a quantum channel is available only once and the transmission was

subject to some non-zero error and secrecy parameters. In the asymptotic regime, however, a memoryless channel is considered to be available for an unlimited number of uses; if we denote the uses of the channel by n, the one-shot scenario corresponds to $n = 1$ where in the asymptotic regime $n \to \infty$. Moreover, in the asymptotic regime, as long as the achievability bounds and weak converses are concerned, the error and secrecy parameters are assumed to be vanishing in the limit of many channel uses, i.e., $\varepsilon \to 0$ as $n \to \infty$. The following formally defines the rate region in the asymptotic regime from the one-shot rate region defined before:

$$\mathcal{R}_\infty(\mathcal{N}) \coloneqq \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathcal{R}^\varepsilon(\mathcal{N}^{\otimes n}), \tag{41}$$

where the tensor power channel $\mathcal{N}^{\otimes n}$ indicates the n independent uses of the channel $\mathcal{N}$. In the following we first prove a theorem then we will recover several well-known results as corollaries.

Theorem 3: The asymptotic rate region $\mathcal{R}_\infty(\mathcal{N})$ of the broadcast channel $\mathcal{N}^{A\to BC}$ for simultaneous transmission of common, individualized and confidential messages with a rate-limited randomness encoder is given as follows:

$$\mathcal{R}_\infty(\mathcal{N}) = \bigcup_{\ell=1}^{\infty}\frac{1}{\ell}\mathcal{R}_\infty^{(1)}(\mathcal{N}^{\otimes\ell}), \tag{42}$$

where $\mathcal{R}_\infty^{(1)}(\mathcal{N}) \coloneqq \bigcup_{\rho^{UVXBC}} \mathcal{R}_\infty^{(2)}(\mathcal{N})$, in which $\mathcal{R}_\infty^{(2)}(\mathcal{N})$ is the set of quadruples (R_0, R_1, R_s, R_d) satisfying the following conditions:

$$R_0 \le \min\left[I(U;B)_\rho, I(U;C)_\rho\right], \tag{43}$$

$$R_0 + R_1 + R_s \le I(V;B|U)_\rho + \min\left[I(U;B)_\rho, I(U;C)_\rho\right], \tag{44}$$

$$R_s \le I(V;B|U)_\rho - I(V;C|U)_\rho, \tag{45}$$

$$R_1 + R_d \ge I(V;C|U)_\rho + I(X;C|V)_\rho, \tag{46}$$

$$R_d \ge I(X;C|V)_\rho, \tag{47}$$

where (R_0, R_1, R_s, R_d) denotes the rates of the common, individualized, confidential and dummy messages, respectively and

$$\rho^{UVXBC} = \sum_{u,v,x} p(u)p(v|u)p(x|v)\,|u\rangle\langle u|^U \otimes |v\rangle\langle v|^V \otimes |x\rangle\langle x|^X \otimes \mathcal{N}(\rho_x^A)$$

is the state arising from the channel.

Proof of Theorem 3: We need to show the direct part and the converse. To establish the direct part, we appeal to our one-shot achievability region and seek to show that the right-hand side of equation (42) is contained inside the left-hand side, i.e., the following:

$$\bigcup_{\ell=1}^{\infty}\frac{1}{\ell}\mathcal{R}_\infty^{(1)}(\mathcal{N}^{\otimes\ell}) \subseteq \mathcal{R}_\infty(\mathcal{N}).$$

From our achievability result, Theorem 1, if we use the channel m times independently (memoryless channel), or equivalently if we consider one use of the tensor power channel $\mathcal{N}^{\otimes m}$, we will have:

$$\bigcup_{\rho^m}\mathcal{R}^{(\text{in})}(\rho^m) \subseteq \mathcal{R}^\varepsilon(\mathcal{N}^{\otimes m}), \tag{48}$$

where $\mathcal{R}^{(\text{in})}(\rho^m)$ is the convex closure over all states ρ^m arising from m uses of the channel, of the rate quadruples (R_0, R_1, R_s, R_d) obeying the condition at the top of the next page. where U^m, V^m and X^m refer to the random variables drawn from the joint distributions $p(u_1, ..., u_m), p(v_1, ..., v_m)$ and $p(x_1, ..., x_m)$, respectively and $B^{\otimes m}$ and $C^{\otimes m}$ refer to the m-fold tensor product of the Hilbert spaces $\mathcal{H}^B$ and $\mathcal{H}^C$, respectively. Since we want to prove an achievability theorem, we can assume that each sequence of random variables is drawn from the corresponding distributions in an i.i.d. fashion, i.e., $p(u_1, ..., u_m) = \prod_{i=1}^m p(u_i)$, $p(v_1, ..., v_m) = \prod_{i=1}^m p(v_i)$ and $p(x_1, ..., x_m) = \prod_{i=1}^m p(x_i)$. Therefore, the state over which the above quantities are assessed, is $\rho^{\otimes m} = \rho \otimes ... \otimes \rho$.

The i.i.d. encoding assumption implies $\rho^m = \rho^{\otimes m}$ and enables us to simplify the entropic quantities in the asymptotic limit of many channel uses. To see this, we divide both sides of (48) by m and let $m \to \infty$:

$$\lim_{m\to\infty}\frac{1}{m}\bigcup_{\rho^{\otimes m}}\mathcal{R}^{(\text{in})}(\rho^{\otimes m}) \subseteq \lim_{\varepsilon\to 0}\lim_{m\to\infty}\frac{1}{m}\mathcal{R}^\varepsilon(\mathcal{N}^{\otimes m}), \tag{49}$$

This results in dividing the entropic quantities comprising $\mathcal{R}^{(\text{in})}(\rho^{\otimes m})$ by m and evaluate limits as $m \to \infty$. All the constant terms will vanish as $m \to \infty$ and from the asymptotic i.i.d. behavior of the quantities given in (5), (7) and Lemma 12, we get the region $\mathcal{R}_\infty^1(\mathcal{N})$. So far we have shown the following:

$$\mathcal{R}_\infty^1(\mathcal{N}) \subseteq \lim_{\varepsilon\to 0}\lim_{m\to\infty}\frac{1}{m}\mathcal{R}^\varepsilon(\mathcal{N}^{\otimes m}).$$

Finally we consider m uses of the tensor power channel $\mathcal{N}^{\otimes\ell}$ and let $n = m\ell$. Taking the limits as $n \to \infty$ concludes the direct part.

For the converse part, from Theorem 2 onward, if the channel $\mathcal{N}$ gets used m independent times, we will have

$$\mathcal{R}^\varepsilon(\mathcal{N}^{\otimes m}) \subseteq \bigcup_{\ell=1}^{m}\bigcup_{\rho^\ell}\mathcal{R}^{(\text{co})}(\mathcal{N}^{\otimes\ell}), \tag{50}$$

where $\mathcal{R}^{(\text{co})}(\mathcal{N}^{\otimes\ell})$ consists of the rate quadruples (R_0, R_1, R_s, R_d) obeying the following:

$$\begin{aligned}
R_0 &\le \min\left[I_{\text{H}}^\varepsilon(U^\ell;B^{\otimes\ell})_{\rho^\ell}, I_{\text{H}}^\varepsilon(U^\ell;C^{\otimes\ell})_{\rho^\ell}\right],\\
R_0 + R_1 + R_s &\le I_{\text{H}}^\varepsilon(V^\ell;B^{\otimes\ell}|U^\ell)_{\rho^\ell}\\
&\quad + \min\left[I_{\text{H}}^\varepsilon(U^\ell;B^{\otimes\ell})_{\rho^\ell}, I_{\text{H}}^\varepsilon(U^\ell;C^{\otimes\ell})_{\rho^\ell}\right],\\
R_s &\le I_{\text{H}}^\varepsilon(V^\ell;B^{\otimes\ell}|U^\ell)_{\rho^\ell} - D_{\max}^{\sqrt{2\varepsilon}}(V^\ell;C^{\otimes\ell}|U^\ell)_{\rho^\ell},\\
R_1 + R_d &\ge D_{\max}^{\sqrt{2\varepsilon}}(V^\ell;C^{\otimes\ell}|U^\ell)_{\rho^\ell} + D_{\max}^{\sqrt{2\varepsilon}}(X^\ell;C^{\otimes\ell}|V^\ell)_{\rho^\ell},\\
R_d &\ge D_{\max}^{\sqrt{2\varepsilon}}(X^\ell;C^{\otimes\ell}|V^\ell)_{\rho^\ell},
\end{aligned}$$

where $(\rho^{UVXBC})^\ell$ is the state inducing by ℓ independent uses of the channel such that its classical systems, U^ℓ, V^ℓ and X^ℓ correspond to the random variables drawn from the

$$
\begin{aligned}
R_0 &\leq \min\left[I_{\mathrm{H}}^{\varepsilon'-\delta_1}(U^m;B^{\otimes m})_{\rho^m} - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right), I_{\mathrm{H}}^{\varepsilon'-\delta_2}(U^m;C^{\otimes m})_{\rho^m} - \log_2\left(\frac{4\varepsilon'}{\delta_2^2}\right)\right],\\
R_0+R_1+R_s &\leq I_{\mathrm{H}}^{\varepsilon'-\delta_3}(V^m;B^{\otimes m}|U^m)_{\rho^m} - \log_2\left(\frac{4\varepsilon'}{\delta_3^2}\right)\\
&\quad + \min\left[I_{\mathrm{H}}^{\varepsilon'-\delta_1}(U^m;B^{\otimes m})_{\rho^m} - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right), I_{\mathrm{H}}^{\varepsilon'-\delta_2}(U^m;C^{\otimes m})_{\rho^m} - \log_2\left(\frac{4\varepsilon'}{\delta_2^2}\right)\right],\\
R_s &\leq I_{\mathrm{H}}^{\varepsilon'-\delta_3}(V^m;B^{\otimes m}|U^m)_{\rho^m} - \widetilde{I}_{\max}^{\varepsilon''}(V^m;C^{\otimes m}|U^m)_{\rho^m} - \log_2\left(\frac{4\varepsilon'}{\delta_1^2}\right) - 2\log_2\left(\frac{1}{\eta}\right),\\
R_1+R_d &\geq \widetilde{I}_{\max}^{\varepsilon''}(V^m;C^{\otimes m}|U^m)_{\rho^m} + \widetilde{I}_{\max}^{\varepsilon''}(X^m;C^{\otimes m}|V^m)_{\rho^m} + 4\log_2\left(\frac{1}{\eta}\right),\\
R_d &\geq \widetilde{I}_{\max}^{\varepsilon''}(X^m;C^{\otimes m}|V^m)_{\rho^m} + 2\log_2\left(\frac{1}{\eta}\right),
\end{aligned}
$$

joint distributions $p(u_1,...,u_\ell), p(v_1,...,v_\ell)$ and $p(x_1,...,x_\ell)$, respectively and quantum systems $B^{\otimes\ell}$ and $C^{\otimes\ell}$ refer to the ℓ-fold tensor product of the Hilbert spaces $\mathcal{H}^B$ and $\mathcal{H}^C$, respectively. We can now consider t i.i.d. uses of the superchannel $\mathcal{N}^{\otimes m}$ for large t. This means we evaluate the region over "tensor product" states $(\rho^m)^{\otimes t}$ and divide both sides of (50) by t and let $t\to\infty$. By invoking the asymptotic results from (5),(7) and (11), $\mathcal{R}^{(\mathrm{co})}(\mathcal{N}^{\otimes\ell})$ can be seen to be included in the following region:

$$
\begin{aligned}
R_0 &\leq \min\left[I(U^\ell;B^{\otimes\ell})_{\rho^\ell}, I(U^\ell;C^{\otimes\ell})_{\rho^\ell}\right],\\
R_0+R_1+R_s &\leq I(V^\ell;B^{\otimes\ell}|U^\ell)_{\rho^\ell} +\\
&\qquad \min\left[I(U^\ell;B^{\otimes\ell})_{\rho^\ell}, I(U^\ell;C^{\otimes\ell})_{\rho^\ell}\right],\\
R_s &\leq I(V^\ell;B^{\otimes\ell}|U^\ell)_{\rho^\ell} - I(V^\ell;C^{\otimes\ell}|U^\ell)_{\rho^\ell},\\
R_1+R_d &\geq I(V^\ell;C^{\otimes\ell}|U^\ell)_{\rho^\ell} + I(X^\ell;C^{\otimes\ell}|V^\ell)_{\rho^\ell},\\
R_d &\geq I(X^\ell;C^{\otimes\ell}|V^\ell)_{\rho^\ell}.
\end{aligned}
$$

The proof will be completed by dividing both sides of (50) by m and letting $m\to\infty$ as well as $\varepsilon\to 0$. □

Corollary 3 (Theorem 1 in [11]): Consider the quantum channel $\mathcal{N}^{A\to B}$ with an isometric extension $V^{A\to BE}$ and let $\rho^{URA} = \sum_u p(u)\,|u\rangle\langle u|\otimes|\phi_u\rangle\langle\phi_u|^{RA}$ be a classical-quantum state in which R is a reference system. The capacity region of simultaneous transmission of classical and quantum information for the channel is given by

$$
\mathrm{S}^\infty(\mathcal{N}) = \bigcup_{\ell=1}^{\infty}\frac{1}{\ell}\mathrm{S}_1^\infty(\mathcal{N}^{\otimes\ell}),
$$

where $\mathrm{S}_1^\infty(\mathcal{N})$ is the union, over all states of the form $\rho^{URB} = \sum_u p(u)\,|u\rangle\langle u|\otimes\mathcal{N}^{A\to B}(|\phi_u\rangle\langle\phi_u|^{RA})$ arising from the channel, of the rate pairs (R_c^∞, R_q^∞) obeying:

$$
\begin{aligned}
R_c^\infty &\leq I(U;B)_\rho,\\
R_q^\infty &\leq I(R\rangle BU)_\rho,
\end{aligned}
$$

where R_c^∞ and R_q^∞ denote respectively the rates of the classical and quantum information and $I(R\rangle BU)_\rho \coloneqq -H(R|BU)_\rho$ is the *coherent information*.

Proof: Following the discussion of Corollary 2 and Theorem 3, we only need to argue that the coherent information of the ensemble $\{p(u), |\phi_u\rangle\langle\phi_u|^{RBE}\}$ is equal to the rate of the confidential message in Theorem 3, i.e., the following:

$$
I(R\rangle BU)_\rho = I(V;B|U)_\rho - I(V;E|U)_\rho.
$$

We apply the Schmidt decomposition to the pure states $\{|\phi_u\rangle^{RBE}\}_u$ with respect to the cut $R|BE$ and then measure the R system in a suitable orthonormal basis. This measurement decoherifies the states such that the R system can be shown by a classcial system, say V. Then the equality of the coherent information and the confidential message rate can be easily checked (see for example exercise 11.6.7 in [47]). □

Corollary 4 (Theorem 3 of [7]): Let $\mathcal{N}_C^{X\to(Y,Z)}$ be a classical channel taking inputs to outputs according to some distribution $p(y,z|x)$. Moreover, let $\mathcal{R}^\infty(\mathcal{N}_C)$ be the capacity region of $\mathcal{N}_C^{X\to(Y,Z)}$ for simultaneous transmission of the common, individualized and confidential messages with a rate-limited randomness encoder, defined similar to (41). Then there exist random variables U and V satisfying $p(u,v,x,y,z) = \sum p(u,v)p(x|v)p(y,z|x)$ such that $\mathcal{R}^\infty(\mathcal{N}_C)$ equals the union over all distributions of rate quadruples (R_0,R_1,R_s,R_d) obeying:

$$
\begin{aligned}
R_0 &\leq \min\left[I(U;Y)_p, I(U;Z)_p\right],\\
R_0+R_1+R_s &\leq I(V;Y|U)_p + \min\left[I(U;Y)_p, I(U;Z)_p\right],\\
R_s &\leq I(V;Y|U)_p - I(V;Z|U)_p,\\
R_1+R_d &\geq I(V;Z|U)_p + I(X;Z|V)_p,\\
R_d &\geq I(X;Z|V)_p,
\end{aligned}
$$

where (R_0,R_1,R_s,R_d) denotes the rates of the common, individualized, confidential and dummy messages, respectively.

Proof: This is a simple corollary of Theorem 3. If we assume the channel outputs B and C are classical, then we know that all systems will be simultaneously diagonalizable and the regularization is not needed. Letting $Y \coloneqq B$ and $Z \coloneqq C$ finishes the proof. □

In the following corollary we recover a result for quantum broadcast channel without any secrecy requirement [46].

Corollary 5 (Theorem in [46]): Consider the quantum broadcast channel $\mathcal{N}^{A\to BC}$. The capacity region for the

transmission of common and individualized messages of $\mathcal{N}$, denoted by $C^{\infty}(\mathcal{N})$, is given as follows[7]:

$$C^{\infty}(\mathcal{N}) = \bigcup_{\ell=1}^{\infty} \frac{1}{\ell} C_1^{\infty}(\mathcal{N}^{\otimes \ell}),$$

where $C_1^{\infty}(\mathcal{N})$ is the union over all states ρ^{UVBC} arising from the channel, of the rate pairs (R_0, R_1) obeying

$$\begin{aligned} R_0 &\leq \min\big[I(U;B)_\rho, I(U;C)_\rho\big], \\ R_0 + R_1 &\leq I(V;B|U)_\rho + \min\big[I(U;B)_\rho, I(U;C)_\rho\big]. \end{aligned}$$

Proof: By dropping the secrecy requirement, the rate of the confidential message in Theorem 3 will add up to that of the individualized message. Note that this region is slightly different in appearance compared to the Theorem 1 in [46]. However, the discussion leading to the equations (17) and (18) in that paper indicates their equivalence: part (or whole) of the common message may contain information intended for Charlie such that Bob does not have any interest in learning those information; this leads to a slightly different region but the scenario and the rate region are essentially the same in that in superposition coding Bob is supposed to decode the common message in whole and maybe ignore its content afterwards. □

VII. Conclusion

We have studied the interplay between common, individualized and confidential messages with rate-limited randomness in the one-shot regime of a quantum broadcast channel. To establish our achievability results, we have proved a conditional version of the convex-split lemma whereby we have shown the channel resolvability problem in the one-shot regime via superpositions. To assess the tightness of our achievability region, we have also derived a (weak) converse region. By evaluating our rate regions in the asymptotic i.i.d setting, we recovered several well-known results in the literature.

Appendix A
Proof of lemmas

To prove Lemma 9, we need the following lemma.

Lemma 18: For quantum states ρ^{AB} and σ^B, there exists a state $\rho'^A \in \mathcal{B}^{\varepsilon}(\rho^A)$ such that:

$$D_{\max}(\rho^{AB} \| \rho'^A \otimes \sigma^B) \leq D_{\max}(\rho^{AB} \| \rho^A \otimes \sigma^B).$$

Proof: Trivial. □

Proof of lemma 9: In the result of Lemma 18, let ρ^{*AB} be the optimizer in the definition of $\widetilde{I}^{\varepsilon}_{\max}(A;B)_\rho$, by substituting this state we will have,

$$D_{\max}(\rho^{*AB} \| \rho'^A \otimes \sigma^B) \leq D_{\max}(\rho^{*AB} \| \rho^{*A} \otimes \sigma^B).$$

Let $\sigma^B \coloneqq \rho^B$ and choose $\rho'^A = \rho^A$ (this is possible since $\mathrm{P}(\rho^A, \rho^{*A}) \leq \varepsilon$) and then

$$D_{\max}(\rho^{*AB} \| \rho^A \otimes \rho^B) \leq D_{\max}(\rho^{*AB} \| \rho^{*A} \otimes \rho^B).$$

Then the result follows by definitions of the quantities. □

[7]This is defined similar to (41).

We need the following lemma to prove Lemma 10.

Lemma 19: For quantum states $\rho^{XAB} = \sum_x p(x) \left|x\right\rangle\!\left\langle x\right| \otimes \rho_x^{AB}$ and $\sigma^{XAB} = \sum_x q(x) \left|x\right\rangle\!\left\langle x\right| \otimes \sigma_x^A \otimes \sigma_x^B$, there exists a state $\rho'^{XAB} \in \mathcal{B}^{\varepsilon}(\rho^{XAB})$ classical on X such that:

$$\begin{aligned} &D_{\max}\big(\rho'^{XAB} \big\| \sum_x p'(x) \left|x\right\rangle\!\left\langle x\right| \otimes \rho_x'^A \otimes \sigma_B^x\big) \\ &\leq D_{\max}\big(\rho^{XAB} \big\| \sum_x q(x) \left|x\right\rangle\!\left\langle x\right| \otimes \sigma_x^A \otimes \sigma_x^B\big) \\ &\qquad + \log\bigg(\frac{1}{1-\sqrt{1-\varepsilon^2}} + 1\bigg). \end{aligned}$$

Proof: The proof is inspired by [29] and [60]. Let ρ^{XABC} be a purification of ρ^{XAB} and $\varepsilon > 0$. Further let $\Pi^{BC} \in \mathcal{H}_{BC}$ be a projector that is defined as the dual projector of the minimum rank projector Π^{XA} with $\mathrm{supp}(\Pi^{XA}) \subseteq \mathrm{supp}(\rho^{XA})$. The projector Π^{XA} is set to minimize $\big\|\Pi^{XA}\Gamma^{XA}\Pi^{XA}\big\|_\infty$ while fulfilling $P(\rho^{XABC}, \tilde{\rho}^{XABC}) \leq \varepsilon$ in which $\Gamma^{XA} \coloneqq (\rho^{XA})^{-\frac{1}{2}} \sigma^{XA} (\rho^{XA})^{-\frac{1}{2}}$ and $\tilde{\rho}^{XABC} \coloneqq \Pi^{BC} \rho^{XABC} \Pi^{BC}$. From Lemma 2, we know the following

$$\begin{aligned} \mathrm{P}(\rho^{XABC}, \Pi^{BC}\rho^{XABC}\Pi^{BC}) &\leq \sqrt{2\mathrm{Tr}\Pi_\perp^{BC}\rho - (\mathrm{Tr}\Pi_\perp^{BC}\rho)^2} \\ &= \sqrt{2\mathrm{Tr}\Pi_\perp^{XA}\rho - (\mathrm{Tr}\Pi_\perp^{XA}\rho)^2}. \end{aligned}$$

If we let $\mathrm{Tr}\Pi_\perp^{XA}\rho \leq 1 - \sqrt{1-\varepsilon^2}$, then we will have $P(\rho^{XABC}, \tilde{\rho}^{XABC}) \leq \varepsilon$ since $t \mapsto \sqrt{2t - t^2}$ is monotonically increasing over $[0,1]$. Now we choose Π^{XA} to be the projector onto the smallest eigenvalues of Γ^{XA} such that the aforementioned restriction holds, which in turn, results in the minimization of $\big\|\Pi^{XA}\Gamma^{XA}\Pi^{XA}\big\|_\infty$. Let Π'^{XA} denote the projector onto the largest remaining eigenvalue of $\Pi^{XA}\Gamma^{XA}\Pi^{XA}$. Notice that Π^{XA} and Π'^{XA} commute with Γ^{XA}. Then we have the following:

$$\big\|\Pi^{XA}\Gamma^{XA}\Pi^{XA}\big\|_\infty = \mathrm{Tr}(\Pi'^{XA}\Gamma^{XA}) = \min_{\mu^{XA}} \frac{\mathrm{Tr}(\mu^{XA}\Gamma^{XA})}{\mathrm{Tr}\mu^{XA}},$$

where the minimization is over all operators in the support of $\Pi'^{XA} + \Pi_\perp^{XA}$. Choosing $\mu^{XA} = (\Pi'^{XA} + \Pi_\perp^{XA})\rho^{XA}(\Pi'^{XA} + \Pi_\perp^{XA})$, we will have:

$$\begin{aligned} &\big\|\Pi^{XA}\Gamma^{XA}\Pi^{XA}\big\|_\infty \\ &\leq \frac{\mathrm{Tr}\{(\Pi'^{XA} + \Pi_\perp^{XA})\rho^{XA}(\Pi'^{XA} + \Pi_\perp^{XA})\Gamma^{XA}\}}{\mathrm{Tr}\{(\Pi'^{XA} + \Pi_\perp^{XA})\rho^{XA}(\Pi'^{XA} + \Pi_\perp^{XA})\}} \\ &\leq \frac{1}{1-\sqrt{1-\varepsilon^2}}, \end{aligned}$$

where from the fact that Π'^{XA} and $\Pi_\perp^{XA}$ commute with Γ^{XA}, we have $\mathrm{Tr}\{(\Pi'^{XA} + \Pi_\perp^{XA})\rho^{XA}(\Pi'^{XA} + \Pi_\perp^{XA})\Gamma^{XA}\} = \mathrm{Tr}\{(\Pi'^{XA} + \Pi_\perp^{XA})(\rho^{XA})^{1/2}\Gamma^{XA}(\rho^{XA})^{1/2}\} \leq \mathrm{Tr}\{(\rho^{XA})^{1/2}\Gamma^{XA}(\rho^{XA})^{1/2}\} = \mathrm{Tr}\sigma^{XA} = 1$. Moreover, the definition of Π^{XA} implies that $\mathrm{Tr}\{(\Pi'^{XA} + \Pi_\perp^{XA})\rho^{XA}\} \geq 1 - \sqrt{1-\varepsilon^2}$. Let $\gamma \coloneqq D_{\max}\big(\rho^{XAB} \big\| \sum_x q(x) \left|x\right\rangle\!\left\langle x\right| \otimes \sigma_x^A \otimes \sigma_x^B\big)$ and $\sigma^{X-B} \coloneqq \sum_x \left|x\right\rangle\!\left\langle x\right| \otimes \sigma_x^B$. For state $\tilde{\rho}^{XABC}$ introduced above, we can write this as shown at the top of the next page. Define the positive semi-definite operator $\kappa^{XA} \coloneqq \rho^{XA} - \tilde{\rho}^{XA}$ and Let $\bar{\rho}^{XAB} \coloneqq \tilde{\rho}^{XAB} + \kappa^{XA} \otimes \sigma^{X-B}$. It can be easily

$$
\begin{aligned}
&D_{\max}(\tilde{\rho}^{XAB}\|\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\sigma_x^B)\\
&\quad=\log\big\|\big(\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\sigma_x^B\big)^{-\frac{1}{2}}\tilde{\rho}^{XAB}\big(\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\sigma_x^B\big)^{-\frac{1}{2}}\big\|_\infty\\
&\quad=\log\big\|\big(\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\sigma_x^B\big)^{-\frac{1}{2}}\mathrm{Tr}_C\{\Pi^{BC}\rho^{XABC}\Pi^{BC}\}\big(\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\sigma_x^B\big)^{-\frac{1}{2}}\big\|_\infty\\
&\quad=\log\big\|(\sigma^{X-B})^{-\frac{1}{2}}\mathrm{Tr}_C\{(\rho^{XA})^{-\frac{1}{2}}\otimes\Pi^{BC}\rho^{XABC}(\rho^{XA})^{-\frac{1}{2}}\otimes\Pi^{BC}\}(\sigma^{X-B})^{-\frac{1}{2}}\big\|_\infty\\
&\quad=\log\big\|(\sigma^{X-B})^{-\frac{1}{2}}(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}\rho^{XAB}(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}(\sigma^{X-B})^{-\frac{1}{2}}\big\|_\infty\\
&\quad\le\log 2^{\gamma}\big\|(\sigma^{X-B})^{-\frac{1}{2}}(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}(\sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes\sigma_x^B)(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}(\sigma^{X-B})^{-\frac{1}{2}}\big\|_\infty\\
&\quad=\log 2^{\gamma}\big\|(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}\sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes(\sigma_x^B)^{-\frac{1}{2}}\sigma_x^B(\sigma_x^B)^{-\frac{1}{2}}(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}\big\|_\infty\\
&\quad=\log 2^{\gamma}\big\|(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}\sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes\mathbb{1}^B(\rho^{XA})^{-\frac{1}{2}}\Pi^{XA}\big\|_\infty\\
&\quad=\gamma+\log\big\|\Pi^{XA}\Gamma^{XA}\Pi^{XA}\big\|_\infty\\
&\quad\le D_{\max}\big(\rho^{XAB}\big\|\sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes\sigma_x^B\big)+\log\frac{1}{1-\sqrt{1-\varepsilon^2}}.
\end{aligned}
$$

checked that $\bar{\rho}^{XA}=\rho^{XA}$. Moreover, in the following we show that $P(\bar{\rho}^{XAB},\rho^{XAB})\le\varepsilon$:

$$
\begin{aligned}
F(\bar{\rho}^{XAB},\rho^{XAB})&\ge\big\|\sqrt{\tilde{\rho}^{XAB}}\sqrt{\rho^{XAB}}\big\|_1+1-\mathrm{Tr}\rho^{XAB}\\
&\ge\big\|\sqrt{\tilde{\rho}^{XABC}}\sqrt{\rho^{XABC}}\big\|_1+1-\mathrm{Tr}\rho^{XAB}\\
&=1-\mathrm{Tr}\Pi_\perp^{BC}\rho^{BC}\\
&\ge\sqrt{1-\varepsilon^2}.
\end{aligned}
$$

The first inequality follows from Lemma 4 and the fact that by construction $\tilde{\rho}^{XAB}\le\bar{\rho}^{XAB}$, therefore $\big\|\sqrt{\tilde{\rho}^{XAB}}\sqrt{\rho^{XAB}}\big\|_1\le\big\|\sqrt{\bar{\rho}^{XAB}}\sqrt{\rho^{XAB}}\big\|_1$. The second inequality follows from the fact that fidelity is monotonically non-decreasing with respect to CPTP maps. The equality stems from Lemma 4 and the last inequality is the assumption. And finally from the relation between the purified distance and the fidelity the desired inequality follows. We continue as shown at the top of the next page, where in the first inequality we have used $\bar{\rho}^{XAB}\le\tilde{\rho}^{XAB}+\rho^{XA}\otimes\sigma^B$ and in the final inequality we have used the fact that $2^{\gamma}\ge\mathrm{Tr}\rho^{XAB}=1$. Now similar to Remark 1, a pinching map is applied to the left hand-hand side to conclude from the monotonicity of the max-relative entropy that X system is classical. □

Proof of Lemma 10: From the result given in Lemma 19 onward, let ρ^{*XAB} be the optimizer for $D_{\max}^{\varepsilon}\big(\rho^{XAB}\big\|\sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes\sigma_x^B\big)$. We argued that this state will be classical on X. Then there exists a state $\bar{\rho}^{XAB}\in\mathcal{B}^{\varepsilon}(\rho^{*XAB})$ classical on X such that

$$
\begin{aligned}
&D_{\max}\big(\bar{\rho}^{XAB}\big\|\sum_x\bar{p}(x)\,|x\rangle\langle x|\otimes\bar{\rho}_x^A\otimes\sigma_B^x\big)\\
&\qquad\le D_{\max}\big(\rho^{*XAB}\big\|\sum_x q(x)\,|x\rangle\langle x|\otimes\sigma_x^A\otimes\sigma_x^B\big)\\
&\qquad\quad+\log\Big(\frac{1}{1-\sqrt{1-\varepsilon^2}}+1\Big).
\end{aligned}
$$

From the triangle inequality for the purified distance it is seen that $\bar{\rho}^{XAB}\in\mathcal{B}^{2\varepsilon}(\rho^{XAB})$. Choosing $q(x)=p(x),\sigma_x^A=\rho_x^A,\sigma_x^B=\rho_x^B$ for all x, finishes the job. □

To prove Lemma 11, we need to following lemma.

Lemma 20: Let ρ^{XAB} and σ^B be a quantum states. There exists a state $\rho'^{XAB}\in\mathcal{B}^{\varepsilon}(\rho)$ classical on X such that:

$$
\begin{aligned}
&D_{\max}(\rho^{XAB}\|\sum_x p'(x)\,|x\rangle\langle x|\otimes\rho_x'^A\otimes\sigma_x^B)\\
&\qquad\le D_{\max}(\rho^{XAB}\|\sum_x p(x)\,|x\rangle\langle x|\otimes\rho_x^A\otimes\sigma_x^B).
\end{aligned}
$$

Proof: Trivial. □

proof of Lemma 11: Let ρ^{*XAB} be the optimizer in the definition of the PSCMMI. By substituting it in Lemma 20, we will have:

$$
\begin{aligned}
&D_{\max}(\rho^{*XAB}\|\sum_x p'(x)\,|x\rangle\langle x|\otimes\rho_x'^A\otimes\sigma_x^B)\\
&\qquad\le D_{\max}(\rho^{*XAB}\|\sum_x p^*(x)\,|x\rangle\langle x|\otimes\rho_x^{*A}\otimes\sigma_x^B).
\end{aligned}
$$

Let $\rho'^{XA}=\rho^{XA}$ and $\sigma^B=\rho^B$. Then the result follows from the definition of the quantities. □

Proof of Lemma 13: Similar to Lemma 11 in [30], the proof follows by straightforward calculation as shown with the chain starting by Eq. (51).

□

Proof of Lemma 14: The proof is similar to the proof of its uncontional version [30]. For the convenience sake, we let $\sigma_x^{B_{-j}}:=\sigma_x^{B_1}\otimes...\sigma_x^{B_{j-1}}\otimes\sigma_x^{B_{j+1}}\otimes...\otimes\sigma_x^{B_n}$ and $\sigma_x^{B_{+j}}:=\sigma_x^{B_1}\otimes...\otimes\sigma_x^{B_n}$. By adopting this notation, we can see that $\tau^{XAB_1\ldots B_n}=\frac{1}{n}\sum_{j=1}^n\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB}\otimes\sigma_x^{B_{-j}}$. We use Lemma 13 to get equations (52) and (53).

From the invariance of the relative entropy with respect to tensor product states, the term inside the summation in (52) equals $D\big(\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB_j}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes$

$$
\begin{aligned}
&D_{\max}\big(\bar{\rho}^{XAB}\big\|\bar{\rho}^{XA}\otimes\sigma^{X-B}\big)=\log\big\|(\bar{\rho}^{XA})^{-\frac{1}{2}}\otimes(\sigma^{X-B})^{-\frac{1}{2}}\bar{\rho}^{XAB}(\bar{\rho}^{XA})^{-\frac{1}{2}}\otimes(\sigma^{X-B})^{-\frac{1}{2}}\big\|_\infty\\
&=\log\big\|(\rho^{XA})^{-\frac{1}{2}}\otimes(\sigma^{X-B})^{-\frac{1}{2}}\bar{\rho}^{XAB}(\rho^{XA})^{-\frac{1}{2}}\otimes(\sigma^{X-B})^{-\frac{1}{2}}\big\|_\infty\\
&\le\log\Big(\big\|(\rho^{XA})^{-\frac{1}{2}}\otimes(\sigma^{X-B})^{-\frac{1}{2}}\tilde{\rho}^{XAB}(\rho^{XA})^{-\frac{1}{2}}\otimes(\sigma^{X-B})^{-\frac{1}{2}}\big\|_\infty+1\Big)\\
&\le\log\bigg(2^{\gamma}\frac{1}{1-\sqrt{1-\varepsilon^2}}+1\bigg)\\
&\le D_{\max}\big(\rho^{XAB}\big\|\sum_x q(x)\,|x\rangle\!\langle x|\otimes\sigma_x^A\otimes\sigma_x^B\big)+\log\bigg(\frac{1}{1-\sqrt{1-\varepsilon^2}}+1\bigg),
\end{aligned}
$$

$$
\begin{aligned}
&\sum_i p(i)\left(D(\rho_i^{XA}||\theta^{XA})-D(\rho_i^{XA}||\rho^{XA})\right) \qquad (51)\\
&\quad=\sum_i p(i)\left(\mathrm{Tr}\{\rho_i^{XA}\log\rho_i^{XA}\}-\mathrm{tr}\{\rho_i^{XA}\log\theta^{XA}\}-\mathrm{Tr}\{\rho_i^{XA}\log\rho_i^{XA}\}+\mathrm{Tr}\{\rho_i^{XA}\log\rho^{XA}\}\right)\\
&\quad=\mathrm{Tr}\{\sum_i p(i)\rho_i^{XA}\log\rho^{XA}\}-\mathrm{Tr}\{\sum_i p(i)\rho_i^{XA}\log\theta^{XA}\}=\mathrm{Tr}\{\rho^{XA}\log\rho^{XA}\}-\mathrm{Tr}\{\rho^{XA}\log\theta^{XA}\}\\
&\quad=D(\rho^{XA}||\theta^{XA}).
\end{aligned}
$$

$$
\begin{aligned}
&D\big(\tau^{XAB_1\ldots B_n}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_{+j}}\big)\\
&\qquad=\frac{1}{n}\sum_j D\big(\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB_j}\otimes\sigma_x^{B_{-j}}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_{+j}}\big) \qquad (52)\\
&\qquad-\frac{1}{n}\sum_j D\big(\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB_j}\otimes\sigma_x^{B_{-j}}\big\|\tau^{XAB_1\ldots B_n}\big). \qquad (53)
\end{aligned}
$$

$\rho_x^A\otimes\sigma_x^{B_j}\big)$. Besides, from the monotonicity of the quantum relative entropy, by applying $\mathrm{Tr}_{B_1,\ldots B_{j-1},B_{j+1},\ldots,B_n}\{.\}$ to the term inside summation in (53), it is lower bounded by $D\big(\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^{AB_j}\big\|\tau^{XAB_j}\big)$ where $\tau^{XAB_j}:=\sum_x p(x)|x\rangle\langle x|^X\otimes\big(\frac{1}{n}\rho_x^{AB_j}+(1-\frac{1}{n})(\rho_x^A\otimes\sigma_x^{B_j})\big)$. Let k be such that $\rho^{XAB_j}\le 2^k\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_j}$. Therefore, we will have $\rho^{XAB_j}\le(1+\frac{2^k-1}{n})\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_j}$. Consider the chain at the top of the next page, where the inequality comes from the fact that if A and B are positive semidefinite operators and $A\le B$, then $\log A\le\log B$. Plugging the findings above into (52) and (53) yields:

$$
\begin{aligned}
&D\big(\tau^{XAB_1\ldots B_n}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_{+j}}\big)\\
&\le\frac{1}{n}\sum_j D\big(\rho^{XAB_j}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_j}\big)\\
&\qquad-\frac{1}{n}\sum_j D\big(\rho^{XAB_j}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_j}\big)\\
&\qquad+\log\bigg(1+\frac{2^k-1}{n}\bigg)\\
&\le\log\bigg(1+\frac{2^k}{n}\bigg).
\end{aligned}
$$

By choosing $n=\lceil\frac{2^k}{\delta^2}\rceil$, it follows that $D\big(\tau^{XAB_1\ldots B_n}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_{+j}}\big)\le\log\big(1+\delta^2\big)$. From Pinsker's inequality (2), we also can see that $F^2\big(\tau^{XAB_1\ldots B_n},\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_{+j}}\big)\ge\frac{1}{1+\delta^2}\ge 1-\delta^2$. From definition of the purified distance, it can be easily seen that $P\big(\tau^{XAB_1\ldots B_n},\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_{+j}}\big)\le\delta$. □

Proof of Corollary 1: Let $\tilde{\rho}^{XAB}$ be the optimal state achieving the minimum for k. Then from the conditional convex-split lemma we know that:

$$
P(\tilde{\tau}^{XAB_1\ldots B_n},\sum_x\tilde{p}(x)|x\rangle\langle x|^X\otimes\tilde{\rho}_x^A\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_n})\le\delta, \qquad (54)
$$

where

$$
\begin{aligned}
\tilde{\tau}^{XAB_1\ldots B_n}&:=\sum_x\tilde{p}(x)|x\rangle\langle x|^X\\
&\quad\otimes\big(\frac{1}{n}\sum_{j=1}^n\tilde{\rho}_x^{AB_j}\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_{j-1}}\otimes\sigma_x^{B_{j+1}}\otimes\sigma_x^{B_n}\big).
\end{aligned}
$$

From the concavity of the fidelity as well as its invariance with respect to tensor product states, the following can be seen:

$$
P(\tilde{\tau}^{XAB_1\ldots B_n},\tau^{XAB_1\ldots B_n})\le P(\tilde{\rho}^{XAB},\rho^{XAB})\le\varepsilon. \qquad (55)
$$

Analogously, we have Eq. (56). Then the desired result is

$$
\begin{aligned}
D\big(\rho^{XAB_j}\big\|\tau^{XAB_j}\big) &= \mathrm{Tr}\big\{\rho^{XAB_j}\log\rho^{XAB_j}\big\} - \mathrm{Tr}\big\{\rho^{XAB_j}\log\tau^{XAB_j}\big\} \\
&\geq \mathrm{Tr}\big\{\rho^{XAB_j}\log\rho^{XAB_j}\big\} - \mathrm{Tr}\big\{\rho^{XAB_j}\log\bigg(\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_j}\bigg)\big\} - \log\bigg(1+\frac{2^k-1}{n}\bigg) \\
&= D\big(\rho^{XAB_j}\big\|\sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_j}\big) - \log\bigg(1+\frac{2^k-1}{n}\bigg),
\end{aligned}
$$

$$
P\Big(\sum_x \tilde{p}(x)|x\rangle\langle x|^X\otimes\tilde{\rho}_x^A\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_n}, \sum_x p(x)|x\rangle\langle x|^X\otimes\rho_x^A\otimes\sigma_x^{B_1}\otimes\ldots\otimes\sigma_x^{B_n}\Big) \leq P(\tilde{\rho}^{XA},\rho^{XA}) \leq \epsilon. \tag{56}
$$

inferred by applying the triangle inequality to (54), (55) and (56). □

ACKNOWLEDGMENT

The first author would like to thank Andreas Winter for a lot of discussions related to this work. He is also grateful to Shun Watanabe for walking him through the classical result [7] and Marco Tomamichel for useful discussions regarding the entropic quantities appeared in this paper. The work of Farzin Salek and Javier R. Fonollosa is supported by the "Ministerio de Ciencia, Innovación y Universidades", of the Spanish Government, TEC2015-69648-REDC and TEC2016-75067-C4-2-R AEI/FEDER, UE, and the Catalan Government, 2017 SGR 578 AGAUR and 001-P-001644 QuantumCAT within the ERDF Program of Catalunya. Farzin Salek acknowledges partial financial support by the Baidu-UAB collaborative project 'Learning of Quantum Hidden Markov Models', the Spanish MINECO (project FIS2016-86681-P) with the support of FEDER funds, and the Generalitat de Catalunya (project 2017-SGR-1127).

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, May 1978.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[4] Y. Steinberg and S. Verdu, "Channel simulation and coding with side information," *IEEE Transactions on Information Theory*, vol. 40, pp. 634–646, May 1994.

[5] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2 ed., 2011.

[6] M. R. Bloch and J. Kliewer, "On secure communication with constrained randomization," in *2012 IEEE International Symposium on Information Theory Proceedings*, pp. 1172–1176, July 2012.

[7] S. Watanabe and Y. Oohama, "The optimal use of rate-limited randomness in broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 61, pp. 983–995, Feb 2015.

[8] Y. K. Chia and A. E. Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 58, pp. 2748–2765, May 2012.

[9] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318–336, Oct 2004.

[10] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, pp. 44–55, Jan 2005.

[11] I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Communications in Mathematical Physics*, vol. 256, pp. 287–303, Jun 2005.

[12] M. Hsieh and M. M. Wilde, "Trading classical communication, quantum communication, and entanglement in quantum shannon theory," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4705–4730, 2010.

[13] M. Hsieh and M. M. Wilde, "Entanglement-assisted communication of classical and quantum information," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4682–4704, 2010.

[14] E. Y. Zhu, Q. Zhuang, M.-H. Hsieh, and P. W. Shor, "Superadditivity in trade-off capacities of quantum channels," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3973–3989, 2019.

[15] E. Chitambar, M.-H. Hsieh, and A. Winter, "The private and public correlation cost of three random variables with collaboration," *IEEE Transactions on Information Theory*, vol. 62, pp. 2034–2043, April 2016.

[16] M. M. Wilde and M.-H. Hsieh, "Public and private resource trade-offs for a quantum channel," *Quantum Information Processing*, vol. 11, no. 6, pp. 1465–1501, 2012.

[17] M. M. Wilde and M.-H. Hsieh, "The quantum dynamic capacity formula of a quantum channel," *Quantum Information Processing*, vol. 11, no. 6, pp. 1431–1463, 2012.

[18] M.-H. Hsieh and M. Wilde, "Public and private communication with a quantum channel and a secret key," *Phys. Rev. A*, vol. 80, p. 022306, Aug 2009.

[19] M.-H. Hsieh, T. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A*, vol. 79, p. 032340, Mar 2009.

[20] M.-H. Hsieh, Z. Luo, and T. Brun, "Secret-key-assisted private classical communication capacity over quantum channels," *Phys. Rev. A*, vol. 78, p. 042306, Oct 2008.

[21] M.-H. Hsieh, I. Devetak, and A. Winter, "Entanglement-assisted capacity of quantum multiple-access channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 3078–3090, July 2008.

[22] M. Tomamichel, *Quantum information processing with finite resources : mathematical foundations*. SpringerBriefs in mathematical physics ; v. 5, 2016.

[23] R. Renner, S. Wolf, and J. Wullschleger, "The single-serving channel capacity," in *2006 IEEE International Symposium on Information Theory*, pp. 1424–1427, July 2006.

[24] M. Mosonyi and N. Datta, "Generalized relative entropies and the capacity of classical-quantum channels," *Journal of Mathematical Physics*, vol. 50, no. 7, p. 072104, 2009.

[25] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 49, pp. 1753–1768, July 2003.

[26] M. Hayashi, "Role of hypothesis testing in quantum information," 2017.

[27] L. Wang and R. Renner, "One-shot classical-quantum capacity and hypothesis testing," *Phys. Rev. Lett.*, vol. 108, p. 200501, May 2012.

[28] M. M. Wilde, "Position-based coding and convex splitting for private communication over quantum channels," *Quantum Information Processing*, vol. 16, p. 264, Sep 2017.

[29] A. Anshu, R. Jain, and N. A. Warsi, "Building blocks for communication over noisy quantum networks," *IEEE Transactions on Information Theory*, vol. 65, pp. 1287–1306, Feb 2019.

[30] A. Anshu, V. K. Devabathini, and R. Jain, "Quantum communication using coherent rejection sampling," *Phys. Rev. Lett.*, vol. 119, p. 120506, Sep 2017.

[31] J. Radhakrishnan, P. Sen, and N. A. Warsi, "One-Shot Private Classical Capacity of Quantum Wiretap Channel: Based on one-shot quantum covering lemma," *ArXiv e-prints*, p. arXiv:1703.01932, Mar. 2017.

[32] R. Ahlswede and A. Winter, "Strong converse for identification via quantum channels," *IEEE Transactions on Information Theory*, vol. 48, pp. 569–579, March 2002.

[33] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Transactions on Information Theory*, vol. 57, pp. 7377–7385, Nov 2011.

[34] F. Buscemi and N. Datta, "The quantum capacity of channels with arbitrarily correlated noise," *IEEE Transactions on Information Theory*, vol. 56, pp. 1447–1460, March 2010.

[35] F. Salek, A. Anshu, M. Hsieh, R. Jain, and J. R. Fonollosa, "One-shot capacity bounds on the simultaneous transmission of public and private information over quantum channels," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 296–300, June 2018.

[36] F. Salek, A. Anshu, M. Hsieh, R. Jain, and J. R. Fonollosa, "One-shot capacity bounds on the simultaneous transmission of classical and quantum information," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2141–2164, 2020.

[37] N. Datta and M.-H. Hsieh, "One-shot entanglement-assisted quantum and classical communication," *IEEE Transactions on Information Theory*, vol. 59, pp. 1929–1939, March 2013.

[38] N. Datta, M. Mosonyi, M.-H. Hsieh, and F. G. Brandao, "A smooth entropy approach to quantum hypothesis testing and the classical capacity of quantum channels," *IEEE Transactions on Information Theory*, vol. 59, pp. 8014–8026, Dec 2013.

[39] N. Datta and M.-H. Hsieh, "The apex of the family tree of protocols: optimal rates and resource inequalities," *New Journal of Physics*, vol. 13, no. 9, p. 093042, 2011.

[40] N. Datta, M.-H. Hsieh, and J. Oppenheim, "An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution," *Journal of Mathematical Physics*, vol. 57, no. 5, 2016.

[41] I. Savov and M. M. Wilde, "Classical codes for quantum broadcast channels," *IEEE Transactions on Information Theory*, vol. 61, pp. 7017–7028, Dec 2015.

[42] J. Radhakrishnan, P. Sen, and N. Warsi, "One-shot marton inner bound for classical-quantum broadcast channel," *IEEE Transactions on Information Theory*, vol. 62, pp. 2836–2848, May 2016.

[43] C. Hirche and C. Morgan, "An improved rate region for the classical-quantum broadcast channel," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2782–2786, June 2015.

[44] A. Anshu, M. Hayashi, and N. A. Warsi, "Secure communication over fully quantum Gel'fand-Pinsker wiretap channel," *arXiv e-prints*, p. arXiv:1801.00940, Jan. 2018.

[45] P. Sen, "Inner bounds via simultaneous decoding in quantum network information theory," *arXiv e-prints*, p. arXiv:1806.07276, Jun 2018.

[46] J. Yard, P. Hayden, and I. Devetak, "Quantum broadcast channels," *IEEE Transactions on Information Theory*, vol. 57, pp. 7147–7162, Oct 2011.

[47] M. M. Wilde, *Quantum Information Theory*. New York, NY, USA: Cambridge University Press, 1st ed., 2013.

[48] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *Journal of Mathematical Physics*, vol. 54, pp. 122203–122203, Dec. 2013.

[49] M. Tomamichel, R. Colbeck, and R. Renner, "Duality between smooth min- and max-entropies," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4674–4681, 2010.

[50] M. Tomamichel, *A framework for non-asymptotic quantum information theory*. PhD thesis, ETH Zurich, 2012. Diss., EidgenÃ¶ssische Technische Hochschule ETH ZÃŒrich, Nr. 20213.

[51] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, pp. 5524–5535, Aug 2011.

[52] T. Ogawa and H. Nagaoka, "Strong converse and stein's lemma in quantum hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, pp. 2428–2433, Nov 2000.

[53] F. Hiai and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Comm. Math. Phys.*, vol. 143, no. 1, pp. 99–114, 1991.

[54] N. Datta, "Min- and max-relative entropies and a new entanglement monotone," *IEEE Transactions on Information Theory*, vol. 55, pp. 2816–2826, June 2009.

[55] M. Tomamichel and M. Hayashi, "A hierarchy of information quantities for finite block length analysis of quantum tasks," *IEEE Transactions on Information Theory*, vol. 59, pp. 7693–7710, Nov 2013.

[56] F. Dupuis, L. Kraemer, P. Faist, J. M. Renes, and R. Renner, "Generalized Entropies," *arXiv e-prints*, p. arXiv:1211.3141, Nov 2012.

[57] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Transactions on Information Theory*, vol. 45, pp. 2481–2485, Nov 1999.

[58] H. Qi, Q. Wang, and M. M. Wilde, "Applications of position-based coding to classical communication over quantum channels," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, no. 44, p. 444002, 2018.

[59] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[60] N. Ciganović, N. J. Beaudry, and R. Renner, "Smooth max-information as one-shot generalization for mutual information," *IEEE Transactions on Information Theory*, vol. 60, pp. 1573–1581, March 2014.