Quantum Channel State Masking

Uzi Pereg, *Member, IEEE*, Christian Deppe, *Member, IEEE*, and Holger Boche, *Fellow, IEEE*

***Abstract*—Communication over a quantum channel that depends on a quantum state is considered when the encoder has channel side information (CSI) and is required to mask information on the quantum channel state from the decoder. A full characterization is established for the entanglement-assisted masking equivocation region with a maximally correlated channel state, and a regularized formula is given for the quantum capacity-leakage function without assistance. For Hadamard channels without assistance, we derive single-letter inner and outer bounds, which coincide in the standard case of a channel that does not depend on a state.**

***Index Terms*—Quantum information, Shannon theory, quantum communication, channel capacity, state masking, entanglement assistance, state information.**

I. Introduction

SECURITY and privacy are critical aspects in modern communication systems [1]–[4]. The classical wiretap channel was first introduced by Wyner [5], [6] to model communication in the presence of a passive eavesdropper, and further studied in various scenarios, as in [7]–[15]. On the other hand, Merhav and Shamai [16] introduced a different communication system with the privacy requirement of masking. In this setting, the sender transmits a sequence X^n over a memoryless state-dependent channel $p_{Y|X,S}$, where the state sequence S^n has a fixed memoryless distribution and is not affected by the transmission. The transmitter of X^n is informed of S^n and is required to send information to the receiver while limiting the amount of information that the receiver can learn about S^n. It was shown in [16] that the achievable masking equivocation region consists of rate-leakage pairs (R, L) such that

$$R \leq I(U;Y) - I(U;S) \tag{1}$$

$$L \geq I(S;U,Y) \tag{2}$$

for $(S, U, X, Y) \sim p_S \times p_{U|S} \times p_{X|U,S} \times p_{Y|X,S}$, where U is an auxiliary random variable, with cardinality $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{S}|$. Related settings and extensions are also considered in [17]–[24].

The field of quantum information is rapidly evolving in both practice and theory [25]–[32]. As technology approaches the atomic scale, we seem to be on the verge of the "Quantum Age" [33], [34]. Dynamics can be modeled by a noisy quantum channel, describing physical evolutions, density transformation, discarding of sub-systems, quantum measurements, etc. [35] [36, Section 4.6]. Quantum information theory is the natural extension of classical information theory. Nevertheless, this generalization reveals astonishing phenomena with no parallel in classical communication [37]. For example, two memoryless quantum channels, each with zero quantum capacity, can have a nonzero quantum capacity when used together [38]. This property is known as super-activation.

Communication through quantum channels can be separated into different categories. For classical communication, the Holevo-Schumacher-Westmoreland (HSW) Theorem provides a regularized ("multi-letter") formula for the capacity of a quantum channel without assistance [39], [40]. Although calculation of such a formula is intractable in general, it provides computable lower bounds, and there are special cases where the capacity can be computed exactly. The reason for this difficulty is that the Holevo information is not necessarily additive [41]. A similar difficulty occurs with transmission of quantum information. A regularized formula for the quantum capacity is given in [42]–[45], in terms of the coherent information. A computable formula is obtained in the special case where the channel is degradable or less noisy [46].

Another scenario of interest is when Alice and Bob are provided with entanglement resources [47], [48]. While entanglement can be used to produce shared randomness, it is a much more powerful aid [36], [49]. In particular, superdense coding [50] is a well known communication protocol where two classical bits are transmitted using a single use of a noiseless qubit channel and a maximally entangled pair. Thereby, entanglement assistance doubles the transmission rate

Manuscript received June 7, 2020; revised November 8, 2020; accepted December 23, 2020. Date of publication January 11, 2021; date of current version March 18, 2021. The work of Uzi Pereg was supported in part by the Bundesministerium für Bildung und Forschung (BMBF) under Grant 16KIS0856 and in part by the Viterbi Scholarship of the Technion. The work of Christian Deppe was supported by the Bundesministerium für Bildung und Forschung (BMBF) under Grant 16KIS0856. The work of Holger Boche was supported in part by the Bundesministerium für Bildung und Forschung (BMBF) under Grant 16KIS0858, in part by the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Post Shannon Communication (NewCom)" under Grant 16KIS1003K, in part by the German Research Foundation (DFG) within the Gottfried Wilhelm Leibniz Prize under Grant BO 1734/20-1, and in part by the German Research Foundation (DFG) within the Germany's Excellence Strategy under Grant EXC-2092 - 390781972 and Grant EXC-2111 - 390814868. This article was presented in part at the 2020 Munich Conference on Quantum Science and Technology (MCQST), in part at the 2020 IEEE Information Theory Workshop (ITW), and in part at the 24th Annual Conference on Quantum Information Processing (QIP 2021). *(Corresponding author: Uzi Pereg.)*

Uzi Pereg and Christian Deppe are with the Institute for Communications Engineering, Technische Universität München, 80333 Munich, Germany (e-mail: uzi.pereg@tum.de; christian.deppe@tum.de).

Holger Boche is with the Institute of Theoretical Information Technology, Technische Universität München, 80290 Munich, Germany, also with the Munich Center for Quantum Science and Technology (MCQST), 80799 Munich, Germany, and also with the CASA—Cyber Security in the Age of Large-Scale Adversaries–Excellenzcluster, Ruhr-Universität Bochum, 44801 Bochum, Germany (e-mail: boche@tum.de).

Communicated by M. M. Wilde, Associate Editor for Quantum Information Theory.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2021.3050529.

Digital Object Identifier 10.1109/TIT.2021.3050529

of classical messages over a noiseless qubit channel. The entanglement-assisted capacity of a noisy quantum channel was fully characterized by Bennett *et al.* [51], [52] in terms of the quantum mutual information. Entanglement resources are thus instrumental for the performance analysis of quantum communication systems, as the characterization with entanglement assistance provides a computable upper bound for unassisted communication as well. In the other direction, i.e. using information measures to understand quantum physics, the quantum mutual information plays a role in investigating the entanglement structure of quantum field theories [53]–[56].

The entanglement-assisted capacity theorem can be viewed as the quantum generalization of Shannon's classical capacity theorem [57] (see page 2640 in [52]). Nonetheless, there are communication settings where entanglement can increase the capacity of a *classical* channel, such as the zero-error capacity problem [58] and the multiple access channel with entangled encoders [59]. Entanglement assistance also has striking effects in communication games and their security applications [59]–[64]. Furthermore, entanglement can assist the transmission of quantum information. By employing the teleportation protocol [65], qubits can be sent at half the rate of classical bits given entanglement resources. Thus, for a given quantum channel, the entanglement-assisted quantum capacity has half the value of the entanglement-assisted classical capacity in units of qubits per channel use.

From a practical standpoint, it is also important to determine the amount of entanglement supply that is consumed in the process of sending information. The tradeoff between communication and resource rates is considered in [66]–[71]. Furthermore, the study of such tradeoffs led to the development of general "father" and "mother" protocols [72]–[76], which produce achievability schemes for various settings including those mentioned above. Many of those protocols can be presented as a consequence of the decoupling theorem [77]–[79]. Roughly speaking, the decoupling approach shows that quantum information can be reliably communicated when Bob's environment is decoupled from Alice's purifying reference system. Further work on entanglement-assisted communication can be found in [80]–[89] and references therein.

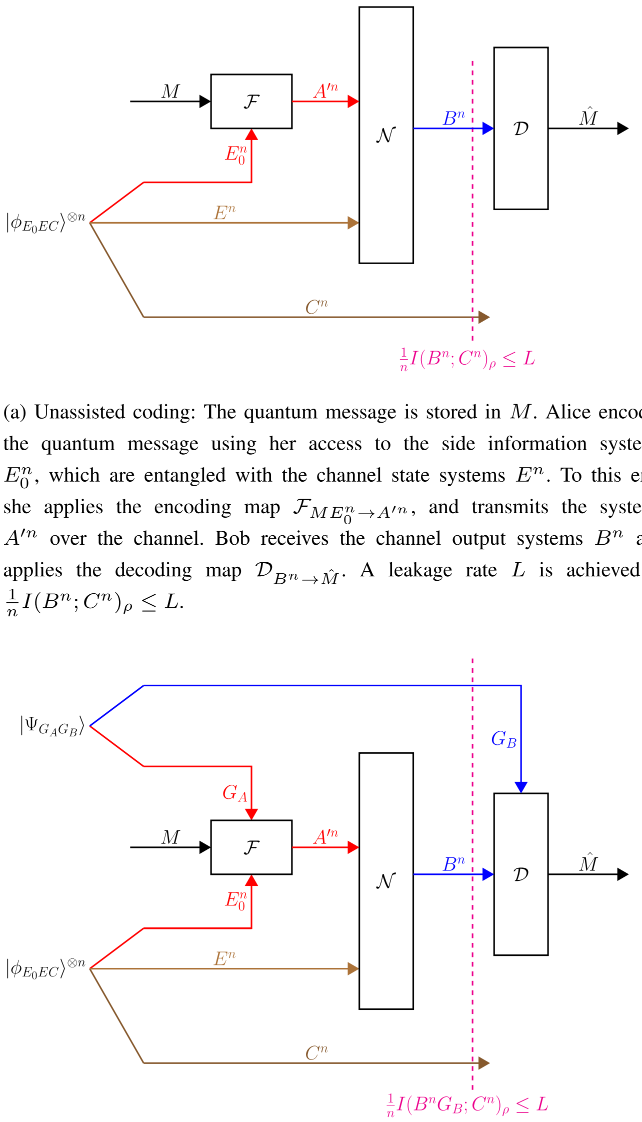
Boche, Cai, and Nötzel [90] addressed the classical-quantum channel with channel state information (CSI) at the encoder. The capacity was determined given causal CSI, and a regularized formula was provided given non-causal CSI [90] (see also [91], [92]). Warsi and Coon [93] used an information-spectrum approach to derive multi-letter bounds for a similar setting, where the side information has a limited rate. The entanglement-assisted capacity of a quantum channel with non-causal CSI was determined by Dupuis in [78], [94], and with causal CSI in [95], [96]. One-shot communication with CSI is considered in [89] as well. Luo and Devetak [97] considered channel simulation with source side information (SSI) at the decoder, and also solved the quantum generalization of the Wyner-Ziv problem [98]. Quantum data compression with SSI is also studied in [99]–[105]. Compression with SSI given entanglement assistance was recently considered by Khanian and Winter [106]–[108].

Considering secure communication over the quantum wiretap channel, Devetak [45] and Cai *et al.* [109] established a regularized characterization of the secrecy capacity without assistance. Connections to the coherent information of a quantum point to point channel were drawn in [110]. Related models appear in [111]–[116] as well. The entanglement-assisted secrecy capacity was determined by Qi *et al.* [117] (see also [68], [118]). Boche *et al.* [14], [119] studied the quantum wiretap channel with an active jammer. Furthermore, the capacity-equivocation region was established, characterizing the tradeoff between secret key consumption and private classical communication [111], [113] (see also [120] [36, Section 23.5.3]). In [45], Devetak considered entanglement generation using a secret-key-assisted quantum channel. The quantum Gel'fand-Pinsker wiretap channel is considered in [116] and other related scenarios can be found in [121]–[123]. The quantum broadcast and multiple access channels with confidential messages were recently considered in [124], [125] and [126], [127], respectively.

In this paper, we consider a quantum state-dependent channel $\mathcal{N}_{EA'\to B}$, when the encoder has CSI and is required to mask information on the quantum channel state from the decoder. Specifically, Alice maps the state of the quantum message system M and the CSI systems E_0^n to the state of the channel input systems A'^n in such a manner that limits the leakage-rate of Bob's information on C^n from B^n, where the systems E_0^n and C^n are entangled with the channel state systems E^n (see Figure 1a). Another significant distinction from the classical case is that the leakage requirement involves Bob's share of the entanglement resources, since the decoder has access to both the output systems and his part of the entangled pairs (see Figure 1b). In the classical setting, shared randomness does not need to be included in the leakage constraint as it cannot help the decoder. On the other hand, we know that Bob can extract quantum information by performing measurements on his entanglement resources, using the teleportation protocol for example.

We note that in the quantum information literature, the term 'masking' is sometimes used in a different context of an invertible process that distributes a quantum state to two receivers such that each receiver cannot gain information on the original quantum state [128]–[130]. In particular, it was shown in [128] that a universal unitary masker that satisfies this property *for every* input state does not exist. Our setting is fundamentally different as we consider a system with a fixed quantum state $|\phi_{EE_0\ C}\rangle^{\otimes n}$ that is known to all parties and controls a communication channel with a single output.

Analogously to the classical model, we consider channel state systems C^n that store undesired quantum information which leaks to the receiver [16]. This could model a leakage in the system of secret information, or could stand for another transmission to another receiver (Charlie), with a product state, out of our control, and which is not intended to our receiver (Bob), and is therefore to be concealed from him. Thus, the goal of the transmitter (Alice) now is to try and mask this undesired information as much as possible on the one hand, and to transmit reliable independent information rate on the other. The systems E_0^n can be thought of as part of



(a) Unassisted coding: The quantum message is stored in M. Alice encodes the quantum message using her access to the side information systems E_0^n, which are entangled with the channel state systems E^n. To this end, she applies the encoding map $\mathcal{F}_{ME_0^n \to A'^n}$, and transmits the systems A'^n over the channel. Bob receives the channel output systems B^n and applies the decoding map $\mathcal{D}_{B^n \to \hat{M}}$. A leakage rate L is achieved if $\frac{1}{n}I(B^n;C^n)_\rho \leq L$.

(b) Entanglement-assisted coding: The quantum message is stored in M, while Alice and Bob's entanglement resources are in the quantum systems G_A and G_B, respectively. Alice encodes the quantum message using G_A along with her access to the side information systems E_0^n, which are entangled with the channel state systems E^n. To this end, she applies the encoding map $\mathcal{F}_{MG_AE_0^n \to A'^n}$, and transmits the systems A'^n over the channel. Bob receives the channel output systems B^n and applies the decoding map $\mathcal{D}_{B^nG_B \to \hat{M}}$ to B^n and G_B. A leakage rate L is achieved if $\frac{1}{n}I(B^nG_B;C^n)_\rho \leq L$.

Fig. 1. Coding for a quantum state-dependent channel $\mathcal{N}_{EA' \to B}$ given state information at the encoder and masking from the decoder, with and without entanglement assistance. The quantum systems of Alice and Bob are marked in red and blue, respectively. The channel state systems E^n and C^n are marked in brown.

the environment of both our transmitter and the transmitter of C^n, possibly entangled if those transmitters had previous interaction, while E^n belong to the channel's environment. Dupuis' interpretation [94] for the entanglement between E_0^n and E^n is that Alice shares entanglement with the channel itself.

A full characterization is established for the entanglement-assisted masking equivocation region with maximally correlated channel state systems, and a regularized formula is given for the quantum masking region without assistance. We also derive a single-letter outer bound on the unassisted masking region for Hadamard channels, and verify that the inner and outer bounds coincide in the standard case of a channel that does not depend on its state. To prove the direct part, we first determine an achievable masking region with rate-limited entanglement. Here, we are most interested in the asymptotic characterization of achievable communication rates. On the other hand, in previous work, the decoupling approach typically produces such characterizations as a consequence of results for the one-shot setting, where the blocklength is $n = 1$ [77]–[79]. Therefore, we derive an asymptotic version of the decoupling theorem that can be applied directly, without considering the one-shot counterpart. While the derivation follows from the one-shot decoupling theorem using familiar arguments, it provides an analytic tool that is easier to combine with classical techniques, without a one-shot proxy. Here, the decoupling approach is used such that both Bob's environment and the channel state systems E^n and C^n are decoupled from Alice's purifying reference system. In order to establish the masking requirement, we approximate the leakage rate using the decoupled state that results from the decoupling theorem. The approximation relies on the Alicki-Fannes-Winter inequality [131], [132], as the decoupled state is close to the actual output state and its leakage rate has a simpler bound. This demonstrates how the decoupling approach is suitable to our needs. Further explanation on the decoupling nature of our problem is given in Section V.

Our result with entanglement assistance requires the assumption that the channel state systems E, E_0, and C are maximally correlated. Analytically, the presence of three channel state systems poses a difficulty that does not exist in the classical setting of Merhav and Shamai [16], and this is where the maximal correlation assumption comes into play. We note that the maximal correlation assumption holds in the special case of a classical channel state, yet our setting is more general. The converse proof without assistance is based on different considerations from those in the classical converse proof by Merhav and Shamai [16]. In the classical proof, the derivation of the bounds on both the communication and leakage rates begins with Fano's inequality, followed by arguments that do not hold in our model since conditional quantum entropies can be negative. Hence, we bound the leakage rate in a different manner using the coherent information bound on the communication rate.

II. Definitions and Related Work

A. Notation, States, and Information Measures

We use the following notation conventions. Calligraphic letters $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots$ are used for finite sets. Lowercase letters $x, y, z, \ldots$ represent constants and values of classical random variables, and uppercase letters $X, Y, Z, \ldots$ represent classical random variables. The distribution of a random variable X is specified by a probability mass function (pmf) $p_X(x)$ over a finite set $\mathcal{X}$. We use $x^j = (x_1, x_2, \dots, x_j)$ to denote a sequence of letters from $\mathcal{X}$. A random sequence X^n and its distribution $p_{X^n}(x^n)$ are defined accordingly.

The state of a quantum system A is given by a density operator ρ on the Hilbert space $\mathcal{H}_A$. A density operator is an Hermitian, positive semidefinite operator, with unit trace, *i.e.* $\rho^\dagger = \rho$, $\rho \succeq 0$, and $\mathrm{Tr}(\rho) = 1$. The state is said to be pure if $\rho = |\psi\rangle\langle\psi|$, for some vector $|\psi\rangle \in \mathcal{H}_A$, where $\langle\psi|$ is the Hermitian conjugate of $|\psi\rangle$. In general, a density operator has a spectral decomposition of the following form,

$$\rho = \sum_{z \in \mathcal{Z}} p_Z(z) |\psi_z\rangle\langle\psi_z| \tag{3}$$

where $\mathcal{Z} = \{1, 2, \dots, |\mathcal{H}_A|\}$, $p_Z(z)$ is a probability distribution over $\mathcal{Z}$, and $\{|\psi_z\rangle\}_{z\in\mathcal{Z}}$ forms an orthonormal basis of the Hilbert space $\mathcal{H}_A$. The density operator can thus be thought of as an average of pure states. A measurement of a quantum system is any set of operators $\{\Lambda_j\}$ that forms a positive operator-valued measure (POVM), *i.e.* the operators are positive semi-definite and $\sum_j \Lambda_j = \mathbb{1}$, where $\mathbb{1}$ is the identity operator (see [36, Definition 4.2.1]). According to the Born rule, if the system is in state ρ, then the probability of the measurement outcome j is given by $p_A(j) = \mathrm{Tr}(\Lambda_j \rho)$. The trace distance between two density operators ρ and σ is $\|\rho - \sigma\|_1$ where $\|F\|_1 = \mathrm{Tr}(\sqrt{F^\dagger F})$.

Define the quantum entropy of the density operator ρ as

$$H(\rho) \triangleq -\mathrm{Tr}[\rho \log(\rho)] \tag{4}$$

which is the same as the Shannon entropy associated with the eigenvalues of ρ. We may also consider the state of a pair of systems A and B on the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of the corresponding Hilbert spaces. Given a bipartite state σ_{AB}, define the quantum mutual information as

$$I(A;B)_\sigma = H(\sigma_A) + H(\sigma_B) - H(\sigma_{AB}). \tag{5}$$

Furthermore, conditional quantum entropy and mutual information are defined by $H(A|B)_\sigma = H(\sigma_{AB}) - H(\sigma_B)$ and $I(A;B|C)_\sigma = H(A|C)_\sigma + H(B|C)_\sigma - H(A,B|C)_\sigma$, respectively. The coherent information is then defined as

$$I(A\rangle B)_\sigma = -H(A|B)_\sigma \tag{6}$$

and $I(A\rangle B|C)_\sigma = I(A\rangle BC)_\sigma = -H(A|BC)_\sigma$ accordingly.

A pure bipartite state is called *entangled* if it cannot be expressed as the tensor product of two states in $\mathcal{H}_A$ and $\mathcal{H}_B$. The maximally entangled state between two systems of dimension D is defined by $|\Phi_{AB}\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |j\rangle_A \otimes |j\rangle_B$, where $\{|j\rangle_A\}_{j=0}^{D-1}$ and $\{|j\rangle_B\}_{j=0}^{D-1}$ are respective orthonormal bases. Note that $I(A;B)_{|\Phi\rangle\langle\Phi|} = 2 \cdot \log(D)$ and $I(A\rangle B)_{|\Phi\rangle\langle\Phi|} = \log(D)$.

B. Quantum Channel

A quantum channel maps a quantum state at the sender system to a quantum state at the receiver system. Here, we consider a channel with two inputs, where one of the inputs, which is referred to as the channel state, is not controlled by the encoder. Formally, a quantum state-dependent channel $(\mathcal{N}_{EA'\to B}, |\phi_{EE_0 C}\rangle)$ is defined by a linear, completely positive, trace preserving map $\mathcal{N}_{EA'\to B}$ and a quantum state $|\phi_{EE_0 C}\rangle$. This model can be interpreted as if the channel is entangled with the systems E, E_0, and C. A quantum channel has a Kraus representation

$$\mathcal{N}_{EA'\to B}(\rho_{EA'}) = \sum_j N_j \rho_{EA'} N_j^\dagger \tag{7}$$

for all $\rho_{EA'}$, and for some set of operators N_j such that $\sum_j N_j^\dagger N_j = \mathbb{1}$. Every quantum channel $\mathcal{N}_{EA'\to B}$ has an isometric extension $\mathcal{U}^{\mathcal{N}}_{EA'\to BK}$, also called a Stinespring dilation, such that

$$\mathcal{U}^{\mathcal{N}}_{EA'\to BK}(\rho_{EA'}) = U \rho_{EA'} U^\dagger \tag{8}$$

$$\mathcal{N}_{EA'\to B}(\rho_{EA'}) = \mathrm{Tr}_K(U \rho_{EA'} U^\dagger) \tag{9}$$

where the operator U is an isometry, *i.e.* $U^\dagger U = \mathbb{1}$ [133, Section VII]. The system K is often associated with the decoder's environment, or with a malicious eavesdropper in the wiretap channel model [45], and the channel $\widehat{\mathcal{N}}_{EA'\to K}(\rho_{EA'}) = \mathrm{Tr}_B(U \rho_{EA'} U^\dagger)$ is called the complementary channel for $\mathcal{N}_{EA'\to B}$.

We assume that both the channel state systems and the quantum channel have a product form. That is, the joint state of the systems $E^n = (E_1, \dots, E_n)$, $E_0^n = (E_{0,1}, \dots, E_{0,n})$ and $C^n = (C_1, \dots, C_n)$ is $|\phi_{EE_0 C}\rangle^{\otimes n}$, and if the systems $A'^n = (A'_1, \dots, A'_n)$ are sent through n channel uses, then the input state $\rho_{E^n A'^n}$ undergoes the tensor product mapping $\mathcal{N}_{E^n A'^n \to B^n} \equiv \mathcal{N}^{\otimes n}_{EA'\to B}$. Given CSI, the transmitter has access to the systems E_0^n, which are entangled with the channel state systems E^n. We will further consider a secrecy requirement that limits the information that the receiver can obtain on C^n. The sender and the receiver are often referred to as Alice and Bob.

Remark 1: Our results apply to the case where E, E_0, and C are in a mixed state as well. Specifically, given a mixed state $\varphi_{EE_0 C}$, there exists a purification $|\phi_{TEE_0 C}\rangle$, such that the reduced density operator for this purification is $\varphi_{EE_0 C}$. Hence, we can redefine the channel as follows. First, replace the channel state system E by $\tilde{E} = (T, E)$, and then consider the quantum state-dependent channel $\widetilde{\mathcal{N}}_{\tilde{E}A'\to B}$, where

$$\widetilde{\mathcal{N}}_{TEA'\to B}(\rho_{TEA'}) = \mathcal{N}_{EA'\to B}(\mathrm{Tr}_T(\rho_{TEA'})). \tag{10}$$

C. Less Noisy, Degradable, and Hadamard Channels

In the unassisted setting, we will also be interested in the following special cases.

1) Less Noisy Output: First, we define the class of state-dependent channels with a less noisy output.

Definition 1: A quantum state-dependent channel $(\mathcal{N}_{EA'\to B}, |\phi_{EE_0 C}\rangle)$ is said to have a less noisy output if there exists an isometric extension $\mathcal{U}^{\mathcal{N}}_{EA'\to BK}$ such that for every $\rho_{AA'EC}$ with $\rho_{EC} = \phi_{EC}$,

$$H(A|B)_\rho \le H(A|KC)_\rho \tag{11}$$

where $\rho_{ABKC} = \mathcal{U}^{\mathcal{N}}_{EA'\to BK}(\rho_{AEA'C})$.

The definition for a channel with a less noisy output can be equivalently stated as

$$I(A;B)_\rho \ge I(A;KC)_\rho \tag{12}$$

or

$$I(A\rangle B)_\rho \geq I(A\rangle K|C)_\rho \tag{13}$$

for all $\rho_{AA'EC}$ with $\rho_{EC} = \phi_{EC}$. Intuitively, the channel output is less noisy than its environment. Specifically, if we could use $\mathcal{U}^{\mathcal{N}}_{EA'\to BK}$ as a broadcast channel, with Receiver B and Receiver K, then (13) would imply that quantum information can be reliably sent to Receiver B at a higher rate than it can be sent to Receiver K, even if Receiver K has complete knowledge of C^n, i.e. Receiver K has C^n as CSI. For a quantum channel $\mathcal{P}_{A'\to B}$ that does have a state, the definition above coincides with the standard definition of a less noisy broadcast channel [134, Section II.C].

A stronger requirement is that of a degradable channel [46], [134].

Definition 2: A quantum state-dependent channel $(\mathcal{N}_{EA'\to B}, |\phi_{EE_0C}\rangle)$ is said to be degradable if there exists an isometric extension $\mathcal{U}^{\mathcal{N}}_{EA'\to BC_1\ K}$ such that the complementary channel $\widehat{\mathcal{N}}_{EA'\to C_1\ K}$ is a concatenation of the main channel $\mathcal{N}_{EA'\to B}$ and a degrading channel $\mathcal{D}_{B\to C_1K}$, i.e.

$$\widehat{\mathcal{N}}_{EA'\to C_1\ K} = \mathcal{D}_{B\to C_1K} \circ \mathcal{N}_{EA'\to B} \tag{14}$$

and for every $\rho_{AA'EC}$ with $\rho_{EC} = \phi_{EC}$,

$$\rho_{ABKC_1} = \rho_{ABKC} \tag{15}$$

where $\rho_{ABC_1\ KC} \equiv \mathcal{U}^{\mathcal{N}}_{EA'\to BC_1\ K}(\rho_{AEA'C})$.

Based on the data processing theorem, the conditions of the definition above imply that $I(A;B)_\rho \geq I(A;KC_1)_\rho = I(A;KC)_\rho$. Thereby, if a channel is degradable, then it has a less noisy output. Similarly, the intuition is that the state of the decoder's environment is a noisy version of the channel output state.

2) Hadamard Channels: Next, we consider the special case of Hadamard channels, which are defined as channels with an entanglement-breaking complementary [135]. Here, we will use the following definition. Consider an isometric channel

$$\mathcal{V}_{EA'\to C_1KB}(\rho_{EA'}) = V\rho_{EA'}V^\dagger \tag{16}$$

with

$$V \equiv \sum_{x\in\mathcal{X}} |\eta^x_{C_1K}\rangle\langle\zeta^x_{EA'}| \otimes |\psi^x_B\rangle \tag{17}$$

for some pure states $|\eta^x_{C_1\ K}\rangle$, $|\zeta^x_{EA'}\rangle$, and $|\psi^x_B\rangle$, such that $\sum_x |\zeta^x_{EA'}\rangle\langle\zeta^x_{EA'}| = \mathbb{1}_{EA'}$, where $\{|\psi^x_B\rangle\}_{x\in\mathcal{X}}$ is an orthonormal basis for the output Hilbert space $\mathcal{H}_B$. Given a state $\rho_{AA'EC}$ at the input, the output state is then

$$\rho_{AC_1KBC} = \mathcal{V}_{EA'\to C_1KB}(\rho_{AEA'C}). \tag{18}$$

The definition of a Hadamard channel is given below.

Definition 3: A Hadamard state-dependent channel $(\mathcal{N}^H_{EA'\to B}, |\phi_{EE_0\ C}\rangle)$ is a channel of the form

$$\mathcal{N}^H_{EA'\to B}(\rho_{EA'}) = \mathrm{Tr}_{C_1K}\left(V(\rho_{EA'})V^\dagger\right) \tag{19}$$

with the isometry V as in (17), and such that for every input state $\rho_{AA'EC}$ with $\rho_{EC} = \phi_{EC}$, the output state satisfies

$$\rho_{AKBC_1} = \rho_{AKBC} \tag{20}$$

where $\rho_{AC_1\ KBC} = V\rho_{AEA'C}V^\dagger$.

It can be shown that the definition of a Hadamard channel above coincides with the definition of a channel whose complementary is entanglement breaking (see detailed proof in [136, Section II.C.2]).

Observe that the complementary channel $\widehat{\mathcal{N}}^H_{EA'\to C_1\ K}$ can be simulated as follows. First, Bob performs a projective measurement on the channel output B in the basis $\{|\psi^x_B\rangle\}_{x\in\mathcal{X}}$. Then, given the measurement outcome x^*, the state $|\eta^{x^*}_{C_1\ K}\rangle$ is prepared. It follows that a Hadamard channel is degradable, and thus has a less noisy output.

D. Coding

We define a secrecy code to transmit quantum information given entanglement resources. We denote Alice and Bob's entangled systems by G_A and G_B, respectively. With non-causal CSI, Alice has acess to the systems E_0^n, which are entangled with the channel state sequence E^n.

Definition 4: A $(2^{nQ}, 2^{nR_e}, n)$ quantum masking code with rate-limited entanglement assistance and CSI at the encoder consists of the following: A quantum message state ρ_{MT}, where M is a system of dimension $|\mathcal{H}_M| = 2^{nQ}$ and T is a reference system, a pure entangled state Ψ_{G_A,G_B}, where $|\mathcal{H}_{G_A}| = |\mathcal{H}_{G_B}| = 2^{nR_e}$, an encoding channel $\mathcal{F}_{MG_AE_0^n\to A'^n}$, and a decoding channel $\mathcal{D}_{B^nG_B\to\hat{M}}$. We denote the code by $(\mathcal{F}, \Psi, \mathcal{D})$.

The communication scheme is depicted in Figure 1b. The sender Alice has the systems M, G_A, E_0^n, and A'^n, and the receiver Bob has the systems B^n, G_B, and $\hat{M}$. Alice encodes the quantum state of the message system M using her share of the entangled resources G_A and her access to the systems E_0^n which are entangled with the channel state systems. To this end, she applies the encoding map $\mathcal{F}_{MG_AE_0^n\to A'^n}$, which results in the input state

$$\rho_{C^nE^nA'^nTG_B} = \mathcal{F}_{E_0^nMG_A\to A'^n}(\phi^{\otimes n}_{CEE_0} \otimes \rho_{MT} \otimes \Psi_{G_AG_B}) \tag{21}$$

and transmits the systems A'^n over n channel uses of $\mathcal{N}_{EA'\to B}$. Hence, the output state is

$$\rho_{C^nB^nTG_B} = \mathcal{N}_{E^nA'^n\to B^n}(\rho_{C^nE^nA'^nTG_B}). \tag{22}$$

Bob receives the channel output and applies the decoding map $\mathcal{D}_{B^nG_B\to\hat{M}}$ to the output systems B^n and to his share of the entangled resources G_B, such that the state of $\hat{M}$ is an estimate of the original state of the message system M. The estimation error is given by

$$e^{(n)}(\mathcal{F}, \Psi, \mathcal{D}, \rho_{MT}) = \frac{1}{2}\left\|\rho_{MT} - \mathcal{D}_{B^nG_B\to\hat{M}}(\rho_{B^nG_BT})\right\|_1 \tag{23}$$

where $\rho_{B^nG_BT} = \mathrm{Tr}_{C^n}(\rho_{C^nB^nG_BT})$. The masking leakage rate of the code $(\mathcal{F}, \Psi, \mathcal{D})$ is defined as

$$\ell^{(n)}(\mathcal{F}, \Psi, \mathcal{D}, \rho_{MT}) \triangleq \frac{1}{n} I(C^n; B^nG_B)_\rho. \tag{24}$$

A $(2^{nQ}, 2^{nR_e}, n, \varepsilon, L)$ quantum masking code satisfies $e^{(n)}(\mathcal{F}, \Psi, \mathcal{D}, \rho_{MT}) \leq \varepsilon$ and $\ell^{(n)}(\mathcal{F}, \Psi, \mathcal{D}, \rho_{MT}) \leq L$ for all ρ_{MT}. A triplet (Q, L, R_e), where $Q, L, R_e \geq 0$, is called achievable if for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nQ}, 2^{nR_e}, n, \varepsilon, L + \delta)$ quantum masking code.

Next, we define the masking equivocation region with and without entanglement assistance. A rate-leakage pair (Q, L) is called achievable with entanglement assistance if (Q, L, R_e) is achievable for some $R_e \geq 0$. The entanglement-assisted masking region $\mathbb{R}^{\text{ea}}_{\text{Q}}(\mathcal{N})$ is defined as the set of achievable pairs (Q, L) with entanglement assistance and CSI at the encoder. Alternatively, one may fix the leakage rate and consider the optimal transmission rate. The quantum capacity-leakage function $\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{N}, L)$ is defined as the supremum of achievable rates Q for a given leakage L. Note that $\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{N}, \infty)$ reduces to the standard definition of the entanglement-assisted capacity, without a masking requirement.

Furthermore, a rate-leakage pair (Q, L) is called achievable without assistance if $(Q, L, R_e = 0)$ is achievable. The masking region $\mathbb{R}_{\text{Q}}(\mathcal{N})$ and quantum capacity-leakage function $\mathbb{C}_{\text{Q}}(\mathcal{N}, L)$ without assistance are defined in a similar manner.

One may also consider the transmission of classical information, where the message system is limited to states $|m\rangle$ for $m = 1, 2, \ldots, 2^{nR}$. In this case, we denote the classical masking regions and capacity-leakage functions by $\mathbb{R}^{\text{ea}}_{\text{Cl}}(\mathcal{N})$, $\mathbb{R}_{\text{Cl}}(\mathcal{N})$ and $\mathbb{C}^{\text{ea}}_{\text{Cl}}(\mathcal{N}, L)$, $\mathbb{C}_{\text{Cl}}(\mathcal{N}, L)$, respectively.

Note that $\mathbb{C}_{\text{Q}}(\mathcal{N}, L)$ and $\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{N}, L)$ have the units of *qubits* per channel use, whereas the units of $\mathbb{C}_{\text{Cl}}(\mathcal{N}, L)$ and $\mathbb{C}^{\text{ea}}_{\text{Cl}}(\mathcal{N}, L)$ are *classical bits* per channel use.

Remark 2: Notice that with entanglement assistance, the leakage rate (24) includes Bob's share G_B of the entanglement resources, since the decoder has access to both B^n and G_B. This is another significant distinction from the classical case. In the classical setting, the leakage constraint does not need to include shared randomness, as it cannot help the decoder. On the other hand, in our quantum model, we know that Bob can extract quantum information by performing measurements on G_B, using the teleportation protocol for example.

Remark 3: Observe that if $L \geq 2 \cdot H(C)_\phi$, then the masking requirement trivially holds because $I(C^n; B^n G_B)_\rho \leq 2H(C^n)_\rho = 2nH(C)_\phi$. That is, if $L \geq 2H(C)_\phi$, then $\mathbb{C}_{\text{Q}}(\mathcal{N}, L) = \mathbb{C}_{\text{Q}}(\mathcal{N}, \infty)$, and similarly for $\mathbb{C}_{\text{Cl}}(\mathcal{N}, L)$, $\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{N}, L)$, and $\mathbb{C}^{\text{ea}}_{\text{Cl}}(\mathcal{N}, L)$.

Remark 4: Note that quantum state-dependent channels have in general a complicated behavior with respect to quantum information transmission and we cannot necessarily expect that the region of achievable rate-leakage pairs (Q, L) without entanglement assistance is equal to the limit of achievable rate-leakage pairs for $R_e \to 0$ [137].

E. Related Work

We briefly review known results for the case where there is no masking requirement. First, consider a quantum channel which is not affected by a channel state, *i.e.* $\mathcal{N}_{EA' \to B}(\rho_{EA'}) = \mathcal{P}_{A' \to B}(\text{Tr}_E(\rho_{EA'}))$.

Theorem 1 (see [51], [52]): The entanglement-assisted quantum capacity of a quantum channel $\mathcal{P}_{A' \to B}$ that does not depend on a channel state, without a masking requirement, is given by

$$\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{P}, \infty) = \max_{|\phi_{AA'}\rangle} \frac{1}{2} I(A; B)_\rho \tag{25}$$

with $\rho_{AB} \equiv \mathcal{P}_{A' \to B}(|\phi_{AA'}\rangle\langle\phi_{AA'}|)$, where A is an auxiliary system of dimension $|\mathcal{H}_A| \leq |\mathcal{H}_{A'}|$.

Without assistance, a single letter characterization is an open problem for a general quantum channel. Yet, a regularized formula for the quantum capacity was given in [42]–[45], in terms of the coherent information. Although calculation of such a formula is intractable in general, it provides a computable lower bound, and there are special cases where the capacity can be computed exactly [46]. Define

$$\mathsf{C}_{\text{Q}}(\mathcal{P}, \infty) = \max_{|\phi_{AA'}\rangle} I(A\rangle B)_\rho \tag{26}$$

with $\rho_{AB} \equiv \mathcal{P}_{A' \to B}(|\phi_{AA'}\rangle\langle\phi_{AA'}|)$ and $|\mathcal{H}_A| \leq |\mathcal{H}_{A'}|$.

Theorem 2 (see [42]–[46]): The quantum capacity of a quantum channel $\mathcal{P}_{A' \to B}$ that does not depend on a channel state, without assistance and without a masking requirement, is given by

$$\mathbb{C}_{\text{Q}}(\mathcal{P}, \infty) = \lim_{k \to \infty} \frac{1}{k} \mathsf{C}_{\text{Q}}(\mathcal{P}^{\otimes k}, \infty). \tag{27}$$

Furthermore, if $\mathcal{P}_{A' \to B}$ has a less noisy output, then

$$\mathbb{C}_{\text{Q}}(\mathcal{P}, \infty) = \mathsf{C}_{\text{Q}}(\mathcal{P}, \infty). \tag{28}$$

A multi-letter characterization as in (27) is often referred to as a regularized formula. We note that in some cases, the entanglement-assisted capacity can be significantly higher than the capacity without assistance. For example, the entanglement-assisted quantum capacity of a qubit erasure channel $\mathcal{P}_{A' \to B}(\rho) = (1-\varepsilon)\rho + \varepsilon|e\rangle\langle e|$, where the erasure state $|e\rangle$ is orthogonal to the qubit space, is $\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{P}, \infty) = 1 - \varepsilon$. On the other hand, without assistance, the quantum capacity is $\mathbb{C}_{\text{Q}}(\mathcal{P}, \infty) = 1 - 2\varepsilon$ for $0 \leq \varepsilon < \frac{1}{2}$, and $\mathbb{C}_{\text{Q}}(\mathcal{P}, \infty) = 0$ for $\varepsilon \geq \frac{1}{2}$ [138].

Remark 5: Theorem 1 is an interesting example for a general phenomenon in quantum information theory. As was pointed out in [139], using entanglement resources has two benefits:

1) Entanglement-assisted protocols can accomplish a performance increase compared to unassisted protocols.
2) Introducing entanglement resources transforms the capacity evaluation from an uncomputable task to an optimization that can be easily performed (numerically).

Remark 6: Among other important aspects for the design and development of communication systems, it is crucial to evaluate the current performance, how close it is to the optimum, and whether it is worth to invest in further development of a particular technology [140], [141]. For those purposes, given an estimate of the channel parameters, it can be useful to calculate the capacity as a number, and the general formula may be less interesting for such purposes. At the time of writing, a realization of a full-scale quantum communication system that approaches the Shannon-theoretic limits does not exist, and we can only hope that future systems of quantum communication will reach the level of maturity of classical commercial systems today, which already employ sophisticated error correction codes with near-Shannon limit performance [142], [143].

Remark 7: As Ahlswede remarked in [144], for the purpose of computing the capacity, a regularized characterization as in Theorem 2 is not necessarily a problem. Given a specific quantum channel, e.g. an optical fiber channel with specific parameters, a practitioner is usually interested in computing the channel capacity as a number (see previous remark). Following Ahlswede's argument in [144], given a fixed channel $\mathcal{P}_{A'\to B}$, if the sequence $\{\frac{1}{n}\mathsf{C}_Q(\mathcal{P}^{\otimes n},\infty)\}_{n\geq 1}$ has a sufficiently high convergence rate, say exponentially fast, then the quantum capacity can be approximated numerically up to any desired precision.

Whereas, from a theoretical perspective, a single-letter formula usually offers a lot more insight. We will come back to this in Section V.

Next, we move to Dupuis' result on a quantum state-dependent channel $\mathcal{N}_{EA'\to B}$ with entanglement assistance and CSI at the encoder. Denote the reduced density matrix of the channel state system by $\phi_E \triangleq \mathrm{Tr}_{E_0\ C}(\phi_{EE_0\ C})$.

Theorem 3 (see [78], [94]): The entanglement-assisted quantum capacity of a quantum channel $(\mathcal{N}_{EA'\to B}, \phi_{EE_0})$, with CSI at the encoder and without a masking requirement, is given by

$$\mathbb{C}_Q^{\mathrm{ea}}(\mathcal{N},\infty) = \sup_{\rho_{AEA'}\,:\,\rho_E=\phi_E} \frac{1}{2}[I(A;B)_\rho - I(A;E)_\rho] \tag{29}$$

with $\rho_{AB} \equiv \mathcal{N}_{EA'\to B}(\rho_{AEA'})$.

III. Information Theoretic Tools

In this section, we present tools that will be useful in the analysis. We begin with the decoupling theorem. We establish an *i.i.d.* version of the decoupling theorem, so that we will not have to worry about the one-shot setting in the achievability proof for our capacity theorems.

We use the following definitions. An operator $V_{A\to B}$ that has 0-1 singular values is called a partial isometry. For every pair of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ with orthonormal bases $\{|i_A\rangle\}$ and $\{|j_B\rangle\}$, respectively, define the operator $\mathrm{op}_{A\to B}(|\psi_{AB}\rangle)$ by

$$\mathrm{op}_{A\to B}(|i_A\rangle \otimes |j_B\rangle) \equiv |j_B\rangle\langle i_A|. \tag{30}$$

While the operation above depends on the choice of bases, we will not specify those since it is not important for our purposes. To generalize this definition to any state $|\psi_{AB}\rangle$, consider its decomposition $|\psi_{AB}\rangle = \sum_{i,j} a_{i,j}|i_A\rangle \otimes |j_B\rangle$, and define $\mathrm{op}_{A\to B}(|\psi_{AB}\rangle) = \sum_{i,j} a_{i,j}\mathrm{op}_{A\to B}(|i_A\rangle \otimes |j_B\rangle)$. Before presenting the decoupling theorem, we give the following useful properties of $\mathrm{op}_{A\to B}(|\psi_{AB}\rangle)$, as stated in [79].

Lemma 4 ([79, Lemma 2.7]): For every pure states $|\psi_{AB}\rangle$ and $|\theta_{AC}\rangle$,

$$\mathrm{op}_{A\to B}(|\psi_{AB}\rangle) \cdot |\theta_{AC}\rangle = \mathrm{op}_{A\to C}(|\theta_{AC}\rangle) \cdot |\psi_{AB}\rangle. \tag{31}$$

Lemma 5 ([79, Lemma 2.8]): For every pure state $|\psi_{AB}\rangle$,

$$\sqrt{|\mathcal{H}_A|}\mathrm{op}_{A\to B}(|\psi_{AB}\rangle) \cdot |\Phi_{AA'}\rangle = |\psi_{A'B}\rangle. \tag{32}$$

We give our i.i.d. version of the decoupling theorem below.

Theorem 6 (The i.i.d. Decoupling Theorem): Let $|\omega_{ABK}\rangle$ be a pure state, and S, R, G_1, G_2 be quantum systems at state

$$|\sigma_{SRG_1G_2}\rangle = |\Psi_{SR}\rangle \otimes |\Phi_{G_1G_2}\rangle \tag{33}$$

in the product Hilbert space $\mathcal{H}_S^{\otimes 2} \otimes \mathcal{H}_G^{\otimes 2}$. Let $W_{SG_1\to A^n}$ be a full-rank partial isometry, and denote

$$|\sigma_{A^nRG_2}\rangle = W_{SG_1\to A^n}|\sigma_{SRG_1G_2}\rangle. \tag{34}$$

Define the quantum channel $\mathcal{T}_{A\to K}$ by

$$\mathcal{T}_{A\to K}(\rho_A) = |\mathcal{H}_A|\mathrm{Tr}_B\left[\mathrm{op}_{A\to BK}(|\omega_{ABK}\rangle)(\rho_A)\right]. \tag{35}$$

Then,

$$\int_{\mathbb{U}_{A^n}} dU_{A^n}\ \left\|\mathcal{T}_{A\to K}^{\otimes n}(U_{A^n}\sigma_{A^nR}) - \omega_K \otimes \sigma_R\right\|_1 \leq \sqrt{\frac{|\mathcal{H}_S|}{|\mathcal{H}_G|}2^{-nH(A|K)_\omega + n\varepsilon(n)}} \tag{36}$$

and

$$\int_{\mathbb{U}_{A^n}} dU_{A^n}\ \left\|\mathcal{T}_{A\to K}^{\otimes n}(U_{A^n}\sigma_{A^nRG_2}) - \omega_K \otimes \sigma_{RG_2}\right\|_1 \leq \sqrt{|\mathcal{H}_S||\mathcal{H}_G|2^{-nH(A|K)_\omega + n\varepsilon(n)}} \tag{37}$$

where the integral is over the Haar measure on all unitaries U_{A^n}, and $\varepsilon(n)$ tends to zero as $n \to \infty$.

The proof of Theorem 6 is given in Appendix A, based on the one-shot decoupling theorem along with arguments from [79]. Intuitively, the theorem above shows that by choosing a unitary U_{A^n} uniformly at random, we can decouple between K and R provided that the dimensions satisfy

$$\frac{1}{n}\log\frac{|\mathcal{H}_S|}{|\mathcal{H}_G|} < H(A|K)_\omega - \varepsilon(n). \tag{38}$$

Similarly, K and (R, G_2) can be decoupled if

$$\frac{1}{n}\log(|\mathcal{H}_S||\mathcal{H}_G|) < H(A|K)_\omega - \varepsilon(n). \tag{39}$$

Uhlmann's theorem [145] is often used along the decoupling approach to establish the existence of proper encoding and decoding operations.

Theorem 7 (Uhlmann's Theorem [145] [79, Corollary 3.2]): For every pair of pure states $|\psi_{AB}\rangle$ and $|\theta_{AC}\rangle$ that satisfy $\|\psi_A - \theta_A\|_1 \leq \varepsilon$, there exists an isometry $F_{B\to C}$ such that $\|(\mathbb{1} \otimes F_{B\to C})\psi_{AB} - \theta_{AC}\|_1 \leq 2\sqrt{\varepsilon}$.

Remark 8: We give a rough explanation, in the spirit of [36, Section 24.10], to demonstrate how decoupling can be useful in an achievability proof for quantum communication. Consider a quantum channel $\mathcal{P}_{A'\to B}$ that does not depend on a channel state, without entanglement assistance. Let $|\Psi_{MR}\rangle$ be a purification of the message state ρ_M, where R is Alice's reference system. Suppose that $|\sigma_{RB^nK^nJ_1}\rangle$ is a purification of the joint state of Alice's reference system R, the channel output B^n, and Bob's environment K^n, with a purifying system J_1. Observe that if the reduced state $\sigma_{RK^nJ_1}$ is a product state, i.e. $\sigma_{RK^nJ_1} = \psi_R \otimes \xi_{K^nJ_1}$, then it has a purification of the form $|\Psi_{MR}\rangle \otimes |\xi_{K^nJ_1\ J_2}\rangle$. Since all purifications are related by isometries [36, Theorem 5.1.1], there exists an isometry $D_{B^n\to MJ_2}$ such that $|\Psi_{MR}\rangle \otimes |\xi_{K^nJ_1\ J_2}\rangle = D_{B^n\to MJ_2}|\sigma_{RB^nK^nJ_1}\rangle$. Tracing out R, K^n, J_1, and J_2, it follows that there exists a decoding map $\mathcal{D}_{B^n\to M}$ that recovers the message state, i.e. $\rho_M = \mathcal{D}_{B^n\to M}(\rho_{B^n})$. Therefore, in order to show that there exists a reliable coding scheme, it is sufficient to encode in such a manner that approximately decouples between Alice's reference system and Bob's environment, i.e., such that $\sigma_{RK^nJ_1} \approx \psi_R \otimes \xi_{K^nJ_1}$.

Remark 9: For our purposes, i.e. deriving an asymptotic characterization, the precise value of $\varepsilon(n)$, and the scale at which it tends to zero as $n \to \infty$, are insignificant. In our achievability proof, our ultimate goal is to show that the probability of error tends to zero given that the communication and leakage rates Q and L are bounded appropriately. Taking the logarithm of the dimensions and dividing by n, we obtain bounds of the form $Q \leq I + \varepsilon(n)$ and $L \geq \lambda - \varepsilon(n)$, where $\varepsilon(n)$ tends to zero in some scale, and this is sufficient. Nonetheless, in general, the scale is important in the study of optimal error exponents and the finite blocklength regime (see *e.g.* [146]), which is outside the scope of the present work. Studying the behavior of $\varepsilon(n)$ in the decoupling lemma above is not likely to yield the optimal error exponents, and this is why we do not bother to do so. As can be seen in [146] and in many others works on this topic, the analysis of error exponents and reliability functions requires very different tools from those of the asymptotic Shannon theory. In basic point-to-point classical models, the approach based on the theory of error exponents may be regarded as superior to the asymptotic methods, in the sense that it can determine both the finite-blocklength behavior of an optimal code and the asymptotic capacity, all at once [147]. However, in more advanced settings, the analysis of error exponents often leads to bounds, while the capacity can be determined precisely using other tools, such as the ones that we have chosen here.

IV. Main Results

We state our results on the quantum state-dependent channel $\mathcal{N}_{EA'\to B}$ with masking.

A. Rate-Limited Entanglement Assistance

First, we consider communication with rate-limited entanglement assistance. We give an achievability result which will be used in the sequel to prove the direct part for the quantum masking region, both with and without entanglement assistance.

Theorem 8: Let $(\mathcal{N}_{EA'\to B}, |\phi_{EE_0\ C}\rangle)$ be a quantum state-dependent channel. Let $\rho_{EA'AC}$ be any mixed state with $\rho_{EC} = \phi_{EC}$. Then, any rate point (Q, L, R_e) such that

$$Q + R_e \leq H(A|EC)_\rho \tag{40}$$

$$Q - R_e \leq I(A\rangle B)_\rho \tag{41}$$

$$L \geq I(C; AB)_\rho \tag{42}$$

is achievable for transmission with rate-limited entanglement assistance and CSI at the encoder, where the auxiliary system A is arbitrary, with $\rho_{ABC} = \mathcal{N}_{EA'\to B}(\rho_{AEA'C})$. That is, for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nQ}, 2^{nR_e}, n, \varepsilon, L + \delta)$ quantum masking code with CSI E_0^n at the encoder, and such that C^n is masked from the decoder.

The proof of Theorem 8 is given in Appendix B. The theorem above provides an achievability result that takes into account the tradeoff between communication and resource rates. As a byproduct, the coding scheme executes state merging [74], as Alice effectively sends her share G_A to Bob. Namely, as can be seen in Appendix B, we begin the protocol with an entangled state $\Psi_{G_AG_B}$, where Alice has the system G_A and Bob has G_B; and when the protocol has been completed, Bob ends up with the systems G'_A and G'_B at state $\approx \Psi_{G'_AG'_B}$.

B. Entanglement-Assisted Masking Region

Next, we consider entanglement-assisted masking, where Alice and Bob have unlimited entanglement resources. In this section, we assume that the channel state systems are in maximally correlated state

$$\varphi_{EE_0C} = \sum_{s\in\mathcal{S}} q(s)|s\rangle\langle s|_E \otimes |s\rangle\langle s|_{E_0} \otimes |s\rangle\langle s|_C \tag{43}$$

where $q(s)$ is a probability distribution, and $\{|s\rangle_E\}$, $\{|s\rangle_{E_0}\}$, $\{|s\rangle_C\}$ each form an orthonormal basis of the respective Hilbert space. Notice that the state above is separable and not entangled. We note that in general, one can always apply the spectral theorem to an individual system and obtain a decomposition of the form $\varphi_E = \sum q(s)|s\rangle\langle s|_E$, and similarly for φ_{E_0} and φ_C. Yet, the assumption in (43) implies that E, E_0, and C have the same spectrum. In addition, if Alice performs a projective measurement on the CSI systems in the basis $\{|s\rangle_{E_0}\}_{s\in\mathcal{S}}$, then the problem reduces to that of a quantum channel that depends on a classical random variable $S \sim q(s)$. Hence, this assumption holds in the special case of a classical channel state. However, in our setting, Alice may perform any quantum operation on the CSI systems E_0^n. Thus, given the restriction (43), the setting is less general than our original model, and yet it is more general than that of a classical channel state. The masking problem given entanglement assistance for a general quantum state $\varphi_{EE_0\ C}$ remains open.

We determine the entanglement-assisted masking region and capacity-leakage function, for the transmission of either quantum information or classical information. Define

$$\mathcal{R}_{\text{Q}}^{\text{ea}}(\mathcal{N}) = \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\varphi_{EC}} \left\{ \begin{array}{rl} (Q, L)\ :\ 0 \leq Q & \leq \frac{1}{2}[I(A;B)_\rho - I(A;EC)_\rho] \\ L & \geq I(C;AB)_\rho \end{array} \right\} \tag{44}$$

and

$$\mathcal{R}_{\text{Cl}}^{\text{ea}}(\mathcal{N}) = \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\varphi_{EC}} \left\{ \begin{array}{rl} (R, L)\ :\ 0 \leq R & \leq I(A;B)_\rho - I(A;EC)_\rho \\ L & \geq I(C;AB)_\rho \end{array} \right\} \tag{45}$$

with $\rho_{ABC} = \mathcal{N}_{EA'\to B}(\rho_{AEA'C})$.

Theorem 9: Let $(\mathcal{N}_{EA'\to B}, \varphi_{EE_0\,C})$ be a quantum state-dependent channel with CSI at the encoder, with maximally correlated channel state systems, as in (43). Then, the entanglement-assisted quantum masking region and classical masking region are given by

$$\mathbb{R}^{\text{ea}}_{\text{Q}}(\mathcal{N}) = \mathcal{R}^{\text{ea}}_{\text{Q}}(\mathcal{N}) \tag{46}$$

and

$$\mathbb{R}^{\text{ea}}_{\text{Cl}}(\mathcal{N}) = \mathcal{R}^{\text{ea}}_{\text{Cl}}(\mathcal{N}) \tag{47}$$

respectively.

The proof of Theorem 9 is given in Appendix C. The direct part is based on Theorem 8. As can be seen in Appendix C, the entanglement-assisted capacity can be achieved if the entanglement rate is higher than $\frac{1}{2}I(A\rangle B)_\rho - \frac{1}{2}H(A|EC)_\rho$. The converse proof requires more attention. As we have three channel state systems, namely, E_0^n, E^n, and C^n, we need to choose the auxiliary system A such that both the communication and leakage rate constraints are met. Thereby, the assumption in (43) is only required for the converse proof.

Equivalently, we can characterize the capacity-leakage function with entanglement assistance. The following corollary is an immediate consequence of Theorem 9.

Corollary 10: Given $(\mathcal{N}_{EA'\to B}, \varphi_{EE_0\,C})$ as in Theorem 9, the entanglement-assisted quantum capacity-leakage function and classical capacity-leakage function are given by

$$\mathbb{C}^{\text{ea}}_{\text{Q}}(\mathcal{N}, L) = \sup_{\substack{\rho_{AEA'C}\,:\, I(C;AB)_\rho \leq L \\ \rho_{EC} = \phi_{EC}}} \frac{1}{2}[I(A;B)_\rho - I(A;EC)_\rho] \tag{48}$$

and

$$\mathbb{C}^{\text{ea}}_{\text{Cl}}(\mathcal{N}, L) = \sup_{\substack{\rho_{AEA'C}\,:\, I(C;AB)_\rho \leq L \\ \rho_{EC} = \phi_{EC}}} [I(A;B)_\rho - I(A;EC)_\rho] \tag{49}$$

respectively, with $\rho_{ABC} = \mathcal{N}_{EA'\to B}(\rho_{AEA'C})$.

Remark 10: It was mentioned in Remark 5, point 2), that in various settings entanglement assistance leads to a characterization that is easy to compute. Unfortunately, this goal was not accomplished in the present work nor in the previous results by Dupuis [94]. Clearly, the characterization of the masking region and the capacity-leakage function has a single-letter form with respect to the channel dependency. However, there is no upper bound on the necessary dimension of the auxiliary system A in Theorems 3, 8, and 9, and in Corollary 10. If we could restrict the optimization to pure states $|\psi_{EA'AC}\rangle$, then we would argue that the dimension of A need not be larger than the Schmidt rank of $|\psi_{EA'AC}\rangle$, hence optimizing over a Hilbert space of dimension $|\mathcal{H}_A| = |\mathcal{H}_{A'}||\mathcal{H}_E||\mathcal{H}_C|$ is sufficient. Note that one can always compute achievable rates by choosing an arbitrary dimension, but the optimal rates cannot be computed with absolute precision in general. Yet, in analogy to Remark 7, for a fixed channel $\mathcal{N}_{EA'\to B}$, state $\varphi_{EE_0\,C}$, and leakage rate L, the values of (48) and (49) can be approximated if there exists a computable function to upper bound the dimension of the auxiliary system in the optimization problem as a function of the required precision.

C. Unassisted Masking Region

In this section, we consider masking without assistance. We establish a regularized formula for the quantum masking region and capacity-leakage function for the transmission of quantum information. For the class of Hadamard channels, we obtain single-letter inner and outer bounds, which coincide in the standard case of a channel that does not depend on the state. Define

$$\mathcal{R}_{\text{Q,in}}(\mathcal{N}) = \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\phi_{EC}} \left\{ \begin{array}{llll} (Q,L) \,:\, & 0 \leq Q & \leq \min\{I(A\rangle B)_\rho,\ H(A|EC)_\rho\} \\ & L & \geq I(C;AB)_\rho \end{array} \right\} \tag{50}$$

with $\rho_{ABC} = \mathcal{N}_{EA'\to B}(\rho_{AEA'C})$. Furthermore, given an isometric extension $\mathcal{U}^{\mathcal{N}}_{EA'\to BK}$, define

$$\mathcal{R}_{\text{Q,out}}(\mathcal{U}^{\mathcal{N}}) = \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\phi_{EC}} \left\{ \begin{array}{llll} (Q,L) \,:\, & 0 \leq Q & \leq H(A|CK)_\rho \\ & L & \geq I(C;AB)_\rho \end{array} \right\} \tag{51}$$

with $\rho_{ABKC} = \mathcal{U}^{\mathcal{N}}_{EA'\to BK}(\rho_{AEA'C})$. Recall that we have defined the class of Hadamard channels in Subsection II-C.2, in terms of an isometric extension $\mathcal{V}^{\text{H}}_{EA'\to BC_1\,K}$ of a particular form (see Definition 3). Our main result on channel state masking without assistance is given below.

Theorem 11: Let $(\mathcal{N}_{EA'\to B}, |\phi_{EE_0\,C}\rangle)$ be a quantum state-dependent channel with CSI at the encoder. Then,

1) the quantum masking region is given by

$$\mathbb{R}_{\text{Q}}(\mathcal{N}) = \bigcup_{k=1}^{\infty} \frac{1}{k}\mathcal{R}_{\text{Q,in}}(\mathcal{N}^{\otimes k}). \tag{52}$$

2) For a Hadamard channel $\mathcal{N}^{\text{H}}_{EA'\to B}$, the quantum masking region is bounded by

$$\mathcal{R}_{\text{Q,in}}(\mathcal{N}^{\text{H}}) \subseteq \mathbb{R}_{\text{Q}}(\mathcal{N}^{\text{H}}) \subseteq \mathcal{R}_{\text{Q,out}}(\mathcal{V}^{\text{H}}). \tag{53}$$

The proof of Theorem 11 is given in Appendix D. Our converse proof is based on different arguments from those in the classical converse proof by Merhav and Shamai [16]. In the classical proof, the derivation of the bounds on both communication rate Q and leakage rate L begins with Fano's inequality. Here, on the other hand, entangled states may have a negative conditional entropy; hence the leakage bound is derived in a different manner, using the coherent information bound on the rate. The direct part is a consequence of our previous result on masking with rate-limited entanglement assistance (see Theorem 8). We derive a single-letter outer bound for Hadamard channels using the special properties of those channels. To bound the communication rate Q, we only need to use the fact that Hadamard channels are degradable. As for the bound on the leakage rate L, here we observe that for Hadamard channels, there exists a channel from the output B to BC_1K, i.e. the channel output combined with the decoder's environment.

Remark 11: Observe that for a pure input state $\rho_{EA'AC} = |\psi_{EA'AC}\rangle\langle\psi_{EA'AC}|$, the extended output systems A, B, C, K

are in a pure state as well, which in turn implies that

$$\begin{aligned} H(A|CK)_\rho &= H(ACK)_\rho - H(CK)_\rho \\ &= H(B)_\rho - H(AB)_\rho = I(A\rangle B)_\rho \end{aligned} \tag{54}$$

where K is part of the output of the isometric extension $\mathcal{V}^{\mathrm{H}}_{EA'\to BC_1\ K}$ (see Definition 3). It follows that the quantum masking region is bounded by

$$\mathbb{R}_{\mathrm{Q}}(\mathcal{N}) \supseteq \mathcal{R}_{\mathrm{Q,in}}(\mathcal{N}) \supseteq \bigcup_{|\psi_{EA'AC}\rangle\,:\,\psi_{EC}=\phi_{EC}} \left\{ \begin{array}{ll} (Q,L)\,:\, 0\le Q & \le I(A\rangle B)_\rho \\ \quad\quad\quad\quad\;\; L & \ge I(C;AB)_\rho \end{array} \right\} \tag{55}$$

with $\rho_{ABC} = \mathcal{N}_{EA'\to B}(|\psi_{AEA'C}\rangle\langle\psi_{AEA'C}|)$. In the trivial case of a quantum channel $\mathcal{P}_{A'\to B}$ that does not depend on a state, the masking region can be achieved with pure product states $|\psi_{ECAA'}\rangle = |\phi_{EC}\rangle \otimes |\theta_{AA'}\rangle$, hence the inner bound and the outer bound coincide, i.e.

$$\mathcal{R}_{\mathrm{Q,in}}(\mathcal{P}) = \mathcal{R}_{\mathrm{Q,out}}(\mathcal{U}^{\mathcal{P}}) = \bigcup_{|\theta_{AA'}\rangle} \left\{ \begin{array}{ll} (Q,L)\,:\, 0\le Q & \le I(A\rangle B)_\rho \\ \quad\quad\quad\quad\;\; L & \ge 0 \end{array} \right\}. \tag{56}$$

Then, if $\mathcal{P}_{A'\to B}$ is a Hadamard channel, the quantum masking region is $\mathbb{R}_{\mathrm{Q}}(\mathcal{P}) = \mathcal{R}_{\mathrm{Q,in}}(\mathcal{P}) = \mathcal{R}_{\mathrm{Q,out}}(\mathcal{U}^{\mathcal{P}})$.

As an immediate consequence of Theorem 11, we obtain the following characterization of the capacity-leakage function.

Corollary 12: Let $(\mathcal{N}_{EA'\to B}, |\phi_{EE_0\ C}\rangle)$ be a quantum state-dependent channel with CSI at the encoder.

1) The quantum capacity-leakage function is given by

$$\mathbb{C}_{\mathrm{Q}}(\mathcal{N},L) = \lim_{k\to\infty}\frac{1}{k} \sup_{\substack{\rho_{E^k A'^k A^k C^k}\,:\,\rho_{E^k C^k}=\phi_{EC}^{\otimes k} \\ L\ge \frac{1}{k} I(C^k;A^kB^k)_\rho}} \min\{I(A^k\rangle B^k)_\rho,\ H(A^k|E^kC^k)_\rho\} \tag{57}$$

with $\rho_{A^kB^kC^k} = \mathcal{N}^{\otimes k}_{EA'\to B}(\rho_{A^kE^kA'^kC^k})$.

2) For a Hadamard channel $\mathcal{N}^{\mathrm{H}}_{EA'\to B}$, the quantum masking region is bounded by

$$\mathbb{C}_{\mathrm{Q},L}(\mathcal{N}^{\mathrm{H}}) \ge \sup_{\substack{\rho_{EA'AC}\,:\,\rho_{EC}=\phi_{EC} \\ L\ge I(C;AB)_\rho}} \min\{I(A\rangle B)_\rho,\ H(A|EC)_\rho\} \tag{58}$$

and

$$\mathbb{C}_{\mathrm{Q},L}(\mathcal{N}^{\mathrm{H}}) \le \sup_{\substack{\rho_{EA'AC}\,:\,\rho_{EC}=\phi_{EC} \\ L\ge I(C;AB)_\rho}} H(A|CK)_\rho \tag{59}$$

with $\rho_{ABC_1\ KC} = \mathcal{V}^{\mathrm{H}}_{EA'\to BC_1\ K}(\rho_{AEA'C})$.

The computational issues that were raised in Remarks 7 and 10 apply to the results in Theorem 11 and Corollary 12 as well.

D. Example: State-Dependent Dephasing Channel

To illustrate our results, we consider a quantum dephasing channel that depends on a classical state and compute achievable rate-leakage regions. Consider a pair of qubit dephasing channels

$$\mathcal{P}^{(s)}_{A'\to B}(\rho) = (1-\varepsilon_s)\rho + \varepsilon_s Z\rho Z,\ s=0,1 \tag{60}$$

where Z is the phase-flip Pauli matrix, and $\varepsilon_0, \varepsilon_1$ are given parameters, with $0\le\varepsilon_s\le 1$ for $s\in\{0,1\}$. Suppose the channel state systems E, C, and E_0 contain a copy of a classical random bit $S\sim$ Bernoulli(q), with $0\le q\le\frac{1}{2}$. Then, the qubit state-dependent channel $\mathcal{N}_{EA'\to B}$ is defined such that given an input state

$$\rho_{EA'} = (1-q)|0\rangle\langle 0|_E\otimes\sigma_0 + q|1\rangle\langle 1|_E\otimes\sigma_1 \tag{61}$$

the output state is

$$\mathcal{N}_{EA'\to B}(\rho_{EA'}) = (1-q)\mathcal{P}^{(0)}_{A'\to B}(\sigma_0) + q\mathcal{P}^{(1)}_{A'\to B}(\sigma_1). \tag{62}$$

Observe that the dephasing channel can also be viewed as a controlled phase-flip gate that is controlled by a classical random bit. In particular, the state-dependent channel above is "controlled" by a random variable W_S such that given $S=s$,

$$W_s \sim \text{Bernoulli}(\varepsilon_s). \tag{63}$$

Consider the transmission of classical information while masking the channel state sequence from the receiver. In the special case of $\varepsilon_0 = 0$ and $\varepsilon_1 = 1$, we have $W_S = S$. That is, the channel acts as a controlled-Z gate where the channel state system E (or S) is the controlling qubit. The entanglement-assisted masking region in this case is

$$\mathbb{R}^{\mathrm{ea}}_{\mathrm{Cl}}(\mathcal{N}) = \bigcup_{0\le\lambda\le 1} \left\{ \begin{array}{ll} (R,L)\,:\, 0\le R & \le 2 \\ \quad\quad\quad\quad\;\; L & \ge 0 \end{array} \right\}. \tag{64}$$

To understand why, observe that given CSI at the encoder, Alice can first perform the controlled phase-flip operation on her entangled qubit, and then use the super-dense coding protocol. Doing so, she effectively eliminates the phase flip operation of the channel. Subsequently, Bob receives the information perfectly, at rate of 2 classical bits per channel use, regardless of the values of S^n. Hence, there is no leakage.

Now, let $\varepsilon_0 \le \frac{1}{2} \le \varepsilon_1$, and define

$$\bar{\varepsilon} = (1-q)\varepsilon_0 + q\varepsilon_1 \tag{65}$$

$$\hat{\varepsilon} = (1-q)\varepsilon_0 + q(1-\varepsilon_1). \tag{66}$$

Without CSI, the channel can be reduced to a standard dephasing channel that does not depend on a state, with the average phase-flip parameter $\bar{\varepsilon}$.

First, we use Theorem 9 to show that the entanglement-assisted masking region is bounded by

$$\mathbb{R}^{\mathrm{ea}}_{\mathrm{Cl}}(\mathcal{N}) \supseteq \mathsf{R}_0 = \left\{ \begin{array}{l} (R,L)\,:\, 0\le R\le 2-h_2(\lambda*\bar{\varepsilon}) \\ L\ge h_2(\lambda*\bar{\varepsilon}) - (1-q)h_2(\lambda*\varepsilon_0) - qh_2(\lambda*\varepsilon_1) \end{array} \right\} \tag{67}$$

where $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, and $a * b = (1-a)b + a(1-b)$. To show achievability of the region above, suppose that Alice performs phase-flip operation controlled by a random variable $Y \sim \text{Bernoulli}(\lambda)$ which is statistically independent of S. That is, $\rho_{EA'A} = \phi_E \otimes \rho_{A'A}$, with

$$\rho_{A'A} = [(1-\lambda)\Phi_{AA'} + \lambda(1 \otimes Z)\Phi_{AA'}(1 \otimes Z)]. \quad (68)$$

Then, Bob receives the output of a phase-flip gate that is controlled by $(W_S + Y) \mod 2$, which is distributed according to Bernoulli$(\lambda * \bar{\varepsilon})$ (see (65)). Thus, for the output state $\rho_{SBA} = \mathcal{N}_{EA'\to B}(\rho_{SEA'A})$, we have

$$\begin{aligned} I(A;B)_\rho - I(A;S)_\rho &= I(A;B)_\rho \\ &= H(A)_\rho + H(B)_\rho - H(AB)_\rho = 1 + 1 - h_2(\lambda * \bar{\varepsilon}) \end{aligned} \quad (69)$$

and

$$\begin{aligned} I(S;AB)_\rho &= H(AB)_\rho - H(AB|S)_\rho \\ &= h_2(\lambda * \bar{\varepsilon}) - [(1-q)h_2(\lambda * \varepsilon_0) + qh_2(\lambda * \varepsilon_1)]. \end{aligned} \quad (70)$$

We note that as Alice's input is in a product state with the channel state system E, this rate-leakage region can also be achieved without CSI.

Next, we derive achievability of the following region,

$$\mathbb{R}^{\text{ea}}_{\text{Cl}}(\mathcal{N}) \supseteq \mathsf{R}_1 \equiv \bigcup_{0 \le \lambda \le \frac{1}{2}} \left\{ \begin{array}{l} (R, L) \,:\, 0 \le R \le 2 - h_2(\lambda * \hat{\varepsilon}) \\ L \ge h_2(\lambda * \hat{\varepsilon}) - (1-q)h_2(\lambda * \varepsilon_0) - qh_2(\lambda * \varepsilon_1) \end{array} \right\}. \quad (71)$$

Therefore, higher communication rates can be achieved with CSI at the encoder at the expense of leaking information on the channel state sequence to the receiver. To obtain the region above from Theorem 9, suppose that Alice performs phase-flip operation controlled by the random variable $S + Y$, with addition modulo 2, where $Y \sim \text{Bernoulli}(\lambda)$ is statistically independent of S. Precisely,

$$\begin{aligned} \rho_{EA'A} = (1-q)|0\rangle\langle 0| \otimes [&(1-\lambda)\Phi_{AA'} \\ &+ \lambda(1 \otimes Z)\Phi_{AA'}(1 \otimes Z)] \\ + q|1\rangle\langle 1| \otimes [&(1-\lambda)(1 \otimes Z)\Phi_{AA'}(1 \otimes Z) \\ &+ \lambda\Phi_{AA'}]. \end{aligned} \quad (72)$$

Then, Bob receives the output of a phase-flip gate that is controlled by $(W_S + S + Y)$, which is distributed according to Bernoulli$(\lambda * \hat{\varepsilon})$ (see (66)). Hence, achievability for the region R_1 follows in a similar manner as for R_0.

Similarly, without entanglement assistance, the quantum masking region is bounded by

$$\mathbb{R}_{\text{Q}}(\mathcal{N}) \supseteq \bigcup_{0 \le \lambda \le \frac{1}{2}} \left\{ \begin{array}{l} (Q, L) \,:\, 0 \le Q \le 1 - h_2(\lambda * \hat{\varepsilon}) \\ L \ge h_2(\lambda * \hat{\varepsilon}) - (1-q)h_2(\lambda * \varepsilon_0) - qh_2(\lambda * \varepsilon_1) \end{array} \right\}. \quad (73)$$

V. Summary and Concluding Remarks

In this section, we summarize our results and compare between the techniques in our work and in previous work. We consider a quantum channel $\mathcal{N}_{EA'\to B}$ that depends on quantum state $|\phi_{EE_0\ C}\rangle$, when the encoder has the CSI systems E_0^n and is required to mask the channel state systems C^n from the decoder. First, we established an achievability result for a setting where Alice and Bob share entanglement resources at a limited rate R_e. That is, before communication begins, Alice and Bob are provided with 2^{nR_e}-dimension systems G_A and G_B, respectively, in an entangled state $\Psi_{G_A G_B}$ of their choosing.

A significant distinction from the classical case is that the leakage requirement

$$\frac{1}{n} I(B^n G_B; C^n)_\rho \le L \quad (74)$$

includes Bob's entangled share G_B, since the decoder has access to both the output systems and his part of the entangled pairs. In the classical setting, shared randomness does not need to be included in the leakage constraint as it cannot help the decoder. On the other hand, we know that Bob can extract quantum information by performing measurements on G_B, using the teleportation protocol for example.

Given a small leakage constraint $L \to 0$, we must ensure that Bob's systems $B^n G_B$ are decoupled from the channel state systems C^n. In this sense, masking can be viewed as a *decoupling problem*, and thus it seems natural to solve the problem using the decoupling approach. Here, we are most interested in the asymptotic characterization of achievable communication rates. Therefore, we have derived an asymptotic version of the decoupling theorem that can be applied directly, without considering the one-shot counterpart. While the derivation of our i.i.d. decoupling theorem, Theorem 6, follows from the one-shot decoupling theorem using familiar arguments, it provides an analytic tool that is easier to combine with classical techniques, without a one-shot proxy.

We presented an achievability result for channel state masking with rate-limited entanglement assistance in Theorem 8, taking into account the tradeoff between the entanglement and communication resources. The proof of our achievability theorem is based on the i.i.d. decoupling theorem along with Uhlmann's theorem [145]. To establish the masking requirement, we approximate the leakage rate using the decoupled output state that results from the decoupling theorem, and which approximates the actual output state. This approximation relies on the Alicki-Fannes-Winter inequality [131], [132], as the decoupled state is close to the actual output state and its leakage rate has a simpler bound.

We determined the entanglement-assisted masking equivocation region and the capacity-leakage function in Theorem 9 and Corollary 10, respectively, under the assumption that the channel state systems E, E_0, and C are maximally correlated, i.e.

$$\varphi_{EE_0C} = \sum_{s \in \mathcal{S}} q(s)|s\rangle\langle s|_E \otimes |s\rangle\langle s|_{E_0} \otimes |s\rangle\langle s|_C \quad (75)$$

where $q(s)$ is a probability distribution and the vectors form an orthonormal basis for each of the corresponding Hilbert spaces. Analytically, the presence of three channel state systems poses a difficulty in choosing the auxiliary system A that would satisfy both communication and leakage rate bounds. This difficulty does not exist in the classical setting of Merhav and Shamai [16], since in the classical setting, C, E, and E_0 are simply copies of the same random variable. The direct part follows from our achievability result with rate-limited entanglement, and does not require the assumption above.

Next, we established a regularized formula for the quantum masking region and capacity-leakage function *without* assistance in Theorem 11 and Corollary 12, respectively. The direct part here also follows from our achievability result with rate-limited entanglement. Our converse proof is based on different arguments compared to those of the classical proof by Merhav and Shamai [16]. In both classical and quantum converse proofs, the leakage rate is bounded by an expression of the form

$$L + \delta \geq \frac{1}{n}(I(C^n; MB^n)_\rho - H(M|B^n)_\rho + H(M|B^nC^n)_\rho) \tag{76}$$

(see (155) and Eq. (21) in [16]). The next step in the classical proof in [16] is to use Fano's inequality in order to bound the second term by

$$H(M|B^n)_\rho \leq n\varepsilon_n \tag{77}$$

and to eliminate the last term, as $H(M|B^nC^n)_\rho \geq 0$. In the quantum setting, we can still write (77), but it would not lead to the desired result because the last term $H(M|B^nC^n)_\rho$ is negative and could not be eliminated (see Remark 12). Hence, we bound the leakage rate in a different manner using the coherent information bound on the communication rate.

We also derived single-letter inner and outer bounds for Hadamard channels, using the special properties of those channels, and showed that the bounds coincide in the standard case of a channel that does not depend on a state. To bound the communication rate Q, we only needed to use the fact that Hadamard channels are degradable. To bound the leakage rate L, we observed that for Hadamard channels, there exists a channel from the channel output to the combined system of the output and its environment.

A shortcoming of our results, as well as the previous results by Dupuis [94], is that we do not have a bound on the dimension of the auxiliary system A, as mentioned in Remark 10. Although one can always compute an achievable region by simply choosing the dimension of A, the optimal rates cannot be computed exactly in general. If we could restrict the optimization to pure states $|\psi_{EA'AC}\rangle$, then we would argue that the dimension of A need not be larger than the Schmidt rank of $|\psi_{EA'AC}\rangle$, hence optimizing over a Hilbert space of dimension $|\mathcal{H}_A| = |\mathcal{H}_{A'}||\mathcal{H}_E||\mathcal{H}_C|$ is sufficient. A similar difficulty appears in other quantum models such as the broadcast channel (see Discussion section in [76]), wiretap channel [117, Remark 5], and squashed entanglement [148, Section 1]. Considering the setting where entanglement assistance is not available, we mentioned in Remark 7 that regularization does not necessarily pose a problem for practical purposes. Whereas, from a theoretical perspective, a single-letter formula usually offers a lot more insight than a multi-letter characterization since the latter is not unique (see e.g. [36, Section 13.1.3]). Nonetheless, remarkable properties such as super-activation [38] were derived from the multi-letter characterization as well.

Acknowledgment

The authors would like to thank the anonymous reviewers and the editor for their constructive comments.

Appendix A
Proof of Theorem 6

We prove the i.i.d. decoupling theorem using the one-shot counterpart in [79] along with arguments therein.

To this end, we need the following definitions from [149]. Define the conditional min-entropy by

$$\begin{aligned} H_{\min}(\rho_{AB}|\sigma_B) &= -\log\inf\{\lambda \in \mathbb{R} \,:\, \rho_{AB} \preceq \lambda \cdot (\mathbb{1}_A \otimes \sigma_B)\} \\ H_{\min}(A|B)_\rho &= \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B). \end{aligned} \tag{78}$$

where the supremum is over quantum states of the system B. In general, the conditional min-entropy is bounded by

$$-\log|\mathcal{H}_B| \leq H_{\min}(A|B)_\rho \leq \log|\mathcal{H}_A|. \tag{79}$$

To see this, observe that if we choose $\sigma_B = \frac{\mathbb{1}_B}{|\mathcal{H}_B|}$, then the matrix inequality $\rho_{AB} \preceq \lambda(\mathbb{1}_A \otimes \sigma_B)$ holds for $\lambda = |\mathcal{H}_B|$, hence $H_{\min}(\rho_{AB}|\sigma_B) \geq -\log|\mathcal{H}_B|$. As for the upper bound, the matrix inequality implies that $1 = \mathrm{Tr}(\rho_{AB}) \leq \lambda|\mathcal{H}_A|\mathrm{Tr}(\sigma_B) = \lambda|\mathcal{H}_A|$, hence $H_{\min}(\rho_{AB}|\sigma_B) \leq \log|\mathcal{H}_A|$. Furthermore, the lower bound is saturated when the joint state of A and B is $|\Phi_{AB}\rangle$, whereas the upper bound for a product state $\frac{\mathbb{1}_A}{|\mathcal{H}_A|} \otimes \rho_B$.

Then, define the smoothed min-entropy by

$$H^\varepsilon_{\min}(A|B)_\rho = \max_{\sigma_{AB}\,:\, d_F(\rho_{AB},\sigma_{AB}) \leq \varepsilon} H^\varepsilon_{\min}(A|B)_\sigma. \tag{80}$$

for arbitrarily small $\varepsilon > 0$, where $d_F(\rho, \sigma) = \sqrt{1 - \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2}$ is the fidelity distance between the states. The theorem below follows from Lemma 2.3 and Theorem 3.8 in [79].

Theorem 13 (The One-Shot Decoupling Theorem [79]): Let ρ_{AR} be a quantum state, $\mathcal{T}_{A\to K}$ be a quantum channel, and $\zeta_{A'K} = \mathcal{T}_{A\to K}(\Phi_{A'A})$. Then, for arbitrarily small $\varepsilon > 0$,

$$\int_{\mathbb{U}_A} dU_A \,\left\|\mathcal{T}_{A\to K}(U_A\rho_{AR}) - \zeta_K \otimes \rho_R\right\|_1 \leq 2^{-\frac{1}{2}H^\varepsilon_{\min}(A'|K)_\zeta - \frac{1}{2}H^\varepsilon_{\min}(A|R)_\rho} + 8\varepsilon \tag{81}$$

where the integral is over the Haar measure on all unitaries U_A.

Now, in order to prove the i.i.d. decoupling theorem, we use Theorem 13 as follows. To show (36), plug

$$A \leftarrow A^n,\; \rho_{AR} \leftarrow W_{SG_1\to A^n}(\sigma_{SG_1R}),\; \mathcal{T} \leftarrow \mathcal{T}^{\otimes n}. \tag{82}$$

Then, by Theorem 13,

$$\int_{\mathbb{U}_{A^n}} dU_{A^n} \left\|\mathcal{T}^{\otimes n}_{A\to K}(U_{A^n}\sigma_{A^nR}) - \zeta_K^{\otimes n}\otimes\sigma_R\right\|_1 \leq 2^{-\frac{1}{2}H^{\varepsilon}_{\min}(A'^n|K^n)_{\zeta^{\otimes n}}-\frac{1}{2}H^{\varepsilon}_{\min}(S,G_1|R)_{\sigma}} + 8\varepsilon \quad (83)$$

with arbitrarily small $\varepsilon > 0$, $\sigma_{A^nR} = W_{SG_1\to A^n}(\sigma_{SG_1\ R})$, and

$$\begin{aligned}\zeta_{A'K} &= \mathcal{T}_{A\to K}(\Phi_{A'A})\\ &= |\mathcal{H}_A|\mathrm{Tr}_B\left[\mathrm{op}_{A\to BK}(|\omega_{ABK}\rangle)(\Phi_{A'A})\right]\\ &= \mathrm{Tr}_B\left(\omega_{A'BK}\right)\\ &= \omega_{A'K} \end{aligned}\quad (84)$$

where the second line follows from Lemma 5. Hence, it follows that

$$\begin{aligned}H^{\varepsilon}_{\min}(A'^n|K^n)_{\zeta^{\otimes n}} &= H^{\varepsilon}_{\min}(A^n|K^n)_{\omega^{\otimes n}}\\ &\geq n(H(A|K)_{\omega} - \delta_1(n))\end{aligned}\quad (85)$$

where the last inequality is due to the quantum asymptotic equipartition property (see [150, Theorem 9] and [79, Lemma 2.3]), and where $\delta_1(n)\to 0$ as $n\to\infty$. Thus, by (83)-(85),

$$\int_{\mathbb{U}_{A^n}} dU_{A^n} \left\|\mathcal{T}^{\otimes n}_{A\to K}(U_{A^n}\sigma_{A^nR}) - \omega_K^{\otimes n}\otimes\sigma_R\right\|_1 \leq 2^{-n\frac{1}{2}H(A|K)_{\omega}-\frac{1}{2}H^{\varepsilon}_{\min}(S,G_1|R)_{\sigma}+n\delta_2(n)} \quad (86)$$

where $\delta_2(n) = \delta_1(n) + \frac{\log(8\varepsilon)}{n}$. Since SR and $G_1\ G_2$ are in a product state $|\Psi_{SR}\rangle\otimes|\Phi_{G_1\ G_2}\rangle$ over $\mathcal{H}_S^{\otimes 2}\otimes\mathcal{H}_G^{\otimes 2}$, we have that

$$\begin{aligned}H^{\varepsilon}_{\min}(S,G_1|R)_{\sigma} &\geq H_{\min}(S|R)_{\sigma} + H_{\min}(G_1)_{\Phi}\\ &\geq -\log|\mathcal{H}_S| + \log|\mathcal{H}_G|\end{aligned}\quad (87)$$

where the last inequality holds by (79). Hence, (36) follows.

To show (37), apply Theorem 13 in the same manner with (R,G_2) instead of R, which yields

$$\int_{\mathbb{U}_{A^n}} dU_{A^n} \left\|\mathcal{T}^{\otimes n}_{A\to K}(U_{A^n}\sigma_{A^nRG_2}) - \omega_K^{\otimes n}\otimes\sigma_{R,G_2}\right\|_1 \leq 2^{-n\frac{1}{2}H(A|K)_{\omega}-\frac{1}{2}H^{\varepsilon}_{\min}(S,G_1|R,G_2)_{\sigma}+n\delta_2(n)} \quad (88)$$

with

$$\begin{aligned}H^{\varepsilon}_{\min}(S,G_1|R,G_2)_{\sigma} &\geq H_{\min}(S|R)_{\Psi} + H_{\min}(G_1|G_2)_{\Phi}\\ &\geq -\log|\mathcal{H}_S| - \log|\mathcal{H}_G|.\end{aligned}\quad (89)$$

Thus, (37) follows as well. This completes the proof of Theorem 6. □

Appendix B
Proof of Theorem 8

The achievability proof is based on the i.i.d. decoupling theorem along with Uhlmann's theorem. To establish the masking requirement, we approximate the leakage rate using the decoupled output state that results from the decoupling theorem, and which approximates the actual output state. This approximation relies on the Alicki-Fannes-Winter inequality [131], [132], as the decoupled state is close to the actual output state and its leakage rate is easier to evaluate.

Consider a quantum state-dependent channel $\mathcal{N}_{EA'\to B}$ with state information at the encoder and masking from the decoder, given rate-limited entanglement assistance. The elements of the coding scheme are displayed in Figure 2, where the quantum systems of Alice and Bob are marked in red and blue, respectively; the channel state systems E^n and C^n are marked in brown; and the purifying systems are marked in green. Before we step into the formal proof, we describe the coding scheme in a nutshell. The quantum message is stored in a system M, which is purified by a reference system R. Alice and Bob's entanglement resources are in the quantum systems G_A and G_B, respectively. Now, Alice encodes the quantum message using her share of the entanglement resources, G_A, along with her access to the side information systems, E_0^n, which in turn are entangled with the channel state systems E^n and C^n. To this end, she applies an encoding isometry and transmits the systems A'^n over n channel uses of the isometric extension of the channel, $U^{\mathcal{N}}_{EA'\to BK}$, where K is the receiver's environment. Bob receives the channel output systems B^n and decodes by applying an isometry to B^n and G_B. We will show that there exist encoding and decoding isometries, $F_{MG_AE_0^n\to A'^nJ^n}$ and $D_{B^nG_B\to\hat{M}G'_AG'_BJ^nK^nJ'}$, respectively, that recover the quantum message state and satisfy the leakage requirement, where J^n and J' are purifying reference systems. In our proof, the decoupling approach is used such that both Bob's environment and the channel state systems E^n and C^n are decoupled from Alice's purifying reference system (see Remark 8). To show the leakage requirement, we approximate the leakage rate using the decoupled output state that results from the decoupling theorem, as the decoupled state is close to the actual output state and its leakage rate is easier to evaluate. The details are given below.

Let $|\theta_{ACEA'J}\rangle$ be any pure state with $\theta_{CE} = \phi_{CE}$, where A is an arbitrary system. In the proof below, we will use auxiliary quantum systems A^n such that the channel input systems A'^n are entangled with A^n. Given a quantum message state ρ_M, let

R be a reference system that purifies the message system M, *i.e.* such that the systems M and R have a pure joint state $|\Psi_{MR}\rangle$, with $|\mathcal{H}_R| = |\mathcal{H}_M| = 2^{nQ}$.

Suppose that Alice and Bob share an entangled state $|\Phi_{G_AG_B}\rangle$ of dimension $|\mathcal{H}_{G_A}| = |\mathcal{H}_{G_B}| = 2^{nR_e}$. Then, the joint state is

$$|\psi_{RMG_AG_B}\rangle \equiv |\Psi_{RM}\rangle\otimes|\Phi_{G_A,G_B}\rangle. \quad (90)$$

Let $\mathcal{U}^{\mathcal{N}}_{EA'\to BK}$ be an isometric extension of the channel $\mathcal{N}_{EA'\to B}$, with

$$\mathcal{U}^{\mathcal{N}}_{EA'\to BK}(\rho_{EA'}) = U^{\mathcal{N}}_{EA'\to BK}\rho_{EA'}(U^{\mathcal{N}}_{EA'\to BK})^{\dagger} \quad (91)$$

and let

$$|\omega_{ACBKJ}\rangle = U^{\mathcal{N}}_{EA'\to BK}|\theta_{ACEA'J}\rangle. \quad (92)$$

Denote

$$\Delta_1(n) \equiv 2^{-n[H(A|EC)_{\omega}-Q-R_e-\varepsilon]/2} \quad (93)$$

$$\Delta_2(n) \equiv 2^{-n[H(A|KJ)_{\omega}-Q+R_e-\varepsilon]/2} \quad (94)$$

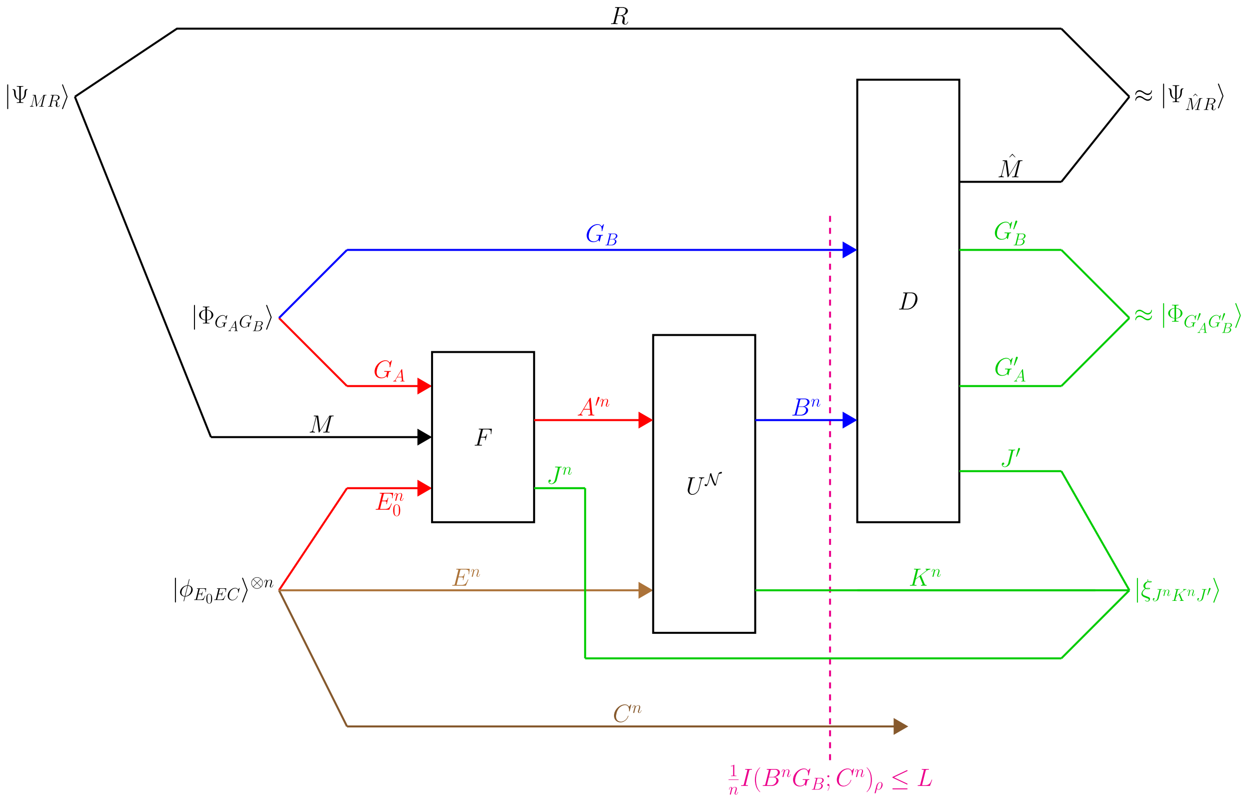


Fig. 2. Coding scheme for a state-dependent quantum channel $\mathcal{N}_{EA'\to B}$ with state information at the encoder and masking from the decoder, given rate-limited entanglement assistance. The quantum systems of Alice and Bob are marked in red and blue, respectively; the channel state systems E^n and C^n are marked in brown; and the purifying systems are marked in green. The quantum message is stored in a 2^{nQ}-dimension system M, which is purified by the reference system R of the same dimension, while Alice and Bob's entanglement resources are in the quantum systems G_A and G_B, respectively, each of dimension 2^{nR_e}. The input state is thus $|\Psi_{RM}\rangle \otimes |\Phi_{G_A,G_B}\rangle \otimes |\phi_{E_0\ EC}\rangle^{\otimes n}$. Alice encodes the quantum message using her share of the entanglement resources, G_A, along with her access to the side information systems E_0^n, which are entangled with the channel state systems E^n and C^n. To this end, she applies the encoding isometry $F_{MG_AE_0^n\to A'^nJ^n}$, where J^n are purifying reference systems. Then, she transmits the systems A'^n over n channel uses of the isometric extension $U^{\mathcal{N}}_{EA'\to BK}$ of the channel $\mathcal{N}_{EA'\to B}$, where K is the receiver's environment. Bob receives the channel output systems B^n, combines them with his share G_B of the entanglement resources, and applies the decoding isometry $D_{B^nG_B\to\hat{M}G'_AG'_BJ^nK^nJ'}$. Using the i.i.d. decoupling theorem and Uhlmann's theorem, it is shown that the resulting state is close in trace distance to $|\Psi_{\hat{M}R}\rangle \otimes |\Phi_{G_AG_B}\rangle \otimes |\xi_{J^nK^nJ'}\rangle$. Given $L \geq I(C;AB)_\omega + \delta$, it is shown that the leakage requirement $\frac{1}{n}I(C^n;B^nG_B)_\rho \leq L$ is satisfied as well.

where $\varepsilon > 0$ is arbitrarily small. Observe that $\Delta_1(n)$ tends to zero exponentially as $n \to \infty$ provided that $Q + R_e < H(A|EC)_\theta - \varepsilon$. As for $\Delta_2(n)$, given a pure quantum state $|\omega_{ACBKJ}\rangle$, we have $H(AKJ)_\omega = H(BC)_\omega$ and $H(KJ)_\omega = H(BCA)_\omega$, hence

$$\begin{aligned} H(A|KJ)_\omega &= H(BC)_\omega - H(BCA)_\omega \\ &= -H(A|BC)_\omega \\ &\geq -H(A|B)_\omega \\ &= I(A\rangle B)_\omega \end{aligned} \tag{95}$$

where the last inequality holds since conditioning does not increase entropy [36, Theorem 11.4.1]. Thus, $\Delta_2(n) \leq 2^{-n(I(A\rangle B)_\omega - Q + R_e - \varepsilon)}$, which tends to zero exponentially as $n \to \infty$ provided that $Q - R_e < I(A\rangle B)_\omega - \varepsilon$.

First, we show that there exist encoding and decoding operations such that the decoding error vanishes. Consider a full-rank partial isometry $W_{MG_A\to A^n}$, *i.e.* an operator with 0-1 singular values and rank $2^{n(Q+R_e)}$, and let

$$\Pi_{A\to CEA'J} \equiv |\mathcal{H}_A|\mathrm{op}_{A\to CEA'J}(|\theta_{ACEA'J}\rangle). \tag{96}$$

Then, define a quantum channel $\mathcal{T}_{A\to KJ}$ by

$$\mathcal{T}_{A\to KJ}(\rho_A) = \mathrm{Tr}_{C,B}\left(U^{\mathcal{N}}_{EA'\to BK}\left(\Pi_{A\to CEA'J}(\rho_A)\right)\right). \tag{97}$$

According to the first part of Theorem 6, the i.i.d. decoupling theorem, applying a random unitary U_{A^n} decouples between the systems (K^n, J^n) and R in the sense that

$$\begin{aligned} \int_{\mathbb{U}_{A^n}} dU_{A^n} \big\|&\mathcal{T}_{A^n\to K^nJ^n}(U_{A^n}W_{MG_A\to A^n}\psi_{RMG_A}) \\ &-\omega_{KJ}^{\otimes n}\otimes\psi_R\big\|_1 \leq 2^{-n[H(A|KJ)_\omega - Q + R_e - \varepsilon_1(n)]/2} \end{aligned} \tag{98}$$

with $\mathcal{T}_{A^n\to K^nJ^n} \equiv \mathcal{T}_{A\to KJ}^{\otimes n}$, where $\varepsilon_1(n)$ tends to zero as $n \to \infty$.

Similarly, the second part of Theorem 6 with $\mathcal{T}'_{A\to CE}(\rho_A) = \mathrm{Tr}_{A'J}\left[\Pi_{A\to CEA'J}(\rho_A)\right]$ yields

$$\begin{aligned} \int_{\mathbb{U}_{A^n}} dU_{A^n} \Big\|&\mathrm{Tr}_{A'^nJ^n}\big[\Pi_{A^n\to C^nE^nA'^nJ^n}U_{A^n} \\ &W_{MG_A\to A^n}\psi_{MG_AG_BR}\big] - \psi_{G_BR}\otimes\phi_{CE}^{\otimes n}\Big\|_1 \\ &\leq 2^{-n[H(A|CE)_\omega - Q - R_e - \varepsilon_2(n)]/2} \end{aligned} \tag{99}$$

with $\Pi_{A^n\to C^nE^nA'^nJ^n} \equiv \Pi^{\otimes n}_{A\to CEA'J}$, where $\varepsilon_2(n)$ tends to zero as $n\to\infty$. Thus, it can be inferred from (98)-(99) that there exists a unitary U_{A^n} such that both of the following inequalities hold,

$$\begin{aligned}\Big\|\mathcal{T}_{A^n\to K^nJ^n}(U_{A^n}W_{MG_A\to A^n}\psi_{RMG_A})\\ -\omega^{\otimes n}_{KJ}\otimes\psi_R\Big\|_1 \leq \Delta_2(n)\end{aligned} \tag{100}$$

and

$$\begin{aligned}\Big\|\mathrm{Tr}_{A'^nJ^n}\left[\Pi_{A^n\to C^nE^nA'^nJ^n}\cdot U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR}\right]\\ -\psi_{G_BR}\otimes\phi^{\otimes n}_{EC}\Big\|_1 \leq \Delta_1(n)\end{aligned} \tag{101}$$

where $\Delta_1(n)$ and $\Delta_2(n)$ are as defined in (93)-(94). In words, there exists a unitary U_{A^n} that decouples both (K^n,J^n) from R, and also (C^n,E^n) from (G_B,R). The existence of a unitary that satisfies both inequalities simultaneously follows from the union of events bound and Markov's inequality, as $\Pr\left(f_1(U)>\Delta_1\vee f_2(U)>\Delta_2\right)\leq\frac{\mathbb{E}f_1(U)}{\Delta_1}+\frac{\mathbb{E}f_2(U)}{\Delta_2}$. We note that such a unitary U_{A^n} need not be unique.

According to Uhlmann's theorem, (101) implies that there exists an isometry $F_{MG_AE_0^n\to A'^nJ^n}$ such that

$$\begin{aligned}\big\|\Pi_{A^n\to C^nE^nA'^nJ^n}\cdot U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR}\\ -F_{MG_AE_0^n\to A'^nJ^n}(\psi_{G_BRMG_A}\otimes\phi^{\otimes n}_{E_0EC})\big\|_1\leq 2\sqrt{\Delta_1(n)}\end{aligned} \tag{102}$$

(see Figure 2). Hence, by applying the isometric extension of the channel and using the triangle inequality and the monotonicity of the trace distance under quantum channels, we obtain

$$\begin{aligned}\Big\|\mathcal{T}_{A^n\to K^nJ^n}(U_{A^n}W_{MG_A\to A^n}\psi_{RMG_A})\\ -\mathrm{Tr}_{C^nB^nG_B}\big((U^{\mathcal{N}}_{EA'\to BK})^{\otimes n}F_{MG_AE_0^n\to A'^nJ^n}\\ (\psi_{G_BRMG_A}\otimes\phi^{\otimes n}_{E_0EC})\big)\Big\|_1\leq 2\sqrt{\Delta_1(n)}.\end{aligned} \tag{103}$$

Together with (100), this implies that

$$\begin{aligned}\Big\|\mathrm{Tr}_{C^nB^nG_B}\big((U^{\mathcal{N}}_{EA'\to BK})^{\otimes n}F_{MG_AE_0^n\to A'^nJ^n}\\ (\psi_{G_BRMG_A}\otimes\phi^{\otimes n}_{E_0EC})\big)-\omega^{\otimes n}_{KJ}\otimes\psi_R\Big\|_1\\ \leq 2\sqrt{\Delta_1(n)}+\Delta_2(n).\end{aligned} \tag{104}$$

Next, by Uhlmann's theorem, there exists a decoding operator $D_{B^nG_B\to\hat{M}G'_AG'_BJ'}$ such that

$$\begin{aligned}\Big\|D_{B^nG_B\to\hat{M}G'_AG'_BJ'}(U^{\mathcal{N}}_{EA'\to BK})^{\otimes n}F_{MG_AE_0^n\to A'^nJ^n}\\ (\psi^{\otimes n}_{G_BRMG_A}\otimes\phi^{\otimes n}_{E_0EC})-\xi_{K^nJ^nJ'}\otimes\psi_{MG_AG_BR}\Big\|_1\\ \leq 2\sqrt{2\sqrt{\Delta_1(n)}+\Delta_2(n)}\end{aligned} \tag{105}$$

for some $\xi_{K^nJ^nJ'}$. By tracing out K^n, J^n, C^n, G'_A, G'_B, and J', we have that there exist an encoding map $\mathcal{F}_{MG_AE_0^n\to A'^n}$ and a decoding map $\mathcal{D}_{B^nG_B\to\hat{M}}$ such that the estimation error is bounded by

$$\begin{aligned}&e^{(n)}(\mathcal{F},\Phi,\mathcal{D},\rho_M)=\\ &\Big\|\mathcal{D}_{B^nG_B\to\hat{M}}\mathcal{N}^{\otimes n}_{EA'\to B}\mathcal{F}_{MG_AE_0^n\to A'^n}(\psi^{\otimes n}_{G_BRMG_A}\otimes\phi^{\otimes n}_{E_0E})\\ &-\Psi_{RM}\Big\|_1\leq 2\sqrt{2\sqrt{\Delta_1(n)}+\Delta_2(n)}.\end{aligned} \tag{106}$$

As for the leakage requirement, let $\delta>0$ be arbitrarily small. Observe that the joint state of the output systems is given by

$$\begin{aligned}&|\sigma_{G_BRK^nJ^nB^nC^n}\rangle\\ &=(U^{\mathcal{N}}_{EA'\to BK})^{\otimes n}F_{MG_AE_0^n\to A'^nJ^n}(\psi^{\otimes n}_{G_BRMG_A}\otimes\phi^{\otimes n}_{E_0EC}).\end{aligned} \tag{107}$$

By (102), $\|\sigma-\eta\|_1\leq 2\sqrt{\Delta_1(n)}$, with

$$\begin{aligned}&|\eta_{G_BRK^nJ^nB^nC^n}\rangle\\ &=(U^{\mathcal{N}}_{EA'\to BK})^{\otimes n}\Pi_{A^n\to C^nE^nA'^nJ^n}\\ &\qquad(U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR})\\ &\overset{(a)}{=}\left(U^{\mathcal{N}}_{EA'\to BK}|\mathcal{H}_A|\mathrm{op}_{A\to CEA'J}(|\theta_{ACEA'J}\rangle)\right)^{\otimes n}\\ &\qquad(U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR})\\ &\overset{(b)}{=}(|\mathcal{H}_A|\mathrm{op}_{A\to CBKJ}(|\omega_{ACBKJ}\rangle))^{\otimes n}\\ &\qquad(U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR})\end{aligned} \tag{108}$$

where (a) follows from the definition of $\Pi_{A^n\to C^nE^nA'^nJ^n}$ in (96), and (b) follows from the definitions of $\mathrm{op}_{A\to B}(\cdot)$ and $|\omega_{ACBKJ}\rangle$ in (30) and (92), respectively. Next, by Lemma 4, we have

$$\begin{aligned}&|\eta_{G_BRK^nJ^nB^nC^n}\rangle\\ &=\left(|\mathcal{H}_A|^n\mathrm{op}_{A^n\to G_BR}(U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR})\right)\\ &|\omega_{ACBKJ}\rangle^{\otimes n}.\end{aligned} \tag{109}$$

Hence,

$$\eta_{G_BRB^nC^n}=\Pi'_{A^n\to G_BR}(\omega^{\otimes n}_{ABC}) \tag{110}$$

with $\Pi'_{A^n\to G_BR}\equiv|\mathcal{H}_A|^n\mathrm{op}_{A^n\to G_BR}(U_{A^n}W_{MG_A\to A^n}\psi_{MG_AG_BR})$.

By the Alicki-Fannes-Winter inequality, the mutual information is continuous in the joint state [131], [132]. In particular, $\|\sigma-\eta\|_1\leq 2\sqrt{\Delta_1(n)}$ implies that

$$\begin{aligned}&|I(C^n;B^nG_B)_\sigma-I(C^n;B^nG_B)_\eta|\\ &\leq 4n\log|\mathcal{H}_B|\sqrt{\Delta_1(n)}+2(1+\sqrt{\Delta_1(n)})\end{aligned} \tag{111}$$

(see [36, Theorem 11.10.3]). Since $\Delta_1(n)$ tends to zero as $n\to\infty$, it follows that for sufficiently large n, the leakage rate is bounded by

$$\begin{aligned}\ell^{(n)}(\mathcal{F},\Psi,\mathcal{D},\rho_M)&=\frac{1}{n}I(C^n;B^nG_B)_\sigma\\ &\leq\frac{1}{n}I(C^n;B^nG_B)_\eta+\delta\\ &\leq\frac{1}{n}I(C^n;B^nG_BR)_\eta+\delta\\ &\leq\frac{1}{n}I(C^n;A^nB^n)_{\omega^{\otimes n}}+\delta\\ &=I(C;AB)_\omega+\delta\end{aligned} \tag{112}$$

where the third inequality follows from (110) and the data processing theorem for the quantum mutual information [36, Theorem 11.9.4]. Thus, the secrecy requirement holds with leakage rate L provided that $I(C;AB)_\omega\leq L-\delta$. □

Appendix C
Proof of Theorem 9

Given unlimited supply of entanglement resources, a qubit is exchangeable with two classical bits. This follows by applying the teleportation protocol and the super-dense coding protocol (see [47, Sections 1.3.7, 2.3]). Therefore, the characterization of the classical masking region follows from that of the quantum masking region, and vice versa. In particular, we prove the theorem by showing achievability for the quantum masking region, and the converse part for the classical masking region. As can be seen below, the maximal correlation assumption in (43) is only required for the converse proof.

A. Achievability Proof

First, consider the direct part for the quantum masking region. Let $(Q,L)\in\mathcal{R}_{\text{Q}}^{\text{ea}}(\mathcal{N})$. Then, for some $\rho_{EA'AC}$ with $\rho_{EC}=\phi_{EC}$, we have $Q\leq\frac{1}{2}[I(A;B)_\rho-I(A;EC)_\rho]$ and $L\geq I(C;AB)_\rho$. We need to show that there exists $R_e\geq 0$ such that (Q,R_e,L) is achievable.

As mentioned in Remark 1, given a mixed state $\varphi_{EE_0\,C}$, we can simply consider the channel $\widetilde{\mathcal{N}}_{\tilde{E}A'\to B}$, with the augmented channel state system $\tilde{E}=(T,E)$, as defined in (10), where $|\phi_{TEE_0\,C}\rangle$ is a purification of the mixed state $\varphi_{EE_0\,C}$. Given the maximal correlation assumption (43), the standard purification is

$$|\phi_{TEE_0C}\rangle=\sum_{s\in\mathcal{S}}\sqrt{q(s)}|s\rangle_T\otimes|s\rangle_E\otimes|s\rangle_{E_0}\otimes|s\rangle_C. \tag{113}$$

Let $\rho_{TEA'AC}$ be an extension of $\rho_{EA'AC}$ with $\rho_{TEC}=\phi_{TEC}$. Then, we can write

$$\rho_{CTEAA'}=\sum_{s\in\mathcal{S}}q(s)|s\rangle\langle s|_C\otimes|s\rangle\langle s|_T\otimes|s\rangle\langle s|_E\otimes\rho^s_{AA'} \tag{114}$$

for some $\rho^s_{AA'}$. Since the eigenvalues of $\rho_{CEAA'}$ are the same as those of $\rho_{CTEAA'}$, it follows that $I(A;TEC)_\rho=I(A;EC)_\rho$.

We now claim that the inequalities (40)-(42) hold for

$$R_e\equiv\frac{1}{2}H(A|\tilde{E}C)_\rho-\frac{1}{2}I(A\rangle B)_\rho. \tag{115}$$

Indeed,

$$\begin{aligned}Q+R_e&\leq\frac{1}{2}[I(A;B)_\rho-I(A;\tilde{E}C)_\rho]\\&\quad+\frac{1}{2}H(A|\tilde{E}C)_\rho-\frac{1}{2}I(A\rangle B)_\rho\\&=H(A|\tilde{E}C)_\rho.\end{aligned} \tag{116}$$

and

$$\begin{aligned}Q-R_e&\leq\frac{1}{2}[I(A;B)_\rho-I(A;\tilde{E}C)_\rho]\\&\quad-\frac{1}{2}H(A|\tilde{E}C)_\rho+\frac{1}{2}I(A\rangle B)_\rho\\&=I(A\rangle B)_\rho\end{aligned} \tag{117}$$

since $I(A;D)_\rho=H(A)_\rho-H(A|D)_\rho$, and due to the definition of the coherent information as $I(A\rangle B)_\rho\equiv-H(A|B)_\rho$.

We also need to verify that $R_e\geq 0$. Let $|\theta_{AC\tilde{E}A'J}\rangle$ be a purification of $\rho_{AC\tilde{E}A'}$ and define $|\omega_{ACBKJ}\rangle$ as in (92). Since the state of $ACBKJ$ is pure, we have $H(A|KJC)_\omega=-H(A|B)_\omega=I(A\rangle B)_\rho$, hence

$$0\leq I(A;KJ|C)_\omega=H(A|C)_\rho-I(A\rangle B)_\rho. \tag{118}$$

As $H(A|C)_\rho=H(A|\tilde{E}C)_\rho$, (118) implies that the assignment of R_e in (115) is non-negative as required. It follows that the conditions of Theorem 8 are satisfied, hence (Q,R_e,L) is achievable. We deduce that $\mathbb{R}_{\text{Q}}^{\text{ea}}(\mathcal{N})\supseteq\mathcal{R}_{\text{Q}}^{\text{ea}}(\mathcal{N})$.

Given unlimited amount of entanglement resources, if Alice can send nQ qubits to Bob with estimation error ε and leakage rate L, then she can send $2nQ$ classical bits with the same error and leakage rate using the superdense coding protocol [47, Section 2.3]. Thus, for the transmission of classical bits, rate-leakage pairs (R,L) such that $R\leq I(A;B)_\rho-I(A;E,C)_\rho$ and $L\geq I(C;AB)_\rho$ are achievable. We deduce that $\mathbb{R}_{\text{Cl}}^{\text{ea}}(\mathcal{N})\supseteq\mathcal{R}_{\text{Cl}}^{\text{ea}}(\mathcal{N})$ as well.

B. Converse Proof

Next, we move to the converse part. While extending the classical arguments, we need to be careful since conditional entropies can be negative in the quantum setting, and since we have three channel state systems, C, E, and E_0. This poses a challenge in defining the auxiliary system A that would satisfy both communication and leakage rate bounds. Here, we will use the assumption that the channel state systems are maximally correlated, as in (43).

Again, due to the superdense coding protocol, if Alice *cannot* send nR classical bits to Bob with estimation error ε and leakage rate L, then she *cannot* send $\frac{1}{2}nR$ qubits with the same error and leakage rate. Thus, it suffices to consider the classical masking region.

Suppose that Alice and Bob are trying to distribute randomness. An upper bound on the rate at which Alice can distribute randomness to Bob also serves as an upper bound on the rate at which they can communicate classical bits. In this task, Alice and Bob share an entangled state $\Psi_{G_AG_B}$. Alice first prepares a maximally corrleated state

$$\pi_{MM'}\equiv\frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}}|m\rangle\langle m|_M\otimes|m\rangle\langle m|_{M'}. \tag{119}$$

locally, where M and M' are classical registers that store the message. Denote the joint state at the beginning by

$$\psi_{MM'G_AG_BE_0^nE^nC^n}=\pi_{MM'}\otimes\Psi_{G_AG_B}\otimes\phi_{E_0EC}^{\otimes n} \tag{120}$$

where E^n are the channel state systems, E_0^n are the CSI systems that are available to Alice, and C^n are the systems that are masked from Bob (see Figure 1). Then, Alice applies an encoding channel $\mathcal{F}_{M'G_AE_0^n\to A'^n}$ to the classical system M', her share G_A of the entangled state $\Psi_{G_AG_B}$, and the CSI systems E_0^n. The resulting state is

$$\rho_{MA'^nG_BE^nC^n}\equiv\mathcal{F}_{M'G_AE_0^n\to A'^n}(\psi_{MM'G_AE_0^nG_BE^nC^n}). \tag{121}$$

After Alice sends the systems A'^n through the channel, Bob receives the systems B^n at state

$$\rho_{MB^nG_BC^n} \equiv \mathcal{N}^{\otimes n}_{EA'\to B}(\rho_{ME^nA'^nG_BC^n}). \tag{122}$$

Then, Bob performs a decoding channel $\mathcal{D}_{B^nG_B\to\hat{M}}$, producing

$$\rho_{M\hat{M}C^n} \equiv \mathcal{D}_{B^nG_B\to\hat{M}}(\rho_{MB^nG_BC^n}). \tag{123}$$

Consider a sequence of codes $(\mathcal{F}_n, \Psi_n, \mathcal{D}_n)$ for randomness distribution, such that

$$\frac{1}{2}\left\|\rho_{M\hat{M}} - \pi_{MM'}\right\|_1 \le \alpha_n \tag{124}$$

$$\frac{1}{n}I(C^n; B^nG_B)_\rho \le L + \beta_n \tag{125}$$

where α_n, β_n tend to zero as $n \to \infty$. By the Alicki-Fannes-Winter inequality [131], [132] [36, Theorem 11.10.3], (124) implies that

$$|H(M|\hat{M})_\rho - H(M|M')_\pi| \le n\varepsilon_n \tag{126}$$

where ε_n tends to zero as $n \to \infty$. Now, observe that $H(\pi_{MM'}) = H(\pi_M) = H(\pi_{M'}) = nR$, hence $I(M;\hat{M})_\pi = nR$. Also, $H(\rho_M) = H(\pi_M) = nR$ implies that $I(M;M')_\pi - I(M;\hat{M})_\rho = H(M|\hat{M})_\rho - H(M|M')_\pi$. Therefore, by (126),

$$\begin{aligned} nR &= I(M;\hat{M})_\pi \\ &\le I(M;\hat{M})_\rho + n\varepsilon_n \\ &\le I(M;B^nG_B)_\rho + n\varepsilon_n \end{aligned} \tag{127}$$

where the last line follows from (123) and the quantum data processing inequality [47, Theorem 11.5].

As in the classical setting, the chain rule for the quantum mutual information states that $I(A;B,C)_\sigma = I(A;B)_\sigma + I(A;C|B)_\sigma$ for all σ_{ABC} (see *e.g.* [36, Property 11.7.1]). As a straightforward consequence, this leads to the Ciszár sum identity,

$$\sum_{i=1}^n I(A_{i+1}^n; B_i|B^{i-1})_\sigma = \sum_{i=1}^n I(B^{i-1}; A_i|A_{i+1}^n)_\sigma \tag{128}$$

for every sequence of systems A^n and B^n. Returning to (127), we apply the chain rule and rewrite the inequality as

$$\begin{aligned} nR &\le I(G_BM;B^n)_\rho + I(M;G_B)_\rho - I(G_B;B^n)_\rho + n\varepsilon_n \\ &\le I(G_BM;B^n)_\rho + I(M;G_B)_\rho + n\varepsilon_n \\ &= I(G_BM;B^n)_\rho + n\varepsilon_n \end{aligned} \tag{129}$$

where the equality holds since the systems M and G_B are in a product state. The chain rule further implies that

$$\begin{aligned} I(G_BM;B^n)_\rho &= \sum_{i=1}^n I(G_BM;B_i|B^{i-1})_\rho \\ &\le \sum_{i=1}^n I(G_BMB^{i-1};B_i)_\rho \\ &= \sum_{i=1}^n I(G_BMB^{i-1}C_{i+1}^n;B_i)_\rho \\ &\quad - \sum_{i=1}^n I(B_i;C_{i+1}^n|G_BMB^{i-1})_\rho \\ &= \sum_{i=1}^n I(G_BMB^{i-1}C_{i+1}^n;B_i)_\rho \\ &\quad - \sum_{i=1}^n I(B^{i-1};C_i|G_BMC_{i+1}^n)_\rho \end{aligned} \tag{130}$$

where the last line follows from the quantum version of the Csiszár sum identity in (128). Since the systems C_i and (G_B, M, C_{i+1}^n) are in a product state, $I(B^{i-1};C_i|G_BMC_{i+1}^n)_\rho = I(G_BMC_{i+1}^nB^{i-1};C_i)_\rho$. Therefore, defining

$$A_i = (G_B, M, B^{i-1}, C_{i+1}^n) \tag{131}$$

we obtain

$$I(G_BM;B^n)_\rho \le \sum_{i=1}^n I(A_i;B_i)_\rho - \sum_{i=1}^n I(A_i;C_i)_\rho. \tag{132}$$

Next, we claim that based on our assumption that $\varphi_{E_0\ EC}$ is as in (43), we have $I(A_i;C_i)_\rho = I(A_i;E_iC_i)_\rho$. To see this, consider the joint state of the systems A_i, C_i, and E_i,

$$\begin{aligned} \rho_{MB^{i-1}G_BC_{i+1}^nC_iE_i} &= \sum_{s^n\in\mathcal{S}^n} q^n(s^n)\frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}} |m\rangle\langle m|_M \\ &\otimes\mathcal{N}^{\otimes i-1}_{EA'\to B}\left(|s^{i-1}\rangle\langle s^{i-1}|_{E^{i-1}} \otimes \rho^{m,s^n}_{A'^{i-1}G_B}\right) \\ &\otimes|s_{i+1}^n\rangle\langle s_{i+1}^n|_{C_{i+1}^n} \otimes |s_i\rangle\langle s_i|_{C_i} \otimes |s_i\rangle\langle s_i|_{E_i} \end{aligned} \tag{133}$$

with $\rho^{m,s^n}_{A'^nG_B} \equiv \mathcal{F}_{M'G_AE_0^n\to A'^n}(|m\rangle\langle m|_{M'} \otimes \Psi_{G_AG_B} \otimes|s^n\rangle\langle s^n|_{E_0^n})$. Observing that the eigenvalues of the state $\rho_{A_iC_iE_i}$ are the same as those of $\rho_{A_iC_i}$, it follows that $H(A_iC_iE_i)_\rho = H(A_iC_i)_\rho$ and $H(C_iE_i)_\rho = H(C_i)_\rho$, thus,

$$I(A_i;C_i)_\rho = I(A_i;E_iC_i)_\rho. \tag{134}$$

Now, let Y be a classical random variable with a uniform distribution over $\{1,\ldots,n\}$, in a product state with the previous quantum systems, *i.e.* C^n, E^n, E_0^n, M, M', G_A, G_B, A'^n, and B^n. Then, by (129), (132), and (134),

$$\begin{aligned} &R - \varepsilon_n \\ &\le \frac{1}{n}\sum_{i=1}^n [I(A_i;B_i)_\rho - I(A_i;E_iC_i)_\rho] \\ &= I(A_Y;B_Y|Y)_\rho - I(A_Y;E_YC_Y|Y)_\rho \\ &= I(A_Y,Y;B_Y)_\rho - I(Y;B_Y)_\rho \\ &- I(A_Y,Y;E_YC_Y)_\rho + I(Y;E_YC_Y)_\rho \\ &\le I(A_Y,Y;B_Y)_\rho - I(A_Y,Y;E_YC_Y)_\rho + I(Y;E_YC_Y)_\rho \\ &= I(A_Y,Y;B_Y)_\rho - I(A_Y,Y;E_YC_Y)_\rho \end{aligned} \tag{135}$$

with $\rho_{YA_YE_YC_YA'_Y} = \frac{1}{n}\sum_{i=1}^n |i\rangle\langle i| \otimes \rho_{A_iE_iC_iA'_i}$ and $\rho_{YA_YC_YB_Y} = \mathcal{N}_{EA'\to B}(\rho_{YA_YC_YE_YA'_Y})$, where the last equality holds since E^n and C^n are in a product state $\phi^{\otimes n}_{EC}$, hence $I(Y;E_YC_Y)_\rho = H(E_YC_Y)_\rho - H(E_YC_Y|Y)_\rho = H(EC)_\phi - H(EC)_\phi = 0$. Thus, defining

$$A \equiv (A_Y, Y),\ E \equiv E_Y,\ C \equiv C_Y,\ A' \equiv A'_Y \tag{136}$$

and B such that $\rho_{ABC} = \mathcal{N}_{EA'\to B}(\rho_{AEA'C})$, we have that

$$R - \varepsilon_n \le I(A;B)_\rho - I(A;EC)_\rho. \tag{137}$$

We have thus shown the desired bound on the coding rate.

As for the leakage rate, by (125),

$$\begin{aligned} n(L+\beta_n) &\geq I(C^n;B^nG_B)_\rho \\ &= I(C^n;B^nG_BM)_\rho - I(C^n;M|B^nG_B)_\rho \\ &= I(C^n;B^nG_BM)_\rho - H(M|B^nG_B)_\rho \\ &\quad + H(M|C^nB^nG_B)_\rho. \end{aligned} \tag{138}$$

Note that the conditional entropy of a classical-quantum state $\rho_{XA} = \sum_{x\in\mathcal{X}} p_X(x)|x\rangle\langle x| \otimes \rho_A^x$ is always nonnegative, since $H(A|X)_\rho = \sum_x p_X(x)H(\rho_A^x) \geq 0$ and $H(X|A)_\rho \geq H(X|A,X) = 0$, as conditioning cannot increase quantum entropy [47, Theorem 11.15]. Since M is classical, the last term in the RHS of (138) is nonnegative, i.e.

$$H(M|C^n,B^n,G_B)_\rho \geq 0. \tag{139}$$

Furthermore, we have by (127) that the second term is bounded by

$$H(M|B^nG_B)_\rho = H(M)_\pi - I(M;B^nG_B)_\rho \leq n\varepsilon_n \tag{140}$$

Thus, by (138)-(140),

$$\begin{aligned} n(L+\beta_n+\varepsilon_n) &\geq I(C^n;B^nG_BM)_\rho \\ &= \sum_{i=1}^{n} I(C_i;B^nG_BM|C_{i+1}^n)_\rho \\ &\geq \sum_{i=1}^{n} I(C_i;B_iB^{i-1}G_BM|C_{i+1}^n)_\rho. \end{aligned} \tag{141}$$

Then, since C_i and C_{i+1}^n are in a product state, $I(C_i;C_{i+1}^n)_\rho = 0$, hence

$$\begin{aligned} &L+\beta_n+\varepsilon_n \\ &\geq \frac{1}{n}\sum_{i=1}^{n} I(C_i;B_iB^{i-1}G_BMC_{i+1}^n)_\rho \\ &= \frac{1}{n}\sum_{i=1}^{n} I(C_i;A_iB_i)_\rho = I(C_Y;A_YB_Y|Y)_\rho \\ &= I(C_Y;A_YYB_Y)_\rho = I(C;AB)_\rho \end{aligned} \tag{142}$$

where the first equality is due to our definition of A_i in (131), the second holds as the classical variable Y is uniformly distributed over $\{1,\dots,n\}$, the third since $I(C_Y;Y)_\rho = H(C_Y)_\rho - H(C_Y|Y)_\rho = H(C)_\phi - H(C)_\phi = 0$, and the last equality follows from (136). This concludes the proof of Theorem 9. □

Appendix D
Proof of Theorem 11

Let $\mathcal{N}_{EA'\to B}$ be a quantum state-dependent channel with state information at the encoder and masking from the decoder, as in Theorem 9. We now consider quantum communication without assistance. The converse proof without assistance is based on different considerations from those in the classical converse proof by Merhav and Shamai [16]. In the classical proof, the derivation of the bounds on both the communication and leakage rates begins with Fano's inequality, followed by arguments that do not hold in our model since conditional quantum entropies can be negative. Hence, we bound the leakage rate in a different manner using the coherent information bound on the communication rate. The direct part is a consequence of our previous result on masking with rate-limited entanglement assistance (see Theorem 8). In the second part, we derive a single-letter outer bound for Hadamard channels using the special properties of those channels. To bound the communication rate Q, we only need to use the fact that Hadamard channels are degradable. As for the bound on the leakage rate L, here we observe that for Hadamard channels, there also exists a channel from the output B to BC_1K, i.e. the channel output combined with the decoder's environment.

Part 1

Achievability of rate-leakage pairs in $\mathcal{R}_{\text{Q}}(\mathcal{N})$ immediately follows from Theorem 8, taking $R_e = 0$. To show that rate-leakage pairs in $\frac{1}{k}\mathcal{R}_{\text{Q}}(\mathcal{N}^{\otimes k})$ are achievable as well, employ the coding scheme in the proof of Theorem 8 in Appendix B for the product channel $\mathcal{N}^{\otimes k}$, where k is arbitrarily large.

Next, we move the converse part. Suppose that Alice and Bob are trying to generate entanglement between them. An upper bound on the rate at which Alice and Bob can generate entanglement also serves as an upper bound on the rate at which they can communicate qubits, since a noiseless quantum channel can be used to generate entanglement by sending one part of an entangled pair. In this task, Alice locally prepares a maximally entangled state,

$$|\Phi_{MM'}\rangle = \frac{1}{\sqrt{2^{nQ}}}\sum_{m=1}^{2^{nQ}} |m\rangle_M \otimes |m\rangle_{M'}. \tag{143}$$

Denote the joint state at the beginning by

$$|\theta_{MM'E_0^nE^nC^n}\rangle = |\Phi_{MM'}\rangle \otimes |\phi_{E_0EC}\rangle^{\otimes n} \tag{144}$$

where E^n are the channel state systems, E_0^n are the CSI systems that are available to Alice, and C^n are the systems that are masked from Bob. Then, Alice applies an encoding channel $\mathcal{F}_{M'E_0^n\to A'^n}$ to the quantum system M' and the CSI systems E_0^n. The resulting state is

$$\rho_{MA'^nE^nC^n} \equiv \mathcal{F}_{M'E_0^n\to A'^n}(\theta_{MM'E_0^nE^nC^n}). \tag{145}$$

After Alice sends the systems A'^n through the channel, Bob receives the systems B^n in the state

$$\rho_{MB^nC^n} \equiv \mathcal{N}_{EA'\to B}^{\otimes n}(\rho_{ME^nA'^nC^n}). \tag{146}$$

Then, Bob performs a decoding channel $\mathcal{D}_{B^n\to\hat{M}}$, producing

$$\rho_{M\hat{M}C^n} \equiv \mathcal{D}_{B^n\to\hat{M}}(\rho_{AB^nC^n}). \tag{147}$$

Consider a sequence of codes $(\mathcal{F}_n, \mathcal{D}_n)$ for entanglement generation, such that

$$\frac{1}{2}\left\|\rho_{M\hat{M}} - \Phi_{MM'}\right\|_1 \leq \alpha_n \tag{148}$$

$$\frac{1}{n}I(C^n;B^n)_\rho \leq L+\beta_n \tag{149}$$

where α_n, β_n tend to zero as $n\to\infty$.

By the Alicki-Fannes-Winter inequality [131], [132] [36, Theorem 11.10.3], (148) implies that $|H(M|\hat{M})_\rho - H(M|M')_\Phi| \leq n\varepsilon_n$, or equivalently,

$$|I(M\rangle\hat{M})_\rho - I(M\rangle M')_\Phi| \leq n\varepsilon_n \tag{150}$$

where ε_n tends to zero as $n \to \infty$. Observe that $I(M\rangle M')_\Phi = H(M)_\Phi - H(MM')_\Phi = nQ - 0 = nQ$. Thus,

$$\begin{aligned} nQ &= I(M\rangle M')_\Phi \\ &\leq I(M\rangle\hat{M})_\rho + n\varepsilon_n \\ &\leq I(M\rangle B^n)_\rho + n\varepsilon_n \end{aligned} \tag{151}$$

where the last line follows from (147) and the data processing inequality for the coherent information [36, Theorem 11.9.3]. In addition,

$$\begin{aligned} nQ = H(M)_\Phi &= H(M)_\theta \\ &= H(M|E^nC^n)_\theta \\ &= H(M|E^nC^n)_\rho \end{aligned} \tag{152}$$

where the second line follows since M and (E^n, C^n) are in a product state. Hence, $Q \leq \frac{1}{n}\min\{I(M\rangle B^n)_\rho, H(M|E^nC^n)_\rho\} + \varepsilon_n$. Let A^n be quantum systems such that for some isometry $W_{M\to A^n}$,

$$\rho_{A^nA'^nE^nC^n} = W_{M\to A^n}\rho_{MA'^nE^nC^n}W^\dagger_{M\to A^n}. \tag{153}$$

Since the von Neumann entropy is isometrically invariant [36, Property 11.1.5], it follows that

$$Q \leq \frac{1}{n}\min\{I(A^n\rangle B^n)_\rho, H(A^n|E^nC^n)_\rho\} + \varepsilon_n. \tag{154}$$

As for the leakage rate, by (149),

$$\begin{aligned} &n(L+\beta_n) \\ &\geq I(C^n;B^n)_\rho \\ &= I(C^n;MB^n)_\rho - I(C^n;M|B^n)_\rho \\ &= I(C^n;MB^n)_\rho - H(M|B^n)_\rho + H(M|B^nC^n)_\rho \quad (155) \\ &= I(C^n;MB^n)_\rho + I(M\rangle B^n)_\rho + H(M|B^nC^n)_\rho \\ &\geq I(C^n;MB^n)_\rho + n(Q-\varepsilon_n) + H(M|B^nC^n)_\rho \quad (156) \end{aligned}$$

where the last line follows from (151). Since

$$H(M|B^nC^n)_\rho \geq -\log|\mathcal{H}_M| = -nQ \tag{157}$$

(see [36, Theorem 11.5.1]), we have

$$\begin{aligned} L + \beta_n + \varepsilon_n &\geq \frac{1}{n}I(C^n;MB^n)_\rho \quad (158) \\ &= \frac{1}{n}I(C^n;A^nB^n)_\rho. \quad (159) \end{aligned}$$

This completes the proof for the regularized capacity-leakage characterization.

Remark 12: We note that in the classical converse proof in [16], the authors obtain an inequality that is similar to (155) (see Eq. (21) in [16]). The next step in their proof is to use Fano's inequality in order to bound the second term by

$$H(M|B^n)_\rho \leq n\varepsilon_n \tag{160}$$

and to eliminate the third term, as $H(M|B^nC^n)_\rho \geq 0$. In the quantum setting, we can still write (160), however, the last term is negative and could not be eliminated, as $H(M|B^nC^n)_\rho \leq H(M|B^n)_\rho \leq -n(Q-\varepsilon_n) < 0$.

Part 2

Suppose that $\mathcal{N}^{\text{H}}_{EA'\to B}$ is a Hadamard channel with an isometric extension $\mathcal{V}^{\text{H}}_{EA'\to BC_1\ K}$ (see Definition 3). The direct part follows from Theorem 8 as in part 1. It remains to prove the single-letter converse part.

Returning to the entanglement generation protocol which we started with in part 1, we now define

$$A_i = (M, B^{i-1}, K^{i-1}, C^{i-1}, C^n_{i+1}). \tag{161}$$

For every $i \in \{1,\ldots,n\}$, consider the spectral representation

$$\rho_{ME^iA'^iC^n_{i+1}} = \sum_{x_i\in\mathcal{X}_i} p_{X_i}(x_i)\psi^{x_i}_{ME^iA'^iC^n_{i+1}} \tag{162}$$

where $p_{X_i}(x_i)$ is a probability distribution and $\{|\psi^{x_i}_{ME^iA'^iC^n_i}\rangle\}_{x_i\in\mathcal{X}_i}$ form an orthonormal basis, hence

$$\rho_{MB^iC^i_1K^iC^n_{i+1}} = \sum_{x_i\in\mathcal{X}_i} p_{X_i}(x_i)\psi^{x_i}_{MB^iC^i_1K^iC^n_{i+1}} \tag{163}$$

where $|\psi^{x_i}_{MB^iC^i_1K^iC^n_{i+1}}\rangle = (\mathcal{V}^{\text{H}}_{EA'\to BC_1\ K})^{\otimes i}|\psi^{x_i}_{ME^iA'^iC^n_{i+1}}\rangle$. By (20), we also have $\rho_{MB^iK^iC^i_1C^n_{i+1}} = \rho_{MB^iK^iC^iC^n_{i+1}}$, hence

$$\rho_{MB^iK^iC^n} = \sum_{x_i\in\mathcal{X}_i} p_{X_i}(x_i)\psi^{x_i}_{MB^iK^iC^n} \tag{164}$$

with $|\psi^{x_i}_{MB^iC^iK^iC^n_{i+1}}\rangle = (\mathcal{V}^{\text{H}}_{EA'\to BCK})^{\otimes i}|\psi^{x_i}_{ME^iA'^iC^n_{i+1}}\rangle$. Given a sequence of codes $(\mathcal{F}_n, \mathcal{D}_n)$ that satisfy (148)-(149),

$$\begin{aligned} n(Q-\varepsilon_n) &\leq -H(M|B^n)_\rho \\ &\leq -H(M|B^nX^n)_\rho \\ &= H(B^n|X^n)_\rho - H(MB^n|X^n)_\rho \end{aligned} \tag{165}$$

where the first inequality is due to (151), and the second inequality holds since conditioning does not increase entropy [36, Theorem 11.4.1]. By (164), the state of M, B^n, K^n, C^n is pure when conditioned on $X^n = x^n$, hence $H(MB^n|X^n)_\rho = H(K^nC^n|X^n)_\rho$. Thus, we can write the last bound as

$$\begin{aligned} &n(Q-\varepsilon_n) \\ &\leq H(B^n|X^n)_\rho - H(K^nC^n|X^n)_\rho \\ &= H(B^nX^n)_\rho - H(K^nC^nX^n)_\rho \\ &= \sum_{i=1}^n [H(B_iX_i|B^{i-1}X^{i-1})_\rho \\ &\quad - H(K_iC_iX_i|K^{i-1}C^{i-1}X^{i-1})_\rho] \\ &= \sum_{i=1}^n \big[H(B_iX_i)_\rho - H(K_iC_iX_i)_\rho \\ &\quad - \big(I(B_iX_i;B^{i-1}X^{i-1})_\rho - I(K_iC_iX_i;K^{i-1}C^{i-1}X^{i-1})_\rho\big)\big] \\ &\leq \sum_{i=1}^n \big[H(B_iX_i)_\rho - H(K_iC_iX_i)_\rho\big] \end{aligned} \tag{166}$$

where the last inequality holds since Hadamard channels are degradable (see Subsection II-C), and thus

$$\begin{aligned} I(B_iX_i;B^{i-1}X^{i-1})_\rho &\geq I(K_iC_{1,i}X_i;K^{i-1}C^{i-1}_1X^{i-1})_\rho \\ &= I(K_iC_iX_i;K^{i-1}C^{i-1}X^{i-1})_\rho \end{aligned} \tag{167}$$

by the data processing theorem for the quantum mutual information [36, Theorem 11.9.4] and due to (20).

Now, according to (164), the state of M, B^i, K^i, C^n is pure for a given $X_i = x_i$, hence

$$\begin{aligned} H(B_i|X_i)_\rho &= H(MB^{i-1}K^iC^n|X_i)_\rho \\ &= H(A_iK_iC_i|X_i) \end{aligned} \tag{168}$$

(see (161)). Then, (166) implies

$$\begin{aligned} n(Q-\varepsilon_n) &\leq \sum_{i=1}^n H(A_i|C_iK_iX_i)_\rho \\ &\leq \sum_{i=1}^n H(A_i|C_iK_i)_\rho \end{aligned} \tag{169}$$

since conditioning does not increase entropy.

Defining Y to be a classical random variable of uniform distribution over $\{1,\ldots,n\}$, in a product state with the previous systems, we have

$$\begin{aligned} Q-\varepsilon_n &\leq \frac{1}{n}\sum_{i=1}^n H(A_i|C_iK_i)_\rho \\ &= H(A_Y|C_YK_YY)_\rho \\ &\leq H(A|CK)_\rho \end{aligned} \tag{170}$$

with $\rho_{YA_YE_YC_YA'_Y} = \frac{1}{n}\sum_{i=1}^n |i\rangle\langle i| \otimes \rho_{A_iE_iC_iA'_i}$, $\rho_{YA_YC_YB_YK_Y} = \mathcal{U}^{\mathcal{N}}_{EA'\to BK}(\rho_{YA_YC_YE_YA'_Y})$, and then

$$A \equiv (A_Y, Y),\ E \equiv E_Y,\ C \equiv C_Y,\ A' \equiv A'_Y \tag{171}$$

and B, C_1, K such that $\rho_{ABC_1\ KC} = \mathcal{V}^{\mathrm{H}}_{EA'\to BC_1\ K}(\rho_{AEA'C})$.

As for the leakage rate, we begin with an observation that follows from our definition of Hadamard state-dependent channels in Subsection II-C. Observe that given a Hadamard channel which is extended by $\mathcal{V}_{EA'\to C_1\ KB}$, there exists a channel from B to $BC_1\ K$. Specifically, if we define a channel $\mathcal{L}_{B\to BC_1\ K}$ as the mapping $\psi^x_B \mapsto \psi^x_B \otimes \eta^x_{C_1\ K}$, then we have

$$\rho_{ABC_1KC} = \mathcal{L}_{B\to BC_1K}(\rho_{ABC}) \tag{172}$$

or explicitly,

$$\mathcal{V}_{EA'\to C_1KB}(\rho_{AEA'C}) = (\mathcal{L}_{B\to BC_1K}\circ\mathcal{N}_{EA'\to B})(\rho_{AEA'C}) \tag{173}$$

for all $\rho_{AA'EC}$ with $\rho_{EC} = \phi_{EC}$.

By (151),

$$\begin{aligned} &n(L+\beta_n) \\ &\quad\geq I(C^n;MB^n)_\rho + n(Q-\varepsilon_n) + H(M|B^nK^nC^n)_\rho \\ &\quad\geq I(C^n;MB^n)_\rho - n\varepsilon_n \end{aligned} \tag{174}$$

since $H(M|B^nK^nC^n)_\rho \geq -\log|\mathcal{H}_M| = -nQ$ (see [36, Theorem 11.5.1]). Next, we apply the chain rule and write

$$\begin{aligned} n(L+\beta_n+\varepsilon_n) &\geq I(C^n;B^nM)_\rho \\ &= \sum_{i=1}^n I(C_i;B^nM|C^n_{i+1})_\rho \\ &\geq \sum_{i=1}^n I(C_i;B_iB^{i-1}M|C^n_{i+1})_\rho \\ &= \sum_{i=1}^n I(C_i;B_iB^{i-1}MC^n_{i+1})_\rho \end{aligned} \tag{175}$$

where the last equality holds since C_i and C^n_{i+1} are in a product state, hence $I(C_i;C^n_{i+1})_\rho = 0$. Using the fact that there exists a channel from B^{i-1} to $B^{i-1}C_1^{i-1}K^{i-1}$ (see (172)), along with the data processing theorem for the quantum mutual information, we deduce that

$$\begin{aligned} I(C_i;B_iMB^{i-1}C^n_{i+1})_\rho &\geq I(C_i;B_iMB^{i-1}K^{i-1}C_1^{i-1}C^n_{i+1})_\rho \\ &= I(C_i;B_iMB^{i-1}K^{i-1}C^{i-1}C^n_{i+1})_\rho \\ &= I(C_i;A_iB_i)_\rho \end{aligned} \tag{176}$$

where the first equality follows from our definition of a Hadamard state-dependent channel (see (20)), and the last line is due to (161). Thus, by (175) and (176),

$$\begin{aligned} L+\beta_n+\varepsilon_n &\geq \frac{1}{n}\sum_{i=1}^n I(C_i;A_iB_i)_\rho = I(C_Y;A_YB_Y|Y)_\rho \\ &= I(C_Y;YA_YB_Y)_\rho = I(C;AB)_\rho \end{aligned} \tag{177}$$

where the first equality holds as the classical variable Y is uniformly distributed over $\{1,\ldots,n\}$, the second since $I(C_Y;Y)_\rho = H(C_Y)_\rho - H(C_Y|Y)_\rho = H(C)_\phi - H(C)_\phi = 0$, and the last equality follows from (171). This concludes the proof of Theorem 11. □

References

[1] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013.

[2] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the Internet of Things," *Future Gener. Comput. Syst.*, vol. 75, pp. 46–57, Oct. 2017.

[3] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *IEEE Access*, vol. 7, pp. 24956–24963, 2019.

[4] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565–2578, May 2019.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[7] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–12, Dec. 2009.

[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[9] M. Bellare, S. Tessaro, and A. Vardy, "A cryptographic treatment of the wiretap channel," 2012, *arXiv:1201.2205*. [Online]. Available: http://arxiv.org/abs/1201.2205

[10] H. Boche, R. F. Schaefer, and H. V. Poor, "On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2531–2546, Dec. 2015.

[11] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3863–3879, Jul. 2016.

[12] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[13] A. Bunin, Z. Goldfeld, H. H. Permuter, S. Shamai (Shitz), P. Cuff, and P. Piantanida, "Key and message semantic-security over state-dependent channels," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1541–1556, 2020.

[14] H. Boche, M. Cai, J. Nötzel, and C. Deppe, "Secret message transmission over quantum channels under adversarial quantum noise: Secrecy capacity and super-activation," *J. Math. Phys.*, vol. 60, no. 6, Jun. 2019, Art. no. 062202.

[15] C. Li, Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity of colored Gaussian noise channels with feedback," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5771–5782, Sep. 2019.

[16] N. Merhav and S. Shamai (Shitz), "Information rates subject to state masking," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2254–2261, Jun. 2007.

[17] M. Le Treust and M. Bloch, "Empirical coordination, state masking and state amplification: Core of the decoder's knowledge," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 895–899.

[18] M. Le Treust and M. R. Bloch, "State leakage and coordination with causal state knowledge at the encoder," *IEEE Trans. Inf. Theory*, early access, Nov. 9, 2020, doi: 10.1109/TIT.2020.3036987.

[19] O. O. Koyluoglu, R. Soundararajan, and S. Vishwanath, "State amplification subject to masking constraints," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6233–6250, Nov. 2016.

[20] O. O. Koyluoglu, R. Soundararajan, and S. Vishwanath, "State amplification under masking constraints," in *Proc. 49th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, Sep. 2011, pp. 936–943.

[21] M. Dikshtein, A. Somekh-Baruch, and S. Shamai (Shitz), "Broadcasting information subject to state masking over a MIMO state dependent Gaussian channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 275–279.

[22] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Information extraction under privacy constraints," *Information*, vol. 7, no. 1, p. 15, Mar. 2016.

[23] K. Tutuncuoglu, O. Ozel, A. Yener, and S. Ulukus, "State amplification and state masking for the binary energy harvesting channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Hobart, TAS, Australia, Nov. 2014, pp. 336–340.

[24] T. A. Courtade, "Information masking and amplification: The source coding setting," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, pp. 189–193.

[25] S. X. Ng *et al.*, "Guest editorial advances in quantum communications, computing, cryptography, and sensing," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 405–412, Mar. 2020.

[26] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution," *Philos. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 361, no. 1809, pp. 1655–1674, Jun. 2003.

[27] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon.*, vol. 7, no. 5, p. 378, 2013.

[28] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, Dec. 2014.

[29] F. Becerra, J. Fan, and A. Migdall, "Photon number resolution enables quantum receiver for realistic coherent optical communications," *Nature Photon.*, vol. 9, no. 1, p. 48, Jan. 2015.

[30] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017.

[31] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Phys. Rev. Lett.*, vol. 118, no. 22, May 2017, Art. no. 220501.

[32] L. Petit *et al.*, "Universal quantum logic in hot silicon qubits," *Nature*, vol. 580, no. 7803, pp. 355–359, Apr. 2020.

[33] D. Bouwmeester and A. Zeilinger, "The physics of quantum information: Basic concepts," in *The Physics of Quantum Information*. Berlin, Germany: Springer, 2000, pp. 1–14.

[34] S. Imre and L. Gyongyosi, *Advanced Quantum Communications: An Engineering Approach*. Hoboken, NJ, USA: Wiley, 2012.

[35] A. Y. Kitaev, "Quantum error correction with imperfect gates," in *Quantum Communication, Computing, and Measurement*. Boston, MA, USA: Springer, 1997, pp. 181–188.

[36] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[37] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart., 2018.

[38] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, vol. 321, no. 5897, pp. 1812–1815, Sep. 2008.

[39] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan. 1998.

[40] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, p. 131, Jul. 1997.

[41] A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, vol. 16. Berlin, Germany: Walter de Gruyter, 2012.

[42] H. Barnum, M. A. Nielsen, and B. Schumacher, "Information transmission through a noisy quantum channel," *Phys. Rev. A, Gen. Phys.*, vol. 57, no. 6, p. 4153, Jun. 1998.

[43] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 3, p. 1613, Mar. 1997.

[44] P. W. Shor, "The quantum channel capacity and coherent information," in *Proc. Lect. Notes MSRI Workshop Quantum Comput.*, 2002.

[45] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.

[46] I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Commun. Math. Phys.*, vol. 256, no. 2, pp. 287–303, Jun. 2005.

[47] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2002.

[48] H. Boche, G. Janßen, and S. Kaltenstadler, "Entanglement-assisted classical capacities of compound and arbitrarily varying quantum channels," *Quantum Inf. Process.*, vol. 16, no. 4, p. 88, Feb. 2017.

[49] E. Chitambar and G. Gour, "Quantum resource theories," *Rev. Modern Phys.*, vol. 91, no. 2, Apr. 2019, Art. no. 025001.

[50] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, p. 2881, Nov. 1992.

[51] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Phys. Rev. Lett.*, vol. 83, no. 15, p. 3081, 1999.

[52] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, Oct. 2002.

[53] B. Swingle, "Mutual information and the structure of entanglement in quantum field theory," 2010, *arXiv:1010.4038*. [Online]. Available: http://arxiv.org/abs/1010.4038

[54] Q. Pan and J. Jing, "Degradation of nonmaximal entanglement of scalar and Dirac fields in noninertial frames," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 2, Feb. 2008, Art. no. 024302.

[55] H. Casini, M. Huerta, R. C. Myers, and A. Yale, "Mutual information and the F-theorem," *J. High Energy Phys.*, vol. 2015, no. 10, p. 3, Oct. 2015.

[56] C. A. Agón and T. Faulkner, "Quantum corrections to holographic mutual information," *J. High Energy Phys.*, vol. 2016, no. 8, p. 118, Aug. 2016.

[57] C. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J*, vol. 27, pp. 379–423 and 623–656, Jul. 1948.

[58] D. Leung, L. Mancinska, W. Matthews, M. Ozols, and A. Roy, "Entanglement can increase asymptotic rates of zero-error classical communication over classical channels," *Commun. Math. Phys.*, vol. 311, no. 1, pp. 97–111, Mar. 2012.

[59] F. Leditzky, M. A. Alhejji, J. Levin, and G. Smith, "Playing games with multiple access channels," *Nature Commun.*, vol. 11, no. 1, pp. 1–5, Dec. 2020.

[60] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, no. 15, p. 880, Oct. 1969.

[61] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties," *Phys. Rev. Lett.*, vol. 108, no. 26, Jun. 2012, Art. no. 260502.

[62] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, no. 14, Sep. 2014, Art. no. 140501.

[63] Z.-A. Jia, L. Wei, Y.-C. Wu, and G.-C. Guo, "Quantum advantages of communication complexity from bell nonlocality," 2020, *arXiv:2004.05098*. [Online]. Available: http://arxiv.org/abs/2004.05098

[64] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "MIP*=RE," 2020, *arXiv:2001.04383*. [Online]. Available: http://arxiv.org/abs/2001.04383

[65] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, p. 1895, Mar. 1993.

[66] P. W. Shor, "The classical capacity achievable by a quantum channel assisted by limited entanglement," *Quantum Inf. Comp.*, vol. 4, no. 6, pp. 537–545, Dec. 2004.

[67] I. Devetak, A. W. Harrow, and A. J. Winter, "A resource framework for quantum Shannon theory," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4587–4618, Oct. 2008.

[68] M.-H. Hsieh and M. M. Wilde, "Entanglement-assisted communication of classical and quantum information," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4682–4704, Sep. 2010.

[69] M.-H. Hsieh and M. M. Wilde, "Trading classical communication, quantum communication, and entanglement in quantum Shannon theory," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4705–4730, Sep. 2010.

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

[71] K. Wang and M. Hayashi, "Permutation enhances classical communication assisted by entangled states," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 1840–1845.

[72] I. Devetak, A. W. Harrow, and A. Winter, "A family of quantum protocols," *Phys. Rev. Lett.*, vol. 93, no. 23, Dec. 2004, Art. no. 230504.

[73] I. Devetak, "Triangle of dualities between quantum communication protocols," *Phys. Rev. Lett.*, vol. 97, no. 14, Oct. 2006, Art. no. 140503.

[74] M. Horodecki, J. Oppenheim, and A. Winter, "Quantum state merging and negative information," *Commun. Math. Phys.*, vol. 269, no. 1, pp. 107–136, Nov. 2006.

[75] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, "The mother of all protocols: Restructuring quantum information's family tree," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 465, no. 2108, pp. 2537–2563, Aug. 2009.

[76] F. Dupuis, P. Hayden, and K. Li, "A father protocol for quantum broadcast channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2946–2956, Jun. 2010.

[77] P. Hayden, M. Horodecki, A. Winter, and J. Yard, "A decoupling approach to the quantum capacity," *Open Syst. Inf. Dyn.*, vol. 15, no. 1, pp. 7–19, Mar. 2008.

[78] F. Dupuis, "Coding for quantum channels with side information at the transmitter," 2008, *arXiv:0805.3352*. [Online]. Available: http://arxiv.org/abs/0805.3352

[79] F. Dupuis, "The decoupling approach to quantum information theory," Ph.D. dissertation, Dept. Comput. Sci. Oper. Res., Université de Montréal, Montreal, QC, Canada, 2010.

[80] A. S. Holevo, "On entanglement-assisted classical capacity," *J. Math. Phys.*, vol. 43, no. 9, pp. 4326–4333, Sep. 2002.

[81] M.-H. Hsieh, I. Devetak, and A. Winter, "Entanglement-assisted capacity of quantum multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3078–3090, Jul. 2008.

[82] M. E. Shirokov, "Conditions for coincidence of the classical capacity and entanglement-assisted capacity of a quantum channel," *Problems Inf. Transmiss.*, vol. 48, no. 2, pp. 85–101, Apr. 2012.

[83] N. Datta and M.-H. Hsieh, "One-shot entanglement-assisted quantum and classical communication," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1929–1939, Mar. 2013.

[84] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, Feb. 2014.

[85] J. Qian and L. Zhang, "On MDS linear complementary dual codes and entanglement-assisted quantum codes," *Designs, Codes Cryptogr.*, vol. 86, no. 7, pp. 1565–1572, Jul. 2018.

[86] A. Anshu, R. Jain, and N. A. Warsi, "One shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach," 2017, *arXiv:1702.01940*. [Online]. Available: http://arxiv.org/abs/1702.01940

[87] M. Berta, H. Gharibyan, and M. Walter, "Entanglement-assisted capacities of compound quantum channels," *IEEE Trans. Inf. Theory*, vol. 63, no. 5, pp. 3306–3321, May 2017.

[88] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum Internet (Invited paper)," 2019, *arXiv:1907.06197*. [Online]. Available: http://arxiv.org/abs/1907.06197

[89] A. Anshu, R. Jain, and N. A. Warsi, "On the near-optimality of one-shot classical communication over quantum channels," *J. Math. Phys.*, vol. 60, no. 1, Jan. 2019, Art. no. 012204.

[90] H. Boche, N. Cai, and J. Nötzel, "The classical-quantum channel with random state parameters known to the sender," *J. Phys. A, Math. Theor.*, vol. 49, no. 19, Apr. 2016, Art. no. 195302.

[91] U. Pereg, "Communication over quantum channels with parameter estimation," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 1818–1823.

[92] U. Pereg, "Communication over quantum channels with parameter estimation," Jan. 2020, *arXiv:2001.00836*. [Online]. Available: http://arxiv.org/abs/2001.00836

[93] N. A. Warsi and J. P. Coon, "Coding for classical-quantum channels with rate limited side information at the encoder: Information-spectrum approach," *IEEE Trans. Inf. Theory*, vol. 63, no. 5, pp. 3322–3331, May 2017.

[94] F. Dupuis, "The capacity of quantum channels with side information at the transmitter," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 948–952.

[95] U. Pereg, "Entanglement-assisted capacity of quantum channels with side information," in *Proc. Int. Zürich Seminar Inf. Commun. (IZS)*, Zürich, Switzerland, Feb. 2020, pp. 1–24.

[96] U. Pereg, "Entanglement-assisted capacity of quantum channels with side information," Sep. 2019, *arXiv:1909.09992*. [Online]. Available: http://arxiv.org/abs/1909.09992

[97] Z. Luo and I. Devetak, "Channel simulation with quantum side information," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1331–1342, Mar. 2009.

[98] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 1, pp. 1–10, Jan. 1976.

[99] I. Devetak and A. Winter, "Classical data compression with quantum side information," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 4, Oct. 2003, Art. no. 042301.

[100] J. T. Yard and I. Devetak, "Optimal quantum source coding with quantum side information at the encoder and decoder," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5339–5351, Nov. 2009.

[101] M.-H. Hsieh and S. Watanabe, "Channel simulation and coded source compression," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6609–6619, Nov. 2016.

[102] N. Datta, C. Hirche, and A. Winter, "Convexity and operational interpretation of the quantum information bottleneck function," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 1157–1161.

[103] N. Datta, C. Hirche, and A. Winter, "Convexity and operational interpretation of the quantum information bottleneck function," 2018, *arXiv:1810.03644*. [Online]. Available: http://arxiv.org/abs/1810.03644

[104] H.-C. Cheng, E. P. Hanson, N. Datta, and M.-H. Hsieh, "Duality between source coding with quantum side information and c-q channel coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 1142–1146.

[105] H.-C. Cheng, E. P. Hanson, N. Datta, and M.-H. Hsieh, "Duality between source coding with quantum side information and c-q channel coding," 2018, *arXiv:1809.11143*. [Online]. Available: http://arxiv.org/abs/1809.11143

[106] Z. B. Khanian and A. Winter, "Distributed compression of correlated classical-quantum sources or: The price of ignorance," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5620–5633, Sep. 2020.

[107] Z. B. Khanian and A. Winter, "Entanglement-assisted quantum data compression," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 1147–1151.

[108] Z. B. Khanian and A. Winter, "Entanglement-assisted quantum data compression," 2019, *arXiv:1901.06346*. [Online]. Available: http://arxiv.org/abs/1901.06346

[109] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems Inf. Transmiss.*, vol. 40, no. 4, pp. 318–336, Oct. 2004.

[110] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 461, no. 2053, pp. 207–235, Jan. 2005.

[111] M.-H. Hsieh, Z. Luo, and T. Brun, "Secret-key-assisted private classical communication capacity over quantum channels," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 4, Oct. 2008, Art. no. 042306.

[112] K. Li, A. Winter, X. Zou, and G. Guo, "Private capacity of quantum channels is not additive," *Phys. Rev. Lett.*, vol. 103, no. 12, Sep. 2009, Art. no. 120501.

[113] M. M. Wilde, "Comment on 'Secret-key-assisted private classical communication capacity over quantum channels,'" *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 4, Apr. 2011, Art. no. 046303.

[114] S. Watanabe, "Private and quantum capacities of more capable and less noisy quantum channels," *Phys. Rev. A, Gen. Phys.*, vol. 85, no. 1, Jan. 2012, Art. no. 012326.

[115] D. Elkouss and S. Strelchuk, "Superadditivity of private information for any number of uses of the channel," *Phys. Rev. Lett.*, vol. 115, no. 4, Jul. 2015, Art. no. 040501.

[116] A. Anshu, M. Hayashi, and N. A. Warsi, "Secure communication over fully quantum Gel'fand-Pinsker wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 2679–2683.

[117] H. Qi, K. Sharma, and M. M. Wilde, "Entanglement-assisted private communication over quantum broadcast channels," *J. Phys. A, Math. Theor.*, vol. 51, no. 37, Sep. 2018, Art. no. 374001.

[118] K. Sharma, E. Wakakuwa, and M. M. Wilde, "Conditional quantum one-time pad," 2017, *arXiv:1703.02903*. [Online]. Available: http://arxiv.org/abs/1703.02903

[119] H. Boche, M. Cai, C. Deppe, and J. Nötzel, "Classical-quantum arbitrarily varying wiretap channel: Common randomness assisted code and continuity," *Quantum Inf. Process.*, vol. 16, no. 1, p. 35, Jan. 2017.

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

[121] R. König, R. Renner, A. Bariska, and U. Maurer, "Small accessible quantum information does not imply security," *Phys. Rev. Lett.*, vol. 98, no. 14, Apr. 2007, Art. no. 140502.

[122] S. Guha *et al.*, "Quantum enigma machines and the locking capacity of a quantum channel," *Phys. Rev. X*, vol. 4, no. 1, Jan. 2014, Art. no. 011016.

[123] C. Lupo, M. M. Wilde, and S. Lloyd, "Quantum data hiding in the presence of noise," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3745–3756, Jun. 2016.

[124] F. Salek, M.-H. Hsieh, and J. R. Fonollosa, "Publicness, privacy and confidentiality in the single-serving quantum broadcast channel," 2019, *arXiv:1903.04463*. [Online]. Available: http://arxiv.org/abs/1903.04463

[125] F. Salek, M.-H. Hsieh, and J. R. Fonollosa, "Publicness, privacy and confidentiality in the single-serving quantum broadcast channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 1712–1716.

[126] H. Aghaee and B. Akhbari, "Classical-quantum multiple access wiretap channel," in *Proc. 16th Int. (ISC), Conf. Inf. Secur. Cryptol. (ISCISC)*, Mashhad, Iran, Aug. 2019, pp. 99–103.

[127] H. Boche, G. Janßen, and S. Saeedinaeeni, "Universal superposition codes: Capacity regions of compound quantum broadcast channel with confidential messages," *J. Math. Phys.*, vol. 61, no. 4, Apr. 2020, Art. no. 042204.

[128] K. Modi, A. K. Pati, A. Sen, and U. Sen, "Masking quantum information is impossible," *Phys. Rev. Lett.*, vol. 120, no. 23, Jun. 2018, Art. no. 230501.

[129] S. H. Lie and H. Jeong, "Randomness cost of masking quantum information and the information conservation law," 2019, *arXiv:1908.07426*. [Online]. Available: http://arxiv.org/abs/1908.07426

[130] S. H. Lie, H. Kwon, M. S Kim, and H. Jeong, "Quantum one-time tables for unconditionally secure qubit-commitment," 2019, *arXiv:1903.12304*. [Online]. Available: http://arxiv.org/abs/1903.12304

[131] R. Alicki and M. Fannes, "Continuity of quantum conditional information," *J. Phys. A, Math. Gen.*, vol. 37, no. 5, pp. L55–L57, Jan. 2004.

[132] A. Winter, "Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints," *Commun. Math. Phys.*, vol. 347, no. 1, pp. 291–313, Oct. 2016.

[133] H. Boche, M. Cai, N. Cai, and C. Deppe, "Secrecy capacities of compound quantum wiretap channels and applications," *Phys. Rev. A, Gen. Phys.*, vol. 89, no. 5, May 2014, Art. no. 052320.

[134] J. Yard, P. Hayden, and I. Devetak, "Quantum broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7147–7162, Oct. 2011.

[135] C. King, K. Matsumoto, M. Nathanson, and M. B. Ruskai, "Properties of conjugate channels with applications to additivity and multiplicativity," *Markov Process Rel. Fields*, vol. 13, nos. 1–2, pp. 391–423, 2007.

[136] K. Brádler, P. Hayden, D. Touchette, and M. M. Wilde, "Trade-off capacities of the quantum Hadamard channels," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 6, Jun. 2010, Art. no. 062312.

[137] H. Boche and J. Nötzel, "Positivity, discontinuity, finite resources, and nonzero error for arbitrarily varying quantum channels," *J. Math. Phys.*, vol. 55, no. 12, Dec. 2014, Art. no. 122201.

[138] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Phys. Rev. Lett.*, vol. 78, no. 16, p. 3217, Apr. 1997.

[139] C. H. Bennett, "Quantum information's birth, growth, and impact on fundamental questions," in *Proc. Special Session Int. Symp. Inf. Theory (ISIT) Pers. Commun.*, Jul. 2019.

[140] K. Arora, J. Singh, and Y. S. Randhawa, "A survey on channel coding techniques for 5G wireless networks," *Telecommun. Syst.*, vol. 73, pp. 1–27, Nov. 2019.

[141] D. J. Costello and G. D. Forney, "Channel coding: The road to channel capacity," *Proc. IEEE*, vol. 95, no. 6, pp. 1150–1177, Jun. 2007.

[142] E. Nisioti and N. Thomos, "Design of capacity-approaching low-density parity-check codes using recurrent neural networks," 2020, *arXiv:2001.01249*. [Online]. Available: http://arxiv.org/abs/2001.01249

[143] T. Richardson and S. Kudekar, "Design of low-density parity check codes for 5G new radio," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 28–34, Mar. 2018.

[144] R. Ahlswede, "Towards a general theory of information transfer Pesonal communication following the Shannon," in *Proc. Shannon Lect. Int. Symp. Inf. Theory (ISIT) Pers. Commun.*, Jul. 2006.

[145] A. Uhlmann, "The 'transition probability' in the state space of a*-algebra," *Rep. Math. Phys.*, vol. 9, no. 2, pp. 273–279, 1976.

[146] M. Hamada, "Lower bounds on the quantum capacity and highest error exponent of general memoryless channels," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2547–2557, Sep. 2002.

[147] R. G. Gallager, *Information Theory and Reliable Communication*, vol. 2. New York, NY, USA: Springer, 1968.

[148] K. Li and A. Winter, "Relative entropy and squashed entanglement," *Commun. Math. Phys.*, vol. 326, no. 1, pp. 63–80, Jan. 2014.

[149] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 1, pp. 1–127, Feb. 2008.

[150] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5840–5847, Dec. 2009.

Uzi Pereg (Member, IEEE) received the B.Sc. degree *(summa cum laude)* in electrical engineering from the Azrieli College of Engineering, Jerusalem, Israel, in 2011, and the M.Sc. and Ph.D. degrees from the Technion–Israel Institute of Technology, Haifa, Israel, in 2015 and 2019, respectively. In 2020, he joined the Theory Group of the German Federal Government (BMBF) project for the design and analysis of quantum communication and repeater systems. He is currently a Post-Doctoral Researcher with the Institute for Communications Engineering, Technical University of Munich, Munich, Germany. His research interests include quantum communications, information theory, and coding theory. He was a recipient of the 2018 Pearl Award for outstanding research work in the field of communications, the 2018 KLA-Tencor Award for Excellent Conference Paper, the 2018–2019 Viterbi Fellowship, and the 2020–2021 Israel CHE Fellowship for Quantum Science and Technology.

Christian Deppe (Member, IEEE) received the Dipl.Math. and Dr. Math. degrees in mathematics from the Universität Bielefeld, Bielefeld, Germany, in 1996 and 1998, respectively. He was a Research and Teaching Assistant with the Fakultät für Mathematik, Universität Bielefeld, from 1998 to 2010. From 2011 to 2013, he was the Project Leader of the project Sicherheit und Robustheit des Quanten-Repeaters of the Federal Ministry of Education and Research, Fakultät für Mathematik, Universität Bielefeld. In 2014, he was supported by a DFG Project at the Institute of Theoretical Information Technology, Technische Universität München. In 2015, he had a Temporary Professorship with the Fakultät für Mathematik und Informatik, Friedrich-Schiller Universität Jena. Since 2018, he has been with the Department of Communications Engineering, Technische Universität München. He is currently the Project Leader of the project Abhörsichere Kommunikationüber Quanten-Repeater of the Federal Ministry of Education and Research, Fakultät für Mathematik, Universität Bielefeld.

Holger Boche (Fellow, IEEE) received the Dr.rer.nat. degree in pure mathematics from the Technische Universität Berlin, Berlin, Germany, in 1998, the Dipl.Ing. and Dr.Ing. degrees in electrical engineering from the Technische Universität Dresden, Dresden, Germany, in 1990 and 1994, respectively, and the degree in mathematics from the Technische Universität Dresden, in 1992. From 1994 to 1997, he was involved in postgraduate studies in mathematics with the Friedrich-Schiller Universität Jena, Jena, Germany. In 1997, he joined the Heinrich-HertzInstitut (HHI) für Nachrichtentechnik Berlin, Berlin. In 2002, he was a Full Professor of mobile communication networks with the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became the Director of the Fraunhofer German-Sino Laboratory for Mobile Communications, Berlin, and the Director of HHI in 2004. He was a Visiting Professor with ETH Zurich, Zürich, Switzerland, in Winter 2004 and 2006, and KTH Stockholm, Stockholm, Sweden, in Summer 2005. Since 2010, he has been with the Institute of Theoretical Information Technology and a Full Professor with the Technische Universität München, Munich, Germany. He is currently with the Institute of Theoretical Information Technology, Technische Universität München, the Munich Center for Quantum Science and Technology (MCQST), Munich, and the CASA–Cyber Security in the Age of Large-Scale Adversaries–Excellenzcluster, Ruhr Universität Bochum, Bochum, Germany. He was elected as a member of the German Academy of Sciences Leopoldina in 2008 and the Berlin Brandenburg Academy of Sciences and Humanities in 2009. Since 2014, he has been a member and an Honorary Fellow of the TUM Institute for Advanced Study, Munich. He is also a member of the IEEE Signal Processing Society SPCOM and the SPTM Technical Committee. He was a recipient of the Research Award Technische Kommunikation from the Alcatel SEL Foundation in 2003, the Innovation Award from the Vodafone Foundation in 2006, the Gottfried Wilhelm Leibniz Prize from the German Research Foundation in 2008, and the 2007 IEEE Signal Processing Society Best Paper Award, and a co-recipient of the 2006 IEEE Signal Processing Society Best Paper Award.