Quantum Inf Process (2012) 11:1465–1501
DOI 10.1007/s11128-011-0317-z

Public and private resource trade-offs for a quantum channel

Mark M. Wilde · Min-Hsiu Hsieh

Received: 20 May 2010 / Accepted: 1 October 2011 / Published online: 18 October 2011

Abstract Collins and Popescu realized a powerful analogy between several resources in classical and quantum information theory. The Collins–Popescu analogy states that public classical communication, private classical communication, and secret key interact with one another somewhat similarly to the way that classical communication, quantum communication, and entanglement interact. This paper discusses the information-theoretic treatment of this analogy for the case of noisy quantum channels. We determine a capacity region for a quantum channel interacting with the noiseless resources of public classical communication, private classical communication, and secret key. We then compare this region with the classical-quantum-entanglement region from our prior efforts and explicitly observe the information-theoretic consequences of the strong correlations in entanglement and the lack of a super-dense coding protocol in the public-private-secret-key setting. The region simplifies for several realistic, physically-motivated channels such as entanglement-breaking channels, Hadamard channels, and quantum erasure channels, and we are able to compute and plot the region for several examples of these channels.

Keywords Quantum Shannon theory · Public classical communication · Private classical communication · Secret key

M. M. Wilde (✉)
School of Computer Science, McGill University, Montreal, QC H3A 2A7, Canada
e-mail: mark.wilde@mcgill.ca

M.-H. Hsieh
ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency, 5-28-3, Hongo, Bunkyo-ku, Tokyo, Japan
e-mail: minhsiuh@gmail.com

Present Address:
M.-H. Hsieh
Statistical Laboratory, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WB, UK

1 Introduction

One of the first breakthroughs in quantum information theory was the discovery of a protocol for establishing secret correlations with the use of a quantum channel [3]. Such a task is now well known as quantum key distribution [40]. This thriving area of research has resulted in a currently available quantum technology, and efforts are now underway to construct space-to-ground quantum communication devices [38,47].

These initial results on quantum key distribution inspired the quantum information-theoretic study of secret communication over quantum channels, and this line of inquiry has subsequently led to an improved understanding of the relations between private classical information and quantum information. Schumacher and Westmoreland were one of the first to study this connection [42], and Collins and Popescu then discussed a useful analogy between the classical world and the quantum world [14]. The Collins–Popescu analogy states that the way that a public classical bit, a private classical bit, and a bit of secret key interact is qualitatively similar to the way that a classical bit, a quantum bit, and a bit of entanglement interact [14]. They justify this analogy operationally, by comparing the teleportation protocol [4] to the one-time pad protocol [48]. Teleportation consumes two classical bits and one maximally entangled pair to generate a qubit channel, whereas the one-time pad protocol consumes one public bit and a bit of secret key to establish a private classical bit. A qubit channel can establish entanglement, and a private classical bit channel can establish a bit of secret key—these protocols have the respective names entanglement distribution and secret key distribution. Additionally, a qubit channel can generate a classical bit, and a private classical bit channel can generate a public classical bit.[1] But the lack of an analogy of the super-dense coding protocol [6] in the public-private-secret-key setting is where this analogy breaks down.

Shortly after this initial work, Devetak and Cai et al. independently established the private capacity of a quantum channel as one of its fundamental capacities [13,16]. These results and the ideas involved are formally similar to private information transmission in the classical setting [1,2,15,36,51]. In addition to determining the private classical capacity, Devetak provided a good lower bound on the quantum capacity of a quantum channel by showing how to construct good quantum error-correcting codes from classical codes that transmit classical information privately [16]. Devetak and Winter continued these efforts, demonstrating many further important connections between private classical information and quantum information [18,19], and Smith et al. then employed these capacity formulas to determine good bounds on the secret key rate of the standard protocol for quantum key distribution [46].

In this article, we study how a noisy quantum channel interacts with the noiseless resources of public classical communication, private classical communication, and secret key. That is, we determine trade-off formulas for how a sender and receiver can use any of the noiseless resources to assist a noisy quantum channel in generating any of the other noiseless resources. In earlier work, we determined trade-off formulas in the setting where the noiseless resources are classical communication, quantum

[1] This latter protocol, that we call private-to-public transmission, follows from the particular communication model that we consider in this paper.

communication, and entanglement [29–31,50]. Thus, one could view the present work as the completion of the information-theoretic treatment of the Collins–Popescu analogy (at least for the case of channels) that began in the aforementioned papers and continued in Refs. [17,27].

Our main result is the private dynamic capacity theorem. This theorem determines the capabilities for a noisy quantum channel to generate any of the three noiseless classical resources when assisted by the others. The rates in the private dynamic capacity region can be either positive or negative, depending on whether a protocol generates or consumes a given resource, respectively. The result of this theorem is that combinations of only four protocols are sufficient to generate the entire capacity region: the publicly-enhanced private father protocol [28], the one-time pad protocol, secret key distribution, and private-to-public transmission. This result is in line with the Collins–Popescu analogy because we found that the classically-enhanced father protocol [31], teleportation, entanglement distribution, and super-dense coding are sufficient to realize the quantum dynamic capacity region of a quantum channel [29–31,50]. This theorem also explicitly demonstrates the aforementioned breakdown of the Collins–Popescu analogy—the last two inequalities in each theorem are similar by inspection, but the first one in each is different because of the lack of a super-dense coding protocol in the public-private-secret-key setting and because the rates in teleportation and the one-time pad protocol are different.

We also explicitly compute and plot the private dynamic capacity region for several realistic, physically motivated quantum channels: entanglement-breaking channels [25,43], dephasing channels, cloning channels [8–11], and erasure channels [23]. Entanglement-breaking channels have application in entanglement detection protocols [33,39]. Dephasing noise occurs in superconducting qubit systems [12], the cloning channel represents a natural process that occurs during stimulated emission [34,37,44], and the erasure channel is a simplified model for photon loss [20,21,35,49]. Brádler et al. pointed out in Ref. [11] that both dephasing channels and cloning channels are examples of Hadamard channels [32], and this Hadamard property is useful in proving that the private dynamic capacity region is tractable. The proof for the quantum erasure channel follows by exploiting its particular structure. We prove these results first by showing that a formula, named the private dynamic capacity formula, is additive for each of these channels. We then analyze each channel individually and show that a particular ensemble suffices to achieve the boundary points of the private dynamic capacity region.

We structure this paper as follows. We first review the communication model, some definitions, and notation that are essential in understanding the rest of the paper. Section 3 states the private dynamic capacity theorem and the next two sections prove the achievability part and the converse part. We then introduce the private dynamic capacity formula, show how its additivity implies that the computation of the capacity region boundary is a tractable convex optimization program, analyze special cases of the formula, and compare the region to the quantum dynamic capacity region from Refs. [29,30,50]. Sections 7 and 8 prove that the private dynamic capacity formula is additive for entanglement-breaking channels and the Hadamard class of channels, respectively. We finally compute and plot the private dynamic capacity region for

dephasing channels, cloning channels, and erasure channels in Sect. 9. We conclude with a discussion and some open problems.

2 Definitions and notation

We first establish some definitions and notation that we employ throughout the paper, and we review a few important properties of the entropy. Consider a random variable M with a uniform distribution on D values. Let $\overline{\Phi}^{M_A M_B}$ denote an embedding of this random variable into a maximally correlated state shared between two parties M_A and M_B:

$$\overline{\Phi}^{M_A M_B} \equiv \frac{1}{D} \sum_{m=1}^{D} |m\rangle\langle m|^{M_A} \otimes |m\rangle\langle m|^{M_B}. \tag{1}$$

A common randomness bit corresponds to the special case where $D = 2$. Suppose a third party Eve possesses a quantum system E. A state $\rho^{M_A M_B E}$ on the systems M_A, M_B, and E is a public common randomness state if

$$\begin{aligned} \mathrm{Tr}_E\{\rho^{M_A M_B E}\} &= \overline{\Phi}^{M_A M_B}, \\ \rho^{M_A M_B E} &\neq \overline{\Phi}^{M_A M_B} \otimes \sigma^E, \end{aligned}$$

for some state σ^E. The above conditions imply that Eve has some correlations with the above state and could learn about the random variable M by performing a measurement on her system. A state $\omega^{M_A M_B E}$ is a secret key state if

$$\begin{aligned} \mathrm{Tr}_E\{\omega^{M_A M_B E}\} &= \overline{\Phi}^{M_A M_B}, \\ \omega^{M_A M_B E} &= \overline{\Phi}^{M_A M_B} \otimes \sigma^E, \end{aligned}$$

for some state σ^E. In this case, Eve cannot learn anything about the random variable M by performing a measurement on her share of $\omega^{M_A M_B E}$.

A completely-positive trace-preserving (CPTP) map $\mathcal{N}^{A' \to B}$ is the most general map we consider that maps from a quantum system A' to another quantum system B (we usually call them "Alice" and "Bob"). It acts as follows on any density operator ρ:

$$\mathcal{N}^{A' \to B}(\rho) = \sum_k A_k \rho A_k^\dagger,$$

where the operators A_k satisfy the condition $\sum_k A_k^\dagger A_k = I$. A quantum channel admits an isometric extension $U_{\mathcal{N}}^{A' \to BE}$, which is a unitary embedding into a larger Hilbert space. One recovers the original channel by taking a partial trace over the "environment" system E (we usually call this system "Eve"). One obtains the complementary channel $(\mathcal{N}^c)^{A' \to E}$ by taking a partial trace over the system B.

A channel is degradable if there is a degrading map $\mathcal{D}^{B\to E}$ such that Bob can simulate the map to Eve [17]:

$$\forall \rho \qquad \mathcal{D}^{B\to E} \circ \mathcal{N}^{A'\to B}(\rho) = \left(\mathcal{N}^{c}\right)^{A'\to E}(\rho).$$

A channel is antidegradable if there is a map $\mathcal{T}^{E\to B}$ such that Eve can simulate the map to Bob:

$$\forall \rho \qquad \mathcal{T}^{E\to B} \circ \left(\mathcal{N}^{c}\right)^{A'\to E}(\rho) = \mathcal{N}^{A'\to B}(\rho).$$

A channel $\mathcal{N}_{\mathrm{EB}}^{A'\to B}$ is entanglement-breaking if its output is a separable state whenever the input is entangled [25,43]:

$$\mathcal{N}_{\mathrm{EB}}^{A'\to B}(|\Gamma\rangle\langle\Gamma|^{AA'}) = \sum_{x} p_X(x)\,\sigma_x^A \otimes \theta_x^B.$$

Such a channel is antidegradable and the antidegrading map consists of two parts: 1) a measurement of the system E that gives a classical variable and 2) a state preparation conditional on the classical outcome of the measurement. A quantum Hadamard channel is one whose complementary channel is entanglement-breaking [32]. It is thus degradable with a similar degrading map that consists of a measurement and state preparation.

We employ a particular model of communication in this paper (depicted in Fig. 1). We define a public channel as one for which an eavesdropper Eve can gain some information about what Alice and Bob transmit over it. A private channel is one for which Eve cannot gain any information about what they transmit. In this model, we

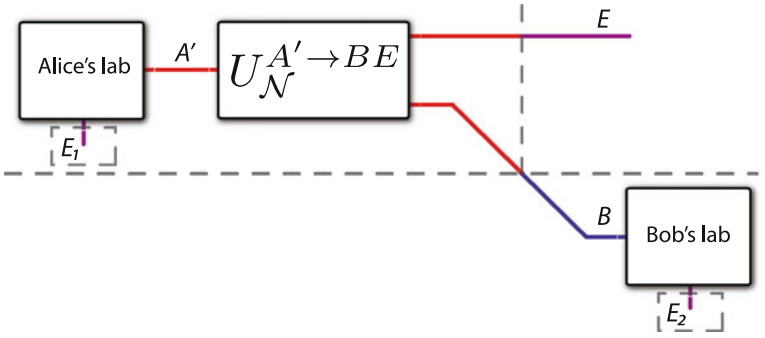

Fig. 1 (Color online) The communication model in this paper. Alice can prepare local states in her lab and choose to send them through a noisy channel or dump them locally at no cost in a bin E_1 to which Eve has access. We depict the isometric extension $U_{\mathcal{N}}^{A'\to BE}$ of the channel $\mathcal{N}^{A'\to B}$ and give Eve full access to the environment E of the channel. Bob receives the output B of the channel and can process it locally at his end or dump it in a bin E_2 to which Eve has access. In this model, Alice and Bob can simulate a public classical channel from a private classical channel because Bob can choose to dispose quantum states in the bin E_2 to which Eve has access

give Eve access to the environment of a noisy quantum channel and particular registers that Alice and Bob can discard locally from their laboratories. We do not count this discarding as a resource because it results from local actions that Alice and Bob take. This particular model allows us to make close contact with the result from the classical-quantum-entanglement trade-off [29–31,50].

We consider a three-dimensional capacity region throughout this work (as in Ref. [30]), whose points (R, P, S) correspond to rates of public classical communication, private classical communication, and secret key generation/consumption, respectively. For example, the one-time pad protocol corresponds to the following point:

$$(-1, 1, -1)\,,$$

because it consumes a public bit and a bit of secret in order to generate a private bit. Secret key distribution corresponds to

$$(0, -1, 1)\,,$$

and a private-to-public transmission corresponds to

$$(1, -1, 0)\,.$$

The entropy $H(A)_\rho$ of a density operator ρ^A on some quantum system A is as follows:

$$H(A)_\rho \equiv -\text{Tr}\left\{\rho^A \log \rho^A\right\},$$

where the logarithm is base two. The entropy can never exceed the logarithm of the dimension of system A. The quantum mutual information of a bipartite density operator ρ^{AB} is

$$I(A;B)_\rho \equiv H(A)_\rho + H(B)_\rho - H(AB)_\rho\,,$$

and the conditional quantum mutual information for a tripartite state ρ^{ABC} is

$$I(A;B|C)_\rho = H(AC)_\rho + H(BC)_\rho - H(C)_\rho - H(ABC)_\rho\,.$$

The quantum mutual information obeys a chain rule:

$$I(AB;C)_\rho = I(A;C)_\rho + I(B;C|A)_\rho\,. \tag{2}$$

A classical-quantum state σ^{XYBE} of the following form plays an important role throughout this paper:

$$\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}(x,y)\,|x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_{x,y}^{A'}),$$

where the states $\rho_{x,y}^{A'}$ are mixed states and $U_{\mathcal{N}}^{A'\to BE}$ is the isometric extension of some noisy channel $\mathcal{N}^{A'\to B}$. Applying the above chain rule gives the following relation:

$$I\left(YX;B\right)_{\sigma} = I\left(X;B\right)_{\sigma} + I\left(Y;B|X\right)_{\sigma}. \tag{3}$$

An accessible introduction to concepts in quantum Shannon theory is available in Yard's thesis [52].

3 The private dynamic capacity theorem

The private dynamic capacity theorem gives bounds on the reliable communication rates of a noisy quantum channel when combined with the noiseless resources of public classical communication, private classical communication, and a secret key. The theorem applies regardless of whether a protocol consumes the noiseless resources or generates them.

Theorem 1 (Private Dynamic Capacity) *The private dynamic capacity region $\mathcal{C}_{\mathrm{RPS}}(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is equal to the following expression:*

$$\mathcal{C}_{\mathrm{RPS}}(\mathcal{N}) = \overline{\bigcup_{k=1}^{\infty} \frac{1}{k}\mathcal{C}_{\mathrm{RPS}}^{(1)}(\mathcal{N}^{\otimes k})}, \tag{4}$$

where the overbar indicates the closure of a set. The "one-shot" region $\mathcal{C}_{\mathrm{RPS}}^{(1)}(\mathcal{N})$ is the union of the "one-shot, one-state" regions $\mathcal{C}_{\mathrm{RPS},\sigma}^{(1)}(\mathcal{N})$:

$$\mathcal{C}_{\mathrm{RPS}}^{(1)}(\mathcal{N}) \equiv \bigcup_{\sigma} \mathcal{C}_{\mathrm{RPS},\sigma}^{(1)}(\mathcal{N}).$$

The "one-shot, one-state" region $\mathcal{C}_{\mathrm{RPS},\sigma}^{(1)}(\mathcal{N})$ is the set of all rates R, P, and S such that

$$R + P \leq I\left(YX;B\right)_{\sigma}, \tag{5}$$

$$P + S \leq I\left(Y;B|X\right)_{\sigma} - I\left(Y;E|X\right)_{\sigma}, \tag{6}$$

$$R + P + S \leq I\left(YX;B\right)_{\sigma} - I\left(Y;E|X\right)_{\sigma}. \tag{7}$$

The above entropic quantities are with respect to a classical-quantum state σ^{XYBE} where

$$\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}\left(x,y\right)|x\rangle\langle x|^{X} \otimes |y\rangle\langle y|^{Y} \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_{x,y}^{A'}), \tag{8}$$

and the states $\rho_{x,y}^{A'}$ are mixed. It is implicit that one should consider states on A'^{k} instead of A' when taking the regularization in (4).

The above theorem is a "multi-letter" capacity theorem because of the regularization in (4). Though, we show later that the regularization is not necessary for entanglement-breaking channels, the Hadamard class of channels, or the quantum erasure channels. We prove the private dynamic capacity theorem in two parts:

1. The direct coding theorem below shows that combining the "publicly-enhanced private father protocol" with the one-time pad, secret key distribution, and private-to-public transmission achieves the above region.
2. The converse theorem demonstrates that any coding scheme cannot do better than the regularization in (4), in the sense that a scheme with vanishing error should have its rates below the above amounts. We prove the converse theorem directly in "one fell swoop," by employing a catalytic, information-theoretic approach (similar to the method introduced in Ref. [50]).

4 Dynamic achievable rate region

The unit resource achievable region is what Alice and Bob can achieve with the protocols secret key distribution, the one-time pad, and private-to-public transmission. It is the cone of the rate triples corresponding to these protocols:

$$\{\alpha\,(0,-1,1)+\beta\,(-1,1,-1)+\gamma\,(1,-1,0):\alpha,\beta,\gamma\geq 0\}\,.$$

We can also write any rate triple (R, P, S) in the unit resource capacity region with a matrix equation:

$$\begin{bmatrix} R \\ P \\ S \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}. \tag{9}$$

The inverse of the above matrix is as follows:

$$\begin{bmatrix} -1 & -1 & 0 \\ -1 & -1 & -1 \\ 0 & -1 & -1 \end{bmatrix},$$

and gives the following set of inequalities for the unit resource achievable region:

$$\begin{aligned} R+P &\leq 0,\\ R+P+S &\leq 0,\\ P+S &\leq 0, \end{aligned}$$

by inverting the matrix equation in (9) and applying the constraints $\alpha, \beta, \gamma \geq 0$.

Now, let us include the publicly-enhanced private father protocol [28]. Hsieh and Wilde [28] proved that we can achieve the following rate triple by channel coding over a noisy quantum channel $\mathcal{N}^{A'\to B}$:

$$(I(X;B)_\sigma, I(Y;B|X)_\sigma, -I(Y;E|X)_\sigma),$$

for any state σ^{XYBE} of the form:

$$\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}(x,y)\,|x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_{x,y}^{A'}), \tag{10}$$

where $U_{\mathcal{N}}^{A'\to BE}$ is an isometric extension of the quantum channel $\mathcal{N}^{A'\to B}$. Specifically, we showed in Ref. [28] that one can achieve the above rates with vanishing error in the limit of large blocklength. Thus the achievable rate region is the following translation of the unit resource achievable region in (9):

$$\begin{bmatrix} R \\ P \\ S \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} + \begin{bmatrix} I(X;B)_\sigma \\ I(Y;B|X)_\sigma \\ -I(Y;E|X)_\sigma \end{bmatrix}.$$

We can now determine bounds on an achievable rate region that employs the above coding strategy. We apply the inverse of the matrix in (9) to the LHS and RHS. Then using the constraints $\alpha, \beta, \gamma \geq 0$, we obtain the inequalities in (5–7), corresponding exactly to the one-shot, one-state region in Theorem 1. Taking the union over all possible states σ in (10) and taking the regularization gives the full private dynamic achievable rate region.

5 Catalytic and information theoretic converse proof

This section provides a catalytic, information theoretic converse proof of the private dynamic capacity region, showing that (4) gives a multi-letter characterization of it. The catalytic approach means that we are considering the most general protocol that *consumes and generates* public classical communication, private classical communication, and secret key in addition to the uses of the noisy quantum channel. Figure 2 depicts the most general protocol for generating public classical communication, private classical communication, and a secret key with the consumption of a noisy quantum channel $\mathcal{N}^{A'\to B}$ and the same respective resources. This approach has the advantage that we can prove the converse theorem in "one fell swoop." We employ the Alicki-Fannes' inequality, the chain rule for quantum mutual information, elementary properties of quantum entropy, and the quantum data processing inequality to prove the converse.

There are some subtleties in our proof for the converse theorem. We prove that the bounds in (5–7) hold for common randomness generation and private key generation instead of public classical communication and private classical communication, respectively, because a capacity for generating common randomness and a private key can only be better than that for generating public classical communication and private classical communication. This setting is slightly different from that depicted in Fig. 2.

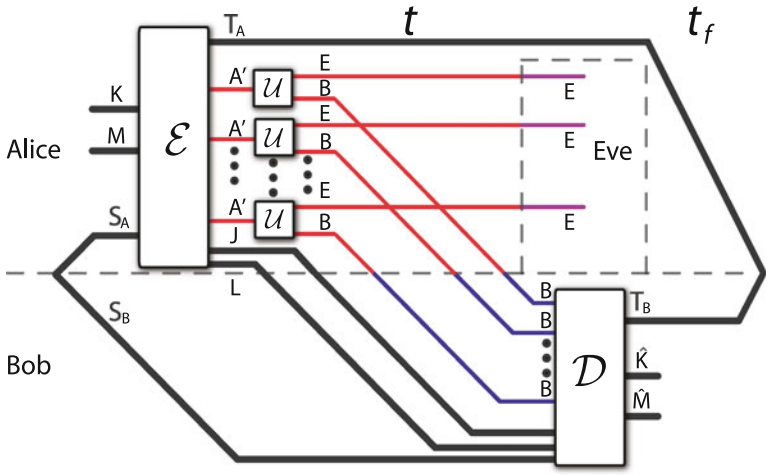

Fig. 2 (Color online) The most general protocol for generating public classical communication, private classical communication, and secret key with the help of the same respective resources and many uses of a noisy quantum channel. Alice begins with her public classical register K, her private classical register M, and her share of the secret key in S_A. She encodes according to some CPTP encoding map $\mathcal{E}$ that outputs a classical register T_A, many quantum registers A'^n, a public classical register L, and a private classical register J. She inputs A'^n to many uses of the noisy channel $\mathcal{N}^{A'\to B}$ (with isometric extension $U_{\mathcal{N}}^{A'\to BE}$), transmits J over a noiseless private classical channel, and transmits L over a noiseless public classical channel. Bob receives the channel outputs B^n, the private classical register J, and the public classical register L and performs a decoding $\mathcal{D}$ that recovers the public and private classical information. The decoding also generates secret key with system T_A

We prove that the converse theorem holds for a state of the following form:

$$\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}(x,y)\,|x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_{x,y}^{A'}), \tag{11}$$

where the states $\rho_{x,y}^{A'}$ are mixed.

We prove all three bounds in (5–7). Alice possesses the following classical registers:

1. Two public classical registers K and K_A in the maximally correlated state $\overline{\Phi}^{KK_A}$ where the dimension of both systems is $2^{n\overline{R}}$. The register K_A is for public classical communication.
2. Two private classical registers M and M_A in the maximally correlated state $\overline{\Phi}^{MM_A}$ where the dimension of both systems is $2^{n\overline{P}}$. The register M_A is for private classical communication.
3. One share S_A of a secret key. The shared secret key is in the maximally correlated state $\overline{\Phi}^{S_AS_B}$ where the dimension of both systems is $2^{n\widetilde{S}}$. Bob possesses the other share S_B of the secret key.

Our convention above is that the protocol generates a resource whose rate has an overbar and consumes a resource whose rate has a tilde.

The initial state is as follows:

$$\omega^{MM_AKK_AS_AS_B} \equiv \overline{\Phi}^{MM_A} \otimes \overline{\Phi}^{KK_A} \otimes \overline{\Phi}^{S_AS_B}.$$

She passes the registers K_A, M_A, and S_A into an encoding map $\mathcal{E}^{K_AM_AS_A\to A'^nT_ALJ}$. This map outputs a classical register T_A of dimension $2^{n\overline{S}}$, a public classical register L of dimension $2^{n\tilde{R}}$, a private classical register J of dimension $2^{n\tilde{P}}$, and many quantum systems A'^n for input to the channel. The register T_A is for creating a secret key with Bob. The state after this encoding map is as follows:

$$\omega^{MKS_BA'^nT_ALJ} \equiv \mathcal{E}^{K_AM_AS_A\to A'^nT_ALJ}(\omega^{MM_AKK_AS_AS_B}).$$

She sends the systems A'^n through many uses $\mathcal{N}^{A'^n\to B^n}$ of the noisy channel $\mathcal{N}^{A'\to B}$, transmits L over a noiseless public classical channel, and transmits J over a noiseless private classical channel, producing the following state:

$$\omega^{MKB^nE^nT_ALJS_B} \equiv U_{\mathcal{N}}^{A'^n\to B^nE^n}(\omega^{MKS_BA'^nT_ALJ}), \tag{12}$$

where $U_{\mathcal{N}}^{A'^n\to B^nE^n}$ is the isometric extension of the channel $\mathcal{N}^{A'^n\to B^n}$. The above state is a state of the form in (11) with $X \equiv KL$ and $Y \equiv MJS_BT_A$. Bob then applies a map $\mathcal{D}^{B^nS_BLJ\to T_B\hat{M}\hat{K}}$ that outputs classical registers T_B, $\hat{M}$, $\hat{K}$. Let ω' denote the final state.

The following condition should hold for a catalytic private dynamic protocol that transmits the public and private classical data and establishes secret key with ϵ-error:

$$\left\| \overline{\Phi}^{M\hat{M}} \otimes \rho^{K\hat{K}E^n} \otimes \overline{\Phi}^{T_AT_B} - \left(\omega'\right)^{M\hat{M}K\hat{K}E^nT_AT_B} \right\|_1 \leq \epsilon, \tag{13}$$

where $\rho^{K\hat{K}E^n}$ is some state such that $\mathrm{Tr}_{E^n}\{\rho^{K\hat{K}E^n}\} = \overline{\Phi}^{K\hat{K}}$. Condition (13) implies that Alice and Bob establish maximal classical correlations in M and $\hat{M}$, in K and $\hat{K}$, and in T_A and T_B. The following security condition should hold as well:

$$\left\| \omega^{MKE^nT_ALJS_B} - \pi^{MT_AJS_B} \otimes \sigma^{KLE^n} \right\|_1 \leq \epsilon,$$

where $\omega^{MKE^nT_ALJS_B}$ is the state in (12) obtained from tracing over Bob's systems, π is the maximally mixed state, and σ^{KLE^n} is some state on the public registers and Eve's systems. This security criterion implies that Eve cannot learn anything about any of the private data if she has access to all of the public data in addition to her registers. It also implies that the following information-theoretic bound holds:

$$I\left(MJS_BT_A; E^nKL\right)_\omega \leq \epsilon. \tag{14}$$

The net rate triple for the protocol is as follows: $(\overline{R} - \widetilde{R}, \overline{P} - \widetilde{P}, \overline{S} - \widetilde{S})$. The protocol generates a resource if its corresponding rate is positive, and it consumes a resource if its corresponding rate is negative.

We prove the first bound in (5). Consider the following chain of inequalities:

$$\begin{aligned}
n\left(\overline{R} + \overline{P}\right) &= I(KM; \hat{K}\hat{M})_{\overline{\Phi}\otimes\overline{\Phi}} \\
&\leq I(KM; \hat{K}\hat{M})_{\omega'} + n\delta' \\
&\leq I\left(KM; B^n LJS_B\right)_\omega \\
&= I(KM; B^n LJ|S_B)_\omega \\
&= H(KMS_B)_\omega + H(B^n LJS_B)_\omega - H(KMB^n LJS_B)_\omega - H(S_B)_\omega \\
&\leq H(KMS_B)_\omega + H(B^n)_\omega + H(LJS_B)_\omega - H(KMB^n LJS_B)_\omega - H(S_B)_\omega \\
&= I(KLMJS_B; B^n)_\omega - H(KLMJS_B)_\omega + H(KMS_B)_\omega \\
&\quad + H(LJS_B)_\omega - H(S_B)_\omega \\
&= I(KLMJS_B; B^n)_\omega + I(KM; LJ|S_B)_\omega \\
&\leq I(KLMJS_BT_A; B^n)_\omega + I(KM; LJ|S_B)_\omega \\
&\leq I(XY; B^n)_\omega + n(\widetilde{R} + \widetilde{P}).
\end{aligned}$$

The first equality follows by evaluating the mutual information $I(MK; \hat{M}\hat{K})$ on the state $\overline{\Phi}^{K\hat{K}} \otimes \overline{\Phi}^{M\hat{M}}$. The first inequality follows from the condition in (13) and an application of the Alicki-Fannes' inequality where δ' vanishes as $\epsilon \to 0$. We suppress this term in the rest of the inequalities for convenience. The second inequality follows from quantum data processing. The second equality follows by applying the mutual information chain rule in (2) and because $I(KM; S_B)_\omega = 0$ for this protocol. The third equality follows from expanding the conditional mutual information $I(KM; B^n LJ|S_B)_\omega$. The third inequality follows by subadditivity of the entropy $H(B^n LJS_B)_\omega$. The fourth equality follows because

$$H(B^n)_\omega - H(KMB^n LJS_B)_\omega = I(KLMJS_B; B^n)_\omega - H(KLMJS_B)_\omega,$$

and the fifth equality follows because

$$-H(KLMJS_B)_\omega + H(KMS_B)_\omega + H(LJS_B)_\omega - H(S_B)_\omega = I(KM; LJ|S_B)_\omega.$$

The fourth inequality follows from quantum data processing. The final inequality follows from the definitions $X \equiv KL$ and $Y \equiv MJS_BT_A$ and because the quantum mutual information $I(KM; LJ|S_B)_\omega$ can never be larger than the logarithm of the dimension of the classical registers LJ.

We now prove the bound in (6). Consider the following chain of inequalities:

$$\begin{aligned}
n\left(\overline{P} + \overline{S}\right) &= I(MT_A; \hat{M}T_B)_{\overline{\Phi}\otimes\overline{\Phi}} \\
&\leq I(MT_A; \hat{M}T_B)_{\omega'} + n\delta' \\
&\leq I(MT_A; B^n JLKS_B)_\omega
\end{aligned}$$

$$
\begin{aligned}
&\leq I(MT_A; B^n JLKS_B)_\omega - I(MT_A JS_B; E^n KL)_\omega + \epsilon \\
&= I(MT_A; B^n JS_B|KL)_\omega + I(MT_A; KL)_\omega - I(MT_A JS_B; E^n|KL)_\omega \\
&\quad - I(MT_A JS_B; KL)_\omega + \epsilon \\
&= I(MT_A JS_B; B^n|KL)_\omega + I(MT_A; JS_B|KL)_\omega - I(B^n; JS_B|KL)_\omega \\
&\quad + I(MT_A; KL)_\omega - I(MT_A JS_B; KL)_\omega - I(MT_A JS_B; E^n|KL)_\omega + \epsilon \\
&\leq I(MT_A JS_B; B^n|KL)_\omega - I(MT_A JS_B; E^n|KL)_\omega \\
&\quad + I(MT_A; JS_B|KL)_\omega + \epsilon \\
&\leq I(Y; B^n|X)_\omega - I(Y; E^n|X)_\omega + n(\widetilde{P} + \widetilde{S}) + \epsilon.
\end{aligned}
$$

The first equality follows by evaluating the entropy for the state $\overline{\Phi}^{T_A T_B} \otimes \overline{\Phi}^{M\hat{M}}$. The first inequality follows from the condition in (13) and an application of the Alicki-Fannes' inequality where $\delta' \to 0$ as $\epsilon \to 0$. We suppress this term in the rest of the inequalities for convenience. The second inequality follows from quantum data processing. The third inequality follows from the bound in (14) on Eve's information. The second and third equalities follow from the chain rule for quantum mutual information. The fourth inequality follows from quantum data processing $I(MT_A JS_B; KL)_\omega \geq I(MT_A; KL)_\omega$ and the fact that $I(B^n; JS_B|KL)_\omega \geq 0$. The last inequality follows from the definitions $X \equiv KL$ and $Y \equiv MJS_B T_A$ and because the mutual information $I(MT_A; JS_B|KL)_\omega$ can never be larger than the logarithm of the dimensions of the registers J, S_B.

We finally prove the bound in (7). Consider the following chain of inequalities:

$$
\begin{aligned}
n\left(\overline{R} + \overline{P} + \overline{S}\right) &= I(KMT_A; \hat{K}\hat{M}T_B)_{\overline{\Phi}\otimes\overline{\Phi}\otimes\overline{\Phi}} \\
&\leq I(KMT_A; \hat{K}\hat{M}T_B)_{\omega'} + n\delta' \\
&\leq I(KMT_A; B^n JLS_B)_\omega \\
&\leq I(KMT_A; B^n JLS_B)_\omega - I(MT_A JS_B; E^n|KL)_\omega + \epsilon \\
&= I(KLMT_A JS_B; B^n)_\omega + I\left(JLS_B; KMT_A\right)_\omega - I\left(JLS_B; B^n\right)_\omega \\
&\quad - I(MT_A JS_B; E^n|KL)_\omega + \epsilon \\
&\leq I(YX; B^n)_\omega - I(Y; E^n|X)_\omega + n(\widetilde{R} + \widetilde{P} + \widetilde{S}) + \epsilon.
\end{aligned}
$$

The first equality follows by evaluating the entropy for the state $\overline{\Phi}^{K\hat{K}} \otimes \overline{\Phi}^{M\hat{M}} \otimes \overline{\Phi}^{T_A T_B}$. The first inequality follows from the condition in (13) and an application of the Alicki-Fannes' inequality where $\delta' \to 0$ as $\epsilon \to 0$. We suppress this term in the rest of the inequalities for convenience. The second inequality follows from quantum data processing. The third inequality follows from the condition in (14) (note that $I(MT_A JS_B; E^n|KL)_\omega + I(MT_A JS_B; KL)_\omega = I(MT_A JS_B; E^n KL)_\omega$ from the chain rule and both terms on the LHS are non-negative). The second equality follows from the chain rule for quantum mutual information. The final inequality follows from the definitions $X \equiv KL$ and $Y \equiv MJS_B T_A$, because $I\left(JLS_B; B^n\right)_\omega \geq 0$, and because the mutual information $I\left(JLS_B; KMT_A\right)_\omega$ can never be larger than the logarithm of the dimensions of the registers J, L, S_B.

6 The private dynamic capacity formula

The private dynamic capacity formula is a particular formula that is relevant in the computation of the private dynamic capacity region. If this formula is additive for a particular channel, then the computation of the region is a tractable convex optimization program [7]. The reasoning for this is similar to our discussion in Section 6 of Ref. [50], appealing to ideas from Pareto-optimal trade-off analysis (see Chapter 4 of Ref. [7]). Thus, we keep the discussion to a minimum here and instead refer the reader to Section 6 of Ref. [50] for further explanations.

Definition 1 (*Private Dynamic Capacity Formula*) The private dynamic capacity formula of a quantum channel $\mathcal{N}$ is as follows:

$$\begin{aligned} P_{\lambda,\mu}(\mathcal{N}) \equiv \max_{\sigma} I(YX;B)_{\sigma} + \lambda\left[I(Y;B|X)_{\sigma} - I(Y;E|X)_{\sigma}\right] \\ +\mu\left[I(YX;B)_{\sigma} - I(Y;E|X)_{\sigma}\right], \end{aligned} \tag{15}$$

where $\lambda, \mu \geq 0$.

Definition 2 The regularized private dynamic capacity formula is as follows:

$$P^{\text{reg}}_{\lambda,\mu}(\mathcal{N}) \equiv \lim_{n\to\infty} \frac{1}{n} P_{\lambda,\mu}\left(\mathcal{N}^{\otimes n}\right).$$

Lemma 1 *Suppose the private dynamic capacity formula is additive for channels $\mathcal{N}$ and $\mathcal{M}$:*

$$P_{\lambda,\mu}(\mathcal{N}\otimes\mathcal{M}) = P_{\lambda,\mu}(\mathcal{N}) + P_{\lambda,\mu}(\mathcal{M}).$$

Then the regularized private dynamic capacity formula is equal to the private dynamic capacity formula:

$$P^{reg}_{\lambda,\mu}(\mathcal{N}) = P_{\lambda,\mu}(\mathcal{N}).$$

In this sense, the regularized formula "single-letterizes" and it is not necessary to take the limit.

Proof The proof is similar to the proof of Lemma 1 in Ref. [50]. □

Theorem 2 *Single-letterization of the private dynamic capacity formula implies that the computation of the Pareto optimal trade-off surface (the boundary surface) of the private dynamic capacity region is a tractable convex optimization program.*

Proof The proof exploits the same techniques as the proof of Theorem 2 in Ref. [50]. □

6.1 Special cases of the private dynamic capacity formula

We now consider several special cases of the private dynamic capacity formula. These special cases have similar geometric interpretations as discussed in Section 6 of Ref. [50]. The first case corresponds to considering a supporting hyperplane of the capacity region with normal vector $(1, 1, 0)$, the second corresponds to considering a supporting hyperplane with normal vector $(0, 1, 1)$, and the last a supporting hyperplane with normal vector $(1, 1, 1)$. Each of these choices corresponds to singling out only one of the inequalities in Theorem 1 and maximizing with respect to that inequality.

Corollary 1 *The private dynamic capacity formula is equivalent to the HSW classical capacity formula [24,41] when $\lambda, \mu = 0$, in the sense that*

$$\max_{\sigma} I(YX; B)_{\sigma} = \max_{\rho^{XA'}} I(X; B)_{\rho},$$

where

$$\rho^{XA'} \equiv \sum_{x} p_X(x) |x\rangle\langle x|^X \otimes \rho_x^{A'},$$

and σ is a state of the form in Theorem 1.

Proof The proof of this statement follows merely by redefining the joint classical variable XY in the first formula to be the classical variable X in the second formula. □

Corollary 2 *The private dynamic capacity formula is equivalent to the Devetak–Cai–Winter–Yeung private classical capacity formula [13,16] in the limit where $\lambda \to \infty$ and μ is fixed, in the sense that*

$$\max_{\sigma} \left[I(Y; B|X)_{\sigma} - I(Y; E|X)_{\sigma} \right] = \max_{\rho^{XA'}} \left[I(X; B)_{\rho} - I(X; E)_{\rho} \right],$$

where ρ is a state of the form in the above corollary and σ is a state of the form in Theorem 1.

Proof The inequality LHS $\geq$ RHS follows by choosing the distribution $p_{X,Y}(x, y) = p_X(x)\, p_{Y|X}(y|x)$ with $p_{Y|X}(y|x) = p_X^*(y)$ and $p_X(x) = \delta_{x,x_0}$ and choosing the conditional density operators $\rho_{x_0,y}^{A'} = \left(\rho_x^*\right)^{A'}$ where the asterisked quantities are optimal for the RHS. The inequality LHS $\leq$ RHS follows because the quantity $I(Y; B|X)_{\sigma} - I(Y; E|X)_{\sigma} = \sum_x p_X(x) \left[I(Y; B)_{\sigma_x} - I(Y; E)_{\sigma_x} \right]$ and an average is always less than a maximum. □

Corollary 3 *The private dynamic capacity formula is equivalent to the HSW classical capacity formula in the limit where $\mu \to \infty$ and λ is fixed, in the sense that*

$$\max_{\sigma} \left[I(YX; B)_{\sigma} - I(Y; E|X)_{\sigma} \right] = \max_{\{p_X(x), \psi_x\}} I(X; B).$$

Proof The inequality LHS $\geq$ RHS follows by choosing the distribution $p_{X,Y}(x, y) = p_X(x)\, p_{Y|X}(y|x)$ with $p_{Y|X}(y|x) = \delta_{y,y_0}$ and $p_X(x) = p^*_X(x)$ and choosing the conditional density operators $\rho^{A'}_{x,y_0} = \left(\rho^*_x\right)^{A'}$. The inequality LHS $\leq$ RHS because

$$I(YX; B)_\sigma - I(Y; E|X)_\sigma \leq I(YX; B)_\sigma \leq \max_{\{p_X(x), \psi_x\}} I(X; B).$$

□

6.1.1 Comparison between public-private and classical-quantum regions

We now compare the Devetak–Shor classical-quantum trade-off formula [17] with a special case of our above formula that applies to a trade-off between public and private classical communication. We should expect these two formulas to be comparable from the Collins–Popescu analogy because no entanglement or secret key is involved. The result is that the public-private region is generally larger than the classical-quantum region, but the two regions are equivalent for degradable quantum channels.

First consider the following refinement of the Devetak–Shor formula (see Section IV-A-4 of Ref. [31]):

$$f_\mu(\mathcal{N}) \equiv \max_\rho I(X; B)_\rho + I(A\rangle BX)_\rho + \mu I(A\rangle BX)_\rho,$$

where ρ^{XAB} is a state of the form

$$\rho^{XAB} \equiv \sum_x p_X(x) |x\rangle\langle x|^X \otimes \mathcal{N}^{A'\to B}(\phi^{AA'}_x).$$

The formula for the public-private trade-off is a special case of the private dynamic capacity formula:

$$\begin{aligned} P_\mu(\mathcal{N}) \equiv \max_\sigma & I(X; B)_\sigma + I(Y; B|X)_\sigma - I(Y; E|X)_\sigma \\ & + \mu\left[I(Y; B|X)_\sigma - I(Y; E|X)_\sigma\right], \end{aligned}$$

where σ^{XYBE} is a state of the form

$$\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}(x, y) |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U^{A'\to BE}_{\mathcal{N}}(\rho^{A'}_{x,y}),$$

Lemma 2 *The classical-quantum trade-off formula is never greater than the public-private trade-off formula:*

$$f_\mu(\mathcal{N}) \leq P_\mu(\mathcal{N}).$$

Proof The proof technique is similar to that of Lemma 3 in Ref. [45]. First let us rewrite the function f so that it is a function on the systems X, B, and E:

$$\begin{aligned} f_\mu(\mathcal{N}) &= \max_\rho I(X;B)_\rho + I(A\rangle BX)_\rho + \mu I(A\rangle BX)_\rho \\ &= \max_\rho I(X;B)_\rho + (\mu+1)\left[H(B|X)_\rho - H(E|X)_\rho\right]. \end{aligned}$$

Thus, it is only important to consider the input system A' when evaluating the above formula. Let

$$\rho_x^{A'} = \mathrm{Tr}_A\{\phi_x^{AA'}\},$$

so that the maximization above is over a state of the following form:

$$\rho^{XBE} \equiv \sum_x p_X(x)\,|x\rangle\langle x|^X \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_x^{A'}),$$

where U is the isometric extension of the channel $\mathcal{N}$. Take a spectral decomposition of the states $\rho_x^{A'}$:

$$\rho_x^{A'} = \sum_y p_{Y|X}(y|x)\,\psi_{x,y}^{A'},$$

where the states $\psi_{x,y}^{A'}$ are pure. Then the following state θ^{XYBE} is a particular state of the form σ^{XYBE}:

$$\theta^{XYBE} \equiv \sum_{x,y} p_X(x)\,p_{Y|X}(y|x)\,|x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A'\to BE}(\psi_{x,y}^{A'}),$$

such that $\mathrm{Tr}_Y\{\theta\} = \rho^{XBE}$. Consider the following chain of inequalities:

$$\begin{aligned} & I(X;B)_\rho + (\mu+1)\left[H(B|X)_\rho - H(E|X)_\rho\right] \\ &= I(X;B)_\theta + (\mu+1)\left[H(B|X)_\theta - H(E|X)_\theta\right] \\ &= I(X;B)_\theta + (\mu+1)\left[H(B|X)_\theta - H(B|YX)_\theta - H(E|X)_\theta + H(E|YX)_\theta\right] \\ &= I(X;B)_\theta + (\mu+1)\left[I(Y;B|X)_\theta - I(Y;E|X)_\theta\right] \\ &\le P_\mu(\mathcal{N}). \end{aligned}$$

The first equality follows because $\mathrm{Tr}_Y\{\theta\} = \rho^{XBE}$. The second equality follows because the entropies of θ on systems B and E are equal when conditioned on X and Y. The third equality follows from the definition of conditional mutual information. The final inequality follows from the definition of $P_\mu(\mathcal{N})$. □

Lemma 3 *Suppose that a quantum channel is degradable. Then the classical-quantum trade-off formula is equivalent to the public-private trade-off formula.*

Proof The proof is again similar to that of Lemma 3 in Ref. [45]. Consider the state definitions in the previous lemma and the definition of σ^{XYBE} from before. Consider a state σ^{XYZBE} defined as follows:

$$\sigma^{XYZBE} \equiv \sum_{x,y,z} p_{X,Y}(x,y)\, p_{Z|X,Y}(z|x,y)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes |z\rangle\langle z|^Z \otimes U_{\mathcal{N}}^{A'\to BE}(\varphi_{x,y,z}^{A'}),$$

where $\rho_{x,y}^{A'} = \sum_z p_{Z|X,Y}(z|x,y)\, \varphi_{x,y,z}^{A'}$ is a spectral decomposition of $\rho_{x,y}^{A'}$. Consider the following chain of inequalities that applies to an arbitrary state σ^{XYBE}:

$$\begin{aligned}
&I(X;B)_\sigma + (\mu+1)\left[I(Y;B|X)_\sigma - I(Y;E|X)_\sigma\right] \\
&\quad = I(X;B)_\sigma + (\mu+1)\left[I(YZ;B|X)_\sigma - I(Z;B|XY)_\sigma\right. \\
&\qquad \left. - \left[I(YZ;E|X)_\sigma - I(Z;E|XY)_\sigma\right]\right] \\
&\quad = I(X;B)_\sigma + (\mu+1)\left[I(YZ;B|X)_\sigma - I(YZ;E|X)_\sigma\right. \\
&\qquad \left. - \left[I(Z;B|XY)_\sigma - I(Z;E|XY)_\sigma\right]\right] \\
&\quad \leq I(X;B)_\sigma + (\mu+1)\left[I(YZ;B|X)_\sigma - I(YZ;E|X)_\sigma\right] \\
&\quad = I(X;B)_\sigma + (\mu+1)\left[H(B|X)_\sigma - H(B|XYZ)_\sigma - H(E|X)_\sigma + H(E|XYZ)_\sigma\right] \\
&\quad = I(X;B)_\sigma + (\mu+1)\left[H(B|X)_\sigma - H(E|X)_\sigma\right] \\
&\quad \leq f_\mu(\mathcal{N}).
\end{aligned}$$

The first equality follows by applying the chain rule for quantum mutual information. The second equality follows by rearranging terms. The first inequality follows because $I(Z;B|XY)_\sigma - I(Z;E|XY)_\sigma \geq 0$ for a degradable quantum channel. The third equality follows by expanding mutual informations. The fourth equality follows because the entropies of the state σ on systems B and E are equal when conditioned on X, Y, and Z. The final inequality follows from the definition of $f_\mu(\mathcal{N})$. □

6.1.2 Comparison between quantum dynamic and private dynamic formulas

We can compare the quantum dynamic and private dynamic capacity formulas for the class of degradable channels. The proof exploits the simplified form of the private dynamic capacity formula that results from Lemma 6, and the quantum dynamic capacity formula appears in the proof below.

Lemma 4 *Suppose that a quantum channel $\mathcal{N}_{\mathrm{D}}$ is degradable. Then the quantum dynamic capacity formula can never be less than the private dynamic capacity formula.*

Proof We prove this theorem by showing that

$$P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) \leq D_{\lambda,\mu}(\mathcal{N}_D),$$

where $D_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$ is the quantum dynamic capacity formula given by

$$D_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) \equiv \max_\sigma I(AX;B)_\sigma + \lambda I(A\rangle BX)_\sigma + \mu\left[I(X;B)_\sigma + I(A\rangle BX)_\sigma\right].$$

The state σ^{XABE} is a state of the form

$$\sigma^{XABE} \equiv \sum_x p_X(x) |x\rangle\langle x|^X \otimes U_{\mathcal{N}_D}^{A' \to BE}(\phi_x^{AA'}),$$

where the states $\phi_x^{AA'}$ are pure. Suppose that the following state is the one that maximizes $P_{\lambda,\mu}(\mathcal{N}_D)$ for a given λ and μ:

$$\omega^{XYBE} \equiv \sum_{x,y} p_X(x)\, p_{Y|X}(y|x) |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}_D}^{A' \to BE}(\psi_{x,y}^{A'})$$

Then we choose the states $\phi_x^{AA'}$ in a given σ^{XABE} to be as follows:

$$|\phi_x\rangle^{AA'} = \sum_y \sqrt{p_{Y|X}(y|x)}\, |y\rangle^A \left|\psi_{x,y}\right\rangle^{A'}.$$

We can obtain the state ω^{XYBE} from the state σ^{XABE} by performing a complete dephasing $\Delta^{A \to Y}$ where the dephasing basis is $\{|y\rangle\langle y|\}$. Then the following inequalities hold

$$\begin{aligned}
&I(YX;B)_\omega + \lambda\left[H(B|X)_\omega - H(E|X)_\omega\right] + \mu\left[H(B)_\omega - H(E|X)_\omega\right] \\
&= I(YX;B)_\omega + \lambda\left[H(B|X)_\sigma - H(E|X)_\sigma\right] + \mu\left[H(B)_\sigma - H(E|X)_\sigma\right] \\
&\leq I(AX;B)_\sigma + \lambda\left[H(B|X)_\sigma - H(E|X)_\sigma\right] + \mu\left[H(B)_\sigma - H(E|X)_\sigma\right] \\
&= I(AX;B)_\sigma + \lambda I(A\rangle BX)_\sigma + \mu\left[I(X;B)_\sigma + I(A\rangle BX)_\sigma\right] \\
&\leq D_{\lambda,\mu}(\mathcal{N}_D).
\end{aligned}$$

The first equality follows because the entropies of ω and σ without the Y system are equivalent. The first inequality follows from quantum data processing: one can obtain the state ω^{XYBE} be performing a von Neumann measurement of the A system of the state σ^{XABE} in the basis $\{|y\rangle^A\}$. The second equality follows by rearranging terms. The final equality follows from the definition of $D_{\lambda,\mu}$. □

The above lemma explicitly shows how the analogy between the classical and quantum worlds breaks down for the case of a degradable channel. The quantum dynamic capacity formula is always larger than the private dynamic formula because of the strong correlations in entanglement and because of the lack of a super-dense coding protocol in the public-private-secret-key setting.

7 Single-letter private dynamic capacity regions for entanglement-breaking channels

Our first class of channels for which the private dynamic capacity region simplifies is the class of entanglement-breaking channels. Shor found that such channels have an

additive classical capacity [43], and we can extend his method of proof to show that the full private dynamic capacity region for these channels is single-letter.

Theorem 3 (Private dynamic capacity for entanglement-breaking channels) *The private dynamic capacity region $\mathcal{C}_{\mathrm{RPS}}(\mathcal{N}_{\mathrm{EB}})$ of an entanglement-breaking quantum channel $\mathcal{N}_{\mathrm{EB}}$ is the set of all rates R, P, and S, such that*

$$R + P \leq \max_{\omega} I(X;B)_{\omega}, \tag{16}$$

$$P + S \leq 0, \tag{17}$$

$$R + P + S \leq \max_{\omega} I(X;B)_{\omega}. \tag{18}$$

The above entropic quantities are with respect to a classical-quantum state σ^{XB} where

$$\sigma^{XB} \equiv \sum_x p_X(x) |x\rangle\langle x|^X \otimes \mathcal{N}_{\mathrm{EB}}^{A' \to B}(\psi_x^{A'}), \tag{19}$$

and the states $\psi_x^{A'}$ are pure.

We prove this theorem in a few steps. We first show that the private dynamic capacity formula simplifies dramatically for antidegradable channels (recall that entanglement-breaking channels are a special case of antidegradable ones). We then show that this simplified formula is additive for an entanglement-breaking channel and this result implies the form of the region in the statement of the above theorem.

Lemma 5 *Suppose that a quantum channel $\mathcal{N}_{\mathrm{AD}}$ is antidegradable. Then the private dynamic capacity formula simplifies as follows:*

$$P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}) = h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}),$$

where

$$h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}) \equiv (1+\mu) \max_{\omega} I(X;B)_{\omega},$$

and ω^{XBE} is a state of the following form:

$$\omega^{XBE} \equiv \sum_x p_X(x) |x\rangle\langle x|^X \otimes U_{\mathcal{N}_{\mathrm{AD}}}^{A' \to BE}(\psi_x^{A'}),$$

and the states $\psi_x^{A'}$ are pure.

Proof The inequality $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}) \geq h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}})$ follows by carefully choosing the state σ^{XYBE} for the maximization on the LHS: choose the distribution $p_{X,Y}(x,y) = p_X^*(x)\,\delta_{y,y_0}$ and each state $\rho_{x,y_0}^{A'} = \left(\psi_x^*\right)^{A'}$ where the terms with asterisks are optimal for the RHS. The other inequality $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}) \leq h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}})$ follows from the following chain of inequalities:

$$
\begin{aligned}
&I\left(YX;B\right)_{\sigma}+\lambda\left[I\left(Y;B|X\right)_{\sigma}-I\left(Y;E|X\right)_{\sigma}\right]+\mu\left[I\left(YX;B\right)_{\sigma}-I\left(Y;E|X\right)_{\sigma}\right]\\
&\leq I\left(YX;B\right)_{\sigma}+\mu I\left(YX;B\right)_{\sigma}\\
&\leq h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}).
\end{aligned}
$$

The first inequality follows because $\left[I\left(Y;B|X\right)_{\sigma}-I\left(Y;E|X\right)_{\sigma}\right]\leq 0$ (from antidegradability) and by dropping the term $-\mu I\left(Y;E|X\right)_{\sigma}$. The second inequality follows because $I\left(YX;B\right)_{\sigma}\leq\max_{\omega}I\left(X;B\right)_{\omega}$. □

Corollary 4 *The private dynamic capacity formula is additive for an antidegradable channel $\mathcal{N}_{\mathrm{AD}}$ and an entanglement-breaking channel $\mathcal{N}_{\mathrm{EB}}$:*

$$
P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}\otimes\mathcal{N}_{\mathrm{EB}})=P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}})+P_{\lambda,\mu}(\mathcal{N}_{\mathrm{EB}})
$$

Proof The proof is similar to the proof in Ref. [43]. We first note that the tensor product of an antidegradable channel and an entanglement-breaking channel is an antidegradable channel. This observation allows us to employ the simplified formula in Lemma 5. We employ the following states in the proof:

$$
\begin{aligned}
\omega^{XB}&\equiv\sum_{x}p_{X}\left(x\right)\left|x\right\rangle\left\langle x\right|^{X}\otimes\mathcal{N}_{\mathrm{AD}}^{A_1\to B_1}\otimes\mathcal{N}_{\mathrm{EB}}^{A_2\to B_2}(\psi_{x}^{A_1A_2})\\
&=\sum_{x}p_{X}\left(x\right)\left|x\right\rangle\left\langle x\right|^{X}\otimes\sum_{z}p_{Z|X}\left(z|x\right)\mathcal{N}_{\mathrm{AD}}^{A_1\to B_1}(\sigma_{z,x}^{A_1})\otimes\theta_{z,x}^{B_2},\\
\omega^{XZB}&\equiv\sum_{x,z}p_{X}\left(x\right)p_{Z|X}\left(z|x\right)\left|x\right\rangle\left\langle x\right|^{X}\otimes\left|z\right\rangle\left\langle z\right|^{Z}\otimes\mathcal{N}_{\mathrm{AD}}^{A_1\to B_1}(\sigma_{z,x}^{A_1})\otimes\theta_{z,x}^{B_2}.
\end{aligned}
$$

Consider the following chain of inequalities:

$$
\begin{aligned}
P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}\otimes\mathcal{N}_{\mathrm{EB}})&=h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}\otimes\mathcal{N}_{\mathrm{EB}})\\
&=(1+\mu)\,I\left(X;B_1B_2\right)_{\omega}\\
&=(1+\mu)\left[H\left(B_1B_2\right)_{\omega}-H\left(B_1B_2|X\right)_{\omega}\right]\\
&\leq(1+\mu)\left[H\left(B_1\right)_{\omega}+H\left(B_2\right)_{\omega}-H\left(B_1B_2|XZ\right)_{\omega}\right]\\
&=(1+\mu)\left[H\left(B_1\right)_{\omega}+H\left(B_2\right)_{\omega}-H\left(B_1|XZ\right)_{\omega}-H\left(B_2|XZ\right)_{\omega}\right]\\
&=(1+\mu)\left[I\left(X;B_1\right)_{\omega}+I\left(X;B_2\right)_{\omega}\right]\\
&\leq h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}})+h_{\lambda,\mu}(\mathcal{N}_{\mathrm{EB}})\\
&=P_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}})+P_{\lambda,\mu}(\mathcal{N}_{\mathrm{EB}}).
\end{aligned}
$$

The first equality follows from Lemma 5. The second equality follows from the assumption that ω is a state that maximizes $h_{\lambda,\mu}(\mathcal{N}_{\mathrm{AD}}\otimes\mathcal{N}_{\mathrm{EB}})$. The third equality follows from the definition of quantum mutual information. The first inequality follows from subadditivity of entropy and conditioning does not increase entropy. The fourth equality follows because the state ω is product when conditioned on both X and Z. The fifth equality follows from the definition of quantum mutual information.

The second inequality follows because the mutual informations are always less than their maxima, and the final equality follows from Lemma 5. □

Example 1 The private dynamic capacity region of a completely dephasing channel is the set of all R, P, and S satisfying the following inequalities:

$$\begin{aligned} R + P &\leq 1, \\ P + S &\leq 0, \\ R + P + S &\leq 1. \end{aligned}$$

This result follows because the completely dephasing channel is an entanglement-breaking channel with public classical capacity equal to one.

8 Single-letter private dynamic capacity regions for the quantum Hadamard channels

We now prove that the private dynamic capacity region is additive for the class of quantum Hadamard channels. This result is perhaps dual to the above result because Hadamard channels are ones for which the map to the environment is entanglement-breaking, and they are degradable with a degrading map from Bob to the environment Eve. Our method of proof is similar as above—we first prove that the private dynamic capacity formula simplifies for degradable channels and then prove additivity of the simplified formula for the Hadamard channels.

Lemma 6 *Suppose that a quantum channel $\mathcal{N}_{\mathrm{D}}$ is degradable. Then the private dynamic capacity formula simplifies as follows:*

$$P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) = g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}),$$

where

$$\begin{aligned} g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) \equiv \max_{\omega} I\left(YX;B\right)_{\omega} + \lambda\left[H\left(B|X\right)_{\omega} - H\left(E|X\right)_{\omega}\right] \\ + \mu\left[H\left(B\right)_{\omega} - H\left(E|X\right)_{\omega}\right], \end{aligned}$$

and ω^{XYBE} is a state of the following form:

$$\omega^{XYBE} \equiv \sum_{x,y} p_{X,Y}\left(x,y\right)|x\rangle\langle x|^{X} \otimes |y\rangle\langle y|^{Y} \otimes U_{\mathcal{N}_{\mathrm{D}}}^{A'\to BE}(\psi_{x,y}^{A'}),$$

and the states $\psi_{x,y}^{A'}$ are pure.

Proof The inequality $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) \geq g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$ follows by choosing each state $\rho_{x,y}^{A'}$ in σ^{XYBE} for the maximization on the LHS to be the pure state $\psi_{x,y}^{A'}$ that maximizes the RHS. Consider the following chain of inequalities:

$$\begin{aligned}
P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) &\geq I(YX;B)_\sigma + \lambda\left[I(Y;B|X)_\sigma - I(Y;E|X)_\sigma\right] \\
&\quad + \mu\left[I(YX;B)_\sigma - I(Y;E|X)_\sigma\right] \\
&= I(YX;B)_\sigma + \lambda\left[H(B|X)_\sigma - H(B|XY)_\sigma - H(E|X)_\sigma + H(E|XY)_\sigma\right] \\
&\quad + \mu\left[H(B)_\sigma - H(B|XY)_\sigma - H(E|X)_\sigma + H(E|XY)_\sigma\right] \\
&= I(YX;B)_\sigma + \lambda\left[H(B|X)_\sigma - H(E|X)_\sigma\right] + \mu\left[H(B)_\sigma - H(E|X)_\sigma\right] \\
&= g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}).
\end{aligned}$$

We now prove that the other inequality $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) \leq g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$ holds. Suppose the state σ^{XYBE} maximizes $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$. Consider a state σ^{XYZBE} defined as follows:

$$\sigma^{XYZBE} \equiv \sum_{x,y,z} p_{X,Y}(x,y)\, p_{Z|X,Y}(z|x,y)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes |z\rangle\langle z|^Z \otimes U_{\mathcal{N}_{\mathrm{D}}}^{A'\to BE}(\varphi_{x,y,z}^{A'}),$$

where $\rho_{x,y}^{A'} = \sum_z p_{Z|X,Y}(z|x,y)\,\varphi_{x,y,z}^{A'}$ is a spectral decomposition of each $\rho_{x,y}^{A'}$ in the state σ^{XYBE}. This state is a state of the form ω^{XYBE} with Y redefined to be YZ. Consider the following chain of inequalities:

$$\begin{aligned}
P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) &= I(YX;B)_\sigma + \lambda\left[I(Y;B|X)_\sigma - I(Y;E|X)_\sigma\right] \\
&\quad + \mu\left[I(YX;B)_\sigma - I(Y;E|X)_\sigma\right] \\
&= I(YZX;B)_\sigma + \lambda\left[I(YZ;B|X)_\sigma - I(YZ;E|X)_\sigma\right. \\
&\quad \left. - \left[I(Z;B|YX)_\sigma - I(Z;E|YX)_\sigma\right]\right] \\
&\quad + \mu\left[I(X;B)_\sigma + I(YZ;B|X)_\sigma - I(YZ;E|X)_\sigma\right. \\
&\quad \left. - \left[I(Z;B|YX)_\sigma - I(Z;E|YX)_\sigma\right]\right] \\
&\leq I(YZX;B)_\sigma + \lambda\left[I(YZ;B|X)_\sigma - I(YZ;E|X)_\sigma\right] \\
&\quad + \mu\left[I(X;B)_\sigma + I(YZ;B|X)_\sigma - I(YZ;E|X)_\sigma\right] \\
&= I(YZX;B)_\sigma + \lambda\left[H(B|X)_\sigma - H(B|XYZ)_\sigma - H(E|X)_\sigma\right. \\
&\quad \left. + H(E|XYZ)_\sigma\right] + \mu\left[H(B)_\sigma - H(B|XYZ)_\sigma - H(E|X)_\sigma\right. \\
&\quad \left. + H(E|XYZ)_\sigma\right] \\
&= I(YZX;B)_\sigma + \lambda\left[H(B|X)_\sigma - H(E|X)_\sigma\right] + \mu\left[H(B)_\sigma - H(E|X)_\sigma\right] \\
&\leq g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}).
\end{aligned}$$

The first equality follows by definition. The second equality follows from applying the chain rule for mutual information. The first inequality follows because $I(Z;B|YX)_\sigma - I(Z;E|YX)_\sigma \geq 0$ for a degradable channel. The third equality follows by expanding the mutual informations, and the fourth equality follows because $H(B|XYZ)_\sigma = H(E|XYZ)_\sigma$. The final inequality follows from the definition of $g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$. □

Lemma 7 *Suppose that $\mathcal{N}_{\mathrm{H}}$ is a quantum Hadamard channel and that $\mathcal{N}_{\mathrm{D}}$ is a degradable quantum channel. Then the private dynamic capacity formula is additive:*

$$P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}} \otimes \mathcal{N}_{\mathrm{D}}) = P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}}) + P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}).$$

Proof The inequality $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}} \otimes \mathcal{N}_{\mathrm{D}}) \geq P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}}) + P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$ trivially holds by picking the state on the LHS to be a tensor product of the ones that individually maximize the RHS. Thus, we prove the non-trivial inequality $P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}} \otimes \mathcal{N}_{\mathrm{D}}) \leq P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}}) + P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}})$ for the channels in the hypothesis of the lemma. Consider a state of the form $\sigma^{XYB_1E_1B_2E_2}$ that arises from inputting a state of the form in Lemma 6 to the tensor product channel. Let $\omega^{XYZWE_1B_2E_2}$ be the state that arises from applying the first part of the degrading map of the Hadamard channel to system B_1. Then the following chain of inequalities holds:

$$
\begin{aligned}
&P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}} \otimes \mathcal{N}_{\mathrm{D}}) \\
&\quad = g_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}} \otimes \mathcal{N}_{\mathrm{D}}) \\
&\quad = H(B_1B_2)_\sigma - H(E_1E_2|YX)_\sigma + \lambda\left[H(B_1B_2|X)_\sigma - H(E_1E_2|X)_\sigma\right] \\
&\qquad + \mu\left[H(B_1B_2)_\sigma - H(E_1E_2|X)_\sigma\right] \\
&\quad = H(B_1)_\sigma - H(E_1|YX)_\sigma + \lambda\left[H(B_1|X)_\sigma - H(E_1|X)_\sigma\right] \\
&\qquad + \mu\left[H(B_1)_\sigma - H(E_1|X)_\sigma\right] \\
&\qquad + H(B_2|B_1)_\sigma - H(E_2|YXE_1)_\sigma + \lambda\left[H(B_2|XB_1)_\sigma - H(E_2|XE_1)_\sigma\right] \\
&\qquad + \mu\left[H(B_2|B_1)_\sigma - H(E_2|XE_1)_\sigma\right] \\
&\quad \leq H(B_1)_\sigma - H(E_1|YX)_\sigma + \lambda\left[H(B_1|X)_\sigma - H(E_1|X)_\sigma\right] \\
&\qquad + \mu\left[H(B_1)_\sigma - H(E_1|X)_\sigma\right] \\
&\qquad + H(B_2)_\sigma - H(E_2|YXW)_\sigma + \lambda\left[H(B_2|XW)_\sigma - H(E_2|XW)_\sigma\right] \\
&\qquad + \mu\left[H(B_2)_\sigma - H(E_2|XW)_\sigma\right] \\
&\quad \leq g_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}}) + g_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}) \\
&\quad = P_{\lambda,\mu}(\mathcal{N}_{\mathrm{H}}) + P_{\lambda,\mu}(\mathcal{N}_{\mathrm{D}}).
\end{aligned}
$$

The first equality follows from Lemma 6 because a Hadamard channel is degradable and thus the tensor product channel is degradable as well. The second equality follows by definition. The third equality follows by expanding with the chain rule for entropy. The first inequality follows from subadditivity ($H(B_2|B_1)_\sigma \leq H(B_2)_\sigma$) and because there is a degrading map from $B_1 \to W$ and from $W \to E_1$ (and so $H(B_2|XB_1)_\sigma \leq H(B_2|XW)_\sigma$ and $H(E_2|XW)_\sigma \leq H(E_2|XE_1)_\sigma$). The second inequality follows from the definition of $g_{\lambda,\mu}$, and the final equality follows from Lemma 6. □

9 The private dynamic capacity region for special channels

In the forthcoming sections, we explicitly compute and plot the private dynamic capacity region for the qubit dephasing channel, the $1 \to N$ cloning channel, and the quantum erasure channel. Interestingly, the ensemble required to achieve the boundary is the same for all three boundaries. The proofs of the theorems in this section are similar (though with subtle differences) to proofs from Refs. [11,50], and they all appear in the appendix.

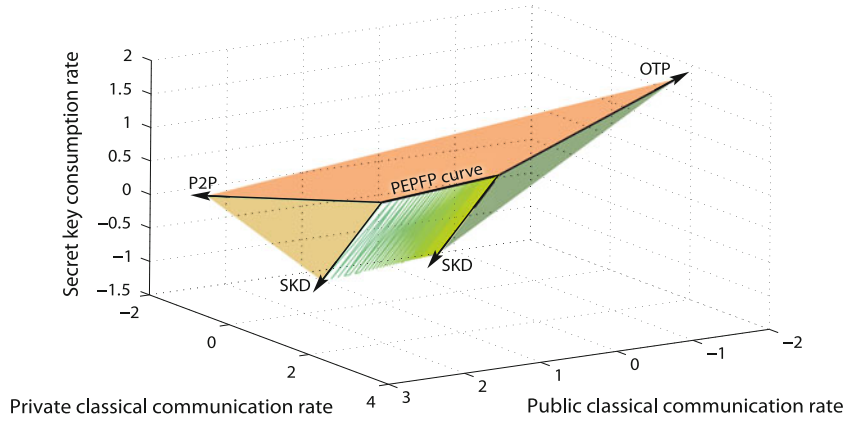

Fig. 3 (Color online) The private dynamic triple trade-off for the qubit dephasing channel with dephasing parameter $p = 0.2$. P2P is in the direction of private-to-public transmission, SKD is in the direction of secret key distribution, OTP is in the direction of the one-time pad protocol, and PEPFP is the publicly-enhanced private father trade-off curve (this convention is the same in the forthcoming figures). The region exhibits a non-trivial resource trade-off only on the surface below the PEPFP trade-off curve in the direction of secret key distribution

9.1 Dephasing channels

Consider the qubit dephasing channel $\mathcal{N}_p$ with dephasing probability p:

$$\mathcal{N}_p(\rho) := (1-p)\rho + p\Delta(\rho), \tag{20}$$

where $\Delta(\rho) := \langle 0|\rho|0\rangle|0\rangle\langle 0| + \langle 1|\rho|1\rangle|1\rangle\langle 1|$ is the completely dephasing channel. The below theorem gives an explicit form for the private dynamic capacity region of this channel, and Fig. 3 plots the region for a dephasing parameter $p = 0.2$.

Theorem 4 *The private dynamic capacity region $\mathcal{C}_{\mathrm{RPS}}(\mathcal{N}_p)$ of a dephasing channel with dephasing parameter p is the set of all R, P, and S such that*

$$R + P \leq 1, \tag{21}$$

$$P + S \leq H_2(\nu) - H_2(\gamma(\nu, p)), \tag{22}$$

$$R + P + S \leq 1 - H_2(\gamma(\nu, p)), \tag{23}$$

where $\nu \in [0, 1/2]$, H_2 is the binary entropy function, and

$$\gamma(\nu, p) \equiv \frac{1}{2} + \frac{1}{2}\sqrt{1 - 16 \cdot \frac{p}{2}\left(1 - \frac{p}{2}\right)\nu(1-\nu)}.$$

9.2 Quantum cloning channels

A $1 \to N$ cloning channel [8–11] is the map induced by a universal cloning machine [22]. It approximately copies the input with a maximal fidelity independent

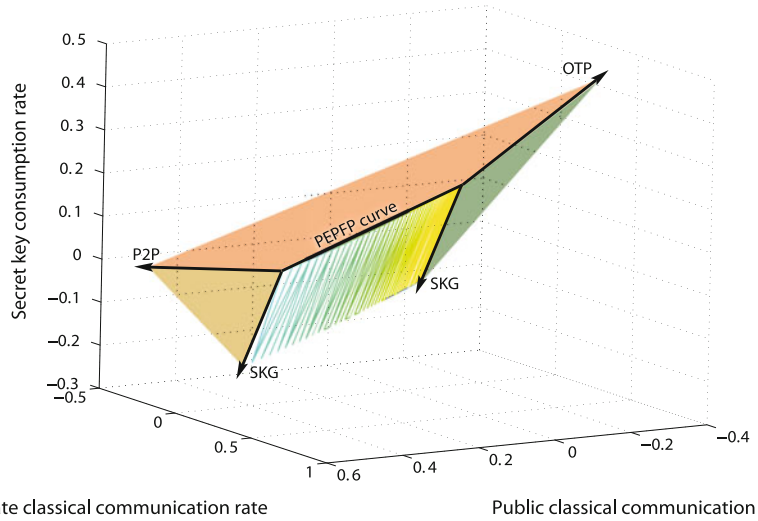

Fig. 4 (Color online) The private dynamic capacity region for a $1 \to 10$ cloning channel. The region exhibits a non-trivial resource trade-off only on the surface below the PEPFP trade-off curve in the direction of secret key distribution

of the input. The communication model for this channel gives all of the approximate clones to the receiver Bob and gives the environment of the map to Eve. The Kraus operators for a $1 \to N$ cloning channel are as follows:

$$\left\{ \frac{1}{\sqrt{\Delta_N}} \left(\sqrt{N-i}\, |i\rangle^B \langle 0|^{A'} + \sqrt{i+1}\, |i+1\rangle^B \langle 1|^{A'} \right) \right\}_{i=0}^{N-1},$$

where $\Delta_N \equiv N(N+1)/2$ and

$$\{|j\rangle^B \equiv |N-j, j\rangle\}_{j=0}^{N},$$

where $|N-j, j\rangle^B$ denotes a normalized state on an N-qubit system that is a uniform superposition of computational basis states with $N-j$ "zeros" and j "ones." Figure 4 plots the capacity region for a $1 \to 10$ cloning channel, and the proof of the below theorem appears in the appendix.

Theorem 5 *The private dynamic capacity region $\mathcal{C}_{\mathrm{RPS}}(\mathcal{N}_{Cl})$ of a $1 \to N$ quantum cloning channel is the set of all R, P, and S such that*

$$\begin{aligned} R + P &\leq 1 - \log N + \frac{1}{\Delta_N} \sum_{i=0}^{N} i \log i, \\ P + S &\leq H(\lambda_i(\mu)/\Delta_N) - H(\eta_i(\mu)/\Delta_N), \\ R + P + S &\leq \log(N+1) - H(\eta_i(\mu)/\Delta_N), \end{aligned}$$

where H is the entropy function $H(\cdot) \equiv -\sum_i (\cdot) \log (\cdot)$,

$$\begin{aligned} \Delta_N &\equiv N(N+1)/2, \\ \lambda_i(\mu) &\equiv (N-2i)\mu + i \quad \textit{for} \quad 0 \leq i \leq N, \\ \eta_i(\mu) &\equiv (N-1-2i)\mu + i + 1 \quad \textit{for} \quad 0 \leq i \leq N-1, \\ \mu &\in [0, 1/2]. \end{aligned}$$

9.3 Quantum erasure channel

Below we show that the private dynamic capacity region simplifies if the quantum channel is a quantum erasure channel. A quantum erasure channel with erasure parameter ϵ is the following map:

$$\mathcal{N}_\epsilon(\rho) \equiv (1-\epsilon)\rho + \epsilon |e\rangle\langle e|.$$

Notice that the receiver can perform a measurement $\{|0\rangle\langle 0| + |1\rangle\langle 1|, |e\rangle\langle e|\}$ and can learn whether the channel erased the state. The receiver can do this without disturbing the state in any way. An isometric extension $U_{\mathcal{N}_\epsilon}^{A' \to BE}$ of it acts as follows on a purification $|\psi\rangle^{AA'}$ of the state $\rho^{A'}$:

$$U_{\mathcal{N}_\epsilon}^{A' \to BE} |\psi\rangle^{AA'} = \sqrt{1-\epsilon}\, |\psi\rangle^{AB} |e\rangle^E + \sqrt{\epsilon}\, |\psi\rangle^{AE} |e\rangle^B.$$

In the above representation, we see that the erasure channel has the interpretation that it hands the input to Bob with probability $1-\epsilon$ while giving an erasure flag $|e\rangle$ to Eve, and it hands the input to Eve with probability ϵ while giving the erasure flag to Bob. Figure 5 plots the region for an erasure channel with erasure parameter $\epsilon = 1/4$, and the proof of the below theorem appears in the appendix.

Theorem 6 *The private dynamic capacity region $\mathcal{C}_{\mathrm{RPS}}(\mathcal{N}_\epsilon)$ of a quantum erasure channel $\mathcal{N}_\epsilon$ is the set of all R, P, and S such that*

$$\begin{aligned} R + P &\leq (1-\epsilon), \\ P + S &\leq (1-2\epsilon) H_2(p), \\ R + P + S &\leq 1 - \epsilon - \epsilon H_2(p), \end{aligned}$$

where $p \in [0, 1/2]$.

10 Conclusion

This paper completes the information-theoretic treatment of the Collins–Popescu analogy between classical communication, quantum communication, entanglement and public classical communication, private classical communication, and secret key (at least for the case of channels). Our main theorem gives the private dynamic capacity

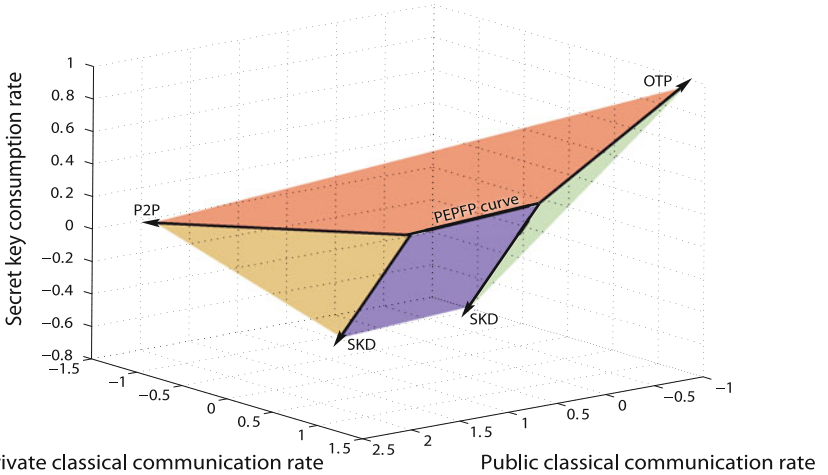

Fig. 5 (Color online) The private dynamic capacity region for a quantum erasure channel with erasure parameter $\epsilon = 1/4$. The erasure channel does not have a non-trivial trade-off, i.e., time-sharing between different protocols is the optimal strategy

region of a quantum channel. The catalytic information theoretic converse proof technique again proves to be useful in obtaining a simplified converse proof. The private dynamic capacity region dramatically simplifies for entanglement-breaking channels, Hadamard channels, and erasure channels, so that we can actually plot the region for several examples of these channels.

The open question remaining is to complete the Collins–Popescu analogy for the case of a static resource (a bipartite state shared between Alice and Bob). We have determined the static region for the classical-quantum-entanglement trade-off [30], and this first step should help in completing the analogy. Another ambitious open question would be to solve the quintuple trade-off between public classical communication, private classical communication, quantum communication, entanglement, and secret key, of which the regions in this paper are merely a projection. The catalytic information-theoretic converse proof technique should be helpful in obtaining a capacity theorem. Completing this larger trade-off problem could further our understanding of the nature of these different resources and their interaction with a noisy quantum resource.

Acknowledgments The authors thank Patrick Hayden for suggesting the communication model in Fig. 1. M.M.W. acknowledges support from the MDEIE (Québec) PSR-SIIRI international collaboration grant.

A Proofs

Proof [Theorem 4 (Dephasing channel region)] We first prove that it is sufficient to consider an ensemble of the following form to characterize the boundary points of the region:

$$\frac{\nu}{2}\left|0\right\rangle\left\langle 0\right|^{X}\otimes\left|0\right\rangle\left\langle 0\right|^{Y}\otimes\left|0\right\rangle\left\langle 0\right|^{A'}+\frac{1-\nu}{2}\left|0\right\rangle\left\langle 0\right|^{X}\otimes\left|1\right\rangle\left\langle 1\right|^{Y}\otimes\left|1\right\rangle\left\langle 1\right|^{A'}$$
$$+\frac{1-\nu}{2}\left|1\right\rangle\left\langle 1\right|^{X}\otimes\left|0\right\rangle\left\langle 0\right|^{Y}\otimes\left|0\right\rangle\left\langle 0\right|^{A'}+\frac{\nu}{2}\left|1\right\rangle\left\langle 1\right|^{X}\otimes\left|1\right\rangle\left\langle 1\right|^{Y}\otimes\left|1\right\rangle\left\langle 1\right|^{A'}, \tag{24}$$

where $\nu\in[0,1/2]$. We can use the simplified form of the private dynamic capacity formula in Lemma 6 because the dephasing channel is a degradable channel. Consider a classical-quantum state with a finite number $N_x N_y$ of conditional density operators $\phi_{x,y}^{A'}$:

$$\rho^{XYA'}\equiv\sum_{x=0}^{N_x-1}\sum_{y=0}^{N_y-1}p_X(x)\,p_{Y|X}(y|x)\,|x\rangle\langle x|^{X}\otimes|y\rangle\langle y|^{Y}\otimes\phi_{x,y}^{A'}.$$

Let $\phi_x^{A'}$ denote the conditional states if X is known but Y is not:

$$\phi_x^{A'}\equiv\sum_{y=0}^{N_y-1}p_{Y|X}(y|x)\phi_{x,y}^{A'}.$$

It suffices for these states to be diagonal in the dephasing basis because the channel output entropy when conditioned on X can only be larger while the environment's entropy when conditioned on X remains constant (see Lemma 9 of Ref. [26]). We can form a new classical-quantum state with quadruple the number of conditional density operators by applying all four Pauli operators to the original conditional density operators:

$$\sigma^{XYJA'}\equiv\sum_{x=0}^{N_x-1}\sum_{y=0}^{N_y-1}\sum_{j=0}^{3}\frac{1}{4}p_X(x)\,p_{Y|X}(y|x)\;|x\rangle\langle x|^{X}\otimes|y\rangle\langle y|^{Y}\otimes|j\rangle\langle j|^{J}\otimes\sigma_j\phi_{x,y}^{A'}\sigma_j,$$

where $\sigma_0=I,\sigma_1=\sigma_Z,\sigma_2=\sigma_X$ and $\sigma_3=\sigma_Y$ are the Pauli matrices. Let ρ^{XYBE} and σ^{XYJBE} be the respective states after sending the A' system of $\rho^{XYA'}$ and $\sigma^{XYJA'}$ through the isometric extension $U_{\mathcal{N}}^{A'\to BE}$ of the dephasing channel. Consider the following chain of inequalities that holds for all $\lambda,\mu\geq 0$:

$$\begin{aligned}
&H(B)_\rho-H(B|YX)_\rho+\lambda\left[H(B|X)_\rho-H(E|X)_\rho\right]+\mu\left[H(B)_\rho-H(E|X)_\rho\right]\\
&\quad=H(B)_\rho-H(B|YXJ)_\sigma+\lambda\left[H(B|XJ)_\sigma-H(E|XJ)_\sigma\right]\\
&\qquad+\mu\left[H(B)_\rho-H(E|XJ)_\sigma\right]\\
&\leq H(B)_\sigma-H(B|YXJ)_\sigma+\lambda\left[H(B|XJ)_\sigma-H(E|XJ)_\sigma\right]\\
&\qquad+\mu\left[H(B)_\sigma-H(E|XJ)_\sigma\right]\\
&\quad=1-H(B|YXJ)_\sigma+\lambda\left[H(B|XJ)_\sigma-H(E|XJ)_\sigma\right]+\mu\left[1-H(E|XJ)_\sigma\right]
\end{aligned}$$

$$
\begin{aligned}
&= 1+\mu+\sum_{x=1}^{N_x-1} p_X(x)\left[-H(B)_{\mathcal{N}(\phi_{x,y})}+\lambda H(B)_{\mathcal{N}(\phi_x)}-(\lambda+\mu)\,H(E)_{\mathcal{N}^c(\phi_x)}\right]\\
&\leq 1+\mu+\max_x\left[-H(B)_{\mathcal{N}(\phi_{x,y})}+\lambda H(B)_{\mathcal{N}(\phi_x)}-(\lambda+\mu)\,H(E)_{\mathcal{N}^c(\phi_x)}\right]\\
&= 1+\mu-H(B)_{\mathcal{N}\left(\phi^*_{x,y}\right)}+\lambda H(B)_{\mathcal{N}(\phi^*_x)}-(\lambda+\mu)\,H(E)_{\mathcal{N}^c(\phi^*_x)}\\
&= 1+\mu+\lambda H(B)_{\mathcal{N}(\phi^*_x)}-(\lambda+\mu)\,H(E)_{\mathcal{N}^c(\phi^*_x)}\\
&= 1+\lambda\left[H(B)_{\mathcal{N}(\phi^*_x)}-H(E)_{\mathcal{N}^c(\phi^*_x)}\right]+\mu\left[1-H(E)_{\mathcal{N}^c(\phi^*_x)}\right].
\end{aligned}
$$

The first equality follows because conditioning on J does not change the conditional entropies. That is, the conditional entropies $H(B|X)$ and $H(B|YX)$ are invariant under a Pauli operator on the input state that commutes with the channel. Furthermore, a Pauli operator on the input state does not change the eigenvalues for the output of the dephasing channel's complementary channel: $H(E)_{\mathcal{N}^c(X\phi_x^{A'}X)} = H(E)_{\mathcal{N}^c(\phi_x^{A'})}$. The first inequality follows because entropy is concave, i.e., the local state σ^B is a mixed version of ρ^B. The second equality follows because

$$
\begin{aligned}
H(B)_{\sigma^B} &= H\left(\sum_{x,y,j}\frac{1}{4}p_X(x)\,p_{Y|X}(y|x)\,\sigma_j\phi^B_{x,y}\sigma_j\right)\\
&= H\left(\sum_{x,y}p_X(x)\,p_{Y|X}(y|x)\,I/2\right)=1.
\end{aligned}
$$

The third equality follows because the system X is classical and conditioning on J does not change the entropies. The second inequality follows because the maximum value of a realization of a random variable is not less than its expectation. The fourth equality follows be defining the ensemble with a $*$ to be the optimal ensemble with respect to the maximization over x. The fifth equality follows from a further optimization: it is better to choose the pure states $\phi^*_{x,y}$ to be pure states in the basis of the dephasing channel. The final equality follows by rearranging terms. The final state ϕ^*_x then has the form $\nu\,|0\rangle\langle 0|^{A'}+(1-\nu)\,|1\rangle\langle 1|^{A'}$ for some value of ν because ϕ^*_x is diagonal in the dephasing basis. The three other states $\sigma_X\phi^*_x\sigma_X$, $\sigma_Y\phi^*_x\sigma_Y$, and $\sigma_Z\phi^*_x\sigma_Z$ have a similar form, but $\phi^*_x=\sigma_Z\phi^*_x\sigma_Z$ and $\sigma_X\phi^*_x\sigma_X=\sigma_Y\phi^*_x\sigma_Y$. Thus, it suffices to choose the state ϕ^*_x and its bit-flipped version, and the variable Y needs only have distribution $(\nu, 1-\nu)$ because of the particular form of ϕ^*_x. Thus, an ensemble of the kind in (24) is sufficient to attain a point on the boundary of the region. Evaluating the entropic quantities in Theorem 1 on a state of the above form gives the expression for the region in Theorem 4. □

Proof [Theorem 5 (Cloning channel region)] We first prove that the same ensemble as in (24) suffices for achieving the limits of the region. We exploit the following classical-quantum states:

$$\rho^{XYA'} \equiv \sum_{x,y} p_X(x)\, p_{Y|X}(y|x)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes \phi_{x,y}^{A'},$$

$$\sigma^{XYIA'} \equiv \sum_{x,i} \frac{1}{4} p_X(x)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes |i\rangle\langle i|^I \otimes (\sigma_i^{A'})\phi_{x,y}^{A'}(\sigma_i^{A'}),$$

where the states $\phi_{x,y}^{A'}$ are pure, and let ρ^{XYBE} and σ^{XYIBE} be the states obtained by transmitting the A' system through the isometric extension of the erasure channel. Let $\sigma_x^{A'Y} \equiv \sum_y p_{Y|X}(y|x)\, |y\rangle\langle y|^Y \otimes \phi_{x,y}^{A'}$. The cloning channel is degradable and covariant [8,10], the latter meaning that the following relationships hold for any input density operator σ and any unitary V acting on the input system A':

$$\mathcal{N}_{\mathrm{Cl}}\left(V\sigma V^\dagger\right) = R_V \mathcal{N}_{\mathrm{Cl}}(\sigma) R_V^\dagger,$$
$$\mathcal{N}_{\mathrm{Cl}}^c\left(V\sigma V^\dagger\right) = S_V \mathcal{N}_{\mathrm{Cl}}^c(\sigma) S_V^\dagger,$$

where R_V and S_V are higher-dimensional irreducible representations of the unitary V on the respective systems B and E. The state σ^B is equal to the maximally mixed state on the symmetric subspace for the following reasons:

$$\sigma^B = \mathcal{N}_{\mathrm{Cl}}\left(\sigma^{A'}\right) = \mathcal{N}_{\mathrm{Cl}}\left(\frac{I^{A'}}{2}\right) = \mathcal{N}_{\mathrm{Cl}}\left(\int V\omega V^\dagger \,\mathrm{d}V\right) = \int R_V \mathcal{N}(\omega) R_{V^\dagger}\,\mathrm{d}V$$
$$= \frac{1}{N+1}\sum_{i=0}^{N} |i\rangle\langle i|^B, \tag{25}$$

where the fourth equality exploits the linearity and covariance of the cloning channel $\mathcal{N}_{\mathrm{Cl}}$. Consider the following chain of inequalities:

$$\begin{aligned}
&H(B)_\rho - H(B|YX)_\rho + \lambda\left[H(B|X)_\rho - H(E|X)_\rho\right] + \mu\left[H(B)_\rho - H(E|X)_\rho\right] \\
&= (\mu+1)H(B)_\rho - H(B|YX)_\rho + \lambda H(B|X)_\rho - (\lambda+\mu)H(E|X)_\rho \\
&= (\mu+1)H(B)_\rho - H(B|YXI)_\sigma + \lambda H(B|XI)_\sigma - (\lambda+\mu)H(E|XI)_\sigma \\
&\leq (\mu+1)H(B)_\sigma - H(B|YXI)_\sigma + \lambda H(B|XI)_\sigma - (\lambda+\mu)H(E|XI)_\sigma \\
&= (\mu+1)\log(N+1) - \sum_{x,y} p_X(x)\, p_{Y|X}(y|x)\, H\left(\frac{i}{\Delta_N}\right) \\
&+ \sum_x p_X(x)\left[\lambda H(B)_{\mathcal{N}(\sigma_x^{A'})} - (\lambda+\mu)H(E)_{\mathcal{N}^c(\sigma_x^{A'})}\right] \\
&\leq (\mu+1)\log(N+1) - H\left(\frac{i}{\Delta_N}\right) + \lambda H(B)_{\mathcal{N}(\sigma_x^*)} - (\lambda+\mu)H(E)_{\mathcal{N}^c(\sigma_x^*)} \\
&= 1 - \log N + \frac{1}{\Delta_N}\sum_{i=0}^{N} i\log i + \lambda\left[H(B)_{\mathcal{N}(\sigma_x^*)} - H(E)_{\mathcal{N}^c(\sigma_x^*)}\right] \\
&\quad + \mu\left[\log(N+1) - H(E)_{\mathcal{N}^c(\sigma_x^*)}\right].
\end{aligned}$$

The first equality follows by rearranging terms. The second equality follows because the conditional entropies are invariant under unitary transformations:

$$H(B)_{R_{\sigma_j}\rho_x^B R_{\sigma_j}^\dagger} = H(B)_{\rho_x^B}, \qquad H(E)_{S_{\sigma_j}\rho_x^E S_{\sigma_j}^\dagger} = H(E)_{\rho_x^E},$$

where R_{σ_j} and S_{σ_j} are higher-dimensional representations of σ_j on systems B and E, respectively. The first inequality follows because entropy is concave, i.e., the local state σ^B is a mixed version of ρ^B. The third equality follows because (25) implies that $H(B)_{\sigma^B} = \log(N+1)$, from applying unitary covariance of the cloning channel to the term $H(B|YXI)_\sigma = \sum_{x,y} p_X(x)\, p_{Y|X}(y|x)\, H(B)_{\mathcal{N}(\psi_{x,y})}$ (all pure states have the same output entropy—thus, it does not matter which particular pure states we input), and from expanding the conditional entropies $H(B|XI)_\sigma$ and $H(E|XI)_\sigma$. The second inequality follows because the maximum value of a realization of a random variable is not less than its expectation. The final equality follows by observing that $\log(N+1) - H\left(\frac{i}{\Delta_N}\right) = 1 - \log N + \frac{1}{\Delta_N}\sum_{i=0}^{N} i \log i$. The entropies $H(B)_{\mathcal{N}(\sigma_x^*)}$ and $H(E)_{\mathcal{N}^c(\sigma_x^*)}$ depend only on the eigenvalues of the input state σ_x^* by the covariance of both the cloning channel and its complement. We can therefore choose σ_x^* to be diagonal in the $\{|0\rangle, |1\rangle\}$ basis of A', and without loss of generality, suppose these eigenvalues are equal to ν and $1-\nu$. The ensemble defined to consist of σ_x^* and $X\sigma_x^* X$ assigned equal probabilities then saturates the upper bound. The final analytic form in the statement of the theorem follows by evaluating the entropies and these calculations are similar to calculations available in Section V-B of Ref. [11]. □

Proof of Theorem 6 (Erasure channel region). We prove Theorem 6 in several steps. □

Lemma 8 *The private dynamic capacity formula in (15) simplifies as follows for a quantum erasure channel $\mathcal{N}_\epsilon$:*

$$P_{\lambda,\mu}(\mathcal{N}_\epsilon) \equiv \max_{p\in[0,1/2]} (1-\epsilon) + \lambda(1-2\epsilon) H_2(p) + \mu((1-\epsilon) - \epsilon H_2(p)). \quad (26)$$

Thus, the "one-shot" dynamic capacity region of a quantum erasure channel is as Theorem 6 states.

Proof We can use the simplified form of the private dynamic capacity formula in Lemma 6 because the quantum erasure channel is a degradable channel. We exploit the following classical-quantum states:

$$\rho^{XYA'} \equiv \sum_{x,y} p_X(x)\, p_{Y|X}(y|x)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes \phi_{x,y}^{A'},$$

$$\sigma^{XYIA'} \equiv \sum_{x,i} \frac{1}{4} p_X(x)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes |i\rangle\langle i|^I \otimes (\sigma_i^{A'})\phi_{x,y}^{A'}(\sigma_i^{A'}), \quad (27)$$

and let ρ^{XYBE} and σ^{XYIBE} be the states obtained by transmitting the A' system through the isometric extension of the erasure channel. Let $\sigma_x^{A'} \equiv \sum_y p_{Y|X}(y|x)\, \phi_{x,y}^{A'}$.

Furthermore, let the eigenvalues of the state $\sigma_x^{A'}$ with highest entropy on system A' be p and $1-p$. Consider that the following chain of inequalities holds for any state ρ^{XYBE}:

$$\begin{aligned}
&H(B)_\rho - H(B|YX)_\rho + \lambda\left[H(B|X)_\rho - H(E|X)_\rho\right] + \mu\left[H(B)_\rho - H(E|X)_\rho\right] \\
&= (\mu+1)H(B)_\rho - H(B|YX)_\rho + \lambda H(B|X)_\rho - (\lambda+\mu)H(E|X)_\rho \\
&= (\mu+1)H(B|X_E)_\rho - H(B|YXX_E)_\rho + \lambda H(B|XX_E)_\rho - (\lambda+\mu)H(E|XX_E)_\rho \\
&= (\mu+1)(1-\epsilon)H\left(A'\right)_\rho - (1-\epsilon)H\left(A'|YX\right)_\rho + \lambda(1-\epsilon)H\left(A'|X\right)_\rho \\
&\quad - (\lambda+\mu)\epsilon H\left(A'|X\right)_\rho \\
&= (\mu+1)(1-\epsilon)H\left(A'\right)_\rho + [\lambda(1-\epsilon) - (\lambda+\mu)\epsilon]H\left(A'|X\right)_\rho \\
&= (\mu+1)(1-\epsilon)H\left(A'\right)_\rho + [\lambda(1-\epsilon) - (\lambda+\mu)\epsilon]H\left(A'|XI\right)_\sigma .
\end{aligned}$$

The first equality follows by rearrnging terms. The second equality follows by incorporating the classical erasure flag variable. The third equality follows by exploiting the properties of the quantum erasure channel. The fourth equality follows by rearranging terms and because the entropy $H\left(A'|YX\right)_\rho$ vanishes (the state on A' conditioned on both X and Y is pure). The fifth equality follows because $H\left(A'|X\right)_\rho = H\left(A'|XI\right)_\sigma$. Continuing,

$$\begin{aligned}
&\leq (\mu+1)(1-\epsilon)H\left(A'\right)_\sigma + [\lambda(1-\epsilon) - (\lambda+\mu)\epsilon]H\left(A'|XI\right)_\sigma \\
&= (\mu+1)(1-\epsilon) + [\lambda(1-\epsilon) - (\lambda+\mu)\epsilon]H\left(A'|XI\right)_\sigma \\
&= (\mu+1)(1-\epsilon) + [\lambda(1-\epsilon) - (\lambda+\mu)\epsilon]\sum_x p_X(x)H\left(A'\right)_{\sigma_x^{A'}} \\
&\leq (\mu+1)(1-\epsilon) + [\lambda(1-\epsilon) - (\lambda+\mu)\epsilon]H\left(A'\right)_{\sigma_x^*} \\
&= (1-\epsilon) + \lambda(1-2\epsilon)H_2(p) + \mu((1-\epsilon) - \epsilon H_2(p)) .
\end{aligned}$$

The first inequality follows because the unconditional entropy of the state ρ is always less than that of the state σ. The first equality follows because $H\left(A'\right)_\sigma = 1$. The second equality follows by expanding the conditional entropy. The second inequality follows because an average is always less than a maximum. The final equality follows by rearranging terms and by plugging in the eigenvalues of σ_x^*. The form of the private dynamic capacity formula then follows because this chain of inequalities holds for any input ensemble. □

Lemma 9 *It suffices to consider the set of* $\lambda, \mu \geq 0$ *for which*

$$\lambda(1-2\epsilon) \geq \mu\epsilon.$$

Otherwise, we are just maximizing the public classical capacity, which we know from Ref. [5] is equal to $1-\epsilon$.

Proof Consider rewriting the expression in (26) as follows:

$$\max_{p\in[0,1/2]} (1-\epsilon) + \mu\,(1-\epsilon) + [\lambda\,(1-2\epsilon) - \mu\epsilon]\,H_2\,(p)\,.$$

Suppose that the expression in square brackets is negative, i.e.,

$$\lambda\,(1-2\epsilon) < \mu\epsilon.$$

Then the maximization over p simply chooses $p = 0$ so that $H_2\,(p)$ vanishes and the negative term disappears. The resulting expression for the private dynamic capacity formula is

$$(1-\epsilon) + \mu\,(1-\epsilon)\,,$$

which corresponds to the following region

$$\begin{aligned} R + P &\leq 1-\epsilon, \\ P + S &\leq 0, \\ R + P + S &\leq 1-\epsilon. \end{aligned}$$

The above region is equivalent to a translation of the unit resource capacity region to the public classical capacity rate triple $(1-\epsilon, 0, 0)$. Thus, it suffices to restrict the parameters λ and μ as above for the quantum erasure channel. □

Lemma 10 *The following additivity relation holds for two quantum erasure channels $\mathcal{N}_\epsilon$ with the same erasure parameter ϵ:*

$$P_{\lambda,\mu}(\mathcal{N}_\epsilon \otimes \mathcal{N}_\epsilon) = P_{\lambda,\mu}(\mathcal{N}_\epsilon) + P_{\lambda,\mu}(\mathcal{N}_\epsilon).$$

Proof We prove the non-trivial inequality $P_{\lambda,\mu}(\mathcal{N}_\epsilon \otimes \mathcal{N}_\epsilon) \leq P_{\lambda,\mu}(\mathcal{N}_\epsilon) + P_{\lambda,\mu}(\mathcal{N}_\epsilon)$. We define the following states:

$$\begin{aligned} \rho^{XYA_1'A_2'} &\equiv \sum_{x,y} p_X\,(x)\,p_{Y|X}\,(y|x)\,|x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes \phi_{x,y}^{A_1'A_2'}, \\ \omega^{XYB_1E_1B_2E_2} &\equiv U_{\mathcal{N}_\epsilon}^{A_1'\to B_1E_1} \otimes U_{\mathcal{N}_\epsilon}^{A_2'\to B_2E_2}(\rho^{XYA_1'A_2'}), \end{aligned}$$

and we suppose that $\rho^{XYA_1A_2}$ is the state that maximizes $P_{\lambda,\mu}(\mathcal{N}_\epsilon \otimes \mathcal{N}_\epsilon)$. Consider the following equality:

$$\begin{aligned} &H\,(B_1B_2)_\omega - H\,(B_1B_2|YX)_\omega + \lambda\left(H\,(B_1B_2|X)_\omega - H\,(E_1E_2|X)_\omega\right) \\ &+ \mu\left(H\,(B_1B_2)_\omega - H\,(E_1E_2|X)_\omega\right) \\ &= (1-\epsilon)^2\,H\left(A_1'A_2'\right)_\rho + \epsilon\,(1-\epsilon)\left(H\left(A_1'\right)_\rho + H\left(A_2'\right)_\rho\right) \end{aligned}$$

$$
\begin{aligned}
&- \epsilon\,(1-\epsilon)\left(H\left(A_1'|YX\right)_\rho + H\left(A_2'|YX\right)_\rho\right)\\
&+ \lambda\left[(1-\epsilon)^2 H\left(A_1'A_2'|X\right)_\rho + \epsilon\,(1-\epsilon)\left(H\left(A_1'|X\right)_\rho + H\left(A_2'|X\right)_\rho\right)\right]\\
&- \lambda\left[\epsilon^2 H\left(A_1'A_2'|X\right)_\rho + \epsilon\,(1-\epsilon)\left(H\left(A_1'|X\right)_\rho + H\left(A_2'|X\right)_\rho\right)\right]\\
&+ \mu\left[(1-\epsilon)^2 H\left(A_1'A_2'\right)_\rho + \epsilon\,(1-\epsilon)\left(H\left(A_1'\right)_\rho + H\left(A_2'\right)_\rho\right)\right]\\
&- \mu\left[\epsilon^2 H\left(A_1'A_2'|X\right)_\rho + \epsilon\,(1-\epsilon)\left(H\left(A_1'|X\right)_\rho + H\left(A_2'|X\right)_\rho\right)\right].
\end{aligned}
$$

The above equality follows by exploiting the properties of the quantum erasure channel and because the entropy $H\left(A_1'A_2'|YX\right)_\rho = 0$. Continuing, the above quantity is less than the following one:

$$
\begin{aligned}
&\leq 2\,(1-\epsilon) - \epsilon\,(1-\epsilon)\left(H\left(A_1'|YXIJ\right)_\sigma + H\left(A_2'|YXIJ\right)_\sigma\right)\\
&\quad + \lambda\,(1-2\epsilon)\,H\left(A_1'A_2'|XIJ\right)_\sigma\\
&\quad + \mu\left[2\,(1-\epsilon) - \epsilon^2 H\left(A_1'A_2'|XIJ\right)_\sigma - \epsilon\,(1-\epsilon)\left(H\left(A_1'|XIJ\right)_\sigma - H\left(A_2'|XIJ\right)_\sigma\right)\right]\\
&= 2\,(1-\epsilon)\\
&\quad + \lambda\,(1-2\epsilon)\left(H\left(A_1'|XIJ\right)_\sigma + H\left(A_2'|XIJ\right)_\sigma\right)\\
&\quad + \mu\left[2\,(1-\epsilon) - \epsilon\left(H\left(A_1'|XIJ\right)_\sigma - H\left(A_2'|XIJ\right)_\sigma\right)\right]\\
&\quad - \epsilon\,(1-\epsilon)\left(H\left(A_1'|YXIJ\right)_\sigma + H\left(A_2'|YXIJ\right)_\sigma\right)\\
&\quad - \left[\left(\lambda\,(1-2\epsilon) - \mu\epsilon^2\right) I\left(A_1'; A_2'|XIJ\right)_\sigma\right]\\
&\leq P_{\lambda,\mu}\left(\mathcal{N}_\epsilon\right) + P_{\lambda,\mu}\left(\mathcal{N}_\epsilon\right) - \epsilon\,(1-\epsilon)\left(H\left(A_1'|YXIJ\right)_\sigma + H\left(A_2'|YXIJ\right)_\sigma\right)\\
&\quad - \left[\left(\lambda\,(1-2\epsilon) - \mu\epsilon^2\right) I\left(A_1'; A_2'|XIJ\right)_\rho\right]\\
&\leq P_{\lambda,\mu}\left(\mathcal{N}_\epsilon\right) + P_{\lambda,\mu}\left(\mathcal{N}_\epsilon\right).
\end{aligned}
$$

The first inequality follows from similar proofs we have seen for a state σ of the form in (27). The first equality follows by rearranging terms. The second inequality follows from the form of $D_{\lambda,\mu}$ in (26). The final inequality follows because Lemma 9 states that it is sufficient to consider $\lambda\,(1-2\epsilon) \geq \mu\epsilon$. Note that this condition implies that

$$\lambda\,(1-2\epsilon) \geq \mu\epsilon^2,$$

and hence that the quantity in square brackets in the line above the last one is positive. □

References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography—Part I: secret sharing. IEEE Trans. Inf. Theory **39**, 1121–1132 (1993)

2. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography—Part II: CR-capacity. IEEE Trans. Inf. Theory **44**, 225–240 (1998)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: IEEE Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179 (1984)
4. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)
5. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A.: Capacities of quantum erasure channels. Phys. Rev. Lett. **78**(16), 3217–3220 (1997). doi:10.1103/PhysRevLett.78.3217
6. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. Phys. Rev. Lett. **69**, 2881–2884 (1992)
7. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004). url:http://www.stanford.edu/~boyd/cvxbook/
8. Brádler, K.: An infinite sequence of additive channels: the classical capacity of cloning channels. IEEE Trans. Inf. Theory. **57**, 5497–5503 (2011)
9. Brádler, K., Dutil, N., Hayden, P., Muhammad, A.: Conjugate degradability and the quantum capacity of cloning channels. J. Math. Phys. **51**, 072201 (2010). doi:10.1063/1.3449555
10. Brádler, K., Hayden, P., Panangaden, P.: Private information via the Unruh effect. J. High Energy Phys. **2009**(08), 074 (2009). url:http://stacks.iop.org/1126-6708/2009/i=08/a=074
11. Brádler, K., Hayden, P., Touchette, D., Wilde, M.M.: Trade-off capacities of the quantum Hadamard channels. Phys. Rev. A **81**(6), 062312 (2010)
12. Brito, F., DiVincenzo, D.P., Koch, R.H., Steffen, M.: Efficient one- and two-qubit pulsed gates for an oscillator-stabilized Josephson qubit. New J. Phys. **10**(3), 033,027 (2008). url:http://stacks.iop.org/1367-2630/10/033027
13. Cai, N., Winter, A., Yeung, R.W.: Quantum privacy and quantum wiretap channels. Prob. Inf. Transm. **40**(4), 318–336 (2004). doi:10.1007/s11122-005-0002-x
14. Collins, D., Popescu, S.: Classical analog of entanglement. Phys. Rev. A **65**(3), 032,321 (2002). doi:10.1103/PhysRevA.65.032321
15. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1967)
16. Devetak, I.: The private classical capacity and quantum capacity of a quantum channel. IEEE Trans. Inf. Theory **51**(1), 44–55 (2005)
17. Devetak, I., Shor, P.W.: The capacity of a quantum channel for simultaneous transmission of classical and quantum information. Commun. Math. Phys. **256**(2), 287–303 (2005)
18. Devetak, I., Winter, A.: Relating quantum privacy and quantum coherence: an operational approach. Phys. Rev. Lett. **93**, 080,501 (2004)
19. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. Roy. Soc. A **461**, 207–235 (2005)
20. Duan, R., Grassl, M., Ji, Z., Zeng, B.: Multi-error-correcting amplitude damping codes. In: Proceedings of the International Symposium on Information Theory. Austin, Texas, USA (2010). ArXiv:1001.2356
21. Gingrich, R.M., Kok, P., Lee, H., Vatan, F., Dowling, J.P.: All linear optical quantum memory based on quantum error correction. Phys. Rev. Lett. **91**(21), 217,901 (2003). doi:10.1103/PhysRevLett.91.217901
22. Gisin, N., Massar, S.: Optimal quantum cloning machines. Phys. Rev. Lett. **79**(11), 2153–2156 (1997). doi:10.1103/PhysRevLett.79.2153
23. Grassl, M., Beth, T., Pellizzari, T.: Codes for the quantum erasure channel. Phys. Rev. A **56**(1), 33–38 (1997). doi:10.1103/PhysRevA.56.33
24. Holevo, A.S.: The capacity of the quantum channel with general signal states. IEEE Trans. Inf. Theory **44**, 269–273 (1998)
25. Horodecki, M., Shor, P.W., Ruskai, M.B.: Entanglement breaking channels. Rev. Math. Phys. **15**(6), 629–641 (2003). ArXiv:quant-ph/0302031
26. Hsieh, M.H., Devetak, I., Winter, A.: Entanglement-assisted capacity of quantum multiple-access channels. IEEE Trans. Inf. Theory **54**(7), 3078–3090 (2008)
27. Hsieh, M.H., Luo, Z., Brun, T.: Secret-key-assisted private classical communication capacity over quantum channels. Phys. Rev. A **78**(4), 042306 (2008). doi:10.1103/PhysRevA.78.042306

28. Hsieh, M.H., Wilde, M.M.: Public and private communication with a quantum channel and a secret key. Phys. Rev. A **80**(2), 022,306 (2009). doi:10.1103/PhysRevA.80.022306
29. Hsieh, M.H., Wilde, M.M.: Theory of Quantum Computation, Communication, and Cryptography, Lecture Notes in Computer Science, vol. 5906, Chap. Optimal Trading of Classical Communication, Quantum Communication, and Entanglement, pp. 85–93. Springer (2009)
30. Hsieh, M.H., Wilde, M.M.: Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. IEEE Trans. Inf. Theory **56**(9), 4705–4730 (2010)
31. Hsieh, M.H., Wilde, M.M.: Entanglement-assisted communication of classical and quantum information. IEEE Trans. Inf. Theory **56**(9), 4682–4704 (2010)
32. King, C., Matsumoto, K., Nathanson, M., Ruskai, M.B.: Properties of conjugate channels with applications to additivity and multiplicativity. Markov Process. Relat. Fields **13**(2), 391–423 (2007). J. T. Lewis memorial issue
33. Korbicz J.K., Almeida M.L., Bae J., Lewenstein M., Acín A. (2008) Structural approximations to positive maps and entanglement-breaking channels. Phys. Rev. A **78**(6), 062,105. doi:10.1103/PhysRevA.78.062105
34. Lamas-Linares, A., Simon, C., Howell, J.C., Bouwmeester, D.: Experimental quantum cloning of single photons. Science **296**, 712–714 (2002)
35. Lu, C.Y., Gao, W.B., Zhang, J., Zhou, X.Q., Yang, T., Pan, J.W.: Experimental quantum coding against qubit loss error. Proc. Natl. Acad. Sci. USA **105**(32), 11,050–11,054 (2008)
36. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**, 733–742 (1993)
37. Milonni, P.W., Hardies, M.L.: Photons cannot always be replicated. Phys. Lett. A **92**(7), 321–322 (1982)
38. Minkel, J.R.: Space Station Could Beam Secret Quantum Codes by 2014. Scientific American (2008). http://www.scientificamerican.com/article.cfm?id=space-station-could-beam&sc=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+ScientificAmerican-News+%2528Scientific+American+-+News%2529
39. Chruściński, D., Pytel, J., Sarbicki, G.: Constructing optimal entanglement witnesses. Phys. Rev. A **80**(6), 062,314 (2009). doi:10.1103/PhysRevA.80.062314
40. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Modern Phys. **81**(3), 1301–1350 (2009). doi:10.1103/RevModPhys.81.1301
41. Schumacher, B., Westmoreland, M.D.: Sending classical information via noisy quantum channels. Phys. Rev. A **56**, 131–138 (1997)
42. Schumacher, B., Westmoreland, M.D.: Quantum privacy and quantum coherence. Phys. Rev. Lett. **80**(25), 5695–5697 (1998). doi:10.1103/PhysRevLett.80.5695
43. Shor, P.W.: Additivity of the classical capacity of entanglement-breaking quantum channels. J. Math. Phys. **43**(9), 4334–4340 (2002). doi:10.1063/1.1498000. url: http://link.aip.org/link/?JMP/43/4334/1
44. Simon, C., Weihs, G., Zeilinger, A.: Optimal quantum cloning via stimulated emission. Phys. Rev. Lett. **84**(13), 2993–2996 (2000). doi:10.1103/PhysRevLett.84.2993
45. Smith, G.: Private classical capacity with a symmetric side channel and its application to quantum cryptography. Phys. Rev. A **78**(2), 022,306 (2008). doi:10.1103/PhysRevA.78.022306
46. Smith, G., Renes, J.M., Smolin, J.A.: Structured codes improve the Bennett-Brassard-84 quantum key rate. Phys. Rev. Lett. **100**(17), 170,502 (2008). doi:10.1103/PhysRevLett.100.170502
47. Ursin, R., et al.: Space-QUEST: experiments with quantum entanglement in space. Europhys. News **40**(3), 26–29 (2009). ArXiv:0806.0945
48. Vernam, G.S.: Cipher printing telegraph systems for secret wire and radio telegraphic communications. J. IEEE **55**, 109–115 (1926)
49. Wasilewski, W., Banaszek, K.: Protecting an optical qubit against photon loss. Phys. Rev. A **75**(4), 042,316 (2007). doi:10.1103/PhysRevA.75.042316
50. Wilde, M.M., Hsieh, M.-H.: The quantum dynamic capacity formula of a quantum channel. Quantum Inf. Process. doi:10.1007/s11128-011-0310-6
51. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **54**, 1355–1387 (1975)
52. Yard, J.: Simultaneous Classical-Quantum Capacities of Quantum Multiple Access Channels. Ph.D. thesis, Stanford University, Stanford, (2005). Quant-ph/0506050