Quantum Channel State Masking

Uzi Pereg
Institute of Communication Engineering
Technical University of Munich
uzzi.pereg@tum.de

Christian Deppe
Institute of Communication Engineering
Technical University of Munich
christian.deppe@tum.de

Holger Boche
Theoretical Information Technology
Technical University of Munich
boche@tum.de

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

Index Terms—Quantum communication, channel capacity, state masking, state information.

I. INTRODUCTION

Security and privacy are critical aspects in modern communication systems [1]. The classical wiretap channel was first introduced by Wyner [2] to model communication in the presence of a passive eavesdropper. On the other hand, Merhav and Shamai [3] introduced a different communication system with the privacy requirement of masking. In this setting, the sender transmits a sequence $X^n$ over a memoryless state-dependent channel $p_Y|X,S^n$, where the state sequence $S^n$ has a fixed memoryless distribution and is not affected by the transmission. The transmitter of $X^n$ is informed of $S^n$ and is required to send information to the receiver while limiting the amount of information that the receiver can learn about $S^n$. Related settings and extensions are also considered in [4–6].

The field of quantum information is rapidly evolving in both practice and theory [7]. Communication through quantum channels can be separated into different categories. For classical communication, the Holevo-Schumacher-Westmoreland (HSW) Theorem provides a regularized (“multi-letter”) formula for the capacity of a quantum channel [8]. Although calculation of such a formula is intractable in general, it provides computable lower bounds, and there are special cases where the capacity can be computed exactly. The quantum capacity is characterized by the regularized coherent information [9].

Another scenario of interest is when Alice and Bob share entanglement resources. While entanglement can be used to produce shared randomness, it is a much more powerful aid [10]. E.g., using super-dense coding [11], entanglement assistance doubles the transmission rate of classical messages over a noiseless qubit channel. The entanglement-assisted capacity of a noisy quantum channel was fully characterized by Bennett et al. [12] in terms of the quantum mutual information. Entanglement resources are thus instrumental for the analysis of quantum communication systems, providing a computable upper bound for unassisted communication as well.

Boche et al. [13] addressed the classical-quantum channel with channel state information (CSI) at the encoder. The capacity was determined given causal CSI, and a regularized formula was provided given non-causal CSI [13] (see also [14]). The entanglement-assisted capacity of a quantum channel with non-causal CSI was determined by Dupuis in [15], and with causal CSI in [16]. Considering secure communication over the quantum wiretap channel, Devetak [9] and Cai et al. [17] established a regularized characterization of the secrecy capacity. The entanglement-assisted secrecy capacity was determined by Qi et al. [18]. The quantum broadcast confidential messages was recently considered in [19].

In this paper, we consider a quantum state-dependent channel $N_{EA→B}$, when the encoder has CSI and is required to mask information on the quantum channel state from the decoder. Specifically, Alice maps the quantum state of a message system $M$ and the CSI systems $E^n_0$ to the state of the channel input systems $A^n$ in such a manner that limits the leakage-rate of Bob’s information on $C^n$ from $B^n$, where the systems $E^n_0$ and $C^n$ are entangled with the channel state systems $E^n$ (see Fig. I). Analogously to the classical model, $C^n$ store undesired quantum information which leaks to the receiver [3]. This could model a leakage in the system of secret information, or could stand for another transmission to another receiver (Charlie), with a product state, out of our control, and which is not intended to our receiver (Bob), and is therefore to be concealed from him. Another significant distinction from the classical case is that the leakage requirement involves Bob’s share of the entanglement resources. In the classical setting, shared randomness does not need to be included in the leakage constraint as it cannot help the decoder. On the other hand, the teleportation protocol, for example, enables Bob to extract information from the entanglement resources.

A full characterization is established for the entanglement-assisted masking equivocation region, and a regularized formula is given for the quantum masking region without assistance. We also derive a single-letter outer bound on the unassisted masking region for Hadamard channels, and verify that the inner and outer bounds coincide in the standard case of a channel that does not depend on its state. First, we determine an achievable masking region with rate-limited entanglement by modifying the decoupling approach [20] such that both the environment and the channel state systems...
$|\Psi_{GAGB}\rangle_{En}$

$0$

$Cn$

$I(B^n_{GB}; C^n)\rho \leq L$

$|\phi_{E_0E_C}\rangle_{En}$

$N DBn \hat{M}$

$GB$

$FM\ An$

$D$

$E^n_C$

$\frac{1}{n}I(B^n_{GB}; C^n\rho) \leq L$

$|\phi_{E_0E_C}\rangle_{En}$

$C^n$

$\rho$

$\rho_{EC}$

$\phi_{EC}$

$V\rho_{EA'C}V^\dagger = \rho_{AKBC}$. The complementary channel can be simulated as follows. First, Bob performs a projective measurement on the channel output $B$ in the basis $\{|\psi_{B}^{\alpha}\rangle\}_{\alpha \in X}$. Then, given the outcome $x^{\ast}$, the state $|\phi_{E_{x^{\ast}C}}\rangle$ is prepared.

We define a masking code to transmit quantum information.

**Definition 1.** A $(2^nQ, 2^nR_e, n)$ quantum masking code with rate-limited entanglement assistance and CSI at the encoder consists of the following: A quantum message $\rho_{M}$, of dimension $|H_M| = 2^nQ$, a pure entangled state $\Psi_{G_A, G_B}$, $|H_{G_A}| = |H_{G_B}| = 2^nR_e$, an encoding map $F_{MG_A E_0^n \rightarrow A^n}$, and a decoding map $D_{B^n_{GB} \rightarrow M}$.

Alice encodes the message by applying $F_{MG_A E_0^n \rightarrow A^n}$, and transmits the systems $A^n$ over $n$ channel uses of $N_{EA \rightarrow B}$ (see Fig. 1). Bob receives $B^n$ and applies $D_{B^n_{GB} \rightarrow M}$ such that the state of $M$ is his estimate of $\rho_{M}$. The estimation error is $e(n)(\mathcal{E}, \Psi, D, \rho_{M}) = \frac{1}{2} \left\| \rho_{M} - D_{B^n_{GB} \rightarrow M}(\rho_{B^n_{GB}}) \right\|_1$, and the masking leakage rate is defined as

$$
e(n)(\mathcal{E}, \Psi, D, \rho_{M}) \triangleq \frac{1}{n} I(C^n; B^n_{GB})\rho.$$

(1)

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

A rate-leakage pair $(Q, L)$ is called achievable with entanglement assistance if $(Q, L, R_e)$ is achievable for some $R_e \geq 0$. The entanglement-assisted masking region $\mathbb{R}_{Q}(\mathcal{N})$ is defined as the set of achievable pairs $(Q, L)$ with entanglement assistance. A rate-leakage pair $(Q, L)$ is called achievable without assistance if $(Q, L, R_e = 0)$ is achievable. The masking region $\mathbb{R}_Q(\mathcal{N})$ without assistance is defined in a similar manner. In transmission of classical information, the message is limited to states $\{|m\rangle\}_{m=1}^{2^n}$. We denote the classical masking regions by $\mathbb{R}_{Q}^{c}(\mathcal{N})$ and $\mathbb{R}_Q^c(\mathcal{N})$.

Notice that with entanglement assistance, the leakage rate (1) includes Bob’s share $G_B$ of the entanglement resources, since the decoder has access to both $B^n$ and $G_B$. This is another significant distinction from the classical case, where the leakage does not need to include shared randomness, as it cannot help the decoder. Here, on the other hand, Bob can extract quantum information from $G_B$, using the teleportation protocol for example.

III. IID DECOUPLING

In this section, we present our i.i.d. version of the decoupling theorem. For every pair of orthonormal bases $\{|i_A\rangle\}$ and $\{|j_B\rangle\}$, define the operator op$_{PA \rightarrow B}[|i_A\rangle \otimes |j_B\rangle] \equiv |j_B\rangle\langle i_A|$. **Theorem 1** (The i.i.d. decoupling theorem). Let $\omega_{ABK}$ be a pure state, and $S, R, G_1, G_2$ be quantum systems at state $|\omega_{SRG_1G_2}\rangle = |\Psi_{SR}\rangle \otimes |\Psi_{G_1G_2}\rangle$ in the product Hilbert space $\mathcal{H}_S^2 \otimes \mathcal{H}_G^2$. Let $W_{SG_1 \rightarrow A^n}$ be a full-rank partial
isometry, and denote $|\sigma_{A^nRG_2}\rangle = W_{S_{G_1A^n}}|\sigma_{SRG_1G_2}\rangle$. Define the quantum channel $T_{A \rightarrow K}$ by $T_{A \rightarrow K}(\rho_A) = |H_A\rangle\langle T_B| o_{A \rightarrow BK}(|\omega_{ABK}\rangle)(\rho_A)$. Then,

$$\int dU_{A^n} \| T_{A \rightarrow K}^{\otimes n}(U_{A^n\sigma_{A^nB}}) - \omega_K \otimes \sigma_R \|_1 \leq \sqrt{|H_S||H_G|2^{-nH(A|K)_\omega + n\epsilon(n)}}$$

(2)

and

$$\int dU_{A^n} \| T_{A \rightarrow K}^{\otimes n}(U_{A^n\sigma_{A^nR_2G_2}}) - \omega_K \otimes \sigma_{RG_2} \|_1 \leq \sqrt{|H_S||H_G|2^{-nH(A|K)_\omega + n\epsilon(n)}}$$

(3)

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

The proof of Theorem 1 is given in [22].

IV. MAIN RESULTS

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

A. Rate-Limited Entanglement Assistance

First, we establish an achievable region for rate-limited entanglement assistance. In the sequel, this will be used in order to prove the direct part for the quantum masking region, both with and without assistance.

Theorem 2. Let $(\mathcal{N}_{EA \rightarrow B}, |\phi_{EE_{0C}}\rangle)$ be a quantum state-dependent channel. Let $\rho_{EA'AC}$ be any mixed state with $\rho_{EC} = |\phi_{EC}\rangle$. Then, any rate point $(Q, L, R_e)$ such that

$$Q + R_e \leq H(A|EC)_\rho$$

$$Q - R_e \leq I(A|B)_\rho$$

(4)

$$L \geq I(C|AB)_\rho$$

is achievable for transmission with rate-limited entanglement assistance and CSI at the encoder, with $\rho_{ABC} = \mathcal{N}_{EA' \rightarrow B}(\rho_{AE'A'C})$.

The theorem demonstrates the tradeoff between communication, leakage, and resource rates. The proof is based on the i.i.d. decoupling theorem along with Uhlmann’s theorem. We approximate the leakage rate using the decoupled state that approximates the actual output state, using the Alicki-Fannes-Winter inequality [21], as the leakage rate of the decoupled state is easier to evaluate. The details can be found in [22].

B. Unassisted Masking Region

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

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

(5)

with $\rho_{ABC} = \mathcal{N}_{EA' \rightarrow B}(\rho_{AE'A'C})$. Furthermore, given an isometric extension $\mathcal{U}_{EC}^{\otimes n}$, define

$$\mathcal{R}_{\text{Q, out}}(\mathcal{N}) = \bigcup_{\rho_{EA'AC}: \rho_{EC} = |\phi_{EC}\rangle} \left\{ (Q, L) : Q \leq H(A|CE)_\rho \right\}$$

(6)

with $\rho_{ABKC} = \mathcal{U}_{EA' \rightarrow BK}(\rho_{AE'A'C})$. Our main result on channel state masking without assistance is given below.

Theorem 3. Let $(\mathcal{N}_{EA' \rightarrow B}, |\phi_{EE_{0C}}\rangle)$ be a quantum state-dependent channel with CSI at the encoder. Then, the quantum masking region is given by

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

(7)

We only give the proof outline, while the details can be found in [22]. Our converse proof is based on different arguments from those in the classical converse proof, which do not apply with negative conditional entropies.

Proof Outline. The direct part is a consequence of Theorem 2, taking $R_e = 0$, by employing the coding scheme for the product channel $\mathcal{N}^\otimes k$. As for the converse part, suppose that Alice and Bob are trying to generate entanglement between them. Alice locally prepares a maximally entangled state, $|\psi_{EC}\rangle$, hence $\rho_{EC} = |\phi_{EC}\rangle$.

Consider a sequence of codes such that

$$\rho_{M^nM'} = \frac{1}{\sum_{m=1}^{2^n} |m\rangle_M \otimes |m\rangle_M}.$$ Denote

$$|\theta_{M^nM'C^n}\rangle = |\Phi_{M^nM'}\rangle \otimes |\phi_{EE_{0C}}\rangle^\otimes n$$

(8)

where $E^n$ are the channel state systems, $E^n_0$ are the CSI systems that are available to Alice, and $C^n$ are the systems that are masked from Bob. Then, Alice applies an encoding channel $\mathcal{F}_{M^nE^n_{0C} \rightarrow A^n}$ to the quantum system $M'$ and the CSI systems $E_0^n$, and sends $A^n$ through the channel. Bob receives the systems $B^n$ and performs a decoding channel $\mathcal{D}_{B^n \rightarrow M'}$. Consider a sequence of codes such that

$$\frac{1}{2} \| \rho_{M^nM'} - |\Phi_{M^nM'}\rangle \|_1 \leq \epsilon_n$$

(9)

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

(10)

By the Alicki-Fannes-Winter inequality [21], (9) implies that $|H(M|\hat{M})_\rho - H(M|M')_\rho| \leq n\epsilon_n$. Observe that $I(M|M')_\rho = H(M)_\rho - H(M|M')_\rho = nQ - 0 = nQ$. Thus,

$$nQ \leq I(M|\hat{M})_\rho + n\epsilon_n' \leq I(M|B^n)_\rho + n\epsilon_n'$$

(11)

by the data processing inequality [11, Theorem 11.9.3]. In addition, $nQ = H(M)_\rho = H(M|E^nC^n)_\rho$, hence

$$Q \leq \frac{1}{n} \min\{I(M|B^n)_\rho, H(M|E^nC^n)_\rho\} + \epsilon_n'$$

As for the leakage rate, by (10),

$$n(L + \delta_n) \geq I(C^n; B^n)_\rho - I(C^n; M|B^n)_\rho$$

(12)

$$= I(C^n; MB^n)_\rho - H(M|B^n)_\rho + H(M|B^nC^n)_\rho$$

$$\geq I(C^n; MB^n)_\rho + n(Q - \epsilon_n') + H(M|B^nC^n)_\rho$$

(13)
where the last line follows from (11). Since
\[ H(M|B^nC^n)_\rho \geq -\log |\mathcal{M}| = -nQ \] (14)
(see [11, Theorem 11.5.1]), we have
\[ L + \delta_n + \varepsilon_n' \geq \frac{1}{n} I(C^n;MB^n)_\rho. \] (15)
This completes the proof outline for the regularized capacity-leakage characterization.

Observe that applying Fano’s inequality to (12), as in the classical proof [3], would not yield the desired result because \( H(M|B^nC^n)_\rho \leq 0 \). Next, we give single-letter bounds for Hadamard channels. Recall that we have defined the class of Hadamard channels in Section II, in terms of an isometric extension \( V^H_{E\rightarrow BC_1K} \) of a particular form.

**Theorem 4.** For a Hadamard channel \( \mathcal{N}^H_{E\rightarrow A'B} \),
\[ \mathcal{R}_{\text{Q,in}}(\mathcal{N}^H) \subseteq \mathcal{R}_Q(\mathcal{N}^H) \subseteq \mathcal{R}_{\text{Q,out}}(\mathcal{V}^H). \] (16)

The proof of Theorem 4 is given in [22]. Observe that for a pure input state \( |\psi_{E\rightarrow A'AC}\rangle \),
\[ H(A|CK)_\rho = H(AC|K)_\rho - H(C|K)_\rho = H(B)_\rho - H(AB)_\rho = I(AB)_\rho. \] (17)

It follows that the quantum masking region is bounded by
\[ \mathcal{R}_Q(\mathcal{N}) \subseteq \bigcup_{|\psi_{E\rightarrow A'AC}\rangle:\psi_{E\rightarrow BC} = \psi_{EC}} \{ (Q,L) : 0 \leq Q \leq I(AB)_\rho, L \geq I(C;AB)_\rho \}. \]

In the trivial case of a quantum channel \( \mathcal{P}_{A\rightarrow B} \) that does not depend on a state, the masking region can be achieved with pure product states \( |\psi_{E\rightarrow A'AC}\rangle = |\phi_{EC}\rangle \otimes |\theta_{AA'}\rangle \), hence the inner bound and the outer bound coincide, and
\[ \mathcal{R}_Q(\mathcal{P}) = \bigcup_{|\theta_{AA'}\rangle} \{ (Q,L) : 0 \leq Q \leq I(AB)_\rho, L \geq 0 \}. \] (18)

**C. Entanglement-Assisted Masking Region**

Next, we consider entanglement-assisted masking, where Alice and Bob have unlimited entanglement resources. In this section, we assume a maximally correlated state,
\[ \varphi_{E_{0}C} = \sum_{s \in S} q(s)\langle s|E \otimes |s|E_{0} \otimes |s|C \rangle \] (19)
where \( q(s) \) is a probability distribution, and \( \{ |s|E \}, \{ |s|E_{0} \}, \{ |s|C \} \) are orthonormal bases. Although one can always apply the spectral theorem to an individual system and obtain a decomposition of the form \( \varphi_E = \sum q(s)|s\rangle \langle s|E \), the assumption in (19) implies that \( E, E_{0}, \) and \( C \) have the same spectrum. Note that if Alice performs a projective measurement in the basis \( \{ |s|E_{0} \}_{s \in S} \), then the problem reduces to that of a quantum channel with a random parameter \( S \sim q(s) \) [14]. However, in our setting, Alice may perform any quantum operation on the CSI systems \( E_{0}^{n} \).

**Theorem 5.** Let \( \mathcal{N}_{E_{0} \rightarrow B' \varphi_{E_{0}C}} \) be a quantum state-dependent channel as in (19), with CSI at the encoder. Then, the entanglement-assisted quantum masking region and classical masking region are given by
\[ \mathcal{R}^Q_{\text{Q}}(\mathcal{N}) = \bigcup_{\rho_{E_{0}A'C} = \rho_{EC}} \left\{ (Q,L) : Q \leq \frac{1}{n} I(A;B)_\rho \right\} \] (20)
and
\[ \mathcal{R}^C_{\text{Q}}(\mathcal{N}) = \bigcup_{\rho_{E_{0}A'C} = \rho_{EC}} \left\{ (R,L) : R \leq I(A;B)_\rho \right\} \] (21)
respectively, with \( \rho_{ABC} = \mathcal{N}_{E_{0} \rightarrow B}(\rho_{AE_{0}A'C}). \)

The proof of Theorem 5 is given in [22]. The direct part is based on Theorem 2. The entanglement-assisted capacity can be achieved if the entanglement rate is higher than \( \frac{1}{2} I(AB|EC)_\rho \).

**D. Example: State-Dependent Dephasing Channel**

Consider a pair of qubit dephasing channels
\[ \mathcal{P}_{A\rightarrow B}^{(0)}(\rho) = (1-\varepsilon_{0})\rho + \varepsilon_{0}Z_{0}^0Z_{0}^1, s = 0,1 \] (22)
where \( Z \) is the phase-flip Pauli matrix, and \( \varepsilon_{0},\varepsilon_{1} \) are given parameters, with \( 0 \leq \varepsilon_{0} \leq 1 \). Suppose the channel state systems \( E, C, \) and \( E_{0} \) contain a copy of a classical random bit \( S \sim \text{Bernoulli}(q) \), with \( 0 \leq q \leq \frac{1}{2} \). Then, the qubit state-dependent channel \( \mathcal{N}_{E_{0} \rightarrow B} \) is defined such that given an input state \( \rho_{AE} = (1-q)|0\rangle\langle 0|E \otimes \sigma_{0} + q|1\rangle\langle 1|E \otimes \sigma_{1} \), the output state is
\[ \mathcal{N}_{E_{0} \rightarrow B}(\rho_{AE}) = (1-q)\mathcal{P}_{A\rightarrow B}^{(0)}(\sigma_{0}) + q\mathcal{P}_{A\rightarrow B}^{(1)}(\sigma_{1}) \] (23)
Observe that the dephasing channel can also be viewed as a controlled phase-flip gate that is controlled by a classical random bit \( W_{S} \) such that given \( S = s, W_{s} \sim \text{Bernoulli}(\varepsilon_{s}) \).

Consider the transmission of classical information while masking the channel state sequence from the receiver. In the special case of \( \varepsilon_{0} = 0 \) and \( \varepsilon_{1} = 1 \), we have \( W_{S} = S \). That is, the channel acts as a controlled-Z gate where the channel state system \( E \) (or \( S \)) is the controlling qubit. The entanglement-assisted masking region in this case is
\[ \mathcal{R}^C_{\text{Q}}(\mathcal{N}) = \left\{ (R,L) : 0 \leq R \leq \frac{2}{L} \right\} \] (24)
To understand why, observe that given CSI at the encoder, Alice can first perform the controlled phase-flip operation on her entangled qubit, and then use the super-dense coding protocol. Doing so, she effectively eliminates the phase flip operation of the channel. Subsequently, Bob receives the information perfectly, at rate of 2 classical bits per channel use, regardless of the values of \( S^n \). Hence, there is no leakage.

Now, let \( \varepsilon_{0} \leq \frac{1}{2} \leq \varepsilon_{1} \), and define
\[ \bar{\varepsilon} = (1-q)\varepsilon_{0} + q\varepsilon_{1} \] (25)
\[ \tilde{\varepsilon} = (1-q)\varepsilon_{0} + q(1-\varepsilon_{1}) \] (26)
Without CSI, the channel can be reduced to a standard dephasing channel that does not depend on a state, with the average phase-flip parameter \( \bar{\epsilon} \). Using Theorem 5, we show that the entanglement-assisted masking region is bounded by

\[
\mathcal{R}^{ea}_{CI}(N) \supseteq \bigcup_{0 \leq \lambda \leq \frac{1}{2}} \left\{ (R, L) : R \leq 2 - h_2(\lambda \cdot \bar{\epsilon}) \right\} \\
\cup \left\{ (R, L) : L \geq h_2(\lambda \cdot \bar{\epsilon}) - (1 - q)h_2(\lambda \cdot \bar{\epsilon}_0) - qh_2(\lambda \cdot \bar{\epsilon}_1) \right\}
\]

and also

\[
\mathcal{R}^{ea}_{CI}(N) \supseteq \bigcup_{0 \leq \lambda \leq \frac{1}{2}} \left\{ (R, L) : R \leq 2 - h_2(\lambda \cdot \bar{\epsilon}) \right\} \\
\cup \left\{ (R, L) : L \geq h_2(\lambda \cdot \bar{\epsilon}) - (1 - q)h_2(\lambda \cdot \bar{\epsilon}_0) - qh_2(\lambda \cdot \bar{\epsilon}_1) \right\}
\]

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

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

Then, Bob receives the output of a phase-flip gate that is controlled by \((W_{S} + Y) \mod 2\), which is distributed according to \( \text{Bernoulli}(\lambda \cdot \bar{\epsilon}) \) (see (25)). Similarly, to show achievability of the second region, we let Alice perform phase-flip operation controlled by the random variable \( Y + S \mod 2 \).

ACKNOWLEDGMENTS

Uzi Pereg, Christian Deppe, and Holger Boche were supported by the BMBF through Grants 16KIS0856 (Pereg, Deppe), 16KIS0858 (Boche), and the CHE Fellowship for Quantum Science and Technology (Pereg).

REFERENCES

[1] J. Lopez, R. Rios, F. Bao, and G. Wang, “Evolving privacy: From sensors to the internet of things,” Future Generation Computer Systems, vol. 75, pp. 46–57, 2017.
[2] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54(8), pp. 1355–1387, 1975.
[3] N. Merhav and S. Shamai, “Information rates subject to state masking,” IEEE Trans. Inf. Theory, vol. 53, no. 6, pp. 2254–2261, June 2007.
[4] O. O. Koyluoglu, R. Soundararajan, and S. Vishwanath, “State amplification subject to masking constraints,” IEEE Trans. Inf. Theory, vol. 62, no. 11, pp. 6233–6250, Nov 2016.
[5] M. Dikshtein, A. Somekh-Baruch, and S. Shamai, “Broadcasting information subject to state masking over a mimo state dependent gaussian channel,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT’2019), Paris, France, July 2019, pp. 275–279.
[6] M. Le Treust and M. R. Bloch, “State leakage and coordination with causal state knowledge at the encoder,” IEEE Trans. Inf. Theory, 2020.
[7] S. X. Ng, A. Conti, G. L. Long, P. Muller, A. Sayeed, J. Yuan, and L. Hanzo, “Guest editorial advances in quantum communications, computing, cryptography, and sensing,” IEEE J. Selected Areas in Commun., vol. 38, no. 3, pp. 405–412, 2020.
[8] A. S. Holevo, Quantum systems, channels, information: a mathematical introduction. Walter de Gruyter, 2012, vol. 16.
[9] I. Devetak, “The private classical capacity and quantum capacity of a quantum channel,” IEEE Trans. Inf. Theory, vol. 51, no. 1, pp. 44–55, 2005.
[10] R. Bassoli, R. Ferrara, S. Saedinaaeni, C. Deppe, H. Boche, F. H. P. Fitzek, and G. Jansen, Quantum Communication Networks. Springer (in prep.), 2020.
[11] M. M. Wilde, Quantum information theory, 2nd ed. Cambridge University Press, 2017.
[12] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem,” IEEE Trans. Inf. Theory, vol. 48, no. 10, pp. 2637–2655, Oct 2002.
[13] H. Boche, N. Cai, and J. Nötzel, “The classical-quantum channel with random state parameters known to the sender,” J. Physics A: Math. and Theor., vol. 49, no. 19, p. 195302, April 2016.
[14] U. Pereg, “Communication over quantum channels with parameter estimation,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT’2020), June 2020.
[15] F. Dupuis, “The capacity of quantum channels with side information at the transmitter,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT’2009), June 2009, pp. 948–952.
[16] U. Pereg, “Entanglement-assisted capacity of quantum channels with side information,” in Int. Zürich Seminar Inf. Commun. (IZS’2020), Zürich, Switzerland, Feb 2020.
[17] N. Cai, A. Winter, and R. W. Yeung, “Quantum privacy and quantum wiretap channels,” Probl. Info. Transm., vol. 40, no. 4, pp. 318–336, 2004.
[18] H. Qi, K. Sharma, and M. M. Wilde, “Entanglement-assisted private communication over quantum broadcast channels,” J. Phys. A: Math. and Theor., vol. 51, no. 37, p. 374001, 2018.
[19] F. Salek, M. Hsieh, and J. R. Fonollosa, “Publicness, privacy and confidentiality in the single-serving quantum broadcast channel,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT’2019), Paris, France, July 2019, pp. 1712–1716.
[20] F. Dupuis, “Coding for quantum channels with side information at the transmitter,” arXiv preprint arXiv:0805.3352, 2008.
[21] A. Winter, “Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints,” Commun. in Math. Phys., vol. 347, no. 1, pp. 291–313, 2016.
[22] U. Pereg, C. Deppe, and H. Boche, “Quantum channel state masking,” arXiv:2006.05925, 2020. [Online]. Available: https://arxiv.org/pdf/2006.05925.pdf