One-shot Capacity Bounds on the Simultaneous Transmission of Public and Private Information Over Quantum Channels

Farzin Salek*, Anurag Anshu†, Min-Hsiu Hsieh§, Rahul Jain†,‡ Javier R. Fonollosa*
*Universitat Politècnica de Catalunya, {farzin.salek, javier.fonollosa}@upc.edu
†National University of Singapore, a0109169@u.nus.edu, rahul@comp.nus.edu.sg
‡MajuLab, UMI 3654, Singapore
§University of Technology Sydney, min-hsiu.hsieh@uts.edu.au

***Abstract*—We aim to study the optimal rates of transmission of public and private classical information over a quantum channel in the most general channel model. To this end, we discuss a scenario in which a quantum channel is being used only once, i.e., one-shot regime is considered. A quantum channel can be used to send classical information (bits) either publicly or privately and for either case, one-shot bounds have been reported in the literature. This paper investigates the one-shot capacity capabilities of a quantum channel for simultaneous transmission of public and private information. We derive an achievable rate region in the form of a tradeoff between public and private rates. We also provide converse bounds assessing the tightness of our achievable rates. Our main tools used in the achievability proofs are position-based decoding and convex-split lemma.**

I. Introduction

Shannon's model of a noisy (classical) channel is a stochastic map $\mathcal{W}_{X\rightarrow Y}$ mapping elements from an input set $x \in [1,...,|\mathcal{X}|]$ to a target output set $y \in [1,...,|\mathcal{Y}|]$ according to some probability distribution, $p_{Y|X}(y|x)$ [1]. Alas, This channel model and the classical information theory in general, were not rich enough to take quantum effects into account. Therefore, quantum information theorists urged to repeal and replace Shannon's channel model with a *quantum channel* model that involves quantum mechanics. Many years after Shannon, in the context of quantum information theory, the notion of a quantum channel, a completely-positive trace-preserving map (CPTP) with possibly different input and output Hilbert spaces was introduced (for a formal definition of a CPTP see [17]).

For a quantum channel, different capacities according to different information-processing tasks that it can accomplish can be defined. The quantum counterpart of the (classcial) capacity of a classcial channel is the classical capacity of a quantum channel, i.e., the highest rate (in bits per use of the channel) at which a sender can trasnmit classical information faithfully to a remote receiver. The classical capacity of a quantum channel also known as HSW theorem, was independently proved in [2] and [3]. Unlike the classical channel, we don't fully know the capabilities of a quantum channel for transmitting classical information. Consider a setup in which a sender and a receiver wish to communicate some information over a quantum channel that is being eavesdropped by an adversary. In this scenario, in addition to reliability criterion, a secrecy condition also comes into play. This information-processing task gives rise to the notion of *private capacity* of a quantum channel. Cai-Winter-Yeung [5] and Devetak [4] showed that the achievable rates for classical private capacity can be formulated as the difference between the Holevo information (see [2]) of the sender and the legitimate receiver and that of the sender and the Eavesdropper(s). They also showed that the private capacity demands a regularization meaning that this ability of the quantum channel is still not fully understood.

All these were studied initially under the assumptions that a channel is available for many uses of it such that each use is independent of the other uses, i.e., stationary and memoryless channels are dealt. However, these hypothese cannot be necessarily the case in many real-world scenarios. Later researchers considered *signle-serving* scenarios where a given channel is used only once. This approach gives rise to a high level of generality that no further constraints are put on the structure of the channel and the associated capacity is usually referred to as *one-shot* capacity. One-shot capacity of a classical channel was characterized in terms of min- and max-entropies in [6]. The one-shot capacity of a classical-quantum channel (or the classical capacity of quantum channel) is addressed by a hypothesis testing approach in [7] and [8], resulting in expressions in terms of the generalized (Rényi) relative entropies and a smooth relative entropy quantity, respectively. By appealing to two primitive information-theoretic protocols, privacy amplification and information reconciliation, authors of [9] proposed coding schemes for one-shot transmission of public and private classical Information. Their results come in terms of the min- and max-entropies. Two new tools, namely, position-based decoding and convex-split lemma are introduced in [11] and [15]. By using these tools, [10] reported achievability bounds on the one-shot public and private communications over a classical-quantum channel. A new one-shot quantum covering lemma (see [13]) and a operator Chernoff bound for non-square matrices are proven in [12], reporting achievable and converse bounds for the one-shot capacity of the wiretap channel.

Our protocol is conceptually based on superposition and Wyner coding as in [14]. Considering position-based decoding and convex-split lemma as the main tools used in this paper, our resource to achieve our achievability bounds is the superposition of two shared states. In fact, our protocol can be used to transmit (simultaneously) common and confidential messages in the sense that a common message to both Bob and Eve and a confidential message only to Bob. However, we do not consider Eve's reliability in our analysis since our goal is to evaluate achievable rates for Bob and so common (res. confidential) will be called public (res. private)[1]. We also assume that the encoder has access to an unlimited amount of dummy randomness to obfuscate the private message. Although we define our code and present our results for the shared state-assisted scenario, the code can be derandomized to achieve unassisted (the same) results.

The rest of the paper is organized as follows. Some definitions and preliminaries are given in section II. In section III, we formally define a one-shot simultaneous public-private code and present our main results, then we describe our protocol. Section IV concludes the paper.

II. Preliminaries and Basic Definitions

We denote quantum systems (or simply "systems") by capital letters, and we will use subscripts to denote the systems on which mathematical objects are defined. The Hilbert space corresponding to a quantum system A is denoted by $\mathcal{H}_A$. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces associated to systems A and B; Then we can consider the composite system of A and B as a single system with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. For a bipartite state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, marginal systems are defined as $\mathrm{Tr}_B\{\rho_{AB}\} = \rho_A$ and $\mathrm{Tr}_A\{\rho_{AB}\} = \rho_B$. For further preliminaries including position-based decoding and convex-splitting lemma we refer the reader to [11] and [15].

Definition 1 (Trace Distance [17]): The trance distance between two quantum states ρ_A, σ_A is given by:

$$D(\rho_A, \sigma_A) := \frac{1}{2}\|\rho_A - \sigma_A\|_1, \text{where } \|\rho_A\|_1 = \mathrm{Tr}\{\sqrt{\rho_A^\dagger \rho_A}\}$$

Definition 2 (Fidelity): The fidelity between two states ρ_A, σ_A is defined as:

$$F(\rho_A, \sigma_A) = \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1.$$

Definition 3 (Purified Distance): Let $\rho_A, \sigma_A \in \mathcal{H}_A$. The purified distance between ρ_A and σ_A is defined as:

$$P(\rho_A, \sigma_A) = \sqrt{1 - \bar{F}(\rho_A, \sigma_A)^2},$$

where $\bar{F}(\rho_A, \sigma_A) = F(\rho_A, \sigma_A) + \sqrt{(1 - \mathrm{Tr}\{\rho_A\})(1 - \mathrm{Tr}\{\sigma_A\})}$ is the generalized fidelity. We use the purified distance to specify an ϵ-ball around $\rho_A \in \mathcal{H}_A$, that is $\mathcal{B}^\epsilon(\rho_A) := \{\rho'_A \in \mathcal{H}_A : P(\rho'_A, \rho_A) \le \epsilon\}$.

Definition 4 (Hypothesis testing relative entropy):

$$D_H^\epsilon(\rho_A, \sigma_A) := -\log_2 \inf_{\substack{0 \le T_A \le \mathbb{1}, \\ \mathrm{Tr}\{T_A \rho_A\} \le \epsilon}} \mathrm{Tr}\{T_A \sigma_A\}$$

Definition 5 (Max-relative Entropy [18]): Max-relative entropy for $\rho_A, \sigma_A \in \mathcal{H}_A$ is defined as:

$$D_{max}(\rho_A \| \sigma_A) := \inf\left\{\lambda \in \mathbb{R} : \rho_A \le 2^\lambda \sigma_A\right\},$$

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

Definition 6 (Smooth max-relative Entropy [18]): For a parameter $\epsilon \in (0,1)$, Smooth max-relative entropy for $\rho_A, \sigma_A \in \mathcal{H}_A$ is defined as:

$$D_{max}^\epsilon(\rho_A \| \sigma_A) := \inf_{\rho'_A \in \mathcal{B}^\epsilon(\rho_A)} D_{max}(\rho'_A \| \sigma_A).$$

Definition 7 (Hypothesis testing mutual information [8]): For a bipartite state ρ_{AB} and a parameter $\epsilon \in (0,1)$, from the hypothesis testing relative entropy (definition (4)), the hypothesis testing mutual information is defined as follows:

$$I_H^\epsilon(A;B)_\rho := D_H^\epsilon(\rho_{AB} \| \rho_A \otimes \rho_B)_\rho.$$

Definition 8 (Max mutual information [19]): For a bipartite state ρ_{AB} and a parameter $\epsilon \in (0,1)$, from the max relative entropy (definition (5)), the max mutual information can be defined as follow:

$$I_{max}(A;B)_\rho := D_{max}(\rho_{AB} \| \rho_A \otimes \rho_B)_\rho.$$

Definition 9 (Smooth max-mutual information [19]): For a bipartite state ρ_{AB} and a parameter $\epsilon \in (0,1)$, from the max mutual information (definition (8)), the smooth max mutual information can be defined as follows:

$$\begin{aligned} I_{max}^\epsilon(A;B)_\rho &:= \inf_{\rho'_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} D_{max}(\rho'_{AB} \| \rho_A \otimes \rho_B) \\ &= \inf_{\rho'_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} I_{max}(A;B)_{\rho'} \end{aligned}$$

Definition 10 (Alternate smooth max-mutual information [11]): For a bipartite state ρ_{AB} and a parameter $\epsilon \in (0,1)$, we have

$$\tilde{I}_{max}^\epsilon(B;A)_\rho := \inf_{\rho'_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} D_{max}(\rho'_{AB} \| \rho_A \otimes \rho'_B)$$

Definition 11 (Conditional smooth hypothesis testing mutual information): Let $\rho_{ABX} := \sum_x p_X(x)|x\rangle\langle x|_X \otimes \rho_{AB}^x$ be a classical-quantum state and $\epsilon \ge 0$. Define

$$I_H^\epsilon(A;B|X)_\rho := \max_{\rho'} \min_{x \in \mathrm{supp}(\rho'_X)} I_H^\epsilon(A;B)_{\rho_{AB}^x},$$

where maximization is over all $\rho'_X = \sum_x p_X(x)|x\rangle\langle x|_X$ satisfying $P(\rho'_X, \theta_X) \le \epsilon$.

Definition 12 (Conditional smooth max-mutual information): Let $\rho_{ABX} := \sum_x p_X(x)|x\rangle\langle x|_X \otimes \rho_{AB}^x$ be a classical-quantum state and $\epsilon \ge 0$. The conditional smooth max mutual information is defined as follows:

$$I_{max}^\epsilon(A;B|X)_\rho := \min_{\rho'} \max_{x \in \mathrm{supp}(\rho'_X)} I_{max}^\epsilon(A;B)_{\rho_{AB}^x},$$

where minimization is over all $\rho'_X = \sum_x p_X(x)|x\rangle\langle x|_X$ satisfying $P(\rho'_X, \rho_X) \le \epsilon$.

[1] Our definition of public and private messages is the same as [16].

III. Problem Setup and Main Results

In this section, we first define a simultaneous public-private code, then we present our main results and finally we provide a concise description of the protocol.

A. Code Definition and Main Results

The sender Alice, by using a channel once, wishes to reliably communicate a public message $m \in \{1, 2, ..., |\mathcal{M}|\}$ and simultaneously a private message $\ell \in \{1, 2, ..., |\mathcal{L}|\}$ to the legitimate receiver Bob, in a way that ℓ must not be leaked to the eavesdropper Eve. To accomplish this task, Alice, Bob and Eve also share some quantum state among them. The quantum (wiretap) channel to be used by three parties is denoted by $\mathcal{N}_{A\to BE}$ and has the following action on an input state:

$$\omega_A \to \rho_{BE}, \tag{1}$$

where Alice has control over an ensemble of input states $\{p_{X,Y}(x,y), \omega_A^{x,y}\}$ and systems B and E are outputs received by Bob and Eve, respectively. Let M and L denote the random variables corresponding to Alice's choice of public and private messages, respectively. We also denote the cardinalities of M and L by $|\mathcal{M}|$ and $|\mathcal{L}|$, respectively. Alice also has access to a source of uniform dummy randomness $k \in \{1, 2, ..., |\mathcal{K}|\}$, given in random variable K. Further let $r = \log_2|\mathcal{M}|$, $R = \log_2|\mathcal{L}|$ and $\tilde{R} = \log_2|\mathcal{K}|$. The state initially shared between three parties is given by equation (2) at the top of the next page; where Alice possesses the quantum system A, Bob possesses the classical systems (X, Y) and Eve has the classical systems (X', Y'). Needless to say that the state belonging to each party can be evaluated simply by tracing out the other systems. For ease of notation, we further define $\Upsilon_{XX'AYY'} := \rho^{\otimes|\mathcal{M}|}_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}}$ with it being clear that $\rho^{\otimes|\mathcal{M}|}_{A^{|\mathcal{L}||\mathcal{K}|}} := \Upsilon_A$ and so on.

A one-shot $(r, R, \epsilon, \epsilon')$-shared state-assisted code for simultaneous transmission of public and private information of corresponding (r, R) rates can be defined by the following position-based encoding and decoding pairs:

- Alice performs some encoding operation $\mathcal{E} : ML\Upsilon_A \to A$. Let us denote the state in (2) after channel transmission as:

  $$\rho^{\otimes|\mathcal{M}|-1}_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}} \otimes \rho^{m,(\ell,k)}_{XX'(YY')^{|\mathcal{L}||\mathcal{K}|}(A)^{|\mathcal{L}||\mathcal{K}|-1}BE}, \tag{3}$$

  where $(m, \ell, k) \in [1 : 2^r] \times [1 : 2^R] \times [1 : 2^{\tilde{R}}]$ are the public message, the private message and a dummy number drawn uniformly at random by the encoder and $\rho^{m,(\ell,k)}_{XX'(YY')^{|\mathcal{L}||\mathcal{K}|}(A)^{|\mathcal{L}||\mathcal{K}|-1}BE}$ is given in equation (4).
- After receiving the channel output B, Bob performs a decoding operation $\mathcal{D}^1 : B\Upsilon_X \to \hat{M}B$ on his $\rho_{\mathcal{X}}$ and B systems, whose outputs are a classical system $\hat{M}$ and a quantum system B. Let $\hat{M}$ denote the random variable for Bob's estimate of the public message. The action of the quantum decoder $\mathcal{D}^1_{B\Upsilon_X\to\hat{M}B}$ on Bob's corresponding systems is as follows:

  $$\mathcal{D}^1_{B\Upsilon_X\to\hat{M}B}(\rho^{m,(\ell,k)}_{X^{|\mathcal{M}|}B}) := \sum_{m'=1}^{|\mathcal{M}|} |m'\rangle\langle m'|_{\hat{M}} \otimes \mathcal{D}^{1,m'}_{B\Upsilon_X\to B}(\rho^{m,(\ell,k)}_{X^{|\mathcal{M}|}B}), \tag{5}$$

  where $\{|m\rangle\}_{m=1}^{|\mathcal{M}|}$ are some orthonormal basis and $\rho^{m,(\ell,k)}_{X^{|\mathcal{M}|}B}$ can be seen from (3) by tracing out other systems. Moreover, tracing out the classical system $\hat{M}$ gives the induced quantum operation $\mathcal{D}^1_{B\rho_{\mathcal{X}}\to B} = \sum_m \mathcal{D}^{1,m}_{B\rho_{\mathcal{X}}\to B}$ such that its sum is trace preserving, i.e., $\mathrm{Tr}\left\{\sum_{m'=1}^{|\mathcal{M}|}\mathcal{D}^{1,m'}_{B\rho_{\mathcal{X}}\to B}(\rho^{m,(\ell,k)}_{X^{|\mathcal{M}|}B})\right\} = 1$. Define $\sum_x p_X(x)\sigma_B^{x,m,(\ell,k)} := \sum_{m'=1}^{|\mathcal{M}|}\mathcal{D}^{1,m'}_{B\rho_{\mathcal{X}}\to B}(\rho^{m,(\ell,k)}_{X^{|\mathcal{M}|}B})$. Considering this state and the state in (4), the disturbed state can be defined as in equation (6).
- Bob's second decoder is another quantum map $\mathcal{D}^2 : \hat{M}B\Upsilon_Y \to \hat{L}$ which is input both classical and quantum outputs of the first decoder, Bob's Υ_Y systems and outputs a classical system $\hat{L}$[2].

  $$\mathcal{D}^2_{\hat{M}B\Upsilon_Y\to\hat{L}}(\sigma^{x,m,(\ell,k)}_{Y^{|\mathcal{L}||\mathcal{K}|}B}) := \sum_{\ell=1}^{|\mathcal{L}|} p_{\hat{L}}(\ell)|\ell\rangle\langle\ell|_{\hat{L}}, \tag{7}$$

  where $\{|l\rangle\}_{l=1}^{|\mathcal{L}|}$ are some orthonormal basis and $\sigma^{x,m,(\ell,k)}_{Y^{|\mathcal{L}||\mathcal{K}|}B}$ is resulted from measuring the X system in (6) and tracing out other systems (see equation (8)).

For a quantum channel $\mathcal{N}_{A\to BE}$ and any fixed $\epsilon, \epsilon' \in (0, 1)$, a rate pair (r, R) is said to be an (ϵ, ϵ')-achievable rate pair for simultaneous transmission of public and private messages if there exists a triple $(\mathcal{E}, \mathcal{D}^1, \mathcal{D}^2)$ of encoding and decoding maps such that (9) and (10) hold. We refer to (9) and (10) as, respectively, the message error and the *privacy error*, the later is named so since it captures the notions of the Bob's error probability in detecting the private message as well as the security of Eve. The capacity region is the closure of the set of achievable rate pairs (r, R). See appendix A for dissection of the position-based decoders.

Theorem 1 (Achievability): For any fixed $\epsilon \geq 0, \epsilon' \geq 0$, and δ, δ' being positive numbers such that $\delta \in (0, \epsilon), \delta' \in (0, \epsilon')$, the ϵ-ϵ'-one-shot shared state-assisted capacity for simultaneous transmission of public and private classical information for the channel $\omega_A \to \rho_{BE}$, i.e., all rate pairs (r, R) for which a $(r, R, \epsilon, \epsilon')$-code exists, satisfies the following bounds:

$$r \geq I_H^{\epsilon-\delta}(X;B)_\rho - \log_2(\frac{4\epsilon}{\delta^2}),$$
$$R \geq I_H^{\epsilon-\delta}(Y;B|X)_\sigma - \tilde{I}_{max}^{\sqrt{\epsilon'}-\delta'}(Y;E|X)_\sigma - \log_2(\frac{4\epsilon}{\delta^2}) - 2\log_2(\frac{1}{\delta'}),$$

such that the conditions given by (9) and (10) hold for all public and private messages;[3] note that $\tilde{\sigma}_E$ is an arbitrary state

[2] This definition is in accord with the one given in [16].

[3] By slightly abuse of notation, we denote the random variables for Bob's estimates of the public and private messages by $\hat{M}$ and $\hat{L}$, respectively.

$$\rho^{\otimes|\mathcal{M}|}_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}} \coloneqq \left(\sum_x p(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes \left(\sum_y p(y|x)|y\rangle\langle y|_Y \otimes |y\rangle\langle y|_{Y'} \otimes \omega_A^{x,y}\right)^{\otimes|\mathcal{L}||\mathcal{K}|}\right)^{\otimes|\mathcal{M}|}. \tag{2}$$

$$\rho^{m,(\ell,k)}_{XX'(YY')^{|\mathcal{L}||\mathcal{K}|}(A)^{|\mathcal{L}||\mathcal{K}|-1}BE} \coloneqq \sum_x p_X(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes \rho^{x,m,(1,1)}_{YY'A} \otimes ... \otimes \mathcal{N}_{A\to BE}\left(\rho^{x,m,(\ell,k)}_{YY'A}\right) ... \otimes \rho^{x,m,(|\mathcal{L}|,|\mathcal{K}|)}_{YY'A}. \tag{4}$$

$$\sigma^{m,(\ell,k)}_{XX'(YY')^{|\mathcal{L}||\mathcal{K}|}(A)^{|\mathcal{L}||\mathcal{K}|-1}BE} \coloneqq \sum_x p_X(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes \sigma^{x,m,(1,1)}_{YY'A} \otimes ... \otimes \sigma^{x,m,(\ell,k)}_{YY'BE} \otimes ... \otimes \sigma^{x,m,(|\mathcal{L}|,|\mathcal{K}|)}_{YY'A}. \tag{6}$$

$$\sigma^{x,m,(\ell,k)}_{Y^{|\mathcal{L}||\mathcal{K}|}BE} = \sigma_Y^{x,m,(1,1)} \otimes ... \otimes \sigma_Y^{x,m,(\ell,k-1)} \otimes \sigma_{YB}^{x,m,(\ell,k)} \otimes \sigma_Y^{x,m,(\ell,k+1)} \otimes ... \otimes \sigma_Y^{x,m,(|\mathcal{L}|,|\mathcal{K}|)}. \tag{8}$$

$$P_e = \{\hat{M} \neq M\} \coloneqq \frac{1}{M}\sum_{m=1}^{|\mathcal{M}|}\frac{1}{2}\left\|\mathcal{D}^1_{B\Upsilon_X\to\hat{M}}(\rho^{m,(\ell,k)}_{X^{|\mathcal{M}|}B}) - |m\rangle\langle m|_{\hat{M}}\right\|_1 \leq \epsilon, \tag{9}$$

$$P_{priv} \coloneqq \frac{1}{|\mathcal{L}|}\sum_{l=1}^{|\mathcal{L}|}\frac{1}{2}\left\|\mathcal{D}^2_{\hat{M}B\Upsilon_Y\to\hat{L}}(\sigma^{m,(\ell,k)}_{XX'Y^{|\mathcal{L}||\mathcal{K}|}Y'^{|\mathcal{L}||\mathcal{K}|}BE}) - |l\rangle\langle l|_{\hat{L}} \otimes \hat{\sigma}_{X'Y'^{|\mathcal{L}||\mathcal{K}|}E}\right\|_1 \leq 2(\epsilon + \sqrt{\epsilon}) + \sqrt{\epsilon'}, \tag{10}$$

where

$$\hat{\sigma}_{X'Y'^{|\mathcal{L}||\mathcal{K}|}E} \coloneqq \sum_x p_X(x)|x\rangle\langle x|_{X'} \otimes \sigma^{x,m,(\ell,k)}_{Y'^{|\mathcal{L}||\mathcal{K}|}} \otimes \tilde{\sigma}_E^{x,m} \quad \text{and} \quad P(\sigma^x_{YE}, \tilde{\sigma}^x_{YE}) \leq \sqrt{\epsilon'}.$$

and all the entropic quantities above are with respect to "one-shot" quantum states in (4) and (6).

Theorem 2 (Converse): For a quantum (wiretap) channel $\omega_A \to \rho_{BE}$, without loss of generality, the joint state of input and output for an input chosen according to the joint distribution $p_{X,Y}(x,y)$ with $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, can be denoted by $\rho_{XYBE} = \sum_{x,y} p_{XY}(x,y)|x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \rho^{x,y}_{BE}$. Fix $\epsilon \geq 0, \epsilon' \geq 0$ and positive numbers δ, δ' such that $\delta \in (0,\epsilon)$ and $\delta' \in (0, \sqrt{\epsilon'})$ and let σ_{XYBE} be a quantum state satisfying $\|\rho_{XYBE} - \sigma_{XYBE}\|_1 \leq 2\sqrt{\epsilon}$.
For every sequence of $(r, R, \epsilon, \epsilon')$, ϵ-ϵ'-one-shot public-private codes for the channel $\omega_A \to \rho_{BE}$, the public-private rate pair must satisfy the following conditions:

$$\begin{aligned} r \leq & I_H^\epsilon(X;B)_\rho, \\ R \leq & I_H^\epsilon(Y;B|X)_\sigma - I_{max}^{\sqrt{\epsilon'}-\delta'}(Y;E|X)_\sigma. \end{aligned}$$

B. Protocol Description

Fix a joint probability distribution $p_{X,Y}(x,y)$ over the finite alphabets $\{\mathcal{X},\mathcal{Y}\}$ and let

$$\begin{aligned} & r \leq I_H^{\epsilon-\delta}(X;B)_\rho + O(\log_2\frac{\epsilon}{\delta}), \\ & R + \tilde{R} \leq I_H^{\epsilon-\delta}(Y;B|X)_\sigma + O(\log_2\frac{\epsilon}{\delta}), \\ & \tilde{R} \geq \tilde{I}_{max}^{\sqrt{\epsilon'}-\delta'}(Y;E|X)_\sigma + O(\log_2\frac{1}{\delta'}), \end{aligned}$$

where ρ and σ are defined in the preceding subsection. We choose $|\mathcal{M}| = 2^r$, $|\mathcal{L}| = 2^R$ and $|\mathcal{K}| = 2^{\tilde{R}}$ implying that r and R denote our public and private rates, respectively and $|\mathcal{K}|$ stands for the size of the local key. In order to accomplish this information-processing task, before communication begins, Alice, Bob and Eve have access to a shared quantum state given in (2). Upon receiving the messages pair (m,ℓ), Alice goes to the m-th copy of $\rho^{\otimes|\mathcal{M}|}_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}}$. There she runs the protocol for the private capacity, by dividing $|\mathcal{L}||\mathcal{K}|$ copies into $|\mathcal{L}|$ bins (this structure is revealed to all parties) and selecting uniformly at random one of the A systems (among $|\mathcal{K}|$ copies) inside the ℓ-th bin. Upon receiving B, Bob performs a position-based decoding to obtain the public message m (and hence the correct copy of $\rho_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}}$). The choice of the rate for public message r ensures that this is possible and gentle measurement lemma ([17]) ensures that the quantum state of the correct copy of $\rho_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}}$ is almost unchanged after Bob's decoding. To decode ℓ, Bob performs another position-based decoding strategy, conditioned on X, meaning that having found the correct copy of $\rho_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}}$ used in the transmission, Bob measures the X system and applies his second decoder conditioned on this x. For this strategy, Bob first appeals to the definition of the conditional smooth hypothesis testing mutual information, to assume that the distribution over X was $p'(x)$ (achieving the infimum in the definition) with negligible error. Then for $x \in$ supp(x'), he performs position-based decoding. The choice of $R+\tilde{R}$ guarantees the successful decoding for every x and at the same time, the security criterion is ensured from the fact that even if Eve is aware of the correct copy of $\rho_{XX'(AYY')^{|\mathcal{L}||\mathcal{K}|}}$, the condition that convex splitting lemma imposes on $|\mathcal{K}|$, gives her very small information about ℓ for every $x \in \mathrm{supp}(p''(x))$ (where $p''(x)$ is the distribution achieving the infimum in the definition of conditional smooth alternative max-mutual information). Now we can derandomize the protocol by fixing the values in corresponding systems. Upon derandomization, the code is publicly available.

IV. Conclusion

By appealing to the concepts of superposition and Wyner's secrecy coding, we come up with a conceptually similar idea to transmit simultaneously public and private messages over a single use of a quantum channel. Our main tools are position-based decoding and convex-split lemma. Achievability and converse regions are presented. Assessing our bounds in i.i.d. regime and comparing them with the existing asymptotic bounds in the literature is a future direction.

Appendix A
Position-Based Decoders

To decode the public message m, Bob employs the following decoding isometry:

$$\mathcal{D}^1_{B\Upsilon_X \to \hat{M}B}(\rho^{m,(\ell,k)}_{X|\mathcal{M}|B}) := \sum_{m=1}^{|\mathcal{M}|} \Bigg(\mathrm{Tr}\{\Lambda^m_{X|\mathcal{M}|B}\rho^{m,(\ell,k)}_{X|\mathcal{M}|B}\}|m\rangle\langle m|_{\hat{M}} \otimes \frac{\sqrt{\Lambda^m_{X|\mathcal{M}|B}}\rho^{m,(\ell,k)}_{X|\mathcal{M}|B}\sqrt{\Lambda^m_{X|\mathcal{M}|B}}}{\mathrm{Tr}\{\Lambda^m_{X|\mathcal{M}|B}\rho^{m,(\ell,k)}_{X|\mathcal{M}|B}\}} \Bigg),$$

where for $m \in [1,|\mathcal{M}|]$:

$$\Lambda^m_{X|\mathcal{M}|B} = \left(\sum_{m'=1}^{|\mathcal{M}|} \Gamma^{m'}_{X|\mathcal{M}|B} \right)^{-\frac{1}{2}} \Gamma^m_{X|\mathcal{M}|B} \left(\sum_{m'=1}^{|\mathcal{M}|} \Gamma^{m'}_{X|\mathcal{M}|B} \right)^{-\frac{1}{2}},$$

and $\quad \Gamma^m_{X|\mathcal{M}|B} = \mathbb{1}^1_X \otimes \mathbb{1}^2_X \otimes ... \otimes T^m_{XB} \otimes ... \otimes \mathbb{1}^{|\mathcal{M}|}_X,$

in which T^m_{XB} is a test operator distinguishing between two hypotheses, namely ρ_{XB} and $\rho_X \otimes \rho_B$ and $\rho^{m,(\ell,k)}_{X|\mathcal{M}|B}$ is given in section III.
Bob's decoder for the private message ℓ is constructed as follows:

$$\mathcal{D}^2_{\hat{M}B\Upsilon_Y \to \hat{L}}(\sigma^{x,m,(\ell,k)}_{Y|\mathcal{L}||\mathcal{K}|B}) := \sum_{l=1}^{|\mathcal{L}|} \mathrm{Tr}\{P^{x,\ell}_{Y|\mathcal{L}||\mathcal{K}|B}\sigma^{x,m,(\ell,k)}_{Y|\mathcal{L}||\mathcal{K}|B}\}|\ell\rangle\langle\ell|_{\hat{L}},$$

where $\quad P^{x,\ell}_{Y|\mathcal{L}||\mathcal{K}|B} = \sum_{k=1}^{|\mathcal{K}|} P^{x,(\ell,k)}_{Y|\mathcal{L}||\mathcal{K}|B}, \quad$ and $\quad P^{x,(\ell,k)}_{Y|\mathcal{L}||\mathcal{K}|B} =$

$$\left(\sum_{\ell'=1}^{|\mathcal{L}|} \sum_{k'=1}^{K} N^{x,(\ell',k')}_{Y|\mathcal{L}||\mathcal{K}|B} \right)^{-\frac{1}{2}} N^{x,(\ell,k)}_{Y|\mathcal{L}||\mathcal{K}|B} \left(\sum_{\ell'=1}^{|\mathcal{L}|} \sum_{k'=1}^{|\mathcal{K}|} N^{x,(\ell',k')}_{Y|\mathcal{L}||\mathcal{K}|B} \right)^{-\frac{1}{2}},$$

and for $\ell \in [1,|\mathcal{L}|]$, and $k \in [1,|\mathcal{K}|]$,

$$N^{x,(\ell,k)}_{Y|\mathcal{L}||\mathcal{K}|B} = \mathbb{1}^{(1,1)}_Y \otimes ... \otimes \mathbb{1}^{(1,|\mathcal{K}|)}_Y \otimes ... \otimes \mathbb{1}^{(\ell,k-1)}_Y \otimes Z^{x,(\ell,k)}_{YB} \otimes \mathbb{1}^{(\ell,k+1)}_Y ... \otimes \mathbb{1}^{(|\mathcal{L}|,|\mathcal{K}|)}_Y,$$

in which $Z^{x,(\ell,k)}_{YB}$ is a binary test operator distinguishing between two hypotheses σ^x_{YB} and $\sigma^x_Y \otimes \sigma^x_B$.

Acknowledgment

The first author would like to thank Prof. Andreas Winter for a lot of fruitful discussions especially those on the classical wiretap channel related to this work. M.-H. Hsieh was supported by an ARC Future Fellowship under Grant FT140100574 and by US Army Research Office for Basic Scientific Research Grant W911NF-17-1-0401. The work of F. Salek and J. R. Fonollosa has been funded by the "Ministerio de Economía, Industria y Competitividad" of the Spanish Government, ERDF funds (TEC2013-41315-R, TEC2015-69648-REDC, TEC2016-75067-C4-2-R) and the Catalan Government (2017 SGR 578 AGAUR). The work of A. Anshu and R. Jain is supported by the Singapore Ministry of Education and the National Research Foundation, through the Tier 3 Grant "random numbers from quantum processes" MOE2012-T3-1-009 and NRF RF AwardNRF-NRFF2013- 13.

References

[1] C. E. Shannon, "A mathematical theory of communication," *Bell system Tech. J.*, Vol. 27, pp. 379-656, 1948.

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

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

[4] I. Deveatk, "The private classical capacity and quantum capacity of a quantum channel," *IEEE. Trans. Inf. Theory,* vol. 51, pp. 44-55, 2005.

[5] n. Cai, A. Winter and R. Yeung, "Quantum privacy and quantum wiretap channels," *problems of information transmission,* vol. 40, no. 4, pp. 1613-1622, 1997.

[6] R. Renner, S. Wolf, and J. Wullschleger, "The signle-serving channel capacity," *Proc. IEEE. Int. Symp. Information Theory,* pp. 1424-1427, 2006.

[7] M. Mosoni and N. Datta, "Generalized relative entropies and the capacity of classical-quantum channel," *J. Mathematical Physics,* vol. 15, no. 7, pp. 072104-14, 2009.

[8] L. Wang and R. Renner, "One-shot classical-quantum capacity and hypothesis testing," *Phys. Rev. Lett.,* vol. 108, no. 20, p. 200501, 2012.

[9] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE. Trans. Inf. Theory,* vol. 57, no. 11, 2011.

[10] M. M. Wilde, "Position-based coding and convex splitting for private communication over quantum channels," *Quantum inf. Process,* vol. 16, no. 10, article no. 264, 2017.

[11] A. Anshu, R. Jain, and N. A. Warsi, "One shot entanglement-assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach," February 2017, arXiv:1702.01940.

[12] J. Radhakrishnan, P. Sen and N. A. Warsi, "One-shot private classical capacity of quantum wiretap channel: based on one-shot quantum covering lemma," ,arXiv: 1703.01932v1, 2017.

[13] R. Ahlswede and A. Winter, "Strong converse for identification via quantum channels," *IEEE Trans. Inf. Theory,* vol. 48, pp. 569-579, 2002.

[14] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory,* vol. 24, no. 3, pp. 339-348, 1978.

[15] A. Anshu, V. K. Devabathini and R. Jain, "Quantum message compression with application," *Phys. Rev. Lett.,* vol. 119, iss. 12, 2017.

[16] I. Devetak, P. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Commmun. Math. Phys.* 256, 287-303, 2005.

[17] Mark M. Wilde,*Quantum Information Theory.* Cambridge University pres, second edition, February 2017.

[18] N. Datta, "Min- max-relative entropies and a new entanglement monotone," *IEEE. Trans. Inf. Theory,* vol. 59, pp. 2816-2816, 2009.

[19] M. Berta, M. Christandl and R. Renner, "The quantum reverse Shannon theorem based on one-shot information theory," *Commun. Math. Phys.,* vol. 306, no. 3, pp. 579-615, 2011.