One-Shot Private Classical Capacity of Quantum Wiretap Channel: Based on one-shot quantum covering lemma

Jaikumar Radhakrishnan * Pranab Sen † Naqueeb Ahmad Warsi ‡

We consider the problem of communication over a quantum wiretap channel with one sender (Alice) and two receivers Bob (legitimate receiver) and Eve (eavesdropper). They have access to a quantum channel whose characteristics is given by the super operator $\mathcal{N}^{A\to BE}$. The channel takes input the register A (supplied by Alice) and produces a quantum state ρ^{BE}, where the register B is Bob's share of the channel output and E is Eve's share of the channel output.

To send a message $m \in [1 : 2^R]$ Alice first encodes her message into a suitable form to mitigate the effect of channel and also to keep it secure from Eve. One widely used security measure is the L_1 distance (trace distance) $\delta := \left\|\rho^{ME} - \rho^M \otimes \rho^E\right\|$ where ρ^{ME} represents the joint state between the message register and the channel output at Eve's end. The states ρ^M, ρ^E are the appropriate marginals of ρ^{ME}. The goal is to obtain bounds on the best possible value of R such that Alice may communicate with high reliability to Bob, and high security against Eve.

Devetak in [2] and Cai-Winter-Yeung in [3] first studied this problem in the limit of many independent channel uses of the channel $\mathcal{N}^{A\to BE}$ (asymptotic iid setting) where in they showed the following:

Fact 1. *The private classical capacity of a quantum channel $\mathcal{N}^{A\to BE}$ in the asymptotic iid setting is the following:* $\lim_{k\to\infty} \frac{1}{k} P(\mathcal{N}^{\otimes k})$, *where $P(\mathcal{N})$ is defined as*

$$P(\mathcal{N}) := \sup_F \left(I[V;B]_\sigma - I[V;E]_\sigma\right),$$

where the supremum is taken over all (auxiliary) random variables V and functions $F : v \mapsto \rho_v^A$, ρ_v^A being states in the input Hilbert space A of the channel. Above, all the information theoretic quantities are calculated with respect to the following state:

$$\sigma^{VBE} = \sum_{v\in\mathcal{V}} p_V(v)|v\rangle\langle v|^V \otimes \mathcal{N}^{A\to BE}(\rho_v^A).$$

Our Result: We consider the above problem in the quantum one-shot setting. We need the following definitions to discuss our results.

*Tata Institute of Fundamental Research, Mumbai, Email: jaikumar@tifr.res.in

†Tata Institute of Fundamental Research, Mumbai, Email: pgdsen@tcs.tifr.res.in

‡SPMS, NTU, CQT, NUS, Singapore, IIITD, Delhi Email: naqueeb@iiitd.ac.in A detailed version of this work appears in arXiv:1703.01932 [1].

Definition 1. *(Quantum hypothesis testing divergence [4]) Let $\rho^{VB} := \sum_{v\in\mathcal{V}} p_V(v)|v\rangle\langle v|^U \otimes \rho_v^B$ be a classical quantum state. For $\varepsilon \in [0,1)$ the hypothesis testing divergence between the systems V and B is defined as follows:*

$$I_0^\varepsilon[V;B] := \sup_{\substack{0\prec\Gamma\prec\mathbb{I} \\ \mathrm{Tr}\left[\Gamma\rho^{VB}\right]\geq 1-\varepsilon}} -\log \mathrm{Tr}\left[\Gamma\left(\rho^V\otimes\rho^B\right)\right].$$

Definition 2. *(Quantum smooth max Rényi divergence) Let $\rho^{VE} := \sum_{v\in\mathcal{V}} p_V(v)|v\rangle\langle v|^V \otimes \rho_v^E$ be a classical quantum state. For $\varepsilon \in [0,1)$ the smooth max Rényi divergence between the systems V and E is defined as follows:*

$$I_\infty^\varepsilon[V;E] := \inf\left\{\gamma : \sum_{v\in\mathcal{V}} p_V(v)\mathrm{Tr}\left[\left\{\rho_v^E \succ 2^\gamma\rho^E\right\}\rho_v^E\right] \leq \varepsilon\right\},$$

where $\rho^E = \mathrm{Tr}_V\left[\rho^{VE}\right]$ and $\left\{\rho_v^E \succ 2^\gamma\rho^E\right\}$ is the projector onto the positive Eigen space of the operator $\rho_v^E - 2^\gamma\rho^E$.

Theorem 1. *(Achievability) Let $\mathcal{N}^{A\to BE}$ be a quantum wiretap channel. Let V be a random variable taking values in $\mathcal{V}$ and $F : \mathcal{V} \to \mathcal{S}(\mathcal{H}_A)$. Consider the state*

$$\rho^{VBE} = \sum_{v\in\mathcal{V}} p_V(v)|v\rangle\langle v|^V \otimes \mathcal{N}^{A\to BE}\left(\rho_v^A\right).$$

For every $\varepsilon \in (0,1)$ and $\delta \in (0,2)$ there exists a code with rate R, error probability at most ε and security at most δ for the quantum wiretap channel $\mathcal{N}^{A\to BE}$ if

$$R \leq \sup_{\{V,F\}}\left(I_0^{\varepsilon'}[V;B] - \max\left\{0, I_\infty^{\hat{\delta}}[V;E]\right\}\right) + \log\left(\varepsilon'\right) + \log\left(\hat{\delta}^9\right) - \mathcal{O}\left(\log\log(\dim(\mathcal{H}_E))\right)$$

where $18\varepsilon' \leq \varepsilon$ and $\hat{\delta}$ is such that $144\sqrt{\hat{\delta}} \leq \delta$. The information theoretic quantities mentioned above are calculated with respect to the state given above.

Theorem 2. *(Converse) For a quantum wiretap channel $\mathcal{N}^{A\to BE}$,*

$$R \leq \sup_{\{V,F\}}\left(I_0^\varepsilon[V;B] - I_\infty^\delta[V;E]\right) + 1.5,$$

where V is a random variable over a set $\mathcal{V}$, $F : \mathcal{V} \to \mathcal{S}(\mathcal{H}_A)$ a map from $\mathcal{V}$ to $\mathcal{S}(\mathcal{H}_A)$ and all the information theoretic quantities are calculated with respect to the following state:

$$\Theta^{VBE} := \sum_{v\in\mathcal{V}} p(v)|v\rangle\langle v|^V \otimes \mathcal{N}^{A\to BE}\left(\rho_v^A\right).$$

Techniques: Our achievability proof follows along the line of the proof in [5]. We generate an array of codewords, with iid entries according to p_V. We then partition this array into bands of an appropriate size and uniquely assign each of these bands to a message. To send a message $m \in [2^R]$, Alice chooses a codeword v uniformly from the band corresponding to m; applies the map F to v and then transmits the resulting state ρ_v^A over the channel. Bob on receiving his share of the channel output tries to determine the codeword v using standard one-shot decoding techniques for a point to point quantum channel. He succeeds with high probability for the given codebook size. It only remains to show that the message m is secret from

Eve. The random choice of v from the band corresponding to m should make Eve's share of the channel output independent of m. This is the main technical hurdle that must be overcome in order to prove the correctness of a code for a wiretap channel. In the asymptotic iid setting, this hurdle is overcome by proving a *quantum covering lemma* [5, Lemma 16.2.1] based on an operator Chernoff bound of Ahlswede-Winter [6] for Hermitian matrices . Unfortunately, a straightforward translation of this technique to one-shot setting fails. In this work, we overcome these difficulties and manage to prove for the first time a *one-shot quantum covering lemma* mentioned below.

Theorem 3. *(***One-shot quantum covering lemma***)*
Let $\mathbf{X}$ *be a random variable taking values in the set* $\mathcal{X}$*. For each* $x \in \mathcal{X}$*, let* ρ_x *be a quantum state in the space* $\mathcal{H}$*. Define* $\rho := \mathbb{E}_{\mathbf{X}}[\rho_{\mathbf{X}}]$*. Let* $\varepsilon > 0$*. Suppose* $\mathbf{s} = (\mathbf{X}[1], \mathbf{X}[2], \ldots, \mathbf{X}[M])$ *is a sequence of independent random samples drawn according to the distribution of* $\mathbf{X}$*, and let* $\tilde{\rho} = \mathbb{E}_{m\in[M]}[\rho_{X[m]}]$*. Then,*

$$\Pr_{\mathbf{s}}\left\{\|\tilde{\rho} - \rho\| \geq 22\sqrt{\varepsilon}\right\} \leq 30(\dim \mathcal{H})^2 \exp\left(-\frac{10^{-16}\varepsilon^9}{\left(\log_2\left(\dim(\mathcal{H})\right)\right)^6}\frac{M}{2^I}\right).$$

On the way, we also prove a novel operator Chernoff bound for non-square matrices.

Proposition 1. *(***Chernoff bound for non-square matrices***)*
Let $d_1 \geq d_2$*. Let* $\mathbf{X}$ *be a random variable taking values in a set* $\mathcal{X}$*. For each* $x \in \mathcal{X}$*, let* $A_x \in \mathbb{C}^{d_1\times d_2}$ *be a matrix. Let* $\mu \geq 0$ *and ,* $\beta \geq 1$ *be such that* $\|A_x\| \leq \mu$ *and* $\|A_x\|_\infty \leq \frac{\beta}{d}$ *for all* $x \in \mathcal{X}$*. Let* $A = \mathbb{E}_{\mathbf{X}}\left[A_{\mathbf{X}}\right]$ *be the average of the matrices* A_x*. Suppose* $\mathbf{s} = (\mathbf{X}[1], \mathbf{X}[2], \ldots, \mathbf{X}[M])$ *is a sequence of random samples drawn according to the distribution of* X*, and* $\tilde{A} = \mathbb{E}_{m\in[M]}[A_{\mathbf{X}[m]}]$*. Then, for* $0 < \varepsilon < \frac{1}{2}$*,*

$$\Pr_{\mathbf{s}}\left\{\|\tilde{A} - A\| \leq \varepsilon\right\} \geq 1 - 4d_1 \exp\left(\frac{-\varepsilon^2}{32\ln(2)\mu}\frac{M}{2\beta+\mu}\right).$$

The proof for the converse (Theorem 2) essentially follows along the line of the proof given in [7]; the translation to the one-shot quantum setting is straightforward.

Related work: In [8] Renes and Renner derive one-shot achievability and converse bounds for the quantum wiretap channel in terms of conditional min and max Rényi entropies. They also show that their result asymptotically yields the results of [2] and [3]. However, the result of Renes and Renner [8] does not seem to yield the asymptotic characterisation of the wiretap channel in the information spectrum (asymptotic non-iid) setting. Such a result is known however for the classical case [7]. We remark that our one-shot bounds allow us to characterise the capacity of the wiretap channel in the information spectrum (asymptotic non-iid) setting; our characterisation turns out to be nothing but the quantum analogue of the result in [7]. This characterisation naturally recovers the results of [2] and [3] in the asymptotic iid setting.

A recent paper by Wilde [9] studies the one-shot quantum wiretap channel, and obtains a very similar result using techniques called convex-split and position based decoding introduced originally in [10, 11]. The technique of convex-split is simpler than the one we introduce in this work. However, the one-shot covering lemma which we introduce in our work has the advantage that it gives an exponential Chernoff style concentration result whereas convex split does not guarantee anything better than Markov style concentration. In the setting where there is one Bob but t Eves, our techniques allow us to get the same security δ with a loss of $\log\log(t/\delta)$ bits of message. Convex split would lose as much as $I_\infty^{\sqrt{\delta/t}}[V;E]$ bits of message which is much larger.

References

[1] J. Radhakrishnan, P. Sen, and N. A. Warsi, "One-shot private classical capacity of quantum wiretap channel: Based on one-shot quantum covering lemma." https://arxiv.org/abs/1703.01932, 2017.

[2] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, Jan. 2005.

[3] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum channel," *Prob. Inf. Trans.*, vol. 40, no. 4, pp. 318–336, 2004.

[4] L. Wang and R. Renner, "One-shot classical-quantum capacity and hypothesis testing," *Phys. Rev. Lett.*, vol. 108, pp. 200501–200505, May 2012.

[5] M. M. Wilde, "From classical to quantum Shannon theory." http://arxiv.org/abs/1106.1445, 2011.

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

[7] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channel," in *Proc. Allerton Conf. Commun. Control, Computing*, (Monticello, IL, USA), Sept. 2008.

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

[9] M. M. Wilde, "Position-based coding and convex splitting for private communication over quantum channels." https://arxiv.org/abs/1703.01733, 2017.

[10] A. Anshu, V. K. Devabathini, and R. Jain, "Quantum message compression with applications." arXiv:1410.3031, 2014.

[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." https://arxiv.org/abs/1702.01940, 2017.