Benchmarking the utility of a quantum channel for secure communications*

David Elkouss and Sergii Strelchuk

Abstract

The private capacity gauges the practical value of quantum channels for secure communications. Unfortunately, this quantity is given by the infinite regularization of the private information. Can we stop the regularization at some finite universal constant independent of the channel and still evaluate the capacity with arbitrary precision? Here we show that this is not the case.

The private capacity of a quantum channel [1] has a clear operational interpretation. It quantifies the maximum rate at which the sender, Alice, can send private *classical* communication to the receiver, Bob. This capacity also characterizes the optimal rates for secret key generation. Hence, a better understanding of this quantity would allow to evaluate precisely the usefulness of quantum channels for secure communications. Little is known about private capacity of individual channels. For instance, the private capacity of Gaussian channels [2] remains open. Beyond the pure loss channel [3] only lower bounds on the private information of a single use are known.

Formally, the private capacity is given by the following regularized quantity:

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}). \tag{1}$$

where $\mathcal{P}^{(1)}(\mathcal{N})$ is the private information of the channel.

Despite the relevance of the private information, we still understand very little about its behaviour when the communication channel is used many times. It is shown in [4, 5] that $\mathcal{P}^{(1)}(\mathcal{N})$ is superadditive for a small finite number of channel uses, although the magnitude of this effect is quantitatively very small.

Here we show that private information can be strictly superadditive for an arbitrarily large number of uses of the channel. This implies that there does not exist a universal constant k, independent of the channel, such that the private information regularized after k uses already gives the private capacity. More precisely, we prove the following theorem:

Theorem 1. *For any n there exists a quantum channel $\mathcal{N}_n$ such that for $n > k \geq 1$:*

$$\frac{1}{k}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes k}) < \mathcal{P}(\mathcal{N}). \tag{2}$$

In the following we introduce our channel construction and give a sketch of the proof.

Channel construction. We start with the definition of the *switch channels*:

$$\mathcal{N}^{SA\to SB}(\rho^{SA}) = \sum_i P_i^{S\to S} \otimes \mathcal{N}_i^{A\to B}(\rho^{SA}), \tag{3}$$

[*] Full technical version in arXiv:1502.05326

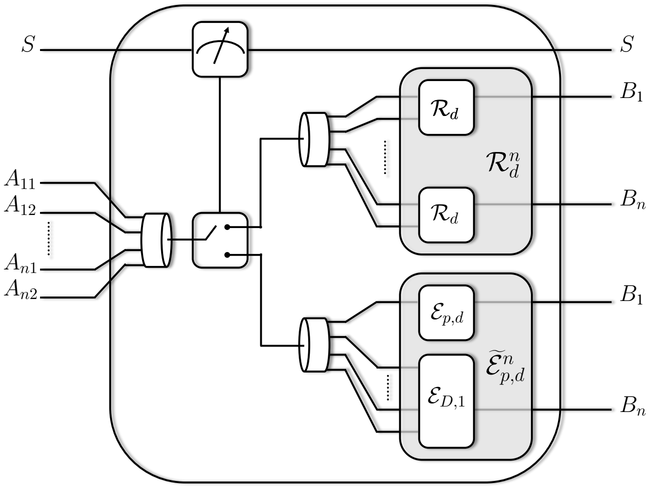

Figure 1: The channel has two input registers the control register S and the data register A. The control register is measured in the computational basis and depending on the output either the erasure channel $\widetilde{\mathcal{E}}_{p,d}^n$ or n copies of the d-dimensional rocket channel are applied.

which consists of two input registers S and A of dimensions d and n respectively. Register S is measured in the standard basis and conditioned on the measurement outcome i a *component* channel $\mathcal{N}_i$ is applied to the second register. The computation of $\mathcal{P}^{(1)}(\mathcal{N})$ when $\mathcal{N}$ is of the form (3) can be simplified; it suffices to restrict inputs to a special form.

There are two types of channels which we will use in place of $\mathcal{N}_i$. The first channel is the erasure channel:

$$\mathcal{E}_{p,d}^{A\to B}(\rho_A) = (1-p)\rho_B + p|e\rangle\langle e|_B, \tag{4}$$

where $|e\rangle\langle e|$ is the erasure flag and d the dimension of the input register A.

The second channel that we use alongside $\mathcal{E}_{p,d}$ is a d-dimensional 'rocket' channel, $\mathcal{R}_d$ [6]. It consists of two d-dimensional input registers A_1 and A_2 and a d-dimensional output register B. A_1 and A_2 are first subject to a random unitary and then jointly decoupled with a controlled dephasing gate. Then, the contents of A_1 becomes the output of the channel and the contents of A_2 is traced out. Bob also receives the classical description of the unitaries which acted on A_1 and A_2. Since dephasing occurs after the input registers have been scrambled by a random unitary, it is very hard for Alice to code for such channel, hence it has a very low classical capacity: $\mathcal{C}(\mathcal{R}_d) \leq 2$.

Our switch channel construction has the following form:

$$\mathcal{N}_{n,p,d} = P_0 \otimes \mathcal{R}_d^n + P_1 \otimes \widetilde{\mathcal{E}}_{p,d}^n. \tag{5}$$

That is, it allows Alice to choose between $\mathcal{R}_d^n = \mathcal{R}_d^{\otimes n}$ and $\widetilde{\mathcal{E}}_{p,d}^n = \mathcal{E}_{p,d} \otimes \mathcal{E}_{1,d^{2n-1}}$; a d-dimensional erasure channel padded with a full erasure channel to match the input dimension of $\mathcal{R}_d^n$ (see Figure 1).

Proof sketch. The first step of the proof consists in showing a strict upper bound on the private information. In general, to upper bound the private information of a switch channel we need to optimize over all the possible different choices of the components. After some careful algebra we can show that there exists a range of p and d such that the private information of k uses of the channel $\mathcal{N}_{n,p,d}$ is strictly upper bounded by:

$$\frac{1}{k}\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k}, \rho) < \frac{k}{k+1}(1-p)\log d, \tag{6}$$

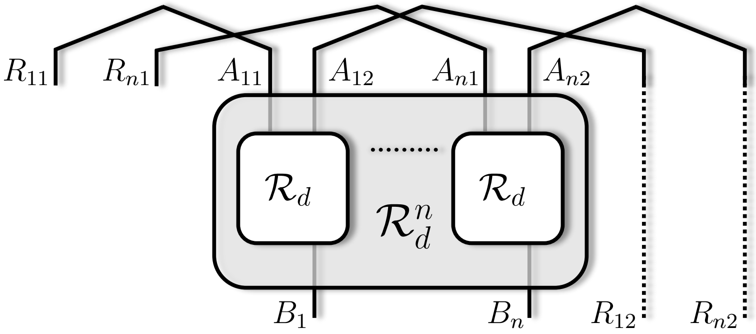

Figure 2: The first part of the protocol consists sending a state maximally entangled between the different inputs of the rocket channel and an external reference.

with $k < n - 2$. The second step of the proof is to show that the right hand side of (6) can be achieved by some concrete input on $k + 1$ uses of the channel. The idea behind the input is to perform a *ping-pong* trick used in [7]. Alice, the sender, prepares a maximally entangled between an external reference and the inputs of the rocket channel (see Figure 2). The inputs to the $A_{11}, A_{21}, \ldots, A_{n1}$ registers get randomly dephased by the rocket channel and almost no privacy can be extracted. However, if Bob, the receiver, had access to the registers $R_{12}, R_{22}, \ldots, R_{n2}$ he would be able to undo the dephasing and distill maximally entangled states between the registers $R_{11}, R_{21}, \ldots, R_{n1}$ and $B_1, B_2, \ldots, B_n$. He has no access to $R_{12}, R_{22}, \ldots, R_{n2}$ but Alice can send these registers to him through the erasure channel. Whenever one register reaches Bob, he can distill a maximally entangled state. The analysis of this protocol shows that the right hand side of (6) is achievable.

Discussion. Here, we prove that it is not possible to compute the private capacity with arbitrary precision if we stop the regularization after a constant number of uses (with the constant being channel independent). However, there are channels for which we know that a single use suffices to compute the private capacity; and we might conjecture that there should be channels for which two or three uses suffice. What are the differences between these channels? The answer to this question, and more generally, to the question of what properties a channel has to verify such that its capacity can be computed after a finite regularization are wide open.

References

[1] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *Information Theory, IEEE Transactions on*, vol. 51, pp. 44–55, Jan 2005.

[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012.

[3] M. M. Wolf, D. Pérez-García, and G. Giedke, "Quantum Capacities of Bosonic Channels," *Phys. Rev. Lett.*, vol. 98, p. 130501, Mar 2007.

[4] G. Smith, J. M. Renes, and J. A. Smolin, "Structured codes improve the Bennett-Brassard-84 quantum key rate," *Phys. Rev. Lett.*, vol. 100, no. 17, p. 170502, 2008.

[5] O. Kern and J. M. Renes, "Improved one-way rates for BB84 and 6-state protocols," *Quantum Information & Computation*, vol. 8, no. 8, pp. 756–772, 2008.

[6] G. Smith and J. A. Smolin, "Extensive Nonadditivity of Privacy," *Phys. Rev. Lett.*, vol. 103, p. 120503, Sep 2009.

[7] C. H. Bennett, I. Devetak, P. W. Shor, and J. A. Smolin, "Inequalities and Separations Among Assisted Capacities of Quantum Channels," *Phys. Rev. Lett.*, vol. 96, p. 150502, Apr 2006.