Quantum data hiding with continuous variable systems

Preprint arXiv:2102.01100

Ludovico Lami

Introduction. Suppose we want to benchmark a quantum device held by a remote party, e.g. by testing its ability to carry out challenging quantum measurements outside of a free set of measurements $\mathscr{M}$. A very simple way to do so is to set up a binary state discrimination task that cannot be solved efficiently by means of free measurements. If one can find pairs of orthogonal states that become arbitrarily indistinguishable under measurements in $\mathscr{M}$, in the sense that the error probability in discrimination approaches that of a random guess, one says that there is data hiding against $\mathscr{M}$. Let us note in passing that quantum data hiding, with which we are concerned here, has a classical analogue that has been studied under the name of *secret sharing* [1, 2].

Prior to our work, data hiding had been investigated exclusively for finite-dimensional systems and mostly against the set of measurements implementable with local operations and classical communication, denoted $\mathscr{M} = \text{LOCC}$. However, substantially new phenomena emerge when we look instead at continuous variable (CV) systems, for the good reason that in experimental practice those systems feature natural sets of measurements that are easily implementable (for example, homodyne and heterodyne detection, or more generally Gaussian measurements).

Here we present three main results: first, a versatile bound on the accuracy of the Braunstein–Kimble teleportation protocol [3, 4] that in itself has nothing to do with data hiding and that we expect to find a variety applications well beyond the study of this problem (Theorem 1); second, a bound on the strength of data hiding against LOCC measurements that is achievable with bipartite states of a fixed local energy (photon number), whose proof rests crucially on Theorem 1; and third, the first ever example of two single-mode states achieving data hiding against the set of CV measurements implementable with Gaussian operations and feed-forward of measurement outcomes.

In short, the reason why we believe that this work fits in the remit of QIP is that it sheds light on a basic phenomenon with a clear operational interpretation that lends itself to potential technological applications, and it does so while developing a set of tools that will be arguably important for the design and analysis of CV quantum circuits (see the discussion after Theorem 1).

The setting. In a *binary quantum state discrimination* problem one of two known states ρ and σ is prepared randomly (with known a priori probabilities p and $1-p$, respectively), and the task consists in guessing which one. We will refer to the triple $(\rho, \sigma; p)$ as a *scheme*. A set of available strategies is modelled by a family $\mathscr{M}$ of quantum measurements, mathematically described by *positive operator-valued measures* (POVM) $E(dx)$ over a measurable space $\mathcal{X}$ that in addition obey the *normalisation condition* $\int_{\mathcal{X}} E(dx) = \mathbb{1}$ [5, Definition 11.29]. The outcome of E on ρ is described by a random variable X over $\mathcal{X}$ with probability measure $\mu_X(dx) = \mathrm{Tr}[\rho E(dx)]$. Using this formula, one can show that a class of measurements $\mathscr{M}$ yields an optimal error probability

$$P_e^{\mathscr{M}}(\rho, \sigma; p) = \frac{1}{2}\left(1 - \|p\rho - (1-p)\sigma\|_{\mathscr{M}}\right), \tag{1}$$

$$\|Z\|_{\mathscr{M}} := \sup_{E\in\mathscr{M}} \int_{\mathcal{X}} |\mathrm{Tr}[Z E(dx)]| \,. \tag{2}$$

Note that in the case where $\mathscr{M} = \text{ALL}$ is the set of all measurements, (2) yields the trace norm, and hence (1) reproduces the well-known Holevo–Helstrom formula $P_e(\rho, \sigma; p) = \frac{1}{2}\left(1 - \|p\rho - (1-p)\sigma\|_1\right)$ for the minimal probability of error [6, 7]. In the general case, the trace norm is replaced by the *distinguishability norm* $\|\cdot\|_{\mathscr{M}}$ associated with $\mathscr{M}$. For a scheme $(\rho, \sigma; p)$ and a set of measurements $\mathscr{M}$, we denote the *bias* with $\beta_{\mathscr{M}}(\rho, \sigma; p) := \|p\rho - (1-p)\sigma\|_{\mathscr{M}}$; accordingly, we also define $\beta_1(\rho, \sigma; p) := \|p\rho - (1-p)\sigma\|_1$. Dropping the dependence on the scheme, as we will do from now on whenever that is clear from the context, we have that $\beta_{\mathscr{M}} = 1 - 2P_e^{\mathscr{M}}$ and $\beta_1 = 1 - 2P_e$, so that the bias is just an alternative and more convenient parametrisation of the error probability.

A family of schemes $(\rho_n, \sigma_n; p_n)_{n\in\mathbb{N}}$ exhibits *data hiding* against a set of measurements $\mathscr{M}$ if [8–18]

$$\lim_{n\to\infty} \beta_1(\rho_n, \sigma_n; p_n) = 1\,, \quad \lim_{n\to\infty} \beta_{\mathscr{M}}(\rho_n, \sigma_n; p_n) = 0\,. \tag{3}$$

In light of (1), this amounts to saying that $\lim_n P_e(\rho_n, \sigma_n; p_n) = 0$ but $\lim_n P_e^{\mathscr{M}}(\rho_n, \sigma_n; p_n) = 1/2$, capturing the intuition that the two states ρ_n and σ_n should become close to perfectly distinguishable under general measurements but almost indistinguishable under measurements in $\mathscr{M}$. As it turns out, thanks to (3) we can prove that the schemes $(\rho_n, \sigma_n; p_n)$ exhibit data hiding if and only if $(\rho_n, \sigma_n; 1/2)$ do as well. In other words, we can assume that $p_n \equiv 1/2$ without loss of generality.

Main results.
1. Braunstein–Kimble teleportation. We first look at a problem that on the surface has nothing to do with data hiding, but whose solution will turn out to play a key role in the analysis of CV data hiding against LOCC measurements. The Braunstein–Kimble teleportation protocol is a fundamental primitive in CV quantum information [3, 4]. It allows to teleport an m-mode system A to a distant location B, using only local operations, in particular homodyne detections, classical communication, and consuming as a resource m two-mode squeezed vacuum states $|\psi(r)\rangle := \operatorname{sech}(r)\sum_{k=0}^{\infty}(-1)^k \tanh^k(r)\,|kk\rangle$. For finite values of the squeezing parameter $r \in \mathbb{R}$ and non-ideal detection efficiency $\eta \in (0,1]$, the output state is not teleported perfectly, but is subjected to a noisy channel. The whole process is described by the transformation [4, Eq. (8)]

$$\rho_{RA} \otimes \left(\psi(r)^{\otimes m}\right)_{A'B} \longmapsto \left(I^R \otimes \mathcal{N}_{\lambda(r,\eta)}^{A\to B}\right)(\rho_{RA}), \tag{4}$$

$$\lambda(r,\eta) := e^{-2r} + \frac{1-\eta^2}{\eta^2}. \tag{5}$$

where R is an arbitrary reference system, and the *Gaussian additive noise channel* $\mathcal{N}_\lambda^{A\to B}$ is defined by the Wigner function transformation $W_\rho \mapsto W_{\mathcal{N}_\lambda(\rho)} := W_\rho \star G_\lambda$, where $G_\lambda(z) := \frac{e^{-\|z\|^2/\lambda}}{\pi^m \lambda^m}$ and $\star$ denotes convolution.

For every fixed ρ_{RA}, the state on the r.h.s. of (4) converges to ρ_{RB}, i.e. the protocol approximates a perfect teleportation, in the limit of $r \to \infty$ and $\eta \to 1^-$. However, it was argued in [19, Section II.B] that such a convergence is strong but not uniform, implying that the values of r and η required to achieve a prescribed accuracy will depend on the input state. Since this dependence is not well understood, and moreover a precise description of the state is often not experimentally available, it is important to have an estimate of the accuracy that is based only on few physically relevant parameters. Our first result goes precisely in this direction.

Theorem 1. *Let A, A', B be m-mode systems, and let R be an arbitrary quantum system. Fix an energy threshold $E > 0$, and consider a state ρ_{RA} such that $\operatorname{Tr}\rho_A N_A - \|z\|^2 \le E$, where N_A is the photon number operator, and $\|z\|^2 := \sum_j |\operatorname{Tr}\rho_A a_j|^2$. Then, the error introduced by Braunstein–Kimble teleportation of ρ_{RA} over a $2m$-mode squeezed vacuum state $\left(\psi(r)^{\otimes m}\right)_{A'B}$ with detection efficiency $\eta \in (0,1]$ can be upper bounded by*

$$\|\widetilde{\rho}_{RB} - \rho_{RB}\|_1 \le \frac{2\,\Gamma\!\left(m+\frac{1}{2}\right)}{(m-1)!}\,\gamma_E\,\sqrt{\lambda(r,\eta)}, \tag{6}$$

$$\gamma_E := \sqrt{E} + \sqrt{E+1}, \tag{7}$$

where $\widetilde{\rho}_{RB} := \left(I^R \otimes \mathcal{N}_{\lambda(r,\eta)}^{A\to B}\right)(\rho_{RA})$, with $\lambda(r,\eta)$ given by (5).

Remark 2. Eq. (6) can be rephrased in terms of a notion called the 'energy-constrained diamond norm' [20–23]. In that language, Eq. (6) implies that $\left\|\mathcal{N}_\lambda^{\otimes m} - I\right\|_\diamond^{N,E} \le \frac{2\,\Gamma(m+1/2)}{(m-1)!}\,\gamma_E\sqrt{\lambda}$, with the same notation as in Theorem 1.

The importance of Theorem 1 lies in the fact that it can be used to determine the values of r and η needed to reach a certain accuracy in the Braunstein–Kimble teleportation (4). Ours is the first such bound that we are aware of. Prior to our work, it was simply not clear how to determine r and η given the desired degree of precision of the overall protocol.

Note that teleportation is a fundamental primitive in a wide variety of quantum algorithms and circuits, as it allows to move around quantum information without physically displacing the systems that carry it. Unsurprisingly, a huge amount of experiments have tried to reproduce it with ever increasing fidelity [24]. Thus, the above Theorem 1 is likely to prove instrumental to design CV quantum circuits with prescribed error tolerance.

2. Data hiding against LOCC. Consider a bipartite quantum system AB in which A is a CV system, and let us look at data hiding against the set of LOCC measurements on AB. In the finite-dimensional case, the maximum gap between the biases β_1 and β_{LOCC} that is achievable can be bounded as a function of the dimension of A [13, 16]. Here A is infinite dimensional, and hence we need to change our approach to the problem. The physical intuition suggests that the local energy E (photon number) on A can play the role of an effective dimension, and hence the maximum gap between β_1 and β_{LOCC} could be bounded as a function of E.

Theorem 3. *Let A be an m-mode CV system, and let B be a generic quantum system. For a scheme $(\rho_{AB}, \sigma_{AB}; p)$ over the bipartite system AB with the property that*

$$\inf_{\alpha\in\mathbb{C}^m} \max\left\{\operatorname{Tr}\left[D(\alpha)\rho_A D(\alpha)^\dagger N_A\right], \operatorname{Tr}\left[D(\alpha)\sigma_A D(\alpha)^\dagger N_A\right]\right\} \le E. \tag{8}$$

for some $E \geq 0$ (for example, it suffices to take $E = \max\{\mathrm{Tr}[\rho_A N_A],\, \mathrm{Tr}[\sigma_A N_A]\}$), it holds that

$$\beta_{\mathrm{LOCC}} \geq \beta_{\mathrm{LOCC}_\rightarrow} \geq c_m \frac{\beta_1^{2m+1}}{\gamma_E^{2m}}\,, \tag{9}$$

where $c_m := \frac{1}{4^{m+1}m}\left(\frac{2m}{2m+1}\right)^{2m+1}\left(\frac{(m-1)!}{\Gamma(m+1/2)}\right)^{2m}$ and as in (7) we set $\gamma_E = \sqrt{E} + \sqrt{E+1}$. For a fixed m, the scaling of (9) with E is tight.

The proof of the above result uses in a crucial way Theorem 1.

3. Data hiding against Gaussian operations and feed-forward of outcomes. In dealing with CV quantum systems, in the experimental practice one is often restricted to implementing measurements that can be obtained via Gaussian operations assisted by classical post-processing of the measurement outcomes (GOCC). Homodyne and heterodyne detections, beam splitters, phase shifters are all examples of GOCC. We can thus wonder: is there data hiding against GOCC?

One could think that the answer should be affirmative, because Gaussian operations are fundamentally limited in so many ways. However, the task of binary state discrimination is also very simple, and in fact Gaussian operations perform surprisingly well at it in so many cases of practical interest. The first such case was investigated by Takeoka and Sasaki [25], who showed that two coherent states can be discriminated 'reasonably well' with GOCC (in fact, with a simple homodyne detection), meaning that there is no data hiding. We extend this intuition further by demonstrating several natural state discrimination problems for which GOCC perform reasonably well in the above sense: any two thermal states, any two consecutive Fock states *of arbitrary photon number*, any two cat states of arbitrary high intensity.

However, and this is our last main result, we are also able to exhibit a (pretty exotic) binary state discrimination problem in a single-mode system that does display data hiding against GOCC. For $\lambda \in [0,1)$, define the states

$$\omega_\lambda^+ := (1-\lambda^2)\sum_{n=0}^{\infty} \lambda^{2n}\, |2n\rangle\!\langle 2n|\,, \qquad \omega_\lambda^- := (1-\lambda^2)\sum_{n=0}^{\infty} \lambda^{2n}\, |2n+1\rangle\!\langle 2n+1|\,, \tag{10}$$

where $|n\rangle$ is the n^{th} Fock state. Consider the scheme $\left(\omega_\lambda^+, \omega_\lambda^-, 1/2\right)$. This can be implemented with a simple experimental procedure starting from a two-mode squeezed vacuum state $|\psi(r)\rangle_{AB}$. By measuring the photon number *parity* on system B [26–29], we are left with the states ω_λ^+ (even) or ω_λ^- (odd), where $\lambda = \tanh(r)$.

We now look at the state discrimination properties of the scheme $\left(\omega_\lambda^+, \omega_\lambda^-, 1/2\right)$. On the one hand, since $\omega_\lambda^\pm$ are orthogonal, they are perfectly distinguishable e.g. by means of photon counting; therefore, $\beta_1 = 1$. On the other hand, discriminating these two states by means of GOCC seems considerably more difficult, and in fact the following holds.

Theorem 4. *For $\lambda \in [0,1)$, the states $\omega_\lambda^+, \omega_\lambda^-$ defined by (10) satisfy that $\frac{1}{2}\left\|\omega_\lambda^+ - \omega_\lambda^-\right\|_1 = 1$ but*

$$\frac{1}{2}\left\|\omega_\lambda^+ - \omega_\lambda^-\right\|_{\mathrm{GOCC}} \leq \frac{1}{2}\left\|\omega_\lambda^+ - \omega_\lambda^-\right\|_{\mathcal{W}_+} \leq 2\left(\frac{1-\lambda}{1+\lambda}\right)^{\frac{1+\lambda^2}{2\lambda}} = 1 - \lambda + O\left((1-\lambda)^2\right)\,. \tag{11}$$

In particular, schemes of the form $(\omega_\lambda^+, \omega_\lambda^-, 1/2)$ exhibit data hiding against GOCC in the limit $\lambda \to 1^-$, i.e.

$$\beta_1 \equiv 1 \quad \forall\ \lambda \qquad \textit{but} \qquad \lim_{\lambda\to 1^-} \beta_{\mathrm{GOCC}} = 0\,. \tag{12}$$

We have thus demonstrated the sought data hiding against GOCC measurements. An analogous but substantially different result has recently been obtained by Sabapathy and Winter [30–33] by means of a completely different construction. Their construction employs random convex mixtures of coherent states only, but has the drawback of requiring asymptotically many modes. Ours, on the contrary, requires a single mode only, but the two states to be prepared are highly non-classical. Because of these differences, depending on the platform chosen for the implementation one may be easier to realise or to break than the other, or vice versa.

We speculate that the data hiding scheme proposed here may be used, in a not-too-distant future, to benchmark the quality of remote devices operating with CV platforms. A simple benchmarking protocol is based on (repetitions of) the state discrimination task $(\omega_\lambda^+, \omega_\lambda^-; 1/2)$ described above: the unknown state is sent to the remote party, which is tasked with identifying it. Since ω_λ^+ and ω_λ^- are almost indistinguishable under GOCC measurements, a correct solution to this problem invariably indicates that the remote device is able to carry out non-Gaussian measurements.

[1] A. Shamir, Commun. ACM **22**, 612 (1979).

[2] G. R. Blakley, in *Managing Requirements Knowledge, International Workshop on* (IEEE Computer Society, Los Alamitos, CA, USA, 1979) p. 313.
[3] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
[4] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[5] A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, 2nd ed., Texts and Monographs in Theoretical Physics (De Gruyter, Berlin, Germany, 2019).
[6] A. S. Holevo, Tr. Mosk. Mat. Obs. **26**, 133 (1972).
[7] C. W. Helstrom, *Quantum detection and estimation theory* (Academic press, New York, USA, 1976).
[8] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).
[9] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).
[10] D. P. DiVincenzo, P. Hayden, and B. M. Terhal, Found. Phys. **33**, 1629 (2003).
[11] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[12] W. Matthews and A. Winter, Commun. Math. Phys. **285**, 161 (2009).
[13] W. Matthews, S. Wehner, and A. Winter, Commun. Math. Phys. **291**, 813 (2009).
[14] E. Chitambar and M.-H. Hsieh, J. Math. Phys. **55**, 112204 (2014).
[15] G. Aubrun and C. Lancien, Quantum Inf. Comput. **15**, 513 (2015).
[16] L. Lami, C. Palazuelos, and A. Winter, Commun. Math. Phys. **361**, 661 (2018).
[17] G. Aubrun, L. Lami, C. Palazuelos, S. J. Szarek, and A. Winter, Commun. Math. Phys. **375**, 679 (2020).
[18] H.-C. Cheng, A. Winter, and N. Yu, Preprint arXiv:2011.13063 (2020).
[19] M. M. Wilde, Phys. Rev. A **97**, 062305 (2018).
[20] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[21] S. Pirandola and C. Lupo, Phys. Rev. Lett. **118**, 100502 (2017).
[22] M. E. Shirokov, Probl. Inf. Transm. **54**, 20 (2018).
[23] A. Winter, Preprint arXiv:1712.10267 (2017).
[24] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Nat. Photonics **9**, 641 (2015).
[25] M. Takeoka and M. Sasaki, Phys. Rev. A **78**, 022320 (2008).
[26] J. J. . Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, Phys. Rev. A **54**, R4649 (1996).
[27] P. M. Anisimov, G. M. Raterman, A. Chiruvelli, W. N. Plick, S. D. Huver, H. Lee, and J. P. Dowling, Phys. Rev. Lett. **104**, 103602 (2010).
[28] J. P. Olson, K. P. Seshadreesan, K. R. Motes, P. P. Rohde, and J. P. Dowling, Phys. Rev. A **91**, 022317 (2015).
[29] R. J. Birrittella, P. M. Alsing, and C. G. Gerry, Preprint arXiv:2008.08658 (2020).
[30] K. K. Sabapathy and A. Winter, Preprint arXiv:2102.01622 (2021).
[31] A. Winter, "Reflections on quantum data hiding," (2016), Nexus of Information and Computation Theories – Secrecy and Privacy Theme.
[32] A. Winter, "Reflections on quantum data hiding," (2017), APS Meeting Abstracts.
[33] A. Winter, "Reading and hiding data in quantum systems," (2017), IEEE Int. Symp. Inform. Theory (ISIT).