New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
27 January 2025

REVISED
17 April 2025

ACCEPTED FOR PUBLICATION
13 May 2025

PUBLISHED
23 May 2025

PAPER

Orthogonality broadcasting and quantum position verification

Ian George[1,*], **Rene Allerstorfer**[2], **Philip Verduyn Lunel**[3] **and Eric Chitambar**[4]

[1] Department of Electrical and Computer Engineering, Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore
[2] QuSoft, CWI Amsterdam, Amsterdam, The Netherlands
[3] Sorbonne Université, CNRS, LIP6 Paris, France
[4] Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Champaign, United States of America
[*] Author to whom any correspondence should be addressed.

E-mail: qit.george@gmail.com

Keywords: quantum cryptography, quantum foundations, uncertainty relations

Abstract

The no-cloning theorem leads to information-theoretic security in various quantum cryptographic protocols. However, this security typically derives from a possibly weaker property that classical information encoded in certain quantum states cannot be broadcast. To formally capture this property, we introduce the study of 'orthogonality broadcasting.' When attempting to broadcast the orthogonality of two different qubit bases, we establish that the power of classical and quantum communication is equivalent. However, quantum communication is shown to be strictly more powerful for broadcasting orthogonality in higher dimensions. We then relate orthogonality broadcasting to quantum position verification and provide a new method for establishing error bounds in the no pre-shared entanglement model that can address protocols previous methods could not. Our key technical contribution is an uncertainty relation that uses the geometric relation of the states that undergo broadcasting rather than the non-commutative aspect of the final measurements.

1. Introduction

The famous no-cloning principle in quantum mechanics prohibits the copying of non-orthogonal quantum states [1]. More precisely, if $|\psi\rangle$ and $|\varphi\rangle$ are two non-orthogonal states of some quantum system, then there does not exist any physically realizable mapping U such that $U|\psi\rangle = |\psi\rangle^{\otimes 2}$ and $U|\varphi\rangle = |\varphi\rangle^{\otimes 2}$. This fundamental fact provides a foundation for designing cryptographic protocols [2], with specific examples being quantum key distribution [3], secret sharing [4], and position verification [5].

Quantum broadcasting extends cloning to a communication setting and relaxes the goal to duplication on the level of reduced density matrices. That is, a set of states $\{\rho_i\}_i$ on system S is broadcast to Alice (A) and Bob (B) if there exists a completely-positive trace-preserving (CPTP) map $\mathcal{E}^{S\to AB}$ such that $\mathcal{E}(\rho_i) = \sigma_i^{AB}$ with $\mathrm{tr}_A(\sigma_i^{AB}) = \rho_i$ and $\mathrm{tr}_B(\sigma^{AB}) = \rho_i$ for all i. Similar to the no-cloning theorem, it has been shown that quantum mechanics [6–8] and even more general theories of nature [9] prohibit universal broadcasting. Only if the input states $\{\rho_i\}_i$ are pairwise commuting can such a broadcasting map $\mathcal{E}^{S\to AB}$ be constructed.

In this work we propose a weaker form of broadcasting called *orthogonality broadcasting*. Let $\mathcal{S}_\Theta = \{\rho_{i|\theta}\}_{i\in\mathcal{I}_\theta,\theta\in\Theta}$ be $|\Theta|$ sets of pairwise orthogonal states $\{\rho_i\}_{i\in\mathcal{I}_\theta}$, i.e. for all $\theta\in\Theta$ and $i\neq j\in\mathcal{I}_\theta$, $\rho_{i|\theta}\perp\rho_{j|\theta}$. We say that a CPTP map $\mathcal{E}^{S\to AB}$ broadcasts the orthogonality of $\mathcal{S}_\Theta$ if

$$\mathrm{tr}_A\left(\sigma_{i|\theta}^{AB}\right)\perp\mathrm{tr}_A\left(\sigma_{j|\theta}^{AB}\right)\ \text{ and }\ \mathrm{tr}_B\left(\sigma_{i|\theta}^{AB}\right)\perp\mathrm{tr}_B\left(\sigma_{j|\theta}^{AB}\right)$$

for all $\theta, i\neq j$, where $\sigma_{i|\theta} = \mathcal{E}(\rho_{i|\theta})$ (see figure 1(a)). Orthogonality broadcasting can be understood as a basic quantum communication task with post-information. Suppose that a quantum system is prepared in some unknown state chosen from an ensemble like $\mathcal{S}$. For example, this could be one of the BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Once the the value θ is revealed as 'post-information,' the system state can be determined by measuring in the correct orthonormal basis; e.g in the BB84 case, this basis is either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Orthogonality broadcasting enables both Alice and Bob to learn the state preparation through local measurement and post-information. This goal is less demanding than state broadcasting since all we require is that the correct orthogonality be preserved by the reduced density matrices of the distributed state $\sigma^{AB}_{i|\theta}$. Nevertheless, through the map $\mathcal{E}^{S\to AB}$, orthogonality broadcasting still requires copying some type of information that is encoded in a family of potentially non-orthogonal states. It can thus be viewed as another communication primitive, in the same spirit as cloning and state broadcasting.

A special type of orthogonality broadcasting arises when one of the output systems is classical. In this case, the broadcasting map takes the form $\mathcal{E}^{S\to AX}$, with X being a classical register, and we refer to this as *classical orthogonality broadcasting*. It is important to note that when describing θ as post-information in the context of broadcasting, it means that θ arrives after the application of the broadcasting map. However, there is another notion of post-information in which θ arrives after the quantum measurement [10, 11]. However, as we observe in proposition 2 below, under a natural measure of error, these two notions of post-information are operationally equivalent when restricting to classical orthogonality broadcasting, meaning that the optimal success probability of identifying i in one task is the same as the other.

1.1. Uncloneable cryptography and quantum position verification

Beyond the foundational importance of understanding the no-cloning theorem in quantum information theory, our primary motivation for studying both classical and non-classical orthogonality broadcasting is quantum cryptography. Most quantum cryptographic protocols derive their security from the no-cloning theorem on some level because the protocol ‘hides’ some classical information in non-commuting quantum states that an adversary cannot perfectly distinguish nor clone. This basic idea has given rise to the study of ‘uncloneable cryptography’ (see [12] for an introduction).

A major method for establishing security in uncloneable cryptography has been monogamy-of-entanglement (MoE) games introduced in [13] and used subsequently, e.g. [2, 14–18]. However, MoE games do not directly capture the limitations of cloning quantum states, but rather test for a property of the entangled state that arises when trying to clone non-commuting states. Indeed, concurrent work [17] defines a specific case of orthogonality broadcasting as a ‘$1 \to 2$ cloning game’ and shows it to be equivalent to a *restricted* variant of the MoE game. This in total means that orthogonality broadcasting can only be captured by a (restricted) MoE game under special conditions. As MoE games and orthogonality broadcasting are generally distinct, they require independent studies. For clarity, appendix A includes a detailed discussion on the relationship between orthogonality broadcasting and MoE games.

A more concrete motivating example comes from establishing the security of quantum position verification (QPV) in the no pre-shared entanglement (no-PE) model. The limitations on orthogonality broadcasting underpins the security of many QPV protocols under the no-PE model. In these QPV protocols, at time t_0, spatially separated verifiers draw a state from a set of globally orthogonal product (GOP) quantum states, $\{|a_k\rangle|b_k\rangle\}_k$, and send it to claimed location of the honest prover (see figure 2). The verifiers ‘accept’ if at time t_1 they both receive the correct index k of the state sent. The honest prover can always achieve this by applying the projective measurement that discriminates the set $\{|a_k\rangle|b_k\rangle\}_k$ at the honest position. However, *dishonest* provers will not be located at the appropriate spacetime point, but spatially separated around this point. Thus they have to attempt to clone the *orthogonality* of $|a_k\rangle$ and $|b_k\rangle$[5]. The simplest example of such a QPV protocol is ‘BB84 QPV’ where the set of $\{|a_k\rangle|b_k\rangle\}$ is given by

$$\left\{|0\rangle^A|0\rangle^B, |0\rangle^A|1\rangle^B, |1\rangle^A|+\rangle^B, |1\rangle^A|-\rangle^B\right\} . \tag{1}$$

In this case, the adversaries’ optimal attack is to approximate orthogonality broadcasting as much as possible. This is because the party who receives system B acts as the broadcasting channel $\mathcal{E}$ and the party who receives the fully classical state, system A, copies it and forwards it, acting as the value $\theta \in \Theta$ arriving after broadcasting (recall figure 1(a)). Note this exact identification holds so long as one of the registers is always classical and the adversaries hold no entanglement, i.e. one considers the no-PE model.

In principle, this above correspondence alone would motivate the study of orthogonality broadcasting. However, in the case of BB84 QPV, it turns out the reduction to an MoE game is tight [13], which is likely why the limitations of cloning and MoE games have been treated as inextricable while distinct. Nonetheless, it is easy to break this exact connection to MoE games: if the set $\{|a_k\rangle^A|b_k\rangle^B\}_k$ is not of the form $\{|\theta\rangle^A\, U_\theta|x\rangle^B\}_{x,\theta}$ where $\{U_\theta\}_\theta$ is some set of unitaries acting on the B space, the reduction to an MoE game breaks down (see appendix A for more details). The set of states not satisfying this aforementioned structure can happen if both parties receive a quantum input or simply by not having the $|b_k\rangle$ be generated by x and a

[5] We stress orthogonality as they only need to be able to extract the index k rather than hold copies of the states $|a_k\rangle$,$|b_k\rangle$.

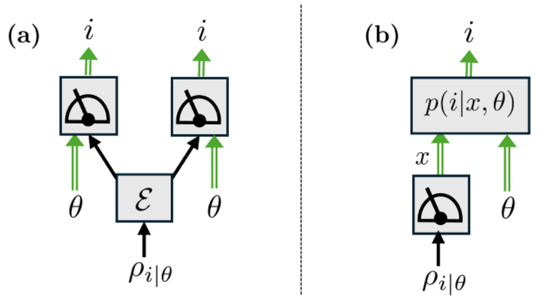

Figure 1. (a) Orthogonality broadcasting a set of states $\mathcal{S}_\Theta = \{\rho_{i|\theta}\}_{i,\theta}$ with $\rho_{i|\theta} \perp \rho_{j|\theta}$ for all $\theta \in \Theta$ and $i \neq j$. A map $\mathcal{E}$ distributes the orthogonality of $\rho_{i|\theta}$ so that both receivers can recover the index i given value θ. (b) In a second task, a quantum measurement must be performed on $\rho_{i|\theta}$ *before* receiving θ, which is used only later to recover the index i in classical post-processing. Orthogonality broadcasting reduces to (b) when one of the broadcast systems is classical. In all figures, green, double-line arrows represent classical information, and black, single-line arrows represent quantum information.

unitary. Both of these situations are natural to consider in designing more powerful, practical QPV protocols as well as studying the structure of no-cloning.

1.2. Summary of results and outline

At a high-level, this work contributes to three domains: the foundations of quantum mechanics, the security of QPV, and, at a technical level, the development of quantitative uncertainty relations. We summarize the contribution to these respective fields below. Any omitted proofs from the main text are collected in the appendices.

Contribution 1: Orthogonality broadcasting and foundations of quantum mechanics In section 2, we introduce orthogonality broadcasting and analyze both the perfect and approximate setting. For perfect orthogonality broadcasting, we show a separation between the power of using classical and quantum communication (theorem 1) and further demonstrate that perfect orthogonality broadcasting sometimes requires the use of entangled states (theorem 2). We however show that when one system is a qubit system, there is generally not an advantage to quantum communication (proposition 3). These results also imply a similar property in the communication setting of a QPV protocol without entangled inputs (theorem 3). This implies a separation between adversaries having access to classical and quantum communication when attacking a QPV protocol without entangled inputs in the no-PE model (corollary 3). This resolves an open question from [19]. As previously highlighted, orthogonality broadcasting is a relaxation of state broadcasting which is itself a relaxation of cloning. Thus, these results refine our understanding of the structure of quantum mechanics through an information-theoretic lens.

Contribution 2: The Security of QPV in the no-PE model In section 3, we consider QPV protocols where the task of the honest party is to distinguish GOP states $\{|a_k\rangle|b_k\rangle\}_k$ (see figure 2). We identify the adversaries' communication structure in attacking such QPV protocols in the no-PE model as optimizing strategies that make up 'local operations and simultaneous quantum communication' (LOSQC). We show how LOSQC relates to orthogonality broadcasting, either through an exact correspondence (as described previously in the case of BB84 QPV) or via relaxations for more involved GOP states. This allows us to upper bound the success probability of state discrimination on GOP ensembles which, by the exact correspondence between LOSQC and QPV attacks in the no-PE model, implies security bounds on these QPV protocols.

Our method culminates in three theorems. The first (theorem 4) provides bounds for any set of product states that contains four product states that generalize the structure of the BB84 states. This may be applied to many well-known GOP ensembles and recovers the tight bound for BB84 QPV (corollary 5). The second (theorem 5) establishes bounds when the set of GOP states to discriminate are in qutrit space such that the 'error per state' outperforms that of BB84 QPV. theorem 5 implies a significant practical advantage in using only slightly higher-dimensional QPV protocols. The third (theorem 6) demonstrates that the adversarial success probability can strictly decrease when requiring *both* adversaries to broadcast locally non-commuting states. While intuitive, to the best of our knowledge, this is the first method that rigorously establishes the added strength of QPV protocols in which both verifiers send quantum states. In particular, in appendix A, we show the ensembles considered in theorems 5 and 6 cannot be analyzed using MoE games with pre-existing methods.

Contribution 3: A new type of uncertainty relation Contributions 1 and 2 stem from a more direct analysis of no-cloning than previous methods. In order to achieve this more direct analysis, one of the main technical

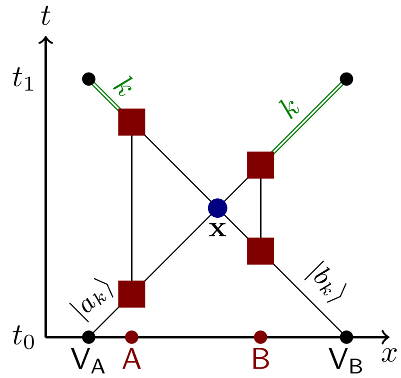

Figure 2. Spacetime diagram of a QPV protocol using GOP set $\mathcal{S} = \{|a_k\rangle|b_k\rangle\}_k$. With probability $p(k)$, the verifiers $\mathsf{V_A}$, $\mathsf{V_B}$ simultaneously send $|a_k\rangle$ and $|b_k\rangle$ respectively at time t_0. An honest prover at spacetime point $\mathbf{x}$ could measure jointly on the states and identify k. In contrast, dishonest provers, A and B, would need to clone the orthogonality of $|a_k\rangle$ and $|b_k\rangle$ at the two lower boxes in order to return the correct value k at time t_1. The adversaries' strategy can be limited by the same tools as studying orthogonality broadcasting (section 3). The communication setting of the dishonest provers is an example of 'local operations and simultaneous quantum communication' (LOSQC).

contributions of this work is a new uncertainty relation that only depends on the relation between the given states to be cloned (lemma 1 and theorem 7), and thus can be used to bound the error in orthogonality broadcasting of more general ensembles than previous methods. In other words, our uncertainty relation differs from entropic uncertainty relations studied in quantum information theory [20–23] as well as the operator inequality used to analyze MOE games [13], which all rely on incompatible measurements. To the best of our knowledge, this is the first such uncertainty relation of its type and we hope it motivates more general and direct methods for bounding strategies based on cloning and thus more direct applications to cryptographic protocols whose security depends on the no-cloning theorem.

2. Orthogonality broadcasting

Let us analyze the task of orthogonality broadcasting in more detail. To prepare us for its application in QPV, suppose that Alice receives an ensemble of states $\mathcal{S}_\Theta = \{\rho_{i|\theta}\}_{i,\theta}$ that are pairwise orthogonal for each fixed $\theta \in \Theta$. Her goal is to broadcast the orthogonality of this ensemble to herself and Bob. We label the input system as A and the output systems as $A'B'$. Let us proceed by distinguishing between the cases of perfect and approximate broadcasting.

2.1. Perfect broadcasting

It is often convenient to assume that Alice's broadcasting map takes the form of an isometry $U : A \to A'B'$. This can always be done without loss of generality since a CPTP map can be built by combining an isometry with a discarding of subsystems, and the latter can always be done by Alice or Bob after the broadcasting. For isometry U, Alice then receives the output of the quantum channel $\mathcal{N}(\cdot) = \mathrm{tr}_{B'} U(\cdot)U^\dagger$ while Bob receives the output of its complementary channel $\mathcal{N}^c(\cdot) = \mathrm{tr}_{A'} U(\cdot)U^\dagger$. From this it follows that $\mathcal{S}_\Theta$ admits orthogonality broadcasting if and only if there exists a channel $\mathcal{N}$ such that

$$\mathrm{Tr}\left[\mathcal{N}\left(\rho_{i|\theta}\right)\mathcal{N}\left(\rho_{j|\theta}\right)\right] = \mathrm{Tr}\left[\mathcal{N}^c\left(\rho_{i|\theta}\right)\mathcal{N}^c\left(\rho_{j|\theta}\right)\right] = 0 \tag{2}$$

for all θ_Θ and $i \neq j$.

In the special case of classical orthogonality broadcasting, when Alice can only communicate classical information to Bob, the isometry U gets replaced by a channel $\mathcal{E} : A \to A'X$ with a quantum–classical (qc) output. We can express this as $\mathcal{E}(\cdot) = \sum_x \mathcal{A}_x(\cdot) \otimes |x\rangle\langle x|$ with the $\{\mathcal{A}_x\}_x$ being a family of CP maps whose sum is CPTP (i.e. an instrument). The condition for orthogonality on Bob's side is $\mathrm{Tr}[\mathcal{A}_x(\rho_{i|\theta})]\mathrm{Tr}[\mathcal{A}_x(\rho_{j|\theta})] = 0$ for all x. Letting $\Pi_x = \mathcal{A}_x^\dagger(\mathbb{I})$ denote elements of a POVM, where $\mathcal{A}_x^\dagger$ is the adjoint map, we can thus express the condition for orthogonality on Bob's side as the existence of a POVM $\{\Pi_x\}_x$ satisfying

$$\mathrm{Tr}\left[\Pi_x \rho_{i|\theta}\right]\mathrm{Tr}\left[\Pi_x \rho_{j|\theta}\right] = 0 \tag{3}$$

for all x, θ, and $i \neq j$. In other words, for every fixed θ, there is at most one value i such that $\mathrm{Tr}[\Pi_x \rho_{i|\theta}] \neq 0$. This means that the POVM $\{\Pi_x\}_x$ is able to perfectly identify the value i given x and θ. In the next section, we will generalize this finding to not only perfect identification but also minimum error state discrimination.

For now, we consider the comparative powers of classical and non-classical orthogonality broadcasting in the case of zero error.

We begin with a simple example that shows that perfect orthogonality broadcasting is possible using only classical communication even when not all states in $\mathcal{S}_\Theta$ are simultaneously diagonalizable. This is in contrast to cloning and state broadcasting described in the introduction, which both require the ensemble to consist of pairwise commuting states. Moreover, it shows that even for qutrits such examples exist, which highlights the nuance of orthogonality broadcasting in any dimension greater than two.

Proposition 1. *Let*

$$\mathcal{S}_\Theta = \begin{Bmatrix} \rho_{0|0} := |0\rangle & \rho_{1|0} := |1\rangle \\ \rho_{0|1} := |\psi_+\rangle & \rho_{1|1} := |\psi_-\rangle \end{Bmatrix} , \tag{4}$$

where $|\psi_\pm\rangle := \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle \pm \frac{1}{\sqrt{2}}|2\rangle = \frac{1}{\sqrt{2}}(|+\rangle \pm |2\rangle)$. *This set admits perfect classical orthogonality broadcasting.*

Proof. We show that perfect discrimination is possible by a broadcasting map with both parties receiving classical information, i.e. $\mathcal{E}(\cdot) = \sum_{x=0}^{3} \mathrm{tr}[\Pi_x(\cdot)]|x\rangle\langle x| \otimes |x\rangle\langle x|$, a general fact that holds for all classical orthogonal broadcasting (see proposition 2). Consider the set of matrices

$$\Pi_0 := \begin{bmatrix} \frac{1}{2} & 0 & \frac{1}{2\sqrt{2}} \\ 0 & 0 & 0 \\ \frac{1}{2\sqrt{2}} & 0 & \frac{1}{4} \end{bmatrix} \quad \Pi_1 := \begin{bmatrix} \frac{1}{2} & 0 & -\frac{1}{2\sqrt{2}} \\ 0 & 0 & 0 \\ -\frac{1}{2\sqrt{2}} & 0 & \frac{1}{4} \end{bmatrix}$$

$$\Pi_2 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2\sqrt{2}} \\ 0 & \frac{1}{2\sqrt{2}} & \frac{1}{4} \end{bmatrix} \quad \Pi_3 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2\sqrt{2}} \\ 0 & -\frac{1}{2\sqrt{2}} & \frac{1}{4} \end{bmatrix} .$$

A direct calculation will verify that each of these matrices have eigenvalues $\{3/4, 0, 0\}$ and by inspection they sum to identity. Thus, $\{\Pi_i\}_{i\in[3]}$ is a POVM. By direct calculation using Born's rule, one may verify that if Alice measures the input state with the given POVM, her possible (non-zero probability) outcomes are captured by the following table:

State $\rho_{i\|\theta}$	Possible Outcomes
$\rho_{0\|0}$	$\{0,1\}$
$\rho_{1\|0}$	$\{2,3\}$
$\rho_{0\|1}$	$\{0,2\}$
$\rho_{1\|1}$	$\{1,3\}$

It follows that her possible outcomes partition upon receiving $\theta \in \{0,1\}$. Thus, if Alice measures the state with the given POVM and broadcasts the answer, then when Alice and Bob receive θ, they can both determine the state correctly. □

It may be surprising that the communication of classical information suffices in the above example. Proposition 3 below implies that in fact classical and quantum communication are equally powerful for perfect orthogonality broadcasting for all ensembles with $|\Theta| = 2$. However, the following theorem shows a separation already exists as soon as $|\Theta| > 2$.

Theorem 1. *Let*

$$\mathcal{S}_\Theta = \begin{Bmatrix} \rho_{0|0} := |+_{01}\rangle & \rho_{1|0} := |-_{01}\rangle \\ \rho_{0|1} := |+_{02}\rangle & \rho_{1|1} := |-_{02}\rangle \\ \rho_{0|2} := |\widetilde{+}_{12}\rangle & \rho_{1|2} := |\widetilde{-}_{12}\rangle \end{Bmatrix} \tag{5}$$

be $|\Theta| = 3$ *pairs of orthogonal states, where* $|\pm_{mn}\rangle = \frac{1}{\sqrt{2}}(|m\rangle \pm |n\rangle)$ *and* $|\widetilde{\pm}_{mn}\rangle = \frac{1}{\sqrt{2}}(|m\rangle \pm i|n\rangle)$. *Then it is possible to broadcast the orthogonality of* $\mathcal{S}_\Theta$*, yet classical orthogonality broadcasting of* $\mathcal{S}_\Theta$ *is impossible.*

Proof. We first construct an orthogonality broadcasting map for $\mathcal{S}_\Theta$. For $A = \mathbb{C}^3$, define the isometry $U : A \to A'B'$ by

$$U|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad U|1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad U|2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) .$$

Then

$$U|+_{01}\rangle = |0\rangle^{A'}|0\rangle^{B'}, \qquad U|-01\rangle = |1\rangle^{A'}|1\rangle^{B},$$
$$U|+_{02}\rangle = |+_{01}\rangle^{A'}|+_{01}\rangle^{B'}, \qquad U|-_{02}\rangle = |-_{01}\rangle^{A'}|-_{01}\rangle^{B'}$$
$$U|\widetilde{+}_{12}\rangle = |\widetilde{+}_{01}\rangle^{A'}|\widetilde{+}_{01}\rangle^{B'}, \qquad U|\widetilde{-}_{12}\rangle = |\widetilde{-}_{01}\rangle^{A'}|\widetilde{-}_{01}\rangle^{B'}.$$

Thus, the necessary orthogonality is preserved for both Alice and Bob for all elements of $\mathcal{S}_\Theta$.

We now show that there is no classical orthogonal broadcasting map for $\mathcal{S}_\Theta$. According to equation (3), this would require a POVM $\{\Pi_x\}_x$ such that

$$0 = \langle +_{01}|\Pi_x|+_{01}\rangle\langle -_{01}|\Pi_x|-_{01}\rangle$$
$$0 = \langle +_{02}|\Pi_x|+_{02}\rangle\langle -_{02}|\Pi_x|-_{02}\rangle$$
$$0 = \langle \widetilde{+}_{12}|\Pi_x|\widetilde{+}_{12}\rangle\langle \widetilde{-}_{12}|\Pi_x|\widetilde{-}_{12}\rangle$$

for all x. These three equalities can be satisfied only if three states from $\mathcal{S}_\Theta$ lie in the kernel of Π_x. However, any subset of three states from $\mathcal{S}_\Theta$ are linearly independent, which means the only solution to these equations is $\Pi_x = 0$. □

2.2. Separable communication in orthogonality broadcasting

With the separation of classical and quantum communication in orthogonality broadcasting established, an interesting question is whether orthogonality broadcasting actually needs the use of entanglement. In other words, does there exist ensembles $\mathcal{S} = \{\rho_{i|\theta}\}_{i,\theta}$ whose orthogonality can be broadcast by map $\mathcal{E} : A \to A'B'$ only if the broadcast states $\sigma_{i|\theta} = \mathcal{E}(\rho_{i|\theta})$ are entangled? This question is fundamental for two reasons. First, the requirement for entangled states in the broadcasting map would be a sharp departure from cloning and state broadcasting, which, when feasible, can always be accomplished by generating product and separable output states, respectively. Second, a more general question in quantum communication is to understand which distributed tasks are possible using the transmission of separable rather than entangled states. For example, it is possible to distribute entanglement through the exchange of separable states [24], indicating the curious utility of quantum correlations beyond entanglement [25, 26]. The following theorem shows that separable carriers are insufficent in general for broadcasting orthogonality.

Theorem 2. *Let*

$$\mathcal{S}_\Theta = \left\{ \begin{matrix} \rho_{0|0} := |1\rangle & \rho_{1|0} := |2\rangle \\ \rho_{0|1} := |+_{23}\rangle & \rho_{1|1} := |-_{23}\rangle \\ \rho_{0|2} := |+_{24}\rangle & \rho_{1|2} := |-_{24}\rangle \\ \rho_{0|3} := |\widetilde{+}_{34}\rangle & \rho_{1|3} := |\widetilde{-}_{34}\rangle \end{matrix} \right\} \tag{6}$$

be $|\Theta| = 4$ pairs of orthogonal states and we remind the reader $|\pm_{mn}\rangle = \frac{1}{\sqrt{2}}(|m\rangle \pm |n\rangle)$ and $|\widetilde{\pm}_{mn}\rangle = \frac{1}{\sqrt{2}}(|m\rangle \pm i|n\rangle)$. Then $P_{\mathbf{bc}}(\mathcal{S}_\Theta) = 1$. Furthermore, any broadcasting map must transform at least one of the states in $\mathcal{S}_\Theta$ into an entangled state.

Theorems 1 and 2 collectively establish different types of orthogonality broadcasting. The ensemble $\mathcal{S}_\Theta$ in theorem 1 requires broadcasting a map that transforms the elements of $\mathcal{S}_\Theta$ into non-classical but possibly separable states. Even stronger, the ensemble $\mathcal{S}_\Theta$ in theorem 2 requires a map that transforms at least one element of $\mathcal{S}_\Theta$ into an entangled state.

2.3. Approximate orthogonality broadcasting

Even if perfect orthogonality broadcasting is not possible for $\mathcal{S}_\Theta$, one can consider approximate orthogonality broadcasting. Here, it is natural to quantify the quality of approximation as the largest worst case error probability among Alice and Bob for correctly guessing the value $i \in \mathcal{I}_\theta$ given $\theta \in \Theta$. For a given ensemble $\mathcal{S}_\Theta = \{\rho_{i|\theta}\}_{i,\theta}$ and joint distribution p over $\Theta \times \mathcal{I}$ where $\mathcal{I} := \cup_\theta \mathcal{I}_\theta$, this gives the measure

$$P_{\text{bc}}(\mathcal{S}_\Theta) := \max_{\mathcal{E}} \min_{P\in\{A,B\}} \sum_{\theta\in\Theta} p(\theta)\, P_{\text{guess}}\left(\left\{\sigma^{P}_{i|\theta}\right\}_i\right), \tag{7}$$

where the maximization is taken over all broadcasting maps $\mathcal{E} : \rho_{i|\theta} \mapsto \sigma^{AB}_{i|\theta}$, and

$$P_{\text{guess}}\left(\left\{\sigma_{i|\theta}\right\}_i\right) := \max_{\{\Pi_i\}_i} \sum_{i\in\mathcal{I}_\theta} p(i|\theta)\,\text{Tr}\left(\Pi_i \sigma_{i|\theta}\right)$$

is the maximum guessing probability for a uniform ensemble of states $\{\sigma_{i|\theta}\}_i$ using a positive operator-valued measure (POVM) $\{\Pi_i\}_i$. Note that this approximation is well-defined for all ensembles $\mathcal{S}_\Theta = \{\rho_{i|\theta}\}_{i,\theta}$ even if pairwise orthogonality does not hold for each θ. Then orthogonality broadcasting of $\mathcal{S}_\Theta$ is possible iff $P_{\text{bc}}(\mathcal{S}_\Theta) = 1$. We let $P_{\text{c-bc}}(\mathcal{S}_\Theta)$ quantify approximate *classical* orthogonality broadcasting, which is defined in the same way except with the maximization in equation (7) restricted to broadcasting maps having a quantum–classical (qc) output. This notion of approximate orthogonality broadcasting proposed here is analogous to the well-studied tasks of approximate cloning and state broadcasting [27, 28].

Note that the choice of local POVMs in the definition of $P_{\text{guess}}(\{\sigma^{AB}_{i|\theta}\})$ can depend on the value θ. The value θ is called post-information since it comes after the broadcasting map $\mathcal{E}$. An alternative notion of post-information state discrimination has been considered in which the post-information comes after the choice of POVM [10, 11] (see figure 1). The optimal guessing probability for ensemble $\mathcal{S}_\Theta$ in this scenario is then given by

$$P_{\text{p-i}}(\mathcal{S}_\Theta) := \max \sum_{\theta,i} \sum_x q(i|x,\theta)\, p(\theta,i)\, \mathrm{Tr}\left(\rho_{i|\theta}\Pi_x\right), \tag{8}$$

where the maximization is taken over all POVMs $\{\Pi_x\}_x$ and all classical post-processing channels $q(i|x,\theta)$. Despite this conceptual difference, it is not difficult to show that they are operationally equivalent.

Proposition 2. *For all $\mathcal{S}_\Theta$ and any choice of prior distribution on $\Theta \times \mathcal{I}$, $P_{\text{c-bc}}(\mathcal{S}_\Theta) = P_{\text{p-i}}(\mathcal{S}_\Theta)$. In particular, this is because $P_{\text{c-bc}}(\mathcal{S}_\Theta)$ is always achieved using a fully classical broadcasting channel $\mathcal{E}^{A\to XY}$.*

Proof. We begin with the second claim. By (7), $P_{\text{c-bc}}(\mathcal{S}_\Theta)$ is always achieved by a fully classical broadcasting map $\mathcal{E}^{A\to XY}$. Indeed if the worse performing player receives classical information, then the minimum success probability for both parties will not change if both players follow the strategy of the classical player; and, if the worse performing party receives quantum information, then they can improve the minimum success probability by both following the classical player's strategy.

To establish the first claim, note the above argument shows the optimal fully classical broadcast map applies some optimal POVM $\{\Pi_x\}$ to $\rho_{i|\theta}$, and broadcasts the outcome to both parties. It follows for each θ both parties hold $\{\sigma^X_{i|\theta}\}_i = \{\sum_x \mathrm{Tr}[\Pi_x\rho_{i|\theta}]|x\rangle\langle x|\}_i$ distributed according to $p(i|\theta)$ and then apply an optimal POVM $\{\tau^\theta_i\}_i$ to guess the value of $i \in \mathcal{I}_\Theta$. As $\{\sigma^X_{i|\theta}\}_i$ are classical distributions, for each $\theta \in \Theta$ the optimal POVM $\{\tau^\theta_i\}_i$ may be reduced to a conditional distribution $\{w_\theta(i|x)\}_{i,x}$. Thus, defining $q(i|x,\theta) := w_\theta(i|x)$ along with $\{\Pi_x\}_x$ defines a feasible strategy for (8), so $P_{\text{c-bc}}(\mathcal{S}_\Theta) \leqslant P_{\text{p-i}}(\mathcal{S}_\Theta)$. On the other hand, the reverse inequality follows from the fact that any POVM and post-processing strategy used to optimize $P_{\text{p-i}}(\mathcal{S}_\Theta)$ can be converted into a fully classical broadcasting map in which the POVM is first performed on $\rho_{i|\theta}$, the classical outcome is then broadcast to both Alice and Bob, and finally they both perform the post-processing locally. □

We can extend the relationship between classical broadcasting and post-information to general quantum broadcasting in the special case that $|\Theta| = 2$. The following proposition is a counterpart to theorem 1.

Proposition 3. *For any prior distribution over $\Theta \times \mathcal{I}$, $P_{\text{c-bc}}(\mathcal{S}_\Theta) = P_{\text{bc}}(\mathcal{S}_\Theta)$ for all $\mathcal{S}_\Theta$ with $|\Theta| \leqslant 2$.*

Proof. It suffices to show $P_{\text{c-bc}}(\mathcal{S}_\Theta) \geqslant P_{\text{bc}}(\mathcal{S}_\Theta)$ for $\Theta = \{0,1\}$. For any broadcasting map $\mathcal{E} : \rho_{i|\theta} \mapsto \sigma^{AB}_{i|\theta}$, there must be a $\theta_0 \in \{0,1\}$ such that

$$\begin{aligned}\min_{P\in\{A,B\}} &\left[p(0)\,P_{\text{guess}}\left(\left\{\sigma^P_{i|0}\right\}_i\right) + p(1)\,P_{\text{guess}}\left(\left\{\sigma^P_{i|1}\right\}_i\right)\right] \\ &\leqslant p(\theta_0)\,P_{\text{guess}}\left(\left\{\sigma^A_{i|\theta_0}\right\}_i\right) + p(\theta_0^c)\,P_{\text{guess}}\left(\left\{\sigma^B_{i|\theta_0^c}\right\}_i\right),\end{aligned} \tag{9}$$

where $\theta_0^c = \theta_0 \oplus 1$. Let $\{\Pi^A_{i|\theta_0}\}_i$ and $\{\tau^B_{i|\theta_0^c}\}_i$ be optimal POVMs attaining the maximum guessing probability in $P_{\text{guess}}(\{\sigma^A_{i|\theta_0}\}_i)$ and $P_{\text{guess}}(\{\sigma^B_{i|\theta_0^c}\}_i)$, respectively. Using these measurements we construct the fully classical broadcasting map

$$\rho_{i|\theta} \mapsto \sum_{j,k} \mathrm{Tr}\left[\Pi^A_{j|\theta_0} \otimes \tau^B_{k|\theta_0^c}\mathcal{E}\left(\rho_{i|\theta}\right)\right] |j,k\rangle\langle j,k|^A \otimes |j,k\rangle\langle j,k|^B.$$

Alice and Bob both hold the classical variables (j,k) with probability $p(j,k) = \mathrm{Tr}[\Pi^A_{j|\theta_0} \otimes \tau^B_{k|\theta_0^c}\mathcal{E}(\rho_{i|\theta})]$. When θ is announced as post-information, they both submit j as their guess if $\theta = \theta_0$ or they both submit k as their guess if $\theta = \theta_1$. Hence, they both have the same overall probability of correctly guessing, which is given by

$$
\begin{aligned}
&p(\theta_0)\sum_j \mathrm{Tr}\left[\Pi^A_{j|\theta_0}\otimes \mathbb{1}^B\mathcal{E}\left(\rho_{j|\theta}\right)\right]+p(\theta_0^c)\sum_k \mathrm{Tr}\left[\mathbb{1}^A\otimes\tau^B_{k|\theta_0^c}\mathcal{E}\left(\rho_{k|\theta}\right)\right]\\
&=p(\theta_0)P_{\mathrm{guess}}\left(\left\{\sigma^A_{i|\theta_0}\right\}_i\right)+p(\theta_0^c)P_{\mathrm{guess}}\left(\left\{\sigma^B_{i|\theta_0^c}\right\}_i\right)\\
&\geqslant \min_{P\in\{A,B\}}\left[p(0)P_{\mathrm{guess}}\left(\left\{\sigma^P_{i|0}\right\}_i\right)+p(1)P_{\mathrm{guess}}\left(\left\{\sigma^P_{i|1}\right\}_i\right)\right]. \qquad (10)
\end{aligned}
$$

Since we originally chose $\mathcal{E}$ as an arbitrary broadcasting map, it follows that $P_{\text{c-bc}}(\mathcal{S}_\Theta)\geqslant P_{\mathrm{bc}}(\mathcal{S}_\Theta)$. □

Note that $P_{\text{p-i}}(\mathcal{S}_\Theta)$ in (8) is always optimized by a deterministic distribution as for any choice of POVM $\{\Pi_x\}$, for each $(\theta,x)\in\Theta\times\mathcal{X}$ there is an i' that maximizes $p(\theta,i)\mathrm{Tr}[\rho_{i|\theta}\Pi_x]$ over i and $P_{\text{p-i}}$ is a maximization. As an extremal POVM has at most d^2 outcomes, the optimal value is determined using one of $N=(\max_{\theta\in\Theta}|\mathcal{I}_\Theta|)^{d^2|\Theta|}$ deterministic distributions to search over. As maximizing the POVM is an SDP, there are N SDPs that need to be evaluated to determine $P_{\text{p-i}}(\mathcal{S}_\Theta)$. Combining propositions 2 and 3, for $|\Theta|\leqslant 2$, this gives a method for determining $P_{\mathrm{bc}}(\mathcal{S}_\Theta)$. In contrast, computing $P_{\mathrm{bc}}(\mathcal{S}_\Theta)$ appears to be a challenging bilinear optimization problem in general. Given this complexity, we next present an uncertainty relation that can be used to compute upper bounds on $P_{\mathrm{bc}}(\mathcal{S}_\Theta)$ for certain ensembles. The intuition behind the uncertainty relation is as follows. Consider a pure state ensemble $\{|a_\mu\rangle\}_\mu$ with $|\alpha_\mu\rangle^{AB'}=U|a_\mu\rangle$. If $|\alpha_0\rangle$ and $|\alpha_1\rangle$ are two entangled states that Alice can distinguish with high probability by measuring subsystem A, then the reduced density matrices α_0^A and α_1^A must be nearly orthogonal. Consequently, tracing out Alice in any superposition of $|\alpha_0\rangle$ and $|\alpha_1\rangle$ will effectively destroy the relative phase between these states, thereby making it difficult for Bob to distinguish superpositions of $|\alpha_0\rangle$ and $|\alpha_1\rangle$. We can quantify this tradeoff in terms of the fidelity $F(\rho,\sigma)=\|\sqrt{\rho}\sqrt{\sigma}\|_1$ and trace distance $D_{\mathrm{tr}}(\rho,\sigma)=\frac{1}{2}\|\rho-\sigma\|_1$ between hermitian operators.

Lemma 1 (uncertainty relation). *For any vectors* $|\alpha_0\rangle^{AB'}$ *and* $|\alpha_1\rangle^{AB'}$, *if* $|\alpha_\theta\rangle^{AB'}=\cos(\theta/2)|\alpha_0\rangle^{AB'}+e^{i\phi}\sin(\theta/2)|\alpha_1\rangle^{AB'}$ *and* $|\alpha_\omega\rangle^{AB'}=\cos(\omega/2)|\alpha_0\rangle^{AB'}+e^{i\phi}{}'\sin(\omega/2)|\alpha_1\rangle^{AB'}$, *then*

$$D_{\mathrm{tr}}\left(\alpha_\theta^{B'},\alpha_\omega^{B'}\right)\leqslant|z_1|F\left(\alpha_0^A,\alpha_1^A\right)+|z_2|D_{\mathrm{tr}}\left(\alpha_0^{B'},\alpha_1^{B'}\right), \qquad (11)$$

where $z_1=\frac{1}{2}(\sin(\theta)e^{-i\phi}-\sin(\omega)e^{-i\phi'})$ *and* $z_2=\frac{1}{2}(\cos(\theta)-\cos(\omega))$.

We remark that we in fact prove a more general uncertainty relation for two vectors that both decompose into linear combinations of the same set of vectors (see the supplemental material), but the above suffices for the main results of this work. Moreover, we highlight that this lemma may be seen as our major technical contribution. As noted earlier, unlike other uncertainty relations that rely upon the incompatibility of the measurement directly (see [23] for a review), ours follows from the geometric relation between the initial quantum states.

To appreciate the utility of proposition 1, we immediately obtain a no-go result for broadcasting the orthogonality of any two distinct pairs of basis vectors $\{|0\rangle,|1\rangle\}$ and $\{|\hat{n}\rangle,|-\hat{n}\rangle\}$, where $|\hat{n}\rangle=\cos(\theta/2)|0\rangle+\sin(\theta/2)e^{i\phi}|1\rangle$ and $|-\hat{n}\rangle=\sin(\theta/2)|0\rangle-\cos(\theta/2)e^{i\phi}|1\rangle$ with $\theta\in(0,\pi)$.

Corollary 1. *Orthogonality broadcasting is not possible for the set of states* $\mathcal{S}_\Theta=\{|0\rangle,|1\rangle,|\hat{n}\rangle,|-\hat{n}\rangle\}$ *if* $|\hat{n}\rangle\notin\{|0\rangle,|1\rangle\}$.

Proof. Without loss of generality, we assume that $\{|0\rangle,|1\rangle\}$ remains locally orthogonal for Alice. The isometry maps $\{|0\rangle,|1\rangle,|\hat{n}\rangle,|-\hat{n}\rangle\}$ into $\{|\alpha_0\rangle^{AB'},|\alpha_1\rangle^{AB'},|\alpha_\theta\rangle^{AB'},|\alpha_{\theta-\pi}\rangle^{AB'}\}$ of proposition 1, where we take $\omega=\theta-\pi$ and $\phi=-\phi$. Equation (11) then reads

$$D_{\mathrm{tr}}\left(\alpha_\theta^{B'},\alpha_{\theta-\pi}^{B'}\right)\leqslant|\sin\theta|F\left(\alpha_0^A,\alpha_1^A\right)+|\cos\theta|D_{\mathrm{tr}}\left(\alpha_0^{B'},\alpha_1^{B'}\right).$$

Orthogonality of α_0^A and α_1^A implies that $F(\alpha_0^A,\alpha_1^A)=0$, and so $D_{\mathrm{tr}}(\alpha_\theta^{B'},\alpha_{\theta-\pi}^{B'})\leqslant|\cos\theta|D_{\mathrm{tr}}(\alpha_0^{B'},\alpha_1^{B'})\leqslant|\cos\theta|<1$, assuming $\theta\notin\{\frac{k\pi}{2}\}_{k\in\mathbb{N}}$, which is equivalent to $|\hat{n}\rangle\notin\{|0\rangle,|1\rangle\}$. This proves the corollary since $\alpha_\theta^{B'}$ and $\alpha_{\theta-\pi}^{B'}$ are orthogonal if and only if $D_{\mathrm{tr}}(\alpha_\theta^{B'},\alpha_{\theta-\pi}^{B'})=1$. □

Before moving forward, we remark that we may relax lemma 1 in terms of guessing probability, which follows from the Fuchs-van de Graaf inequality and the equiprobable case of the Holevo-Helstrom theorem, i.e. $D_{\mathrm{tr}}(\rho,\sigma)=2p_g(\rho,\sigma)-1$ where $p_g(\rho,\sigma)$ denotes the optimal guessing probability when the two states are equiprobable [29].

Corollary 2. *Under the same conditions as lemma* 1,

$$p_g\left(\alpha_\theta^{B'},\alpha_\omega^{B'}\right)\leqslant\frac{1}{2}\left[|z_1|\sqrt{1-\left(2p_g\left(\alpha_0^A,\alpha_1^A\right)-1\right)^2}+|z_2|\left(2p_g\left(\alpha_0^{B'},\alpha_1^{B'}\right)-1\right)+1\right]. \qquad (12)$$

In the case $\mathcal{S}_\Theta$ decomposes into states

$$\rho_{0|0} = |a_0\rangle^S \quad \rho_{1|0} = |a_1\rangle^S \tag{13}$$

$$\rho_{0|1} = \cos(\theta/2)\,|a_0\rangle^S + e^{i\phi}\sin(\theta/2)\,|a_1\rangle^S \tag{14}$$

$$\rho_{1|1} = \cos(\omega/2)\,|a_0\rangle^S + e^{i\phi}\sin(\omega/2)\,|a_1\rangle^S\,. \tag{15}$$

Corollary 2 may be used to provide bounds on $P_{\mathrm{bc}}(\mathcal{S}_\Theta)$ as the constraint will hold for *any* choice of broadcasting channel $\mathcal{E}$. We however use this idea in further generality in a subsequent section, section 3.3, so we omit an example here. We remark, in the special case given above, that propositions 2 and 3 already imply there exists a direct method to determine the optimal value, although it is more computationally intensive.

3. LOSQC/LOSCC state discrimination and QPV in the no pre-shared entanglement model

We now shift to the application of our results to QPV. The class of protocols we consider asks an honest prover to distinguish the state drawn from a GOP ensemble $\{|a_k\rangle|b_k\rangle\}_k$ by performing a joint measurement, which is depicted in figure 3(a). For clarity, we begin by identifying the communication structure of attacking such a QPV protocol, which is depicted in figure 3(b). From the adversarial perspective, there are two dishonest provers, which we can call Alice and Bob, who each receive a portion of the global state that intersects their worldline on the spacetime diagram, split their local state in two to share part with the other party, and then, once each holds their respective shares, they may each guess k to forward to their respective verifier[6]. Formally, Alice intercepts $|a_k\rangle^A$ and performs the isometry $U : |a_k\rangle^A \mapsto |\alpha_k\rangle^{A_0B_1}$ while Bob intercepts $|b_k\rangle^B$ and applies $V : |b_k\rangle^B \mapsto |\beta_k\rangle^{B_0A_1}$. This is without loss of generality as any communication strategy allowed by quantum mechanics under the given timing constraints can be represented by this form. After the quantum communication, Alice holds systems A_0A_1 and Bob holds B_0B_1, and they both must perform local measurements to learn the value k. This is the most general strategy allowed by quantum mechanics in the no-PE model under the time constraints of special relativity. We call such the set of such communication strategies 'LOSQC' and the optimal success probability over all such strategies can be expressed as

$$\Pr_{\mathrm{LOSQC}}[\mathcal{S}] := \max \sum_k p(k)\,\mathrm{Tr}\left[\Pi_k \otimes \tau_k\,(U\otimes V)(\rho_k)(U\otimes V)^\dagger\right]\,, \tag{16}$$

where the $\{\rho_k\}_k$ denote the possible states, and as we just explained, without loss of generality the maximization is over isometries $U^{A\to A_0B_1}$, $V^{B\to B_0A_1}$ and POVMs $\{\Pi_k^{A_0A_1}\}$, $\{\tau_k^{B_0B_1}\}$. In other words, (16) gives the exact optimal success probability of attacking a state discrimination QPV protocol on inputs $\{\rho_k\}_k$ in the no-PE model. If we restricted the adversaries to only using classical communication between them, we would consider 'local operations and simultaneous classical communication' (LOSCC). In this case, rather than general isometries, Alice and Bob perform local instruments $\{\mathcal{A}_x\}_x$ and $\{\mathcal{B}_y\}_y$, respectively, with classical information x going to Bob and y going to Alice.

Remark. Before moving forward, we note that LOSQC is the relevant attack model even if there is pre-shared entanglement. For example, consider Alice and Bob will intercept some state from $\{\widetilde{\sigma}_k^{AB}\}_{k\in\mathcal{K}}$ and pre-share some resource $\zeta^{A'B'}$. Then defining $\rho_k := \widetilde{\sigma}_k \otimes \zeta$ for all k reduces studying attacking the QPV with resource state τ to the form of (16) where the isometries now are $U^{AA'\to A_0B_1}$, $V^{BB'\to B_0A_1}$.

3.1. Zero-error LOSQC and LOSCC state discrimination

Before directly addressing QPV, we study the problem of zero-error state discrimination in LOSQC and LOSCC. For GOPs with one system being a qubit, we find that LOSQC is no more powerful than LOSCC, and we obtain a reduction to classical orthogonality broadcasting.

Theorem 3. *A GOP $\{|a_k\rangle^A|b_k\rangle^B\}_k \subset \mathbb{C}^2\otimes\mathbb{C}^d$ is perfectly distinguishable by LOSCC if and only if it is perfectly distinguishable by LOSQC. Moreover, to be distinguishable by either, the ensemble must have the form*

$$|0\rangle^A|s_{i|0}\rangle^B, \quad |1\rangle^A|s_{i|1}\rangle^B, \quad |\phi_i\rangle^A|t_i\rangle^B, \tag{17}$$

where the $|\phi_i\rangle$ are arbitrary states, the $\{|s_{i|\theta}\rangle\}_{i,\theta}$ is an ensemble whose orthogonality $\langle s_{i|\theta}|s_{j|\theta}\rangle = \delta_{ij}$ can be classically broadcast, and each $|t_i\rangle$ is orthogonal to every other state on Bob's side.

[6] We remark that without loss of generality there are only two dishonest verifiers as there are only two messages to intercept and respond to in this one spatial-dimensional setting.

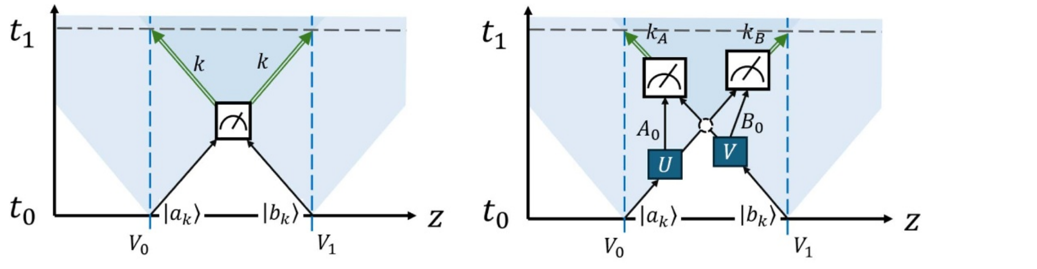

Figure 3. Spacetime diagram of the QPV protocols considered in section 3. Green double-lines denote classical communication, black lines depict quantum communication. Blue dashed lines denote the worldlines of the verifiers V_0, V_1. The dashed grey line denotes the required time to respond to the verifiers. (a) *Honest prover case.* Verifiers V_0, V_1 send $|a_k\rangle, |b_k\rangle$ respectively at time t_0. The honest prover uses any measurement that distinguishes the set of GOP states $\{|a_k\rangle|b_k\rangle\}_k$, which determines k with certainty. The prover then forwards the answer to each verifier to be received at t_1. (b) *Dishonest prover case.* The dishonest provers intercept the states $|a_k\rangle, |b_k\rangle$ respectively. As they both must answer, they split the inputs using isometries $U^{A\to A_0B_1}, V^{B\to A_1B_0}$ and forward the corresponding pieces to eachother. They then perform measurements to guess the value of k and forward the verifiers their guesses. This is the structure of local operations and simultaneous communication (LOSQC). Note the dishonest setting requires neither prover's wordline be where the honest prover should be (the dotted white circle).

While it is straightforward to see one may efficiently determine if an input set of product states has the form in (17) via Gram matrices, it is unclear if there exists an efficient method for determining if a set of the form in (17) is in fact perfectly discriminable under LOSCC. In particular, by propositions 2 and 3, deciding whether a $2\otimes d$ GOP ensemble can be perfectly distinguished by LOSQC/LOSCC reduces to the post-information discrimination problem depicted in figure 1(b). However, the method for determining $P_{\mathrm{bc}}(\mathcal{S}_\Theta)$ provided below the Proof of proposition 3 is not efficient in the sense that it scales exponentially in the dimension of the states. Nonetheless, for the simplest case of two qubits, one yet again recovers corollary 1, so in this case it is easy to determine. On the other hand, proposition 1 shows that in $\mathbb{C}^2\otimes\mathbb{C}^3$ the characterization of all GOP sets perfectly distinguishable under LOSQC or LOSCC is already non-trivial.

The equivalence between LOSCC and LOSQC stated in theorem 3 is an extension of proposition 3 to the QPV setting. We can obtain a separation between LOSCC and LOSQC from the ensemble of theorem 1 as a direct corollary to theorem 3.

Corollary 3. *The following states are distinguishable by LOSQC but not LOSCC:*

$$\begin{aligned} |\psi_1\rangle &= |0\rangle|+_{12}\rangle, & |\psi_2\rangle &= |1\rangle|+_{13}\rangle, & |\psi_3\rangle &= |2\rangle|\widetilde{+}_{23}\rangle \\ |\psi_1^\perp\rangle &= |0\rangle|-_{12}\rangle, & |\psi_2^\perp\rangle &= |1\rangle|-_{13}\rangle, & |\psi_3^\perp\rangle &= |2\rangle|\widetilde{-}_{23}\rangle. \end{aligned}$$

The ensemble in the above corollary provides the first example of a product state input QPV protocol that, in the no-PE model, is secure against attackers restricted to LOSCC but completely broken by attackers restricted to LOSQC operations. This resolves an open question from [19], where a separation between LOSQC and LOSCC attackers was shown when the inputs were entangled.

3.2. Analytic error bounds for QPV in the no-PE model

While the problem of perfect state discrimination is important for understanding the fundamental limitations of LOSCC and the comparative power of LOSQC, in practical QPV and related tasks one typically needs to replace perfect discrimination with bounded error. Specifically, as already shown, to establish security guarantees against adversaries with quantum communication, we need error bounds on how well a GOP ensemble can be discriminated by LOSQC. Establishing such bounds is difficult because the success probability of the optimal attack given by (16) is highly non-linear. However, when the inputs are product $\mathcal{S}=\{|a_k\rangle^A|b_k\rangle^B\}$ we may use the tools and insights we developed for orthogonality broadcasting to obtain upper bounds on (16). A simple way to see this is to note that because the optimal strategy is limited by the party that guesses incorrectly most frequently, we have

$$\Pr_{\mathrm{LOSQC}}[\mathcal{S}] \leqslant \max_{U,V}\min_{P\in\{A,B\}}\max_{\{\gamma_k\}}\sum_k p(k)\,\mathrm{Tr}\left[\gamma_k\sigma_k^{P_0P_1}\right], \tag{18}$$

where $\sigma_k^{P_0P_1} := \mathrm{Tr}_{\overline{P}_0\overline{P}_1}[(U\otimes V)(\rho_k)(U\otimes V)^\dagger]$, $\overline{P}$ denotes the other party than P, and the second maximization is over POVMs. Note that the RHS may be viewed as a direct generalization of $P_{\mathrm{bc}}(\mathcal{S}_\theta)$ in (7). Indeed, in the case that one input is always classical, so that without loss of generality it is simply copied, the optimal

LOSQC (resp. LOSCC) strategy is determined by the optimal orthogonality (resp. classical orthogonality) broadcasting strategy. This observation alone allows us to obtain results from our earlier results.

Corollary 4. *Let $\mathcal{S} = \{|a_k\rangle^A |b_k\rangle^B\}$ where Bob's input is classical, i.e. $|b_k\rangle \in \{|z\rangle\}_{z\in\mathcal{Z}}$ for all k where $\{|z\rangle^Z\}$ is an orthonormal basis of B. Then there exists $\mathcal{S}_\Theta$ induced by $\mathcal{S}$, such that*

$$\Pr_{\text{LOSCC}}[\mathcal{S}] = P_{\text{c-bc}}[\mathcal{S}_\Theta] = P_{\text{p-i}}[\mathcal{S}_\Theta] \ . \tag{19}$$

This in particular implies in this scenario the optimal LOSCC strategy never requires a quantum memory. Moreover, if $|\mathcal{Z}| = 2$, then the optimal LOSQC strategy is an LOSCC strategy.

Proof. By assumption, $\mathcal{S}$ may be taken to be $\mathcal{S}_\Theta$. Thus, $\Pr_{\text{LOSCC}}[\mathcal{S}] = \Pr_{\text{LOSCC}}[\mathcal{S}_\Theta] \leqslant P_{\text{c-bc}}[\mathcal{S}_\theta] = P_{\text{p-i}}[\mathcal{S}_\Theta]$, where the last equality is proposition 2. The concern would be that the inequality is strict. However, as explained below the proof of proposition 3, $\Pr_{\text{p-i}}[\mathcal{S}_\Theta]$ is always achieved by a deterministic conditional distribution. Thus, by Bob performing the optimal POVM for $P_{\text{p-i}}[\mathcal{S}_\Theta]$ (See (8)) and having Alice and Bob use the same deterministic conditional distribution, they always guess the same *i*. Thus, $\Pr_{\text{LOSCC}}[\mathcal{S}_\Theta] = P_{\text{c-bc}}[\mathcal{S}_\theta]$. Moreover, this strategy uses a fully classical broadcast channel, so it requires no quantum memory. This establishes the first point.

For the second, $\Pr_{\text{LOSQC}}[\mathcal{S}_\Theta] \leqslant P_{\text{bc}}[\mathcal{S}_\Theta] = P_{\text{c-bc}}[\mathcal{S}_\Theta] = \Pr_{\text{LOSCC}}[\mathcal{S}_\Theta] \leqslant \Pr_{\text{LOSQC}}[\mathcal{S}_\Theta]$, where the first equality is proposition 3 and the second equality is what we just proved. □

We remark that the second point of corollary 4 generalizes the observation that the optimal strategy for BB84 QPV [30] is an LOSCC strategy as first proven in [13].

While corollary 4 is structurally important, as mentioned, the most important problem for QPV is upper bounds on the achievable state discrimination under LOSQC. We can obtain such bounds as an application of the uncertainty relation in lemma 1.

Theorem 4. *Consider any ensemble containing four states of the form*

$$\begin{aligned}
|\psi_0\rangle^{AB} &= |a_0\rangle^A |b_0\rangle^B \\
|\psi_1\rangle^{AB} &= |a_1\rangle^A |b_1\rangle^B \\
|\psi_2\rangle^{AB} &= |a_2\rangle^A \left(\cos\tfrac{\theta}{2}|b_0\rangle + \sin\tfrac{\theta}{2} e^{i\phi}|b_1\rangle\right)^B \\
|\psi_3\rangle^{AB} &= |a_3\rangle^A \left(\cos\tfrac{\omega}{2}|b_0\rangle + \sin\tfrac{\omega}{2} e^{i\phi'}|b_1\rangle\right)^B ,
\end{aligned} \tag{20}$$

with $\langle a_0||a_1\rangle > 0$. Suppose Alice and Bob can identify each state with at least probability $1-\varepsilon$ using some LOSQC protocol; i.e. given state $|\psi_k\rangle^{AB}$ they both guess k with probability at least $1-\varepsilon$. Then

$$1 \leqslant \frac{2|z_1|\sqrt{\varepsilon(1-\varepsilon)}}{|\langle a_0|a_1\rangle|^2} + |z_2|\sqrt{1-|\langle b_0|b_1\rangle|^2} + \sqrt{1-|\langle a_2|a_3\rangle|^2} + 2\varepsilon, \tag{21}$$

where z_1 and z_2 are defined in lemma 1.

From theorem 4, we can recover the optimal LOSQC error bounds for BB84 QPV determined in [13, 30]. This shows that Theorem 4, and by extension all steps in the proof including our uncertainty relation, are tight.

Corollary 5. *Given the set of globally orthogonal product states*

$$\left\{|0\rangle^A|0\rangle^B, |0\rangle^A|1\rangle^B, |1\rangle^A|\hat{n}\rangle^B, |1\rangle^A|-\hat{n}\rangle^B\right\} ,$$

where $|\hat{n}\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$. The minimal ε such that both parties can guess the state with probability at least ε under LOSQC is

$$\varepsilon^\star(\theta) \geqslant \frac{1-\cos(\theta) + \left(1+\sqrt{2}\right)\sin(\theta)^2}{2\left(1+\sin(\theta)^2\right)} \ . \tag{22}$$

In particular, this recovers the tight bounds for BB84 QPV where $\theta = \pi/2$.

Proof. Note without loss of generality we may let $\phi = 0 = \phi'$ by rotating the states into the $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ plane of the Bloch sphere. For the states we consider, $|-\hat{n}\rangle = \cos(\frac{\theta-\pi}{2})|0\rangle + \sin(\frac{\theta-\pi}{2})|1\rangle$. It follows $z_1 = \sin(\theta)$ and $z_2 = \cos(\theta)$ in theorem 4. Using theorem 4, one finds the condition

$$1 \leqslant 2\sin(\theta)\sqrt{\varepsilon(1-\varepsilon)} + \cos(\theta) + 2\varepsilon \ .$$

Solving this as an equality condition, one finds (22). To recover the BB84 case, one uses $\theta = \pi/2$ to obtain $1 - \varepsilon^\star = 1 - \frac{1}{4}(2+\sqrt{2}) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$. However, this can be achieved by Bob measuring each state in the 'Breidbart basis', so this bound is tight. □

We remark that by generalizing the Breidbart basis measurement to measuring the states equidistant on the Bloch sphere between $|0\rangle, |\hat{n}\rangle$, i.e. projecting $|\hat{m}_\theta\rangle = \cos(\theta/4)|0\rangle + \sin(\theta/4)|1\rangle$ and its orthogonal vector, one can obtain a minimum error of $1-\cos(\theta/4)^2$. This is a slightly larger error than given in (22), which would suggest (22) is loose except for $\theta \in \{0, \pi/2\}$.

We provide another example of how theorem 4 can be used to bound the minimum error guessing probability.

Example 1. An unextendible product basis (UPB). Consider the tripartite UPB known as **Shifts** [31]. Combining two of the parties yields the bipartite ensemble

$$\begin{aligned} |\psi_0\rangle &= |00\rangle|0\rangle, & |\psi_1\rangle &= |+-\rangle|1\rangle, \\ |\psi_2\rangle &= |-1\rangle|+\rangle, & |\psi_3\rangle &= |1+\rangle|-\rangle. \end{aligned} \tag{23}$$

If one of these is chosen with uniform probability and distributed to Alice and Bob, their smallest possible guessing error ε using LOSQC satisfies $\varepsilon > 5.52 \times 10^{-4}$. Clearly this also provides a lower bound on the tripartite error probability for **Shifts** under LOSQC.

Remark . Note that the same sort of analysis may be applied to quantum states shared by more parties. In particular, if one can partition the systems such that one has a set of bipartite states where a subset satisfies the structure of (21), then one may apply theorem 4. The error will then scale governed by theorem 4.

3.3. Semidefinite program bounds

We remark a major appeal of theorem 4 is that it is quick to evaluate. One can however in various cases directly obtain bounds on the probability of distinguishing a set of input states $\mathcal{S} := \{|\psi_k\rangle^{AB}\}_k$ over a given distribution using LOSQC using the uncertainty relation to convert the problem into a SDP over vectors. For example, using the same tools as to establish theorem 4, we can obtain the following SDP, which is provably generally non-trivial.

Proposition 4. *Consider the ensemble $\mathcal{S}$ of the form given in theorem 4 and ψ_0, ψ_1 (resp. ψ_θ, ψ_ω) are each provided with probability $p/2$ (resp. $(1-p)/2$). Then, $\Pr_{\mathrm{LOSQC}}[\mathcal{S}]$ is upper bounded by the optimal value of*

$$\begin{aligned} \max \;\; & \min\{f(p,\mathcal{S},\mathbf{r}), f(p,\mathcal{S},\mathbf{s})\} - 1 \\ \text{s.t.} \;\; & r_1 \leqslant \frac{1}{2}\left[|z_1|\sqrt{1-(2s_0-1)^2} + |z_2|(2r_0-1)+1\right] \\ & s_1 \leqslant \frac{1}{2}\left[|z_1|\sqrt{1-(2r_0-1)^2} + |z_2|(2s_0-1)+1\right] \\ & 0 \leqslant \mathbf{r}, \mathbf{s} \leqslant 1 \end{aligned} \tag{24}$$

where $f(p,\mathcal{S},\mathbf{x}) := p\cdot[p_g(a_0,a_1)+x_0] + (1-p)[p_g(a_3,a_4)+x_1]$. This is a convex optimization problem and equals unity if and only if $\langle a_0|a_1\rangle = 0 = \langle a_3|a_4\rangle$ and $\theta = \pm\arccos(1+\cos(\omega))$.

We remark that proposition 4 may be used as yet another method for proving corollary 5 although we omit this.

There are two key ideas in establishing proposition 4 as well as the other results in this section. The first is captured in (18). The second is that the uncertainty relation (corollary 2) implies constraints on the guessing probabilities independent of Alice and Bob's choices of broadcasting channels, so we may replace maximizing over the isometries by maximizing the guessing probabilities allowed according to the uncertainty relation as may be seen in (24). We refer the reader to the appendices for more information.

The major strength of these semidefinite program bounds is not in proposition 4, but in the more direct analysis of discriminating product state ensembles $\mathcal{S} := \{|a_k\rangle^A|b_k\rangle^B\}$ that are not of the form in theorem 4 but are limited by the inability to broadcast orthogonality. This results in obtaining stronger, i.e. smaller-valued, upper bounds on the optimal distinguishing probability under LOSQC, $\Pr_{\mathrm{LOSQC}}[\mathcal{S}]$[7]. We will in particular establish a qutrit classical-quantum product state that outperforms the BB84 set in terms of amplifying the error (theorem 5) and, to the best of our knowledge, the first proof of error bounds on

[7] Smaller-valued upper bounds are stronger because, in QPV, LOSQC represents the attack model of dishonest provers, so if the probability of success is lower, then the protocol is more secure against dishonest provers.

quantum-quantum product states (theorem 6). We note that, as shown in appendix A, neither of these cases can be analyzed using MOE games.

We begin by showing there exist sets of globally orthogonal classical-quantum product states that result in provably stronger security than using BB84 states. In particular, we consider the following set of states:

$$\mathcal{S}_{OBB} = \left\{ \begin{array}{cc} |\psi_1\rangle = |0\rangle|1\rangle & \\ |\psi_2\rangle = |0\rangle|2\rangle & |\psi_3\rangle = |1\rangle|1+2\rangle \\ |\psi_4\rangle = |1\rangle|1-2\rangle & |\psi_5\rangle = |0\rangle|0\rangle \\ |\psi_6\rangle = |2\rangle|0+1\rangle & |\psi_7\rangle = |2\rangle|0-1\rangle \end{array} \right\} . \tag{25}$$

It is not hard to see that the subsets $\mathcal{S}_1' := \{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, |\psi_4\rangle\}$ and $\mathcal{S}_2' := \{|\psi_1\rangle, |\psi_5\rangle, |\psi_6\rangle, |\psi_7\rangle\}$ are both equivalent to $\mathcal{S}_{\mathrm{BB84}}$ up to local unitaries. However, note that $\mathcal{S}_1', \mathcal{S}_2'$ contain overlapping states on Bob's side, which is why we label them OBB (overlapping BB84 states). It follows that using the optimal strategy for each subset, given in the proof of corollary 5, may do quite poorly on the other set of states. In other words, one expects the optimal approximate broadcasting of $\mathcal{S}_{\mathrm{OBB84}}$ to be lower than $\mathcal{S}_{\mathrm{BB84}}$. Using our methodology, we are indeed able to prove this.

Theorem 5. *Consider the set of globally orthogonal product qutrit states $\mathcal{S}_{\mathrm{OBB84}}$ in (25) where $|\psi_1\rangle$ occurs with probability $1/4$ and the rest occur with probability $1/8$. Then*

$$\Pr_{\mathrm{LOSQC}}[\mathcal{S}_{OBB}] \leqslant 0.603554 . \tag{26}$$

We first stress that the ability to establish such results follows from our ability to work with the geometry of the initial states using lemma 1. Moreover, we note that this result is quite strong in the following sense. By corollary 5, $\Pr_{\mathrm{LOSQC}}[\mathcal{S}_{OBB}] < \Pr_{\mathrm{LOSQC}}[\mathcal{S}_{\mathrm{BB84}}]$, but $\mathcal{S}_{\mathrm{OBB84}}$ requires more resources to implement (namely, a qutrit quantum system and the ability to prepare certain superposition states). To place the two ensembles on an equal footing, we could measure the error 'per state' in comparison to global success probability $\Pr[\mathcal{S}]$:

$$\Delta_{\mathrm{LOSQC}}(\mathcal{S}) = \left(\Pr[\mathcal{S}] - \Pr_{\mathrm{LOSQC}}[\mathcal{S}] \right) / |\mathcal{S}| . \tag{27}$$

A direct calculation will find $\Delta_{\mathrm{LOSQC}}(\mathcal{S}_{\mathrm{BB84}}) < 0.03662$ whereas $\Delta_{\mathrm{LOSQC}}(\mathcal{S}_{\mathrm{OBB84}}) > 0.05663$. Thus, by increasing to a qutrit (resp. trit) space on Bob's (resp. Alice's) side, we may increase the error per state, which may have practical relevance in cryptographic schemes that rely on the impossibility of orthogonality broadcasting.

Intuitively, we should be able to further amplify the result of theorem 5 by giving *both* Alice and Bob non-commuting states from a globally orthogonal set. One would expect under certain conditions this would amplify the result as then Alice will also need to implement approximate orthogonal broadcasting. This is motivated not only from a foundational perspective, but also the possibility of building secret sharing schemes [4] out of product states.

It appears that our uncertainty relation, lemma 1 as well as its generalization, is not strong enough to place constraints to prove that making Alice's states from $\mathcal{S}_{\mathrm{OBB84}}$ in (25) quantum as well will increase the error probability specifically (see appendix E for further discussion), but we are able to construct a different example such that there is a non-trivial increase in the probability of error in distinguishing the states by having both parties receive quantum inputs. In particular, we consider the globally orthogonal classical-quantum product states

$$\mathcal{S}_{cq} = \left\{ \begin{array}{cc} |\psi_1\rangle = |1\rangle|1\rangle & |\psi_2\rangle = |1\rangle|0+2\rangle \\ |\psi_3\rangle = |1\rangle|0-2\rangle & |\psi_4\rangle = |0\rangle|0+1\rangle \\ |\psi_5\rangle = |0\rangle|0-1\rangle & |\psi_6\rangle = |2\rangle|1+2\rangle \\ |\psi_7\rangle = |2\rangle|1-2\rangle & \end{array} \right\} \tag{28}$$

and the set of globally orthogonal quantum-quantum states

$$\mathcal{S}_{qq} = \left\{ \begin{array}{cc} |\psi_1\rangle = |1\rangle|1\rangle & |\phi_2\rangle = |1-0\rangle|2\rangle \\ |\psi_3\rangle = |0\rangle|0+1\rangle & |\psi_4\rangle = |0\rangle|0-1\rangle \\ |\psi_5\rangle = |2\rangle|1+2\rangle & |\psi_6\rangle = |2\rangle|1-2\rangle \\ |\phi_7\rangle = |1+2\rangle|0\rangle & \end{array} \right\} . \tag{29}$$

One may see that $\mathcal{S}_{qq}$ is a globally orthogonal product set obtained from $\mathcal{S}_{cq}$ by altering which party has the coherence for two of the states, i.e. $|\psi_2\rangle \to |\phi_2\rangle$, $|\psi_7\rangle \to |\phi_7\rangle$, which will then suffer from both parties needing to approximately broadcast (see figure 4 for visual comparison).

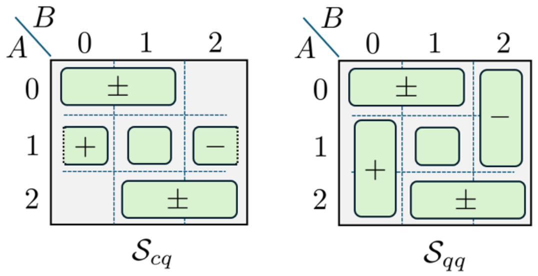

Figure 4. Depiction of the sets $\mathcal{S}_{cq}$ and $\mathcal{S}_{qq}$ (equations (28) and (29) respectively) in terms of 'tilings' [32, 33]. A state $|\psi\rangle^{AB}$ is depicted on a 'tile' (i,j) if $\langle i|^A\langle j|^B|\psi\rangle \neq 0$, i.e. if the state has 'support' on the joint computational basis state. The ± symbol denotes that two superposition states lay on the tile. The dashed tile in the left image means that Bob's state has support on both $|0\rangle$ and $|2\rangle$.

The choice of classical states in $\mathcal{S}_{cq}$ allows us to establish that, independent of the distribution on the states,

$$\Pr_{\text{LOSQC}}\left[\mathcal{S}_{cq}\right] \geqslant \Pr_{\text{LOSCC}}\left[\mathcal{S}_{cq}\right] \geqslant \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right).$$

On the other hand, we are able to show using our semidefinite program method that the success probability of distinguishing $\mathcal{S}_{qq}$ is strictly lower. While intuitive, to the best of our knowledge, this is the first proof of such an example.

Theorem 6. *Consider $\mathcal{S}_{cq}$ and $\mathcal{S}_{qq}$ where in both cases $|\psi_1\rangle$ occurs with probability $1/4$ and the rest occur with probability $1/8$. Then*

$$\Pr_{\text{LOSQC}}\left[\mathcal{S}_{qq}\right] \leqslant 0.7805 < \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) \leqslant \Pr_{\text{LOSQC}}\left[\mathcal{S}_{cq}\right].$$

That is, forcing both parties to approximately broadcast increases the probability of error.

4. Conclusion and outlook

In this paper, we have introduced the study of orthogonality broadcasting. We have established a strong characterization of its properties in low dimensions, related it to the cryptographic task of QPV, and established new methods for error bounds on QPV protocols when there is no-PE. In doing so, we have introduced a new uncertainty relation that uses the geometric relation of the initial states to be broadcasted and shown both its utility and its limitations.

We note that the ability to combine our uncertainty relation to derive semidefinite programming bounds on vectors of guessing probabilities in the LOSQC setting (e.g. proposition 4 and the derivations of theorems 5 and 6) may be of interest in the framework of optimization programs capturing correlations. In particular, it is well-known that non-signaling correlations are quite useful for deriving linear program bounds in various settings [34–36]. However, a key technical issue in LOSQC is the fact that there is signaling (the simultaneous communication), which is what makes it distinct from the framework of non-local games [34, 37]. Roughly speaking, our uncertainty relation is constraining the strength of the correlations achievable via signaling at the expense of the linear program becoming a semidefinite program.

Finally, we highlight two natural future directions based on this work. First, the study of (approximate) orthogonality broadcasting seems deeply related to approximate symmetric quantum cloning and the notion of symmetric extendability. A more in-depth study of the relation between these may be of both fundamental and practical value. Second, in section 3.3, it was highlighted that the SDP bounds are in effect coming from the uncertainty relation bounding the correlations achievable through signaling and that the uncertainty relation can be loose under certain situations. It could be of value to develop more general methods for constraining the achievable correlations under signaling through broadcast channels. In particular, such methods might be able to improve upon and clarify the scaling of error per state under LOSQC for families of states that generalize the overlapping BB84 construction in theorem 5. The hope would be that this would give insight into designing QPV protocols that are hard to break with entanglement given the relation between the no-PE model and the entanglement-assisted case, e.g. [38, lemma 5.3].

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

We thank Harry Buhrman for fruitful initial discussions in the early stages of this work. This research was conducted when R A and P VL were affiliated with CWI Amsterdam and QuSoft. R A was supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (Project Number 024.003.037). The majority of this work was performed while P VL was at CWI. P VL was supported by the Dutch Research Council (NWO/OCW), as part of the NWO Gravitation Programme Networks (Project Number 024.002.003). The majority of this work was performed while I G was at University of Illinois at Urbana-Champaign. E C and I G were supported by the U.S. Department of Energy Office of Science National Quantum Information Science Research Centers.

Appendix A. Monogamy-of-entanglement games, quantum position verification, and orthogonality broadcasting

In this section, we clarify the relation between MoE games, QPV, and orthogonality broadcasting. In particular, we show why MoE games are both a less direct reduction for proving security of QPV in the no-PE model and at times cannot establish security while the orthogonality broadcasting methodology can.

A.1. A review on monogamy-of-entanglement (MoE) games

We begin with the description of a MoE game (see figure A1 for depiction), the physical idea it operationally captures, and the primary tool used to analyze MoE games [13, lemma 2]. For clarity, we describe the procedure with references to the subsequent formal definitions.

As depicted in figure A1, in a MoE game G (definition 1), Alice's measurements $\{\mathcal{M}^\theta = \{F^\theta_x\}\}_\theta$ are publicly known and fix the dimension of the quantum system she is to receive. Bob and Charlie prepare a quantum state ρ_{ABC} according to their strategy $\mathcal{S}$ (definition 2). They then forward the A system to Alice. Alice draws θ from Θ uniformly at random and applies the measurement $\mathcal{M}^\theta = \{F^\theta_x\}$ to the A system, obtaining outcome $x_A \in \mathcal{X}$. Bob and Charlie therefore share the conditional state

$$\rho^{BC}_{x_A|\theta} := \frac{\mathrm{Tr}_A\left[F^\theta_{x_A} \otimes \mathbb{1}^B \otimes \mathbb{1}^C \rho^{ABC}\right]}{\mathrm{Tr}\left[F^\theta_{x_A}\rho^A\right]} \,. \tag{A.1}$$

Alice then announces θ to Bob and Charlie who then apply their corresponding measurements $\{P^\theta_x\}_{x\in\mathcal{X}}$, $\{Q^\theta_x\}_{x\in\mathcal{X}}$ as specified by their strategy $\mathcal{S}$ (definition 2). Bob and Charlie's measurement outcomes are x_B, x_C respectively. Bob and Charlie 'win' whenever $x_A = x_B = x_C$ as by definition 3.

Definition 1. A monogamy-of-entanglement (MoE) game G is defined by a finite-dimensional Hilbert space $A = \mathbb{C}^d$ and a set of $|\Theta|$ POVMs on A, $\mathcal{M}^\theta = \{F^\theta_x\}_{x\in\mathcal{X}}$. $\theta \in \Theta$ indexes the choice of POVM and $x \in \mathcal{X}$ indexes the measurement outcome. $\Theta, \mathcal{X}$ are finite alphabets.

Definition 2. A strategy $\mathcal{S}$ for a MoE game G is specified by a tuple

$$\mathcal{S} = \left(\rho^{ABC}, \{P^\theta_x\}_{x\in\mathcal{X},\theta\in\Theta}, \{Q^\theta_x\}_{x\in\mathcal{X},\theta\in\Theta}\right) \,,$$

where ρ^{ABC} is quantum state, B, C are arbitrary finite-dimensional Hilbert spaces, and $\{P^\theta_x\}_{x\in\mathcal{X}}$ (resp. $\{Q^\theta_x\}_{x\in\mathcal{X}}$) is a POVM on B (resp. C) for every $\theta \in \Theta$.

Definition 3. The winning probability of a MoE game G with a strategy $\mathcal{S}$ is defined as

$$p_{\mathrm{win}}(G,\mathcal{S}) := \sum_{\theta\in\Theta} \mathrm{Tr}\left[\Pi^\theta \rho^{ABC}\right], \quad \text{where} \quad \Pi^\theta := \sum_x F^\theta_x \otimes P^\theta_x \otimes Q^\theta_x \,. \tag{A.2}$$

The optimal winning probability is $p_{\mathrm{win}}(G) := \sup_{\mathcal{S}} p_{\mathrm{win}}(G,\mathcal{S})$.

The intuition behind an MoE game is as follows. Imagine Alice and Bob share a maximally entangled state $|\Psi^+\rangle\langle\Psi^+|^{AB}$ and Alice performs projective measurements, i.e. $\mathcal{M}^\theta = \{U_\theta|x\rangle\langle x|U^\dagger_\theta\}_{x\in\mathcal{X}}$ where U_θ is some unitary for every $\theta \in \Theta$. A standard calculation using the transpose trick [39] will verify that Bob's conditional state $\rho^B_{x|\theta} = U^{\mathrm{T}}|x\rangle\langle x|\overline{U}$ where $\overline{X}$ denotes the entry-wise conjugate of X and T is the matrix

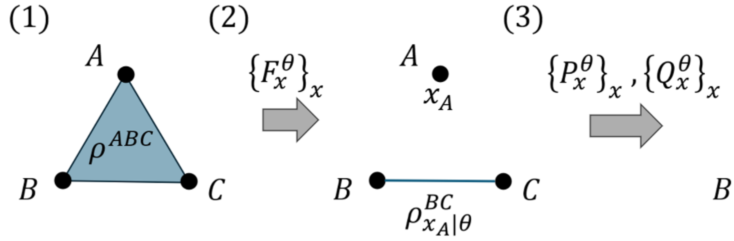

Figure A1. Depiction of a Monogamy-of-Entanglement game. In the first step, Alice, Bob, and Charlie share a joint quantum state ρ^{ABC} that Bob and Charlie chose. In Step 2, Alice chooses θ uniformly randomly and measures the A system with POVM $\{F_x^\theta\}_x$ to obtain outcome x_A. Bob and Charlie then share a conditional state $\rho^{BC}_{x_A|\theta}$. In step 3, Alice has told Bob and Charlie the value of θ, so they perform measurements $\{P_x^\theta\}_x$, $\{Q_x^\theta\}_x$ to their respective portions of the conditional state obtaining outcomes x_B, x_C. Bob and Charlie win the game when $x_A = x_B = x_C$.

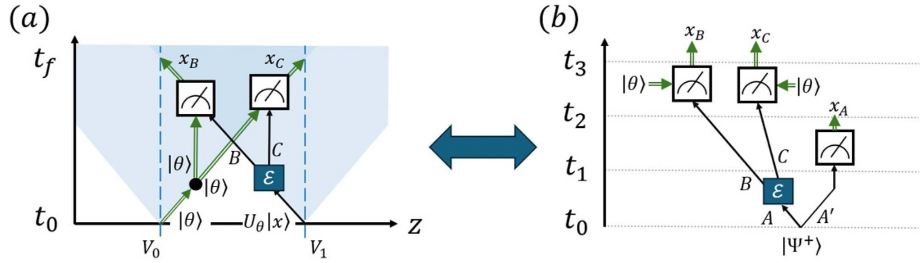

Figure A2. Depiction of the reduction of a certain class of QPV protocols to monogamy-of-entanglement games. (a) Depicts the spacetime diagram of the relevant QPV protocols where one dishonest prover receives $|\theta\rangle$ to copy and forward and the other party receives $U_\theta|x\rangle$ which they attempt to broadcast with $\mathcal{E}^{A\to BC}$. (b) Depicts a mathematically equivalent setup to the QPV protocol. At the initial time, a maximally entangled state is shared. At t_1, $\mathcal{E}^{A\to BC}$ has been applied. At t_2, a random $\theta \in \Theta$ has been chosen and the measurement $\{F_x^\theta := U_x^{\mathrm{T}}|x\rangle\langle x|\overline{U}_x\}_x$ has been applied to the A' system. At t_3, measurements $\{P_x^\theta\}$, $\{Q_x^\theta\}$ have been applied according to θ. Note that t_1, t_2, and t_3 respectively correspond to (1),(2), and (3) in figure A1. In other words, it depicts a specific strategy of a MoE game.

transpose. As $\{\rho^B_{x|\theta}\}_{x\in\mathcal{X}}$ is a set of mutually orthogonal states, this means in this scenario if Alice measures with $\mathcal{M}^\theta$ and tells Bob θ, Bob can always determine x. However, if Bob shares a maximally entangled state with Alice, then Charlie is completely independent, i.e. $\rho_{ABC} = |\Psi^+\rangle\langle\Psi^+|^{AB} \otimes \rho^C$. This implies Charlie's conditional state will be completely independent of Alice's measurement and so it will be hard for *both* Bob and Charlie to guess the value of x correctly. 'MOE' generalizes the above to the idea that the more entangled Bob is with Alice, the less entangled Charlie is with Alice. An MoE game tests this idea operationally. Namely, it tests how entangled ρ_{AB} is versus ρ_{AC} by examining the winning probability, (A.2). If monogamy of entanglement applies, then there does not exist ρ^{ABC} such that $\sum_\theta \mathrm{Tr}[\Pi^\theta \rho^{ABC}] = 1$ where Π^θ is defined in (A.2). Note that this does not directly capture anything about broadcasting or orthogonality broadcasting.

It is difficult to prove there does not exist ρ^{ABC} such that $\sum_\theta \mathrm{Tr}[\Pi^\theta \rho^{ABC}] = 1$ as one needs to optimize over all possible $\{P_x^\theta\}$ and $\{Q_x^\theta\}$ in definition 2. As such, MoE games are instead analyzed using the bound $\sum_\theta \mathrm{Tr}[\Pi^\theta \rho^{ABC}] \leqslant \|\sum_\theta \Pi^\theta\|$, where $\|\cdot\|$ is the operator norm and this follows from $\mathrm{Tr}[M\rho^{ABC}] \leqslant \|M\|$. This is still difficult due to optimizing over both measurements, so further tools are needed. In particular, [13] establishes and uses the following lemma.

Lemma 2 ([13]). *Let $R_0, R_1, \ldots, R_n$ be n positive semidefinite operators. Let $\{\pi^k\}_{k\in[n]}$ be a set of n permutations such that $\pi^{k_1}(i) \neq \pi^{k_2}(i)$ for all $i \in [n]$, $k_1, k_2 \in [n]$ such that $k_1 \neq k_2$. Then the following inequality holds*

$$\left\| \sum_{i\in[n]} R_i \right\| \leqslant \sum_{k\in[n]} \max_{i\in[n]} \left\| \sqrt{R_i}\sqrt{R_{\pi^k(i)}} \right\| . \tag{A.3}$$

A.2. Reduction of specific QPV protocols to monogamy-of-entanglement games

We now explain how the reduction of a specific instance of QPV to MoE works as it will help to clarify how MoE and orthogonality broadcasting compare. Certain systems are labeled differently than in the main text to make the conversion to an MoE game clearer. Consider a QPV protocol where V_0 sends $\theta \in \Theta$ and V_1 sends $\rho^A_{x|\theta} := U_\theta|x\rangle\langle x|U_\theta^\dagger$ where $\{U_\theta\}_{\theta\in\Theta}$ is a set of unitaries and x, θ are drawn uniformly from their sets (see figure A2 for depiction). The dishonest prover that receives $\rho_{x|\theta}$, Bob, must attempt to broadcast the orthogonality using some broadcast channel $\mathcal{E}^{A\to BC}$. The dishonest prover that receives θ, Charlie, simply copies and forwards the value to Charlie. Then, upon receiving θ and their respective quantum system, Bob and Charlie perform local measurements conditioned on $\theta \in \Theta$ to obtain outcomes x_B, x_C and send these to the verifiers closer to them[8].

However, using the 'transpose trick' [39], one may verify $\mathrm{Tr}_{A'}[U_\theta^{\mathrm{T}}|x\rangle\langle x|\overline{U}_\theta \otimes \mathbb{1}_A|\Psi^+\rangle\langle\Psi^+|] = U_\theta|x\rangle\langle x|U_\theta^\dagger$ where $|\Psi^+\rangle_{A'A}$ is the maximally entangled state and the transpose is defined in the computational basis. It follows that the QPV protocol is *mathematically* equivalent to the following procedure (depicted in figure A2):

(i) V_0 sends nothing and V_1 sends the A system of $|\Psi^+\rangle\langle\Psi^+|^{A'A}$ to Charlie.
(ii) Charlie broadcasts the A system with $\mathcal{E}^{A\to BC}$.
(iii) At some point before Bob and Charlie decide to measure their local portions of $\rho^{ABC} := (\mathrm{id}^{A'} \otimes \mathcal{E}^{A\to BC})(|\Psi^+\rangle\langle\Psi^+|)$, θ, V_1 randomly draws θ, measures the A' system with $\{U_\theta^{\mathrm{T}}|x\rangle\langle x|\overline{U}_\theta\}_{x\in\mathcal{X}}$, and provides the value of θ to both Bob and Charlie.
(iv) Bob and Charlie perform their measurements as in the true protocol.

Note this new procedure is an MoE game with some specification of the strategy, namely ρ_{ABC}. It follows that the optimal strategy for the MoE game defined by $\mathcal{M}^\theta := \{U_\theta^{\mathrm{T}}|x\rangle\langle x|\overline{U}_\theta\}$ provides an upper bound on all possible QPV attacks in the no-PE model. Moreover, it just so happens that this is tight when $\{U_\theta\}_\theta = \{\sigma_X, H\}$, which are the Pauli X and Hadamard unitaries, i.e. the bound is tight for BB84 QPV [13].

Remark . The above relation between QPV, orthogonality broadcasting, and MoE games may be slightly generalized. If a QPV protocol has classical-quantum inputs $\{|\theta\rangle\langle\theta| \otimes \rho^A_{x|\theta}\}_{x,\theta}$ sent according to joint distribution $p(x,\theta) = \frac{1}{|\Theta|}p(x|\theta)$. Then the optimal attack in the no preshared entanglement model is exactly orthogonality broadcasting as we have seen in the main text. However, *if* there exists a set of $|\Theta|$ POVMs, $\{F_x^\theta\}_x$, and a joint quantum state $\sigma^{AA'}$ such that

$$\mathrm{Tr}\left[F_x^\theta \sigma^{A'}\right] = p\left(x|\theta\right) \qquad \frac{\mathrm{Tr}\left[I^A \otimes F_x^\theta \sigma^{AA'}\right]}{p\left(x|\theta\right)} = \rho^A_{x|\theta} \quad \forall x, \theta \; , \tag{A.4}$$

then this shows the QPV protocol is mathematically equivalent to the MoE game defined by the POVMs $\{F_x^\theta\}$ using the strategy $\rho^{ABC} := (\mathrm{id}^A \otimes \mathcal{E}^{A'\to BC})(\sigma^{AA'})$. As such, one can further relax analyzing the security of the QPV protocol in the no-PE model to the MoE game defined by the POVMs $\{F_x^\theta\}$ and optimizing over all strategies. Note however this is always a further relaxation from considering orthogonality broadcasting directly.

Remark [**17, appendix A**] introduces a '$1 \to 2$ cloning game' where $\mathcal{E}_{A\to BC}$ is specified. As they show, this is like restricting the strategy of the MoE game to avoid the last reduction to MoE given above.

A.3. Comparing orthogonality broadcasting and monogamy-of-entanglement games

With the sufficient background, we may now separate orthogonality broadcasting from MoE games. First, in the previous subsection, a footnote specified where the equivalence of this specific type of QPV protocol to orthogonality broadcasting occurs. This was prior to converting to an alternative protocol using a maximally entangled state. This alone shows it is at least more direct for the protocols above. Second, as orthogonality broadcasting considers a different aspect of quantum mechanics than MoE games, it can be applied to QPV protocols that do not satisfy the structure necessary for the reduction to an MoE game. Indeed, noting that both systems in (29) used in theorem 6 are quantum, it follows the MoE game reduction given above cannot be done at all for this ensemble. This already distinguishes the two methods. However, even if one of the inputs is classical, the reduction to MoE games is insufficient with current methods as the following example shows.

Example 2. Note that (25) has one system always classical, but the quantum states partition (with respect to the other system's classical value) as $\{|0\rangle,|1\rangle,|2\rangle\}$,$\{|0\pm 1\rangle\}$,$\{|1\pm 2\rangle\}$. Therefore, this is an ensemble that cannot be generated in the form $\{|\theta\rangle\left(U_\theta|x\rangle\right\}_{\theta,x}$ as the reduction in the previous paragraph required. However, the situation is significantly worse—if we tried to complete these bases, the measurements are

$$\begin{aligned}
\mathcal{M}^0 &= \{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\} \\
\mathcal{M}^1 &= \{|0\rangle\langle 0|, |1+2\rangle\langle 1+2|, |1-2\rangle\langle 1-2|\} \\
\mathcal{M}^2 &= \{|0+1\rangle\langle 0+1|, |0-1\rangle\langle 0-1|, |2\rangle\langle 2|\} \; .
\end{aligned} \tag{A.5}$$

[8] Recalling figure 1, this shows this specific type of QPV protocol is exactly orthogonality broadcasting.

If we define G_O to be the MoE game defined by the measurements in (A.5), then the methods of [13] obtain trivial bounds. This is because the measurements pairwise contain a projective POVM element that is identical. For completeness, we show this. First, following the notation of [13, theorem 4],

$$c(G_O) = \max_{\substack{\theta,\theta' \in \Theta \\ \theta \neq \theta'}} \max_{x,x' \in \mathcal{X}} \left\| \sqrt{F_x^\theta} \sqrt{F_{x'}^{\theta'}} \right\| = \| |0\rangle\langle 0| |0\rangle\langle 0| \| = 1 \,, \tag{A.6}$$

where we used $F^0{}_0 = |0\rangle\langle 0| = F^1{}_0$ by (A.5). Then [13, theorem 4] provides the trivial upper bound of 1. Moreover, the more in-depth analysis of [13, theorem 3] is also trivial as we now show. First,

$$p_{\text{win}}\left(G_O\right) = \frac{1}{3} \sum_\theta \operatorname{Tr}\left[\Pi^\theta \rho_{ABC}\right] \leqslant \frac{1}{3} \| \sum_\theta \Pi^\theta \| \leqslant \frac{1}{3} \sum_k \max_\theta \| \Pi^\theta \Pi^{\pi^k(\theta)} \| \,, \tag{A.7}$$

where Π^θ is defined as in (A.2) and the second inequality is lemma 2. In principle we would need to optimize over strategies, but we will just pick one that makes the bound trivial. Let both Bob and Charlie use the same measurements as Alice as given in (A.5). Then $\Pi^\theta = \sum_{i \in [3]} F_i^{\theta \otimes 3}$ for $\theta \in [3]$. Because each θ, θ' share a rank-one projector, $\|\Pi^0 \Pi^1\| = \|\Pi^0 \Pi^2\| = \|\Pi^1 \Pi^2\| = 1$. It follows with this choice $p_{\text{win}}(G_O) \leqslant \frac{1}{3} \sum_k \max_\theta \|\Pi^\theta \Pi^{\pi^k(\theta)}\| = \frac{1}{3} \cdot 3 = 1$. Thus the bound remains trivial. This shows MoE games, at least using the standard tool, (lemma 2) cannot establish security for this ensemble.

Appendix B. Necessity of non-separable communication

In this section we establish theorem 2.

Proof of theorem 2. Consider the eight orthogonal product states stated in the theorem, which we label

$$\begin{array}{ll} |\varphi_1\rangle = |1\rangle^A |1\rangle^B & |\varphi_2\rangle = |1\rangle^A |2\rangle^B \\ |\varphi_3\rangle = |2\rangle^A |+_{23}\rangle^B & |\varphi_4\rangle = |2\rangle^A |-_{23}\rangle^B \\ |\varphi_5\rangle = |3\rangle^A |+_{24}\rangle^B & |\varphi_6\rangle = |3\rangle^A |-_{24}\rangle^B \\ |\varphi_7\rangle = |4\rangle^A |\tilde{+}_{34}\rangle^B & |\varphi_8\rangle = |4\rangle^A |\tilde{-}_{34}\rangle^B \end{array}$$

where we remind the reader $|\pm_{mn}\rangle = \frac{1}{\sqrt{2}}(|m\rangle \pm |n\rangle$ and $|\tilde{\pm}_{mn}\rangle = \frac{1}{\sqrt{2}}(|m\rangle \pm i|n\rangle$. It is clear that Alice's action in any LOSQC discrimination protocol should involve her measuring in the computational basis and distributing the outcome information to Bob. It is therefore Bob's job to broadcast the orthogonality of his portion of the state. More precisely, he must perform a channel $|b_x\rangle^B \mapsto \rho_x^{A_2 B_1}$ such that $\{\rho_x^{A_2}, \rho_{x+1}^{A_2}\}$ and $\{\rho_x^{B_1}, \rho_{x+1}^{B_1}\}$ form sets of orthogonal operators for $x = 1, 3, 5, 7$. Moreover, as per the statement of the theorem, we are interested in establishing that any such broadcasting channel $\mathcal{E}_{B \to A'B'}$ must map one of the states on the B space to the joint space $A'B'$ such that it is entangled. We will prove this is the case by contradiction, i.e. we will look at the structure necessary for $\mathcal{E}_{B \to A'B'}$ to map each state to a separable state.

Recall that a separable operator R is a positive operator from $A \otimes B$ to $A \otimes B$, $X \in \text{Pos}(A \otimes B)$, such that there exists a finite alphabet $\mathcal{I}$ and sets of positive operators $\{P_i\}_{i \in \mathcal{I}} \subset \text{Pos}(A)$, $\{Q_i\}_{i \in \mathcal{I}} \subset \text{Pos}(B)$ such that $R = \sum_i P_i \otimes Q_i$. Note that by the spectral decomposition theorem, we may in fact decompose such an operator into a linear combination of tensor products of unit vectors. Thus, we would say $\rho_k^{A'B'} = \mathcal{E}_{B \to A'B'}(\rho_k)$ is separable if we may write it as $\sum_i |x_i\rangle\langle x_i| \otimes |y_i\rangle\langle y_i|$ where $\{|x_i\rangle\}_{i \in \mathcal{I}} \subset A'$, $\{|y_i\rangle\}_{i \in \mathcal{I}} \subset B'$ are (not necessarily normalized) vectors. Note that, when $\rho_k^{A'B'}$ is separable, this implies a purification, of the form

$$\sum_i |x_i\rangle^{A'} |y_i\rangle^{B'} |i\rangle^E \,, \tag{B.1}$$

where $\{|i\rangle\}_i$ is an orthonormal basis. That this is a purification may be verified by taking the trace over the E system. Moreover, by the isometric equivalence of purifications on the purifying space [29], *all* purifications of $\rho_k^{A'B'}$ are of this form up to a choice of basis on the E system. It follows that if $\mathcal{E}_{A \to A'B'}$ maps a pure state $|\varphi\rangle$ to a separable state $\rho^{A'B'}$, then if we consider the isometric extension of $\mathcal{E}$, $U_{A \to A'B'E}$, $U|\varphi\rangle$ is a pure state and thus a purification of $\rho_k^{A'B'}$. It follows that it must have the form of (B.1). This is the structure we will make use of in the rest of the proof.

Suppose that Bob *does not* distribute entanglement to Alice given the state $|\varphi_2\rangle$. Then by the above explanation, this means he applies an isometry $U : A \to A'B'E$ such that

$$U|2\rangle = \sum_i |x_i\rangle^{A'} |y_i\rangle^{B'} |i\rangle^E. \tag{B.2}$$

Turning to states $|\varphi_3\rangle$ and $|\varphi_4\rangle$, by linearity, the action of Bob's isometry has the form

$$\begin{aligned} |\alpha_3\rangle^{A'B'E} &= U|{+}_{23}\rangle = \frac{1}{\sqrt{2}}\sum_i \left(|x_i\rangle^{A'}|y_i\rangle^{B'} + |\psi_i\rangle^{A'B'}\right)|i\rangle^E \\ |\alpha_4\rangle^{A'B'E} &= U|{-}_{23}\rangle = \frac{1}{\sqrt{2}}\sum_i \left(|x_i\rangle^{A'}|y_i\rangle^{B'} - |\psi_i\rangle^{A'B'}\right)|i\rangle^E \end{aligned}$$

where $U|3\rangle = \sum_i |\psi_i\rangle^{A'B'}|i\rangle^E$, which is without loss of generality as we may always decompose a bipartite entangled state into conditional states [40] where note that $|\psi_i\rangle^{A'B'}$ are not necessarily normalized by our form.

We now wish to consider the requirement that $\alpha_3^{A'} \perp \alpha_4^{A'}$ and $\alpha_3^{B'} \perp \alpha_4^{B'}$. Note that, by the orthonormality of $\{|i\rangle^E\}$, the marginals are

$$\begin{aligned} \alpha_3^{A'B'} &= \frac{1}{2}\sum_i \left[\left(|x_i\rangle^{A'}|y_i\rangle^{B'} + |\psi_i\rangle^{A'B'}\right)\text{h.c.}\right] \\ \alpha_4^{A'B'} &= \frac{1}{2}\sum_i \left[\left(|x_i\rangle^{A'}|y_i\rangle^{B'} - |\psi_i\rangle^{A'B'}\right)\text{h.c.}\right] , \end{aligned} \tag{B.3}$$

where h.c. denotes the adjoint state. Now, to satisfy $\alpha_3^{A'} \perp \alpha_4^{A'}$ and $\alpha_3^{B'} \perp \alpha_4^{B'}$, by linearity, one may verify from (B.3) that it must be the case that the marginals on the A' and B' of

$$\begin{aligned} |x_i\rangle^{A'}|y_i\rangle^{B'} + |\psi_i\rangle^{A'B'} &= \left(|x_i\rangle^{A'} + |x_i'\rangle^{A'}\right)|y_i\rangle + \sum_j |x_{j|i}'\rangle^{A'}|y_{j|i}^{\perp}\rangle^{B'} \\ |x_i\rangle^{A'}|y_i\rangle^{B'} - |\psi_i\rangle^{A'B'} &= \left(|x_i\rangle^{A_2} - |x_i'\rangle^{A'}\right)|y_i\rangle - \sum_j |x_{j|i}'\rangle^{A'}|y_{j|i}^{\perp}\rangle^{B'} \end{aligned}$$

must be orthogonal for each i. Here, all the $\{|y_{j|i}^{\perp}\rangle\}_j$ form an orthonormal set orthogonal to $|y_i\rangle$ which follows from decomposing the state into conditional states based on a basis that includes $|y_i\rangle$. Because of the orthonormality of the set, the requirement of orthogonality of Alice's marginals implies that $|x_{j|i}'\rangle = 0$ for all j. It follows from this simplification that the orthogonality of Bob's marginals then requires that $|x_i\rangle = \pm|x_i'\rangle$ for every i. In summary, we have

$$\begin{aligned} U|2\rangle &= \sum_i |x_i\rangle^{A'}|y_i\rangle^{B'}|i\rangle^E \\ U|3\rangle &= \sum_i (-1)^{r_i}|x_i\rangle^{A'}|y_i\rangle^{B'}|i\rangle^E, \end{aligned}$$

for some $r_i \in \{0,1\}$. But by the same argument, we must have

$$U|4\rangle = \sum_i (-1)^{s_i}|x_i\rangle^{A'}|y_i\rangle^{B'}|i\rangle^E,$$

for some $s_i \in \{0,1\}$. Then turning to states $|\varphi_7\rangle$ and $|\varphi_8\rangle$ gives

$$\begin{aligned} U|\widetilde{+}_{34}\rangle &= \frac{1}{\sqrt{2}}\sum_i \left((-1)^{s_i} + i(-1)^{r_i}\right)|x_i\rangle^{A'}|y_i\rangle^{B'}|i\rangle^E, \\ U|\widetilde{-}_{34}\rangle &= \frac{1}{\sqrt{2}}\sum_i \left((-1)^{s_i} - i(-1)^{r_i}\right)|x_i\rangle^{A'}|y_i\rangle^{B'}|i\rangle^E . \end{aligned}$$

By direct calculation, the reduced density matrices of these states are not orthogonal (in fact they are the same), and hence they cannot be locally distinguished. This proves that the ensemble of states cannot be perfectly distinguished by LOSQC if Bob does not distribute entanglement to Alice.

Let us now show that an entangling LOSQC strategy can perfectly discriminate the states. In fact, it only requires two bits of communication from Alice to Bob, and just one qubit communication from Bob to Alice!

The protocol involves Bob performing an isometry with action

$$\begin{aligned}
U|1\rangle &= |11\rangle^{A'B'} \\
U|2\rangle &= \frac{1}{\sqrt{2}}\left(|22\rangle + |33\rangle\right)^{A'B'} \\
U|3\rangle &= \frac{1}{\sqrt{2}}\left(|22\rangle - |33\rangle\right)^{A'B'} \\
U|4\rangle &= \frac{1}{\sqrt{2}}\left(|23\rangle + |32\rangle\right)^{A'B'} .
\end{aligned} \tag{B.4}$$

Then

$$\begin{aligned}
U|+_{23}\rangle &= |22\rangle, & U|-_{23}\rangle &= |33\rangle \\
U|+_{24}\rangle &= |+_{23}\rangle|+_{23}\rangle, & U|-_{24}\rangle &= |-_{23}\rangle|-_{23}\rangle \\
U|\widetilde{+}_{34}\rangle &= |\widetilde{+}_{23}\rangle|\widetilde{+}_{23}\rangle, & U|\widetilde{-}_{34}\rangle &= |\widetilde{-}_{23}\rangle|\widetilde{-}_{23}\rangle.
\end{aligned}$$

Hence, the correct pairwise orthogonality is achieved. Moreover, the local states for $U|1\rangle, U|2\rangle$ are $|1\rangle\langle 1|$ and $\frac{1}{2}[|2\rangle\langle 2| + |3\rangle\langle 3|]$, so these are also pairwise orthogonal. Thus, the states can be perfectly discriminated. □

Appendix C. Uncertainty relation

We begin with the derivation of the uncertainty relation. We prove the more general form and then provide sufficient details to see how to obtain lemma 1 as a special case of the method.

Theorem 7. *Let $\{|\gamma\rangle_i^{AB}\}_{i\in\mathcal{I}}$ be a set of (possibly unnormalized) vectors. Let*

$$|\gamma_{\boldsymbol{\alpha}}\rangle^{AB} := \sum_i \alpha_i |\gamma_i\rangle^{AB} \quad |\gamma_{\boldsymbol{\beta}}\rangle^{AB} := \sum_i \beta_i |\gamma_i\rangle^{AB} .$$

Then,

$$\begin{aligned}
D_{\mathrm{tr}}\left(\gamma^B_{\boldsymbol{\alpha}}, \gamma^B_{\boldsymbol{\beta}}\right) \leqslant & \min_{\sigma\in\mathcal{S}(|\mathcal{I}|)} \sum_i D_{\mathrm{tr}}\left(\mathbf{p}(i)\gamma_i^B, \mathbf{q}(\sigma(i))\gamma^B_{\sigma(i)}\right) + \sum_i \sum_{j\neq i} |z_{ij}| F\left(\gamma_i^A, \gamma_j^A\right) \\
\leqslant & D_{\mathrm{tr}}(\mathbf{p}, \mathbf{q}) + \sum_i \sum_{j\neq i} |z_{ij}| F\left(\gamma_i^A, \gamma_j^A\right)
\end{aligned}$$

where σ is a permutation on $|\mathcal{I}|$ elements, $\mathbf{p}(i) := |\alpha_i|^2$, $\mathbf{q}(i) := |\beta_i|^2$, and for every $(i, j \neq i)$, $z_{ij} := \alpha_i\alpha_j^* - \beta_i\beta_j^*$.

Proof. By direct calculation,

$$\gamma_{\boldsymbol{\alpha}} = \sum_i |\alpha_i|^2 |\gamma_i\rangle\langle\gamma_i| + \sum_{i,j\neq i} r^{\alpha}_{ij}\left[e^{-i\phi^{\alpha}_{ij}}|\gamma_i\rangle\langle\gamma_j| + e^{i\phi^{\alpha}_{ij}}|\gamma_j\rangle\langle\gamma_i|\right] ,$$

where for every (i,j) $r^{\alpha}_{ij} := |\alpha_i\alpha_j^*|$ and $\varphi^{\alpha}_{ij} := \mathrm{atan2}(\mathrm{Im}(\alpha_i\alpha_j^*), \mathrm{Re}(\alpha_i\alpha_j^*))$. The same calculation holds for $\gamma_{\boldsymbol{\beta}}$.

For every i, let $z_i := |\alpha_i|^2 - |\beta_i|^2$. For every $(i, j \neq i)$, let $z_{ij} := r^{\alpha}_{ij} e^{-i\phi^{\alpha}_{ij}} - r^{\beta}_{ij} e^{-i\phi^{\beta}_{ij}}$. Therefore,

$$\begin{aligned}
&\left\|\gamma^B_{\boldsymbol{\alpha}} - \gamma^B_{\boldsymbol{\beta}}\right\|_1 \\
&\quad = \left\|\mathrm{Tr}_A\left[\gamma^{AB}_{\boldsymbol{\alpha}} - \gamma^{AB}_{\boldsymbol{\beta}}\right]\right\|_1 \\
&\quad = \left\|\sum_i z_i \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right] + \sum_i\sum_{j\neq i}\mathrm{Tr}_A\left[z_{ij}|\gamma_i\rangle\langle\gamma_j| - z^*_{ij}|\gamma_j\rangle\langle\gamma_i|\right]\right\|_1 \\
&\quad \leqslant \left\|\sum_i z_i \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right]\right\|_1 + \sum_i\sum_{j\neq i}|z_{ij}|\left\|\mathrm{Tr}_A\left[|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right]\right\|_1 ,
\end{aligned}$$

where the inequality is the triangle inequality and we have defined $|\widetilde{\gamma}^j_i\rangle := e^{-i\delta\phi_{ij}}|\gamma_i\rangle$ and $\delta\phi_{ij} := \mathrm{atan2}(\mathrm{Im}(z_{ij}), \mathrm{Re}(z_{ij}))$.

To bound the first term, note that we can pick any permutation $\sigma \in \mathcal{S}(|\mathcal{I}|)$ to obtain the following

$$\begin{aligned}
&\left\|\sum_i z_i \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right]\right\|_1 \\
&\quad = \left\|\sum_i |\alpha_i|^2 \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right] - \sum_i |\beta_i|^2 \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right]\right\|_1 \\
&\quad = \left\|\sum_i |\alpha_i|^2 \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right] - \sum_i |\beta_{\sigma(i)}|^2 \mathrm{Tr}_A\left[|\gamma_{\sigma(i)}\rangle\langle\gamma_{\sigma(i)}|\right]\right\|_1 \\
&\quad = \left\|\sum_i \mathbf{p}(i)\, \mathrm{Tr}_A\left[|\gamma_i\rangle\langle\gamma_i|\right] - \sum_i \mathbf{q}(\sigma(i))\, \mathrm{Tr}_A\left[|\gamma_{\sigma(i)}\rangle\langle\gamma_{\sigma(i)}|\right]\right\|_1 \\
&\quad \leqslant \sum_i \|\mathbf{p}(i)\, \gamma_i^B - \mathbf{q}(\sigma(i))\, \gamma_{\sigma(i)}^B\|_1 ,
\end{aligned}$$

where the first equality is definition of z_i, the second is that the second sum is invariant under the permutation on the indices, the third equality is definition of $\mathbf{p}, \mathbf{q}$, and the inequality is triangle inequality. As this held for arbitrary permutation, we can minimize over the permutation.

We now need to handle the cross terms. Define $P^{ij}_{\pm}$ be the projector onto the ± eigenspace of $\mathrm{Tr}_A\left[|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right]$. Then by definition of trace norm,

$$\left\|\mathrm{Tr}_A\left[|\widetilde{\gamma}^i_j\rangle\langle\gamma_i| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right]\right\|_1 = \mathrm{Tr}\left[\left(\mathbb{1}_A \otimes P^{ij}_+ - P^{ij}_-\right)\left(|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right)\right].$$

Now,

$$\begin{aligned}
&F\left(\gamma_i^A, \gamma_j^A\right) \\
&\quad = F\left(\widetilde{\gamma}_i^{j,A}, \gamma_j^A\right) \\
&\quad = \max_U \left|\mathrm{Tr}\left[(\mathbb{1} \otimes U)\, |\widetilde{\gamma}^j_i\rangle\langle\gamma_j|^{AB}\right]\right| \\
&\quad = \frac{1}{2}\left(\max_U \left|\mathrm{Tr}\left[(\mathbb{1} \otimes U)\left(|\widetilde{\gamma}^j_i\rangle\langle\gamma_j|\right)\right]\right| + \max_U \left|\mathrm{Tr}\left[(\mathbb{1} \otimes U)\left(|\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right)\right]\right|\right) \\
&\quad \geqslant \frac{1}{2}\left(\max_U \left|\mathrm{Tr}\left[(\mathbb{1} \otimes U)\left(|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right)\right]\right|\right) ,
\end{aligned}$$

where the first equality is noting $\gamma_i = |\gamma_i\rangle\langle\gamma_i| = |\widetilde{\gamma}^j_i\rangle\langle\widetilde{\gamma}^j_i|$ and the second is Uhlmann's theorem.

Choosing $U = P^{ij}_+ - P^{ij}_- + (\mathbb{1}^A - P^{ij}_+ - P^{ij}_-)$, we have

$$\begin{aligned}
F\left(\gamma_i^A, \gamma_j^A\right) &\geqslant \frac{1}{2}\left(\max_U \left|\mathrm{Tr}\left[(\mathbb{1} \otimes U)\left(|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right)\right]\right|\right) \\
&\geqslant \frac{1}{2}\mathrm{Tr}\left[\mathbb{1} \otimes \left(P^{ij}_+ - P^{ij}_-\right)\left(|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right)\right] \\
&= \frac{1}{2}\left\|\mathrm{Tr}_A\left[|\widetilde{\gamma}^j_i\rangle\langle\gamma_j| + |\gamma_j\rangle\langle\widetilde{\gamma}^j_i|\right]\right\| .
\end{aligned}$$

Reordering gets us

$$\left\|\gamma^B_{\boldsymbol{\alpha}} - \gamma^B_{\boldsymbol{\beta}}\right\|_1 \leqslant \min_{\sigma \in \mathcal{S}(|\mathcal{I}|)} \sum_i \|\mathbf{p}(i)\, \gamma_i^B - \mathbf{q}(i)\, \gamma_{\sigma(i)}^B\|_1 + 2\sum_i \sum_{j \neq i} |z_{ij}| F\left(\gamma_i^A, \gamma_j^A\right) .$$

Dividing by two gets us the trace distance and fidelity bound. □

To obtain the special case in the main text (lemma 1), the proof is largely the same, but we have more structure. Namely, there is only one z_{ij} term, which is $z_1 := \frac{1}{2}(\sin(\theta)e^{-i\phi} - \sin(\omega)e^{-i\phi'})$ and the bound on 'the first term' becomes quite simple in terms of a single scalar, which is $z_2 := \frac{1}{2}(\cos(\theta) - \cos(\omega))$. For clarity, we provide the calculations. By direct calculation, one obtains

$$\begin{aligned}
\gamma_\theta &= \cos^2(\theta/2)\, |\gamma_0\rangle\langle\gamma_0| + \sin^2(\theta/2)\, |\gamma_1\rangle\langle\gamma_1| + \sin(\theta)/2\left[e^{-i\phi}|\gamma_0\rangle\langle\gamma_1| + e^{i\phi}|\gamma_1\rangle\langle\gamma_0|\right] \\
\gamma_\omega &= \cos^2(\omega/2)\, |\gamma_0\rangle\langle\gamma_0| + \sin^2(\omega/2)\, |\gamma_1\rangle\langle\gamma_1| + \sin(\omega)/2\left[e^{-i\phi'}|\gamma_0\rangle\langle\gamma_1| + e^{i\phi'}|\gamma_1\rangle\langle\gamma_0|\right] .
\end{aligned}$$

Starting from linearity,

$$
\begin{aligned}
&\|\gamma^B_\theta - \gamma^B_\omega\|_1 \\
&\quad = \Big\|\mathrm{Tr}_A\Big[\,\{\cos^2(\theta/2) - \cos^2(\omega/2)\}\,|\gamma_0\rangle\langle\gamma_0| + \{\sin^2(\theta/2) - \sin^2(\omega/2)\}\,|\gamma_1\rangle\langle\gamma_1| \\
&\qquad + \frac{1}{2}\{\sin(\theta)e^{-i\phi} - \sin(\omega)e^{-i\phi}\}|\gamma_0\rangle\langle\gamma_1| + \frac{1}{2}\{\sin(\theta)e^{i\phi} - \sin(\omega)e^{i\phi}\}|\gamma_1\rangle\langle\gamma_0|\Big]\Big\|_1 \\
&\quad = \Big\|\mathrm{Tr}_A\Big[z_2|\gamma_0\rangle\langle\gamma_0| - z_2|\gamma_1\rangle\langle\gamma_1| + z_1|\gamma_0\rangle\langle\gamma_1| + z_1^*|\gamma_1\rangle\langle\gamma_0|\Big]\Big\|_1 \\
&\quad \leqslant |z_2|\Big\|\mathrm{Tr}_A\Big[|\gamma_0\rangle\langle\gamma_0| - |\gamma_1\rangle\langle\gamma_1|\Big]\Big\|_1 + \Big\|\mathrm{Tr}_A\Big[z_1|\gamma_0\rangle\langle\gamma_1| + z_1^*|\gamma_1\rangle\langle\gamma_0|\Big]\Big\|_1 \\
&\quad = |z_2|\Big\|\mathrm{Tr}_A\Big[|\gamma_0\rangle\langle\gamma_0| - |\gamma_1\rangle\langle\gamma_1|\Big]\Big\|_1 + |z_1|\Big\|\mathrm{Tr}_A\Big[|\widetilde{\gamma}_0\rangle\langle\gamma_1| + |\gamma_1\rangle\langle\widetilde{\gamma}_0|\Big]\Big\|_1,
\end{aligned}
$$

where the second equality is we have used trigonometric identities and our definitions of z_1, z_2, the inequality is triangle inequality, and the final equality uses $z_1 := |z_2|e^{-i\overline{\phi}}$ and $|\widetilde{\gamma}_0\rangle := e^{-i\overline{\phi}}|\gamma_0\rangle$. The rest of the proof is identical to the main theorem proof.

Appendix D. Reduction of LOSQC to LOSCC for qubit-qudit systems

In this section we prove theorem 3. This is established in two steps. The first is to reduce the type of ensemble that could separate LOSQC and LOSCC in $\mathbb{C}^2 \otimes \mathbb{C}^d$ to be of the form $\mathcal{S}_\Theta$ where $\Theta = 2$ and each set is a set of mutually orthogonal pure states. The second step is to show that LOSQC implies an LOSCC strategy for any such ensemble, which is effectively a corollary of proposition 3.

First we prove the reduction.

Lemma 3. *If there is an orthogonal product set in $\mathbb{C}^2 \otimes \mathbb{C}^d$ that separates LOSQC and LOSCC in the zero-error case, then there exists a set that separates LOSQC and LOSCC of the form*

$$
\left\{|0\rangle^A|b^0_i\rangle\right\}_{i\in\mathcal{K}^0} \cup \left\{|1\rangle^A|b^1_j\rangle\right\}_{j\in\mathcal{K}^1}, \tag{D.1}
$$

where for each $j \in \{0,1\}$, $|\mathcal{K}^j| \leqslant d$ and $\{|b^j_z\rangle\}_{z\in\mathcal{K}^j}$ is a set of orthonormal vectors.

Proof. We start by considering an arbitrary globally orthogonal product set $\mathcal{S} := \{|a_k\rangle^A|b_k\rangle\}$. We define the set of Alice's (resp. Bob's) possible states as $S_A := \{|a_k\rangle\}$ (resp. $S_B := \{|b_k\rangle\}$. If Alice's possible states do not contain two mutually orthogonal states, then Bob has to discriminate all the states. This means there are at most d states on Bob's side and they are mutually orthogonal, and thus an LOSCC strategy exists (Bob just discriminates them locally). Thus, if there is a separation between LOSQC and LOSCC in $\mathbb{C}^2 \otimes \mathbb{C}^d$, then Alice's possible states must contain two mutually orthogonal states.

We now consider the case where Alice has more than two states. Consider Alice's set of states contains two mutually orthogonal states, which up to local unitary are $|0\rangle, |1\rangle$, and some third state $|\varphi\rangle \notin \{|0\rangle, |1\rangle\}$. Then consider $S^0_B := \{|b_k\rangle : |a_k\rangle = |0\rangle\}$ and S^1_B, S^φ_B defined similarly. As $|\varphi\rangle$ overlaps with both $|0\rangle$ and $|1\rangle$, the states in S^φ_B must be each orthogonal to all states in S^0_B and all states in S^1_B for the set of states to be globally orthogonal. Thus, $\mathrm{span}(S^\varphi_B)$ defines a subspace that is orthogonal to $\mathrm{span}(S^0_B \cup S^1_B)$. Furthermore, if $|\varphi^\perp\rangle$ such that $\langle\varphi^\perp||\varphi\rangle = 0$, then $|\varphi^\perp\rangle \notin \{|0\rangle, |1\rangle\}$ but overlaps with both states, because we have a qubit space on Alice's side. Thus, $\mathrm{span}(S^{\varphi^\perp}_B)$ is also a subspace that is orthogonal to $\mathrm{span}(S^0_B \cup S^1_B)$. Thus, Bob can apply a projector to separate $S^0_B \cup S^1_B$ from $S^\varphi_B \cup S^{\varphi^\perp}_B$ prior to communication, where we may take $S^{\varphi^\perp}_B$ to be trivial if $|\varphi^\perp\rangle$ is not relevant. Applying this argument iteratively, we may conclude if Alice has pairs of orthogonal states, $\{|0\rangle, |1\rangle\}$, $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, etc each pair results in its own subspace on Bob's side that Bob can determine prior to communication. Note that if $\mathrm{span}(S^\varphi_B) \cap \mathrm{span}(S^{\varphi^\perp}_B) = \emptyset$, then Bob can determine the state locally for states $|a_k\rangle \in \{|\varphi\rangle, |\varphi^\perp\rangle\}$. Thus we can remove any such pair. In total, we have reduced the existence of a separation in this setting to the existence of a separating ensemble of the form where Alice has sets of orthogonal pairs, $\{|0\rangle, |1\rangle\}$, $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, etc where for each orthogonal pair on Alice's side, there are states on Bob's corresponding set that overlap, e.g. there exists $|b\rangle \in S^0_B, |b'\rangle \in S^1_B, |b''\rangle \in S^\varphi_b, |b'''\rangle \in S^{\varphi^\perp}_B$ such that $\langle b||b'\rangle \neq 0$ and $\langle b''||b'''\rangle \neq 0$. This implies that Alice must broadcast the orthogonality of each pair $\{|0\rangle, |1\rangle\}$, $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, etc. However, the uncertainty relation (lemma 1) shows that Alice cannot broadcast the orthogonality of more than one such pair, so there cannot be more than one pair.

Combining everything we have shown, if there is a separating ensemble $\mathcal{S}$ in $\mathbb{C}^2 \otimes \mathbb{C}^d$, then up to local unitaries, $|a_k\rangle \in \{|0\rangle, |1\rangle\}$ for all k. We then may define $S^0_B := \{|b_k\rangle : |a_k\rangle = |0\rangle\}$ and similarly for S^1_B. This is the structure of the ensemble in (D.1). This completes the proof. □

Lemma 4. *If a globally orthogonal product set of the form*

$$\left\{|0\rangle^A|b_i^0\rangle\right\}_{i\in\mathcal{K}^0}\cup\left\{|1\rangle^A|b_j^1\rangle\right\}_{j\in\mathcal{K}^1}\,, \tag{D.2}$$

is perfectly LOSQC discriminable, then it is also perfectly LOSCC discriminable.

Proof. Assume that the ensemble is perfectly discriminable under LOSQC. As it is perfectly discriminable under LOSQC, it does not matter what the distribution over the set of states is, so we may assume that it is equiprobable. Moreover, as Alice's input is classical, without loss of generality, she just copies it. Thus, without loss of generality, is that Bob applies a broadcast channel $\mathcal{E}^{B\to A'B'}$ sending the A' space to Alice and keeping the B' space for himself and then both Alice and Bob receive the value 0 or 1 that Alice copied. In other words, we have reduced any LOSQC strategy for (D.2) to an orthogonal broadcasting strategy for $\mathcal{S}_\Theta=\{\rho_{i|0}:=|b_i^0\rangle\}_{i\in\mathcal{K}^0}\cup\{\rho_{j|1}:=|b_j^1\rangle\}_{j\in\mathcal{K}^1}$ (Recall figure 1 and the definition of orthogonality broadcasting). Then, as $|\Theta|=2$ and we may assume the inputs are equiprobable, by propositions 2 and 3, we know there exists a fully classical broadcasting map $\mathcal{E}^{B\to XY}$ that achieves the same winning probability. As our assumption is the winning probability is unity and $\mathcal{E}^{B\to XY}$ defines a measurement, there is a perfect LOSCC strategy. □

Proof of theorem 3. By lemma 3, if there was an LOSQC but not LOSCC discriminable ensemble, it would be of the form given in (D.1). By lemma 4, if an ensemble of this form is LOSQC discriminable, then it is LOSCC discriminable. Thus, there cannot exist an LOSQC but not LOSCC discriminable ensemble in $\mathbb{C}^2\otimes\mathbb{C}^d$. Finally, to get the form in the theorem, one may add back any states that are locally determinable on Bob's side. □

Appendix E. LOSQC error bounds

To establish theorem 4, we need the following lemma.

Lemma 5. *If* $0\leqslant W,X,Y,Z\leqslant\mathbb{1}$, *then*

$$\|W\otimes X-Y\otimes Z\|_1\leqslant\|W-Y\|_1+\|X-Z\|_1. \tag{E.1}$$

Proof. Let $-\mathbb{1}\leqslant\tau\leqslant\mathbb{1}$ be such that

$$\begin{aligned}&\|W\otimes X-Y\otimes Z\|_1\\&\quad=\mathrm{Tr}\left[\tau\left(W\otimes X-Y\otimes Z\right)\right]\\&\quad=\mathrm{Tr}\left[\tau\left(W\otimes\frac{X+Z}{2}-Y\otimes\frac{X+Z}{2}+\frac{W+Y}{2}\otimes X-\frac{W+Y}{2}\otimes Z\right)\right]\\&\quad\leqslant\|W-Y\|_1+\|X-Z\|_1,\end{aligned}$$

since $-\mathbb{1}\leqslant\mathrm{Tr}_B\left[\tau^{AB}\left(\mathbb{1}\otimes\frac{X+Z}{2}\right)\right]\leqslant\mathbb{1}$ and $-\mathbb{1}\leqslant\mathrm{Tr}_A\left[\tau^{AB}\left(\frac{W+Y}{2}\otimes\mathbb{1}\right)\right]\leqslant\mathbb{1}$. □

Proof of theorem 4. We assume that Alice and Bob apply local isometries $U^{A\to AB'}$ and $V^{B\to A'B}$, respectively, on their given states. We define $|\alpha_k\rangle:=U|a_k\rangle$ and $|\beta_k\rangle:=V|b_k\rangle$. The simultaneous communication occurs and Alice holds systems AA' while Bob holds systems BB'. The four possible states after the isometries have the form

$$\begin{aligned}U\otimes V|\psi_0\rangle^{AB}&=|\alpha_0\rangle^{AB'}|\beta_0\rangle^{A'B}\\U\otimes V|\psi_1\rangle^{AB}&=|\alpha_1\rangle^{AB'}|\beta_1\rangle^{A'B}\\U\otimes V|\psi_\theta\rangle^{AB}&=|\alpha_2\rangle^{AB'}|\beta_\theta\rangle^{A'B}\\U\otimes V|\psi_\omega\rangle^{AB}&=|\alpha_3\rangle^{AB'}|\beta_\omega\rangle^{A'B},\end{aligned}$$

where $|\beta_\theta\rangle^{A'B}=\cos(\theta/2)|\beta_0\rangle+\sin(\theta/2)e^{i\phi}|\beta_1\rangle$ and $|\beta_\omega\rangle^{A'B}=\cos(\omega/2)|\beta_0\rangle+\cos(\omega/2)e^{i\phi'}|\beta_1\rangle$.

After the communication, POVMs $\{P_k\}^{AA'}$ and $\{Q_k\}^{BB'}$ are performed by Alice and Bob, respectively. The overall (unnormalized) success probability is given by

$$P_S:=\sum_k\mathrm{Tr}\left[\left(P_k^{AA'}\otimes Q_k^{BB'}\right)\left(U^{AB'}\otimes V^{BA'}\right)\psi_k^{AB}\left(U^{AB'}\otimes V^{BA'}\right)^\dagger\right].$$

The completion relation demands that $\sum_k P_k=\mathbb{1}^{AA'}$ and $\sum_k Q_k=\mathbb{1}^{BB'}$. Suppose that

$$\mathrm{Tr}\left[\left(P_k^{AA'}\otimes Q_k^{BB'}\right)\left(\alpha_k^{AB'}\otimes\beta_k^{A'B}\right)\right]\geqslant1-\epsilon\qquad\forall k.$$

From this we obtain constraints on Alice and Bob's POVM elements:

$$\mathrm{Tr}\left[P_k\left(\alpha_k^A \otimes \beta_k^{A'}\right)\right] \geqslant 1-\epsilon \tag{E.2}$$

$$\mathrm{Tr}\left[Q_k\left(\alpha_k^{B'} \otimes \beta_k^{B}\right)\right] \geqslant 1-\epsilon. \tag{E.3}$$

Since $P_k \leqslant \mathbb{1} - P_j$ and $Q_k \leqslant \mathbb{1} - Q_j$ for all $j \neq k$, we use the previous equations to obtain

$$-\mathrm{Tr}\left[P_k\left(\alpha_j^A \otimes \beta_j^{A'}\right)\right] > -\epsilon \tag{E.4}$$

$$-\mathrm{Tr}\left[Q_k\left(\alpha_j^{B'} \otimes \beta_j^{B}\right)\right] > -\epsilon. \tag{E.5}$$

Adding equations (E.4) and (E.5) to equations (E.2) and (E.3) yields

$$\begin{aligned}
1-2\epsilon &< \mathrm{Tr}\left[P_k\left(\alpha_k^A \otimes \beta_k^{A'} - \alpha_j^A \otimes \beta_j^{A'}\right)\right] \\
&< \frac{1}{2}\left\|\alpha_k^A \otimes \beta_k^{A'} - \alpha_j^A \otimes \beta_j^{A'}\right\|_1 \\
&\leqslant \sqrt{1 - F\left(\alpha_k^A, \alpha_j^A\right)^2 F\left(\beta_k^{A'}, \beta_j^{A'}\right)^2} \qquad \text{(E.6)} \\
1-2\epsilon &< \mathrm{Tr}\left[Q_k\left(\alpha_k^{B'} \otimes \beta_k^{B} - \alpha_j^{B'} \otimes \beta_j^{B}\right)\right] \\
&< \frac{1}{2}\left\|\alpha_k^{B'} \otimes \beta_k^{B} - \alpha_j^{B'} \otimes \beta_j^{B}\right\|_1 \\
&\leqslant \sqrt{1 - F\left(\alpha_k^{B'}, \alpha_j^{B'}\right)^2 F\left(\beta_k^{B}, \beta_j^{B}\right)^2}. \qquad \text{(E.7)}
\end{aligned}$$

This says that the isometries U and V must split the states $|a_k\rangle|b_k\rangle$ and $|a_j\rangle|b_j\rangle$ into parts that are (roughly) mutually orthogonal for both parties, for all pairs $j \neq k$.

Applying equation (E.6) on the first two states, $|\alpha_0\rangle|\beta_0\rangle, |\alpha_1\rangle|\beta_1\rangle$, yields

$$\begin{aligned}
1-2\epsilon &\leqslant \sqrt{1 - F\left(\alpha_0^A, \alpha_1^A\right)^2 F\left(\beta_0^{A'}, \beta_1^{A'}\right)^2} \\
&\leqslant \sqrt{1 - |\langle\alpha_0|\alpha_1\rangle|^2 F\left(\beta_0^{A'}, \beta_1^{A'}\right)^2} \\
&= \sqrt{1 - |\langle a_0|a_1\rangle|^2 F\left(\beta_0^{A'}, \beta_1^{A'}\right)^2}\,,
\end{aligned}$$

which under re-ordering means,

$$\Rightarrow \qquad F\left(\beta_0^{A'}, \beta_1^{A'}\right) \leqslant \frac{2\sqrt{\epsilon(1-\epsilon)}}{|\langle a_0|a_1\rangle|^2} =: \delta. \tag{E.8}$$

Applying (11) of lemma 1 multiplied by two,

$$\begin{aligned}
&\frac{4|x|\sqrt{\varepsilon(1-\varepsilon)}}{|\langle a_0|a_1\rangle|^2} \\
&> \|\beta_\theta^B - \beta_\omega^B\|_1 - |w|\|\beta_0^B - \beta_1^B\|_1 \\
&\geqslant \|\alpha_2^{B'} \otimes \beta_\theta^B - \alpha_3^{B'} \otimes \beta_\omega^B\|_1 - \|\alpha_2^{B'} - \alpha_3^{B'}\|_1 - |w|\|\beta_0^B - \beta_1^B\|_1\,, \qquad \text{(E.9)}
\end{aligned}$$

where the second inequality is by lemma 5, $w = \frac{1}{2}(\cos(\theta) - \cos(\omega))$, and $x = \frac{1}{2}(\sin(\theta)e^{-i\phi} - \sin(\omega)e^{-i\phi'})$. Note that $\langle a_2|a_3\rangle = \langle\alpha_2|\alpha_3\rangle$ and $\|\alpha_2^{B'} - \alpha_3^{B'}\|_1 \leqslant 2\sqrt{1 - |\langle\alpha_2|\alpha_3\rangle|^2}$ by Fuchs-van de Graaf inequality, so $\|\alpha_2^{B'} - \alpha_3^{B'}\|_1 \leqslant \sqrt{1 - |\langle a_2|a_3\rangle|^2}$ and similarly $\|\beta_0^B - \beta_1^B\|_1 \leqslant 2\sqrt{1 - |\langle b_0||b_1\rangle|^2}$. Then the inequality given in (E.9) can be relaxed to

$$\frac{4|x|\sqrt{\varepsilon(1-\varepsilon)}}{|\langle a_0|a_1\rangle|^2} + 2\left[\sqrt{1 - |\langle a_2|a_3\rangle|^2} + |w|\sqrt{1 - |\langle b_0||b_1\rangle|^2}\right] \geqslant \|\alpha_2^{B'} \otimes \beta_+^B - \alpha_3^{B'} \otimes \beta_-^B\|_1.$$

We require $1 - 2\varepsilon < \frac{1}{2}\|\alpha_2^{B'} \otimes \beta_+^B - \alpha_3^{B'} \otimes \beta_-^B\|_1$. So in total, we need

$$\frac{2|x|\sqrt{\varepsilon(1-\varepsilon)}}{|\langle a_0|a_1\rangle|^2} + \sqrt{1 - |\langle a_2|a_3\rangle|^2} + |w|\sqrt{1 - |\langle b_0|b_1\rangle|^2} > 1 - 2\varepsilon.$$

□

E.1. Semidefinite program LOSQC error bounds

The rest of the proofs follow roughly the same idea and tools. We therefore first summarize the proof idea and collect the relevant tools. First, as noted in the main text, one can always upper bound LOSQC success probability by what may be viewed as a generalization of the approximate orthogonality broadcasting measure in the main text, (7). To see this, consider Alice and Bob are supplied states $\mathcal{S} = \{|\psi_k\rangle := |a_k\rangle^A|b_k\rangle^B\}_{k\in\mathcal{K}}$ according to some distribution p over $\mathcal{K}$. For any fixed choices of broadcasting isometries[9] U, V, we define $|\alpha_k\rangle^{AB'} := U|a_k\rangle$, $|\beta_k\rangle^{A'B} := V|b_k\rangle$. Then for a fixed choice of U, V, the optimal strategy is

$$\begin{aligned}\Pr_{\text{LOSQC}}[\mathcal{S}_\Theta|U,V] &= \max_{\{\pi_i^{AA'}\},\{\tau_i^{BB'}\}} \sum_i p(i)\,\mathrm{Tr}\left[\pi_i^\theta\otimes\tau_i^\theta U\otimes V\psi_i(U\otimes V)^\dagger\right] \\ &\leqslant \min_{P\in\{A,B\}} \max_{\{\gamma_i^{PP'}\}} \sum_i p(i)\,\mathrm{Tr}\left[\gamma_i^{PP'}\alpha_i\otimes\beta_i\right] ,\end{aligned} \tag{E.10}$$

where each maximization is over choices of POVM and the inequality uses that the probability both parties is correct is limited by the worse of the two parties.

Next, when states are sufficiently equiprobable for it to apply, one may upper bound $\sum_i \frac{1}{2}\mathrm{Tr}[\gamma_i^{PP'}\alpha_i\otimes\beta_i]$ in terms of distinguishing states pairwise as is necessary to apply the uncertainty relation. For example,

$$\begin{aligned}&\sum_{i\in\{1,2,3,4\}}\frac{1}{2}\mathrm{Tr}\left[\gamma_i^{PP'}\alpha_i\otimes\beta_i\right] \\ &\leqslant \frac{1}{2}\left\{\mathrm{Tr}\left[\gamma_1^{PP'}\alpha_1\otimes\beta_1\right]+\mathrm{Tr}\left[\left(\mathbb{1}-\gamma_1^{PP'}\right)\alpha_2\otimes\beta_2\right]\right\} \\ &\quad+\frac{1}{2}\left\{\mathrm{Tr}\left[\gamma_3^{PP'}\alpha_3\otimes\beta_3\right]+\mathrm{Tr}\left[\left(\mathbb{1}-\gamma_4^{PP'}\right)\alpha_4\otimes\beta_4\right]\right\} \\ &\leqslant \max_{0\leqslant\pi\leqslant 1}\frac{1}{2}\left\{\mathrm{Tr}\left[\pi\alpha_1\otimes\beta_1\right]+\mathrm{Tr}\left[(\mathbb{1}-\pi)\alpha_2\otimes\beta_2\right]\right\} \\ &\quad+\max_{0\leqslant\tau\leqslant 1}\frac{1}{2}\left\{\mathrm{Tr}\left[\tau\alpha_3\otimes\beta_3\right]+\mathrm{Tr}\left[(\mathbb{1}-\tau)\alpha_4\otimes\beta_4\right]\right\} \\ &= 1/2\left(1+D_{\mathrm{tr}}(\alpha_1\otimes\beta_1,\alpha_2\otimes\beta_2)\right)+1/2\left(1+D_{\mathrm{tr}}(\alpha_3\otimes\beta_3,\alpha_4\otimes\beta_4)\right) \\ &= \frac{1}{2}+\frac{1}{2}\left[D_{\mathrm{tr}}(\alpha_1\otimes\beta_1,\alpha_2\otimes\beta_2)+D_{\mathrm{tr}}(\alpha_3\otimes\beta_3,\alpha_4\otimes\beta_4)\right] ,\end{aligned} \tag{E.11}$$

where the equality is by the Holevo-Helstrom theorem and we have omitted the P, P' superscripts for simplicity.

One may then split over the tensor product in the trace distance and convert to the guessing probability, i.e.

$$\begin{aligned}D_{\mathrm{tr}}(\alpha_\theta\otimes\beta_\theta,\alpha_\omega\otimes\beta_\omega) &\leqslant D_{\mathrm{Tr}}(\alpha_\theta,\alpha_\omega)+D_{\mathrm{Tr}}(\beta_\theta,\beta_\omega) \\ &= 2\left[p_g(\alpha_\theta,\alpha_\omega)+p_g(\beta_\theta,\beta_\omega)-1\right]\end{aligned} \tag{E.12}$$

where the first follows from dividing lemma 5 by two and the second is by the Holevo-Helstrom theorem.

At this point the remaining idea is to treat the guessing probabilities as optimization variables. One may place bounds on these guessing probabilities in terms of the uncertainty relation for guessing probability, which are constraints that are independent of the choice of U, V. Thus, one reduces the bounds to optimizing over probabilities. This will then be a semidefinite program over these probabilities in disciplined convex programming form [41] and then may be solved using CVXPY [42, 43].

Proof of proposition 4. Following the proof of theorem 4, without loss of generality,

$$\begin{aligned}U\otimes V|\psi_0\rangle^{AB} &= |\alpha_0\rangle^{AB'}|\beta_0\rangle^{A'B} \\ U\otimes V|\psi_1\rangle^{AB} &= |\alpha_1\rangle^{AB'}|\beta_1\rangle^{A'B} \\ U\otimes V|\psi_\theta\rangle^{AB} &= |\alpha_2\rangle^{AB'}|\beta_\theta\rangle^{A'B} \\ U\otimes V|\psi_\omega\rangle^{AB} &= |\alpha_3\rangle^{AB'}|\beta_\omega\rangle^{A'B},\end{aligned}$$

where $|\beta_\theta\rangle^{A'B} = \cos(\theta/2)|\beta_0\rangle + \sin(\theta/2)e^{i\phi}|\beta_1\rangle$ and $|\beta_\omega\rangle^{A'B} = \cos(\omega/2)|\beta_0\rangle + \cos(\omega/2)e^{i\phi'}|\beta_1\rangle$.

[9] The choice of isometries is without loss of generality by considering the isometric extension of the broadcasting channels.

Then, for some a given choice of U, V, starting from (E.10),

$$\min_{P\in\{A,B\}} \max_{\{\gamma_i^{PP'}\}} \sum_i p(i) \operatorname{Tr}\left[\gamma_i^{PP'} \alpha_i \otimes \beta_i\right]$$
$$\leqslant \frac{1}{2} + \min_{P\in\{A,B\}} \frac{p}{2} D_{\mathrm{tr}}(\alpha_0 \otimes \beta_0, \alpha_1 \otimes \beta_1) + \frac{1-p}{2} D_{\mathrm{tr}}(\alpha_\theta \otimes \beta_\theta, \alpha_\omega \otimes \beta_\omega) \; , \tag{E.13}$$

where the inequality uses that $p(0) = p(1) = p/2$, $p(\theta) = p(\omega) = (1-p)/2$ and a similar argument to that in (E.11). Applying (E.12) and simplifying we obtain

$$\Pr_{\mathrm{LOSQC}}[\mathcal{S}_\Theta | U, V]$$
$$\leqslant \min_{P\in\{A,B\}} p \cdot \left[p_g(\alpha_0, \alpha_1) + p_g(\beta_0, \beta_1)\right] + (1-p)\left[p_g(\alpha_\theta, \alpha_\omega) + p_g(\beta_\theta, \beta_\omega)\right] - 1 \; .$$

Thus, we have

$$\Pr_{\mathrm{LOSQC}}[\mathcal{S}_\Theta] \leqslant \max_{U,V} \min_{P\in\{A,B\}} p \cdot \left[p_g(\alpha_0, \alpha_1) + p_g(\beta_0, \beta_1)\right]$$
$$+ (1-p)\left[p_g(\alpha_\theta, \alpha_\omega) + p_g(\beta_\theta, \beta_\omega)\right] - 1 \; .$$

By data-processing, $p_g(\alpha_0, \alpha_1) \leqslant p_g(\psi_0, \psi_1), p_g(\alpha_\theta, \alpha_\omega) \leqslant p_g(\psi_\theta, \psi_\omega)$, which are determinable constants using Holevo-Helstrom. Moreover, we may apply corollary 2 to $\beta_\theta, \beta_\omega$ in terms of β_0, β_1 for any choice of U, V. Therefore, defining $r_0 := p_g(\beta_0^{A'}, \beta_1^{A'})$, $r_1 := p_g(\beta_0^B, \beta_1^B)$ and similarly for s_0, s_1 in terms of Bob completes the derivation of the optimization program.

To see the optimization problem is convex, note that the constraints are concave in the optimization variables and the objective function includes the pointwise minimization of linear functions, i.e. it is a concave objective function. As the problem is a maximization, we may conclude it is a convex optimization program.

To see the unity conditions, note that $f(p, \mathcal{S}, \mathbf{x}) = 1$ if and only if $p_g(a_0, a_1) = p_g(a_3, a_4) = x_0 = x_1 = 1$. This proves the orthogonality conditions and proves s_0, s_1, r_0, r_1 must all be unity. Looking at the constraints, under everything being unity, one obtains $1 \leqslant \frac{1}{2}[|z_2| + 1] \Leftrightarrow 1 = |z_2| = |\cos(\theta) - \cos(\omega)|$, which is equivalent to the stated condition. □

Proof of theorem 5. As usual, we let $U \otimes V|\psi_i\rangle^{AB} = |\alpha_i\rangle^{AB'}|\beta_i\rangle^{A'B}$ for each i. We do not make use of the fact that one register is classical for the majority of the proof as it will simplify the presentation of the subsequent proof.

Starting from (E.10),

$$\min_{P\in\{A,B\}} \max_{\{\gamma_i^{PP'}\}} \sum_i p(i) \operatorname{Tr}\left[\gamma_i^{PP'} \alpha_i \otimes \beta_i\right]$$
$$= \min_{P\in\{A,B\}} \max_{\{\gamma_i^{PP'}\}} \left[\frac{1}{8} \sum_{i\in\{1,2,3,4\}} \operatorname{Tr}\left[\gamma_i^{PP'} \alpha_i \otimes \beta_i\right] + \frac{1}{8} \sum_{i\in\{1,5,6,7\}} \operatorname{Tr}\left[\gamma_i^{PP'} \alpha_i \otimes \beta_i\right]\right]$$
$$= \frac{1}{4} \min_{P\in\{A,B\}} \max_{\{\gamma_i^{PP'}\}} \left[\sum_{i\in\{1,2,3,4\}} \frac{1}{2}\operatorname{Tr}\left[\gamma_i^{PP'} \alpha_i \otimes \beta_i\right] + \sum_{i\in\{1,5,6,7\}} \frac{1}{2}\operatorname{Tr}\left[\gamma_i^{PP'} \alpha_i \otimes \beta_i\right]\right] ,$$

where we have used our assumption on the probabilities so that we may split distinguishing ψ_1 into each sum.

Using the bound of the form (E.11) in both cases, we obtain

$$\Pr_{\mathrm{LOSQC}}[\mathcal{S}_\Theta | U, V]$$
$$\leqslant \frac{1}{4} + \frac{1}{8} \min_{P\in\{A,B\}} \left[\sum_{i\in\{1,3,6\}} D_{\mathrm{tr}}(\alpha_i \otimes \beta_i, \alpha_{i+1} \otimes \beta_{i+1}) + D_{\mathrm{tr}}(\alpha_1 \otimes \beta_1, \alpha_5 \otimes \beta_5)\right] , \tag{E.14}$$

where we have distributed the $1/4$.

Next, introducing p_g^P to denote the guessing probability of party P with access to their portions of the state, by (E.12),

$$D_{\mathrm{tr}}(\alpha_\theta \otimes \beta_\theta, \alpha_\omega \otimes \beta_\omega) \leqslant 2\left[p_g^P(\alpha_\theta, \alpha_\omega) + p_g^P(\beta_\theta, \beta_\omega) - 1\right] ,$$

so we obtain

$$\Pr_{\text{LOSQC}}[\mathcal{S}_\Theta|U,V] \leqslant \frac{1}{4} + \frac{1}{4}\min_{P\in\{A,B\}}\Bigg[\sum_{i\in\{1,3,6\}}\left\{p_g^P(\alpha_i,\alpha_{i+1}) + p_g^P(\beta_i,\beta_{i+1})\right\} \\ + p_g^P(\alpha_1,\alpha_5) + p_g^P(\beta_1,\beta_5) - 4\Bigg]\,. \tag{E.15}$$

At this point we note that, by construction, the α_i term is always the same as the one it is being compared to, so $p_g^P(\alpha_i,\alpha_{i+1}) = 1/2 = p_g^P(\alpha_1,\alpha_5)$ for $i\in\{1,3,6\}$ a term is always $1/2$. This simplifies the objective function to

$$\Pr_{\text{LOSQC}}[\mathcal{S}_\Theta|U,V] \leqslant \frac{1}{4} + \frac{1}{4}\min_{P\in\{A,B\}}\left[\sum_{i\in\{1,3,6\}}\left\{p_g^P(\beta_i,\beta_{i+1})\right\} + p_g^P(\beta_1,\beta_5) - 2\right]\,. \tag{E.16}$$

Then to bound the optimal strategy we would optimize over the choice of U,V. However the bound is now independent of U and we may replace maximizing over V via constraints that hold from corollary 2, which apply for any choice of V. We define $p_0 := p_g^P(V|1\rangle, V|2\rangle)$, $p_1 := p_g^P(V|1+2\rangle, V|1-2\rangle)$, $p_2 := p_g^P(V|1\rangle, V|0\rangle)$, $p_3 := p_g^P(V|0+1\rangle, V|0-1\rangle)$ for $P\in\{A,B\}$. Applying lemma 1 to (E.16), we obtain $4(\Pr_{\text{LOSQC}}[\mathcal{S}] - 1/4)$ is upper bounded by

$$\begin{aligned}
&\max\ \min\left\{\sum_{i\in[3]} a_i, \sum_{i\in[3]} b_i\right\} - 2 \\
&\text{s.t. } p_0 \leqslant \frac{1}{2}\sqrt{1-(2\overline{p}_1-1)^2} + \frac{1}{2} \quad p\in\{a,b\} \\
&\qquad p_1 \leqslant \frac{1}{2}\sqrt{1-(2\overline{p}_0-1)^2} + \frac{1}{2} \quad p\in\{a,b\} \\
&\qquad p_2 \leqslant \frac{1}{2}\sqrt{1-(2\overline{p}_3-1)^2} + \frac{1}{2} \quad p\in\{a,b\} \\
&\qquad p_3 \leqslant \frac{1}{2}\sqrt{1-(2\overline{p}_2-1)^2} + \frac{1}{2} \quad p\in\{a,b\} \\
&\qquad 0 \leqslant \mathbf{a},\mathbf{b} \leqslant 1\,,
\end{aligned} \tag{E.17}$$

where $[3] = \{0,1,2,3\}$, $\overline{p}$ represents the opposite party, and in applying lemma 1 we have used $|i\pm j\rangle = \frac{1}{\sqrt{2}}|i\rangle \pm \frac{1}{\sqrt{2}}|j\rangle$ and $|i\rangle = \frac{1}{\sqrt{2}}[|i+j\rangle + |i-j\rangle]$ so that $z_1 = 1$ and $z_2 = 0$ always. Finally, we directly solve this SDP using CVXPY. □

As presented in the main text, our method is general enough to apply to the case where both Alice and Bob receive non-commuting states. Here we present a lemma that will both allow us to establish the separation in theorem 6 as well as explain why we cannot decrease the success probability of theorem 5 by adding coherence to Alice's side using our methodology.

Lemma 6. *Consider the set of globally orthogonal, fully quantum, product qutrit states*

$$\widetilde{\mathcal{S}}_{qq} = \left\{\begin{array}{cc} \multicolumn{2}{c}{|\psi_1\rangle = |1\rangle|1\rangle} \\ |\psi_2\rangle = |1-2\rangle|2\rangle & |\psi_3\rangle = |0\rangle|1+2\rangle \\ |\psi_4\rangle = |0\rangle|1-2\rangle & |\psi_5\rangle = |0+1\rangle|0\rangle \\ |\psi_6\rangle = |2\rangle|0+1\rangle & |\psi_7\rangle = |2\rangle|0-1\rangle \end{array}\right\}\,, \tag{E.18}$$

where $|\psi_1\rangle$ *occurs with probability* $1/4$ *and the rest occur with probability* $1/8$. *Then*

$$\Pr_{\text{LOSQC}}\left[\widetilde{\mathcal{S}}_{qq}\right] \leqslant 0.78033\,. \tag{E.19}$$

Proof. First, note that for all i, $|b_i\rangle$ in $\mathcal{S}_{qq}$ is the same as $|b_i\rangle$ in $\mathcal{S}_{\text{OBB84}}$ as given in (25). This means the majority of the proof is identical to the previous. In particular, we may start at (E.15). However, we now make choices on how to bound the probabilities on Alice's side that are no longer identical states. In particular, we may use data-processing to bound the guessing probability by the original state, e.g.

$$\begin{aligned}
p_g^P(W|1\rangle, W|1-2\rangle) \leqslant & p_g(|1\rangle, |1-2\rangle) \\
&= \frac{1}{2}\left(1 + \frac{1}{2}\||1\rangle\langle 1| - |1-2\rangle\langle 1-2|\|_1\right) = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) =: t\,.
\end{aligned}$$

Then we obtain

$$\begin{aligned}\sum_{i\in\{1,3,6\}} & \left\{p_g^P(\alpha_i,\alpha_{i+1})+p_g^P(\beta_i,\beta_{i+1})\right\}+p_g^P(\alpha_1,\alpha_5)+p_g^P(\beta_1,\beta_5)-4\Big] \\ &= t+p_g^P(V|1\rangle,V|2\rangle)+\frac{1}{2}+p_g^P(V|1+2\rangle,V|1-2\rangle) \\ &\quad +\frac{1}{2}+p_g^P(V|0+1\rangle,V|0-1\rangle)+t+p_g^P(V|0\rangle,V|1\rangle)-4 \\ &= p_g^P(V|1\rangle,V|2\rangle)+p_g^P(V|1+2\rangle,V|1-2\rangle) \\ &\quad +p_g^P(V|0\rangle,V|1\rangle)+p_g^P(V|0+1\rangle,V|0-1\rangle)+\frac{1}{\sqrt{2}}-2\,. \end{aligned} \tag{E.20}$$

By the same argument as in the previous proof, this ultimately results in an SDP the upper bounds $4(\Pr_{\mathrm{LOSQC}}[\mathcal{S}_{qq}]-1/4)$:

$$\begin{aligned} \max\ \min & \left\{\sum_{i\in[3]} a_i, \sum_{i\in[3]} b_i\right\}+\frac{1}{\sqrt{2}}-2 \\ \text{s.t. } p_0 &\leqslant \frac{1}{2}\sqrt{1-(2\bar{p}_1-1)^2}+\frac{1}{2} \quad p\in\{a,b\} \\ p_1 &\leqslant \frac{1}{2}\sqrt{1-(2\bar{p}_0-1)^2}+\frac{1}{2} \quad p\in\{a,b\} \\ p_2 &\leqslant \frac{1}{2}\sqrt{1-(2\bar{p}_3-1)^2}+\frac{1}{2} \quad p\in\{a,b\} \\ p_3 &\leqslant \frac{1}{2}\sqrt{1-(2\bar{p}_2-1)^2}+\frac{1}{2} \quad p\in\{a,b\} \\ 0 &\leqslant \mathbf{a},\mathbf{b}\leqslant 1\,, \end{aligned} \tag{E.21}$$

where $\bar{p}$ represents the opposite party, and in applying lemma 1 we have used $|i\pm j\rangle=\frac{1}{\sqrt{2}}|i\rangle\pm\frac{1}{\sqrt{2}}|j\rangle$ and $|i\rangle=\frac{1}{\sqrt{2}}[|i+j\rangle+|i-j\rangle]$ so that $z_1=1$ and $z_2=0$ always. Finally, this is a semidefinite program which we solved using CVXPY. □

We now use lemma 6 to prove theorem 6.

Proof of theorem 6. Note that $\mathcal{S}_{qq}$ in (29) is equivalent to $\widetilde{\mathcal{S}}_{qq}$ in (E.18) up to applying the local unitary on Alice's side defined by

$$U|0\rangle=|2\rangle \quad U|1\rangle=|1\rangle \quad U|2\rangle=|0\rangle\,.$$

Thus, we know $\Pr_{\mathrm{LOSQC}}[\mathcal{S}_{qq}]\leqslant 0.7805$ by lemma 6. It therefore suffices to prove $\Pr_{\mathrm{LOSQC}}[\mathcal{S}_{cq}]\geqslant\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)$ for $\mathcal{S}_{cq}$ given in (28). We do this by construction of an LOSCC strategy achieving this lower bound.

Consider the POVM $\{|\varphi_y\rangle\langle\varphi_y|\}_{y=1}^4$ defined by vectors

$$\begin{aligned} |\varphi_1\rangle &= \frac{1}{\sqrt{2}}\left[\cos(\pi/8)\,|1\rangle+\sin(\pi/8)\,(|0\rangle+|2\rangle)\right], \\ |\varphi_2\rangle &= \frac{1}{\sqrt{2}}\left[\cos(\pi/8)\,|1\rangle+\sin(\pi/8)\,(|0\rangle-|2\rangle)\right], \\ |\varphi_3\rangle &= \frac{1}{\sqrt{2}}\left[\sin(\pi/8)\,|1\rangle-\cos(\pi/8)\,(|0\rangle+|2\rangle)\right], \\ |\varphi_4\rangle &= \frac{1}{\sqrt{2}}\left[\sin(\pi/8)\,|1\rangle-\cos(\pi/8)\,(|0\rangle-|2\rangle)\right]. \end{aligned} \tag{E.22}$$

Our LOSCC protocol involves Alice measuring in the computational basis (obtaining outcome x) and Bob performing the above POVM (obtaining outcome y). Their guessing strategy is given by the following table:

Outcomes (x,y)	Guess	Prob. the guess is correct
$\{(1,1),(1,2)\}$	$\vert\psi_1\rangle$	$\cos^2(\pi/8)$
$\{(1,3)\}$	$\vert\psi_2\rangle$	$\cos^2(\pi/8)$
$\{(1,4)\}$	$\vert\psi_3\rangle$	$\cos^2(\pi/8)$
$\{(0,1),(0,2)\}$	$\vert\psi_4\rangle$	$\frac{1}{2}(\cos(\pi/8)+\sin(\pi/8))^2$
$\{(0,3),(0,4)\}$	$\vert\psi_5\rangle$	$\frac{1}{2}(\cos(\pi/8)+\sin(\pi/8))^2$
$\{(2,1),(2,2)\}$	$\vert\psi_6\rangle$	$\frac{1}{2}(\cos(\pi/8)+\sin(\pi/8))^2$
$\{(2,3),(2,4)\}$	$\vert\psi_7\rangle$	$\frac{1}{2}(\cos(\pi/8)+\sin(\pi/8))^2$

Noting that $\frac{1}{2}(\cos(\pi/8)+\sin(\pi/8))^2=\cos^2(\pi/8)$, using this strategy, regardless of the priors, the success probability is $\cos^2(\pi/8)=\frac{1}{2}(1+\frac{1}{\sqrt{2}})$. This proves that $P_{\mathrm{LOSQC}}(\mathcal{S}_{cq})\geqslant P_{\mathrm{LOSCC}}(\mathcal{S}_{cq})\geqslant\frac{1}{2}(1+\frac{1}{\sqrt{2}}))$. This completes the proof. □

Finally, we explain why lemma 6 shows that our methodology is too loose to amplify theorem 5 by making both parties have to do approximate broadcasting. First, note that one may obtain $\widetilde{\mathcal{S}}_{qq}$ from $\mathcal{S}_{\mathrm{OBB}}$ in (25) from first applying the unitary

$$U|0\rangle=|1\rangle\quad U|1\rangle=|0\rangle\quad U|2\rangle=|2\rangle$$

to Alice's side and then altering $U|a_2\rangle\to|1-2\rangle$, $U|a_5\rangle\to|0+1\rangle$. This is to say, up to a local unitary, we may view $\widetilde{S}_{qq}$ as a method for making $\mathcal{S}_{\mathrm{OBB}}$ coherent on both sides. Then, we see the reason this does not tighten the result in this scenario is that our bound on $p_g^P(W|1\rangle,W|1-2\rangle)>1/2$ where the latter value is what we could use in theorem 5. It is not clear how to improve this using the uncertainty relation. In particular, if one applies theorem 7 to these states in terms of $W|0\rangle,W|1\rangle,W|2\rangle$, a direct calculation shows

$$\begin{aligned}D_{\mathrm{tr}}\left((W|0\rangle)^B,(W|1\rangle)^B\right)&\leqslant\frac{1}{2}+2F\left((W|0\rangle)^A,(W|1\rangle)^A\right)\\&\leqslant\frac{1}{2}+2\sqrt{1-\left(2p_g^A\left(W|0\rangle,W|1\rangle\right)-1\right)^2}\,,\end{aligned}$$

where we used Fuchs-van de Graaf inequality and Holevo-Helstrom theorem. A direct calculation will verify this constraint is non-trivial (i.e. strictly less than unity) only when $p_g^A(W|0\rangle,W|1\rangle)\geqslant 0.984123$, but the other constraints already guarantee that it is smaller than this. This seems to be a common issue in trying to apply theorem 7 more generally.

ORCID iDs

Ian George https://orcid.org/0000-0002-2803-2421
Eric Chitambar https://orcid.org/0000-0001-6990-7821

References

[1] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3

[2] Broadbent A and Lord S 2020 Uncloneable quantum encryption via oracles *15th Conf. on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)* (Schloss Dagstuhl - Leibniz-Zentrum für Informatik) (https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.TQC.2020.4)

[3] Bennett C H and Brassard G 2014 Quantum cryptography: Public key distribution and coin tossing *Theor. Comput. Sci.* **560** 7–11

[4] Cleve R, Gottesman D and Lo H-K 1999 How to share a quantum secret *Phys. Rev. Lett.* **83** 648–51

[5] Kent A, Munro W J and Spiller T P 2011 Quantum tagging: authenticating location via quantum information and relativistic signaling constraints *Phys. Rev. A* **84** 012326

[6] Barnum H, Caves C M, Fuchs C A, Jozsa R and Schumacher B 1996 Noncommuting mixed states cannot be broadcast *Phys. Rev. Lett.* **76** 2818–21

[7] Lindblad G 1999 A general no-cloning theorem *Lett. Math. Phys.* **47** 189–96

[8] Kalev A and Hen I 2008 No-broadcasting theorem and its classical counterpart *Phys. Rev. Lett.* **100** 210502

[9] Barnum H, Barrett J, Leifer M and Wilce A 2007 Generalized no-broadcasting theorem *Phys. Rev. Lett.* **99** 240501

[10] Ballester M A, Wehner S and Winter A 2008 State discrimination with post-measurement information *IEEE Trans. Inf. Theory* **54** 4183–98

[11] Carmeli C, Heinosaari T and Toigo A 2022 Quantum guessing games with posterior information *Rep. Prog. Phys.* **85** 074001

[12] Sattath O 2023 Uncloneable cryptography *Commun. ACM* **66** 78–86

[13] Tomamichel M, Fehr S, Kaniewski J and Wehner S 2013 A monogamy-of-entanglement game with applications to device-independent quantum cryptography *New J. Phys.* **15** 103002

[14] Broadbent A and Culf E 2023 Rigidity for monogamy-of-entanglement games *14th Innovations in Theoretical Computer Science Conf. (ITCS 2023)* (Schloss Dagstuhl - Leibniz-Zentrum für Informatik) (https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2023.28)

[15] Ananth P, Kaleoglu F and Liu Q 2023 Cloning games: a general framework for unclonable primitives *Annual Int. Cryptology Conf.* (Springer) pp 66–98

[16] Goyal V, Malavolta G and Raizes J 2024 Unclonable commitments and proofs *Theory of Cryptography Conf.* (Springer) pp 193–224

[17] Poremba A, Ragavan S and Vaikuntanathan V 2024 Cloning games, black holes and cryptography (arXiv:2411.04730)

[18] Escolá-Farrás L and Speelman F 2024 Lossy-and-constrained extended non-local games with applications to cryptography: Bc, qkd and qpv (arXiv:2405.13717)

[19] Allerstorfer R, Buhrman H, Speelman F and Verduyn Lunel P 2022 On the role of quantum communication and loss in attacks on quantum position verification (arXiv:2208.04341)

[20] Deutsch D 1983 Uncertainty in quantum measurements *Phys. Rev. Lett.* **50** 631–3

[21] Renes J M and Boileau J-C 2009 Conjectured strong complementary information tradeoff *Phys. Rev. Lett.* **103** 020402

[22] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 The uncertainty principle in the presence of quantum memory *Nat. Phys.* **6** 659–62

[23] Coles P J, Berta M, Tomamichel M and Wehner S 2017 Entropic uncertainty relations and their applications *Rev. Mod. Phys.* **89** 015002

[24] Cubitt T S, Verstraete F, Dür W and Cirac J I 2003 Separable states can be used to distribute entanglement *Phys. Rev. Lett.* **91** 037902

[25] Chuan T K, Maillard J, Modi K, Paterek T, Paternostro M and Piani M 2012 Quantum discord bounds the amount of distributed entanglement *Phys. Rev. Lett.* **109** 070501

[26] Streltsov A, Kampermann H and Bruß D 2012 Quantum cost for sending entanglement *Phys. Rev. Lett.* **108** 250501

[27] Bužek V and Hillery M 1996 Quantum copying: beyond the no-cloning theorem *Phys. Rev. A* **54** 1844–52

[28] Scarani V, Iblisdir S, Gisin N and Acín A 2005 Quantum cloning *Rev. Mod. Phys.* **77** 1225–56

[29] Watrous J 2018 *The Theory of Quantum Information* (Cambridge University Press) (https://doi.org/10.1017/9781316848142)

[30] Buhrman H, Chandran N, Fehr S, Gelles R, Goyal V, Ostrovsky R and Schaffner C 2014 Position-based quantum cryptography: impossibility and constructions *SIAM J. Comput.* **43** 150–78

[31] Bennett C H, DiVincenzo D P, Mor T, Shor P W, Smolin J A and Terhal B M 1999 Unextendible product bases and bound entanglement *Phys. Rev. Lett.* **82** 5385

[32] Bennett C H, DiVincenzo D P, Fuchs C A, Mor T, Rains E, Shor P W, Smolin J A and Wootters W K 1999 Quantum nonlocality without entanglement *Phys. Rev. A* **59** 1070–91

[33] Childs A M, Leung D, Mančinska L and Ozols M 2013 A framework for bounding nonlocality of state discrimination *Commun. Math. Phys.* **323** 1121–53

[34] Ito T 2010 Polynomial-space approximation of no-signaling provers *Automata, Languages and Programming: 37th Int. Coll., ICALP 2010 (Bordeaux, France, 6–10 July 2010) Proc., Part I* vol 37 (Springer) pp 140–51

[35] Brandao F G S L and Harrow A W 2017 Quantum de Finetti theorems under local measurements with applications *Commun. Math. Phys.* **353** 469–506

[36] Fawzi O and Fermé P 2023 Multiple-access channel coding with non-signaling correlations *IEEE Trans. Inf. Theory* **70** 1693–719

[37] Palazuelos C and Vidick T 2016 Survey on nonlocal games and operator space theory *J. Math. Phys.* **57** 015220

[38] Beigi S and König R 2011 Simplified instantaneous non-local quantum computation with applications to position-based cryptography *New J. Phys.* **13** 093036

[39] Wilde M M 2013 *Quantum Information Theory* (Cambridge University Press) (https://doi.org/10.1017/CBO9781139525343)

[40] Schumacher B and Westmoreland M 2010 *Quantum Processes Systems and Information* (Cambridge University Press) (https://doi.org/10.1017/CBO9780511814006)

[41] Grant M, Boyd S and Yinyu Y 2006 Disciplined convex programming *Global Optimization: From Theory to Implementation* (Springer) pp 155–210

[42] Diamond S and Boyd S 2016 CVXPY: a Python-embedded modeling language for convex optimization *J. Mach. Learn. Res.* **17** 1–5 (available at: www.jmlr.org/papers/v17/15-408.html)

[43] Agrawal A, Verschueren R, Diamond S and Boyd S 2018 A rewriting system for convex optimization problems *J. Control Decis.* **5** 42–60