Local simultaneous state discrimination

Christian Majenz
Technical University of Denmark, Anker Engelunds Vej 1, Bygning 101A, 2800 Kongens Lyngby, Denmark

Maris Ozols and Christian Schaffner
QuSoft, University of Amsterdam, Science Park 123, 1098 XG Amsterdam, Netherlands

Mehrdad Tahmasbi[*]
University of Illinois Urbana-Champaign, Champaign, Illinois 61820, USA

(Received 12 December 2023; accepted 20 March 2024; published 14 May 2024)

Quantum state discrimination is one of the most fundamental problems in quantum information theory, with applications ranging from channel coding to metrology and cryptography. In this work, we introduce a variant of this task: local simultaneous state discrimination (LSSD). While previously studied distributed variants of state discrimination allowed some communication between the parties to come up with a joint answer, in LSSD they cannot communicate and have to simultaneously answer correctly. We illustrate by multiple examples that this problem significantly differs from single-party state discrimination, even when the states are completely classical. We show that an additional entangled resource can increase the optimal success probability in LSSD, and stronger-than-quantum no-signaling resources can allow for an even higher success probability. We also show that finding the optimal strategy in (classical) three-party LSSD is NP-hard. Furthermore, we provide an example of symmetric LSSD for which the optimal strategy is not symmetric, and prove a sufficient condition for the existence of an optimal symmetric strategy. While interesting in its own right, the LSSD problem also arises in quantum cryptography. In particular, we explore the connections between the problem of unclonable encryption and LSSD. We give an explicit cloning-indistinguishable attack that succeeds with probability $1/2 + \mu/16$ where μ is related to the largest eigenvalue of the resulting quantum ciphertext states.

DOI: 10.1103/PhysRevA.109.052217

I. INTRODUCTION

Discriminating among a known set of quantum states is a well-studied and fundamental problem in quantum information theory [1–3], with a vast range of applications ranging from cryptography [4,5] and quantum computing [6] to quantum information and metrology [7]. In this problem, a referee prepares a classical register X in a random state x, based on which they prepare a quantum register A in a fixed quantum state depending on x. The referee then sends A to Alice who tries to determine x. An intriguing extension of the problem is *distributed* state discrimination, wherein the referee prepares a bipartite state with two registers AB that are accessible to Alice and Bob, respectively. Investigating the task of distributed state discrimination is one possible avenue for understanding quantum *nonlocality*, a fundamental feature of quantum theory which has been key to charting the foundations of quantum physics (see, e.g., [8] and references therein). The most commonly considered scenario of distributed state discrimination in the context of nonlocality is when Alice and Bob are allowed to use *local operations and classical communication* (LOCC) in the discrimination process [9]. For example, any orthonormal set of product states can be prepared by local operations and discriminated by a global operation. However, when the requirement is to discriminate these states solely using local operations, even with classical communication between the parties, it generally becomes infeasible [10,11]. In the LOCC setting, the discrimination task does not become more demanding by asking Alice and Bob to answer correctly *simultaneously* since the result can be communicated between the parties. Surprisingly, the more restricted scenario where Alice and Bob can only use *local operations* (LO) without any classical communication has received only little attention in the published literature so far (see below for an overview of related work). As depicted in Fig. 1, we are particularly interested in a scenario where Alice and Bob have to *locally and simultaneously* discriminate the states (as opposed to the case when at least one of the players should succeed). We call the resulting task *local simultaneous state discrimination* (LSSD). When the states involved in LSSD are characterized by classical probabilities, the task of distinguishing them resembles the situation of winning a nonlocal game. This is because general distinguishing strategies can be articulated through a conditional distribution denoted as $P_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$. This distribution presents the likelihood that Alice and Bob, based on their respective inputs A and B, jointly produce estimations X_A and X_B. Analogous to nonlocal games, one can categorize different strategy classes contingent on the resources available in advance to Alice and Bob. Consequently, from classical LSSDs, a different category of Bell inequalities emerges, which, to the best of our

[*] Corresponding author: mehrdad.tahmasbi6@gmail.com

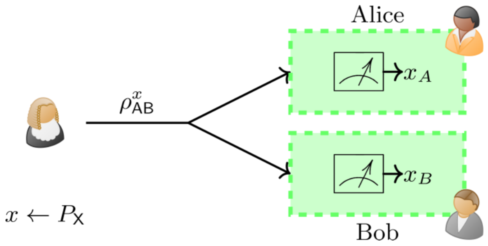


FIG. 1. LSSD setup: The referee samples x according to P_X and transmits a correlated bipartite state ρ^x_{AB} to Alice and Bob who need to simultaneously guess x based on their received state.

knowledge, has not been explored in the existing body of literature. Our primary contribution lies in the presentation of a concrete example of LSSD, in which quantum strategies exhibit an advantage over classical ones. LSSD, therefore, introduces a family of tasks joining the zoo of operational problems where the nonlocal nature of quantum correlations can provide an advantage over purely classical strategies.

While studying LSSD is interesting in its own right, a concrete motivation arises from a specific area of quantum cryptography known as *unclonable cryptography* [12]. The so-called *quantum no-cloning principle* stipulates that, in its simplest form, quantum information cannot be replicated [13]. This distinctive property of quantum information has been extensively leveraged in the design of unclonable cryptographic schemes where a certain asset (like a token, message, or functionality) is encrypted in a way that makes it impossible to copy. A general observation in the literature of unclonable cryptography is that providing formal proofs of security of these protocols is a challenging endeavor [12,14,15]. We present a rationale for the complexity of this security analysis by establishing a link between LSSD and the security of unclonable cryptography protocols. As elaborated later, the security analysis of a wide range of protocols ultimately hinges on establishing upper bounds on the optimal success probabilities of LSSDs. We demonstrate that determining the optimal probability of a multiparty LSSD is an NP-hard problem. Consequently, the precise security analysis of unclonable protocols may entail computationally intractable challenges. On the other hand, gaining a deeper understanding of LSSD could aid in advancing the security analysis of unclonable cryptography protocols.

II. NOTATION

We will denote by $\delta[\cdot]$ the indicator function that evaluates to one when its argument is true and to zero otherwise. We will use $\mathscr{X}, \mathscr{A}, \mathscr{B}$, respectively, to denote the finite sets from which the inputs to the referee, Alice, and Bob are drawn. Their joint input is described by a probability distribution P_{XAB} on $\mathscr{X} \times \mathscr{A} \times \mathscr{B}$, where the system X belongs to the referee while A and B belong to Alice and Bob, respectively. The input and output sets will often be of the form $[d] := \{0, \dots, d-1\}$, for some integer $d \geqslant 1$.

When Alice and Bob's inputs are quantum, the overall input is a classical-quantum-quantum (cqq) state ρ_{XAB} where the classical register X belongs to the referee while the quantum registers A and B belong to Alice and Bob, respectively. We will denote the finite-dimensional complex Euclidean spaces underlying these registers by $\mathcal{X} = \mathbb{C}^{\mathscr{X}}$, $\mathcal{A} = \mathbb{C}^{\mathscr{A}}$, and $\mathcal{B} = \mathbb{C}^{\mathscr{B}}$.

A *quantum state* on $\mathbb{C}^d$ is a $d \times d$ positive-semidefinite matrix of unit trace, i.e., $\rho \in \mathbb{C}^{d\times d}$ such that $\rho \succeq 0$ and $\operatorname{tr}\rho = 1$. We denote the set of all quantum states on $\mathbb{C}^d$ by $\mathrm{D}(\mathbb{C}^d)$. Operations on quantum states are described by *unitary* matrices, i.e., $U \in \mathbb{C}^{d\times d}$ such that $U^\dagger U = \mathbb{1}$ where $\mathbb{1}$ is the identity matrix. We denote the set of all unitaries on $\mathbb{C}^d$ by $\mathrm{U}(\mathbb{C}^d)$.

An n-outcome *measurement* or positive-operator-value measures (POVM) on $\mathbb{C}^d$ is a collection of n positive-semidefinite $d \times d$ matrices that sum to identity. We will denote a measurement by $M = \{M_1, \dots, M_n\}$ where $M_i \succeq 0$ and $\sum_{i=1}^n M_i = \mathbb{1}$. We denote the set of all n-outcome measurements on $\mathbb{C}^d$ by $\mathrm{M}(\mathbb{C}^d)$ (since the outcome set is always clear from the context, we do not specify it). If $M_i^2 = M_i$ for all $i = 1, \dots, n$, we call the measurement *projective*. We denote the set of all n-outcome projective measurements on $\mathbb{C}^d$ by $\mathrm{PM}(\mathbb{C}^d)$.

III. MATHEMATICAL FORMALISM

A referee prepares a tripartite system XAB in a cqq state

$$\rho_{\mathsf{XAB}} = \sum_{x\in\mathscr{X}} P_{\mathsf{X}}(x)|x\rangle\langle x|_{\mathsf{X}} \otimes \rho^x_{\mathsf{AB}} \tag{1}$$

and passes the A and B subsystems to two distant parties, Alice and Bob, respectively, while keeping the system X. Alice and Bob know the state ρ_{XAB} and might share some resources (as will be precisely quantified later) prior to receiving their states, but no communication is allowed between them afterwards. Based on their received states and preshared resources, Alice and Bob output guesses x_A and x_B, respectively, to the referee. They win if both guesses are correct, i.e., $x = x_A = x_B$, and they aim at maximizing their probability of winning.

Most of our results are concerned with the case where ρ_{XAB} is completely classical, i.e., there exist orthonormal bases $\{|a\rangle : a \in \mathscr{A}\}$ and $\{|b\rangle : b \in \mathscr{B}\}$ for $\mathcal{A}$ and $\mathcal{B}$, respectively, that are independent of $x \in \mathscr{X}$, and probability distributions P^x_{AB} over $\mathscr{A} \times \mathscr{B}$ such that

$$\rho^x_{\mathsf{AB}} = \sum_{\substack{a\in\mathscr{A}\\ b\in\mathscr{B}}} P^x_{\mathsf{AB}}(a,b)|a\rangle\langle a|_{\mathsf{A}} \otimes |b\rangle\langle b|_{\mathsf{B}}. \tag{2}$$

a. Classical strategies. In this case, there are no additional resources available to Alice and Bob beyond their received state.[1] The optimal probability of simultaneously guessing x

[1] One can equivalently define classical strategies when only shared randomness is allowed between Alice and Bob. However, for the same reason as in nonlocal games, this purely classical resource does not help, as Alice and Bob could fix their randomness to a realization conditioned on which their probability of winning is maximized.

correctly is

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{\rho} := \sup_{\substack{M\in\mathrm{M}(\mathcal{A})\\ N\in\mathrm{M}(\mathcal{B})}} \sum_{x\in\mathscr{X}} P_{\mathsf{X}}(x)\mathrm{tr}\big[\rho^{x}_{\mathsf{AB}}(M_x\otimes N_x)\big]. \tag{3}$$

When ρ_{XAB} is classical and described by a probability distribution P_{XAB}, we can rewrite the optimal probability of winning as

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P} \tag{4}$$

$$= \max_{\substack{Q_{\mathsf{X}_a|\mathsf{A}}\\ Q_{\mathsf{X}_b|\mathsf{B}}}} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)Q_{\mathsf{X}_a|\mathsf{A}}(x_a|a)Q_{\mathsf{X}_b|\mathsf{B}}(x_b|b) \tag{5}$$

$$\overset{(1)}{=} \max_{f,g} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\delta[f(a)=g(b)=x], \tag{6}$$

where the first maximum is taken over all conditional probability distributions $Q_{\mathsf{X}_a|\mathsf{A}}$ and $Q_{\mathsf{X}_b|\mathsf{B}}$, the second maximum is taken over all functions $f:\mathscr{A}\to\mathscr{X}$ and $g:\mathscr{B}\to\mathscr{X}$, and (1) follows since Alice and Bob can condition any local randomness on the realization that maximizes their probability of winning.

b. Quantum strategies. In this case, Alice and Bob can share an entangled state prior to receiving their inputs. Let $\mathcal{A}'=\mathcal{B}'=\mathbb{C}^d$ be two complex Euclidean spaces of dimension d. Alice and Bob first jointly prepare a quantum state $\sigma_{\mathsf{A}'\mathsf{B}'}$ on $\mathcal{A}'\otimes\mathcal{B}'$, after which Alice and Bob keep systems A' and B', respectively. After receiving their inputs, Alice and Bob determine their output by measuring the registers AA' and BB' with local measurements M and N, respectively (this is the most general strategy because no communication is allowed).

When the local dimensions of the shared entangled state $\sigma_{\mathsf{A}'\mathsf{B}'}$ are limited to d for both parties, the optimal probability of winning is

$$\omega^{d}_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{\rho} := \sup_{\sigma_{\mathsf{A}'\mathsf{B}'}\in\mathrm{D}(\mathbb{C}^d\otimes\mathbb{C}^d)} \sup_{\substack{M\in\mathrm{M}(\mathcal{A}\otimes\mathbb{C}^d)\\ N\in\mathrm{M}(\mathcal{B}\otimes\mathbb{C}^d)}} \times \sum_{x\in\mathscr{X}} P_{\mathsf{X}}(x)\mathrm{tr}\big[\big(\rho^{x}_{\mathsf{AB}}\otimes\sigma_{\mathsf{A}'\mathsf{B}'}\big)(M_x\otimes N_x)\big]. \tag{7}$$

When the dimensions of A' and B' are not limited, the optimal winning probability is

$$\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{\rho} := \sup_{d\geqslant 1}\omega^{d}_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{\rho}. \tag{8}$$

When ρ_{XAB} is classical and described by a probability distribution P_{XAB}, we can simplify (7) as follows:

$$\omega^{d}_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P} \tag{9}$$

$$= \sup_{\sigma_{\mathsf{A}'\mathsf{B}'}\in\mathrm{D}(\mathbb{C}^d\otimes\mathbb{C}^d)} \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)\\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \times \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\mathrm{tr}[\sigma_{\mathsf{A}'\mathsf{B}'}(M_x(a)\otimes N_x(b))] \tag{10}$$

$$= \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)\\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)M_x(a)\otimes N_x(b) \right\|, \tag{11}$$

where M and N are collections of measurements, i.e., for every input $a\in\mathscr{A}$ and $b\in\mathscr{B}$, we have that $M(a)=\{M_x(a):x\in\mathscr{X}\}$ and $N(b)=\{N_x(b):x\in\mathscr{X}\}$ are measurements on $\mathbb{C}^d$ with outcomes in $\mathscr{X}$. We show in corollary 5 that the optimization in $\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P}$ can be restricted to projective measurements.

c. No-signaling strategies. We define no-signaling strategies only when ρ_{XAB} is classical and described by a probability distribution P_{XAB}. Given classical inputs $a\in\mathscr{A}$ and $b\in\mathscr{B}$ for Alice and Bob, respectively, they output their estimates x_A and x_B of $x\in\mathscr{X}$ according to a conditional probability distribution $Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ on $\mathscr{X}\times\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ satisfying

$$\forall\, x_B,a,a',b: \sum_{x_A\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b) \tag{12}$$

$$= \sum_{x_A\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a',b), \tag{13}$$

$$\forall\, x_A,a,b,b': \sum_{x_B\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b) \tag{14}$$

$$= \sum_{x_B\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b'). \tag{15}$$

An optimal no-signaling strategy succeeds with probability

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P} := \sup_{Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x,x|a,b). \tag{16}$$

IV. EXAMPLES

We discuss here two examples of LSSD games. The first example highlights particular features of LSSD such as the optimal local strategies are not necessarily optimal for simultaneous guessing, or the optimal guessing probability for product distributions is not the product of the optimal guessing probability of distributions in general. The second example is related to applications of LSSD to quantum cryptography.

Example 1. Let X, Y, and Z be independent binary random variables such that $\Pr[X=1]=\frac{1}{2}$, $\Pr[Y=1]=\Pr[Z=1]=\alpha$ for some $0\leqslant\alpha\leqslant\frac{1}{2}$. We also set $A:=X\oplus Y$ and $B:=X\oplus Z$ and denote the joint probability mass function of (X,A,B) by $P^{\alpha}_{\mathsf{XAB}}$. In other words, A and B are independent noisy versions of the uniform bit X. Consider the problem of simultaneously guessing X from A and B. When $1-\frac{1}{\sqrt{2}}<\alpha<\frac{1}{2}$, both parties always output 0 regardless of their inputs, which is a correct guess of X with probability $\frac{1}{2}$. When $0\leqslant\alpha\leqslant 1-\frac{1}{\sqrt{2}}$, Alice and Bob estimate X as A and B, respectively, which are simultaneously correct when $Y=Z=0$, an event that has probability $(1-\alpha)^2$. By a brute-force check, one finds that the aforementioned strategies are optimal without any extra resources and therefore

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}} = \begin{cases} \frac{1}{2}, & 1-\frac{1}{\sqrt{2}}\leqslant\alpha\leqslant\frac{1}{2},\\ (1-\alpha)^2, & 0\leqslant\alpha\leqslant 1-\frac{1}{\sqrt{2}}. \end{cases} \tag{17}$$

Note that when $1-\frac{1}{\sqrt{2}}\leqslant\alpha\leqslant\frac{1}{2}$, optimal local estimators of X are not optimal for simultaneous guessing of X. We later show in proposition 1 that when all X, A, B are binary, $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha} = \omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha} = \omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha}$.

As a next observation, we set $\alpha := 1 - \frac{1}{\sqrt{2}}$ and let (X', A', B') be an independent copy of (X, A, B). We consider the simultaneous guessing of (X, X') from (A, A') and (B, B'), and define a strategy as follows: both Alice and Bob output $(1, 1)$ if their input bits are $(1, 1)$ and output $(0, 0)$ otherwise. The probability of simultaneously guessing correctly is

$$\tfrac{1}{4}(1-\alpha^2)^2 + \tfrac{1}{4}(1-\alpha)^4 \approx 0.271\,447. \tag{18}$$

Hence, $\omega_{\mathrm{c}}(\mathsf{XX'}|\mathsf{AA'};\mathsf{BB'})_{P^\alpha \times P^\alpha} > \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha}\omega_{\mathrm{c}}(\mathsf{X'}|\mathsf{A'};\mathsf{B'})_{P^\alpha}$ while (X, A, B) and (X', A', B') are independent. Because $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha} = \omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha} = \omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha}$, we also have

$$\omega_{\mathrm{q}}(\mathsf{XX'}|\mathsf{AA'};\mathsf{BB'})_{P^\alpha \times P^\alpha} > \omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha}\omega_{\mathrm{q}}(\mathsf{X'}|\mathsf{A'};\mathsf{B'})_{P^\alpha}, \tag{19}$$

$$\omega_{\mathrm{ns}}(\mathsf{XX'}|\mathsf{AA'};\mathsf{BB'})_{P^\alpha \times P^\alpha} > \omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^\alpha}\omega_{\mathrm{ns}}(\mathsf{X'}|\mathsf{A'};\mathsf{B'})_{P^\alpha}. \tag{20}$$

Example 2. Let $\mathcal{A} = \mathcal{B} = \mathbb{C}^3$ with an orthonormal basis $\{|0\rangle, |1\rangle, |\perp\rangle\}$ and let $|\phi^x\rangle_{\mathsf{AB}} := \frac{1}{\sqrt{2}}(|x\rangle \otimes |\perp\rangle + |\perp\rangle \otimes |x\rangle)$ for $x \in [2]$. We also set $\rho_{\mathsf{XAB}} := \frac{1}{2}\sum_{x\in[2]} |x\rangle\langle x|_{\mathsf{X}} \otimes |\phi^x\rangle\langle\phi^x|_{\mathsf{AB}}$. The authors of [16] showed that $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_\rho \geqslant \frac{9}{16}$ and used this fact to prove impossibility of unclonable encryption, as defined in [16], using pure states as ciphertext.

V. STRICT QUANTUM AND NO-SIGNALING SEPARATIONS FOR LSSD

Our main result is the following theorem that gives a simple example of an LSSD problem for which the guessing probabilities for players with different types of shared resources are all distinct. Namely, $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B}) < \omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B}) < \omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})$.

Theorem 1. Let $\mathscr{X} = \{0, 1, 2\}$ and $\mathscr{A} = \mathscr{B} = \{0, 1\}$, and let P_{XAB} be the uniform distribution over $\{(0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 1, 0), (2, 0, 1)\}$. Then

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = 2/5 = 0.4, \tag{21}$$

$$\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{q}}^2(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \frac{16+\sqrt{13}}{45} \approx 0.435\,679, \tag{22}$$

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = 1/2 = 0.5. \tag{23}$$

Our proof relies on the following characterization of the classical and no-signaling guessing probabilities $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ and $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ when $|\mathscr{A}| = |\mathscr{B}| = 2$ (see Appendix A for proof).

Lemma 1. Let P_{XAB} be a probability distribution over $\mathscr{X} \times \mathscr{A} \times \mathscr{B}$ with $\mathscr{A} = \mathscr{B} = \{0, 1\}$ and $\mathscr{X} = [d]$, $d \geqslant 2$. The classical and no-signaling winning probabilities for P_{XAB} are given by

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max_{\substack{s,t\in\mathscr{X}\\ s\neq t}} \max\{P_{\mathsf{X}}(s), P_{\mathsf{XAB}}(s,0,0) + P_{\mathsf{XAB}}(t,1,1), P_{\mathsf{XAB}}(s,0,1) + P_{\mathsf{XAB}}(t,1,0)\}, \tag{24}$$

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max\left\{\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \max_{k\in\{2,\dots,d\}} \max_{f,g} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(f(x,a), g(x,b)|a,b)\right\}, \tag{25}$$

where the final maximization in (25) is over all functions $f : \mathscr{X} \times \mathscr{A} \to \mathscr{X}$ and $g : \mathscr{X} \times \mathscr{B} \to \mathscr{X}$ such that $f(\cdot, a), g(\cdot, b) : \mathscr{X} \to \mathscr{X}$ are permutations for every $a \in \mathscr{A}$ and $b \in \mathscr{B}$, and the conditional probability distribution $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ on $\mathscr{X} \times \mathscr{X} \times \mathscr{A} \times \mathscr{B}$ is given by

$$Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A, x_B|a, b) := \begin{cases} \frac{1}{k} & (x_A - x_B) \bmod k = ab, \\ 0 & \text{otherwise.} \end{cases} \tag{26}$$

Proof (of Theorem 1) The given distribution P_{XAB} has $P_{\mathsf{X}}(0) = P_{\mathsf{X}}(1) = \frac{2}{5}$, $P_{\mathsf{X}}(2) = \frac{1}{5}$, and $P_{\mathsf{XAB}}(x, a, b) \leqslant \frac{1}{5}$ for all x, a, b. Equation (21) then follows by applying Lemma 1. An explicit strategy achieving success probability $\frac{2}{5}$ is when both parties ignore their inputs and always output 0.

Next, let us prove Eq. (23). Since $|\mathscr{X}| = 3$, we only need to consider $k = 2$ and 3 in Eq. (25) of Lemma 1. Note from Eq. (26) that $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A, x_B|a, b) \leqslant \frac{1}{k}$ for any x_A, x_B, a, b, so the corresponding term in Eq. (25) is at most

$$\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(f(x,a), g(x,b)|a,b)$$
$$\leqslant \frac{1}{k} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) = \frac{1}{k}. \tag{27}$$

If $k = 2$ and we choose $f, g : [3] \times [2] \to [3]$ according to Table I then, for all (x, a, b) with $P_{\mathsf{XAB}}(x, a, b) > 0$, we have $f(x, a), g(x, b) \in \{0, 1\}$ and $f(x, a) \oplus g(x, b) = ab$, so the inequality in (27) becomes tight. According to (25), this lower

TABLE I. (Left) An optimal choice of functions f and g for no-signaling strategies [see Eq. (25)]. (Right) We verify that for any (x, a, b) with $P_{\mathsf{XAB}}(x) > 0$, $f(x, a), g(x, b) \in \{0, 1\}$ (in bold) and $f(x, a) \oplus g(x, b) = ab$, hence this choice is compatible with Eq. (26) when $k = 2$.

x	0	1	2
$f(x, 0)$	2	**1**	**0**
$f(x, 1)$	**0**	**1**	2
$g(x, 0)$	**0**	**1**	2
$g(x, 1)$	**1**	2	**0**

x	a	b	ab	$f(x, a)$	$g(x, b)$
0	1	0	0	0	0
0	1	1	1	0	1
1	0	0	0	1	1
1	1	0	0	1	1
2	0	1	0	0	0

TABLE II. Measurements for Alice and Bob's quantum strategies. The projector $\Pi(\theta)$ is defined in Eq. (31) and their angles are given in Eq. (34).

x	0	1	2
$M_x(0)$	0	$\Pi(\alpha_0)$	$\mathbb{1} - \Pi(\alpha_0)$
$M_x(1)$	$\Pi(\alpha_1)$	$\mathbb{1} - \Pi(\alpha_1)$	0
$N_x(0)$	$\Pi(\beta_0)$	$\mathbb{1} - \Pi(\beta_0)$	0
$N_x(1)$	$\Pi(\beta_1)$	0	$\mathbb{1} - \Pi(\beta_1)$

bounds the success probability by $\frac{1}{2}$. Since $k = 3$ can lower bound it by at most $\frac{1}{3}$, we do not need to consider this case. Thus, according to Lemma 1, $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max\{\frac{2}{5}, \frac{1}{2}\} = \frac{1}{2}$ which proves Eq. (23).

It remains to prove Eq. (22). Let us denote the claimed optimal quantum value in (22) by

$$t_* := \frac{16 + \sqrt{13}}{45}. \tag{28}$$

We will first settle the case when the local dimension of the shared entangled state is $d = 2$, i.e., each party has a single qubit, and then reduce the general case of $d \geqslant 2$ to this one.

Towards establishing Eq. (22), let us first prove that $\omega_{\mathrm{q}}^2(\mathsf{X}|\mathsf{A};\mathsf{B})_P \geqslant t_*$. Alice and Bob can achieve the value t_* by using the following strategy. Their shared two-qubit state is

$$|\sigma\rangle_{\mathsf{A}'\mathsf{B}'} := s_+|00\rangle_{\mathsf{A}'\mathsf{B}'} + s_-|11\rangle_{\mathsf{A}'\mathsf{B}'},$$
$$s_\pm := \sqrt{\frac{1}{2} \pm \frac{1}{78}\sqrt{715 - 182\sqrt{13}}}. \tag{29}$$

To describe their measurements, we denote the qubit state at angle θ and the corresponding projector by

$$|\psi(\theta)\rangle := \cos\theta\,|0\rangle + \sin\theta\,|1\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \tag{30}$$

$$\Pi(\theta) := |\psi(\theta)\rangle\langle\psi(\theta)| = \begin{pmatrix} \cos^2\theta & \cos\theta\,\sin\theta \\ \sin\theta\,\cos\theta & \sin^2\theta \end{pmatrix}. \tag{31}$$

Depending on their local inputs $a, b \in \{0, 1\}$, Alice and Bob apply the projective measurements $M(a) := \{M_0(a), M_1(a), M_2(a)\}$ and $N(b) := \{N_0(b), N_1(b), N_2(b)\}$ given in Table II.

For each measurement, one of their operators is 0 while the other two are of the form $\Pi(\theta)$ and $\mathbb{1} - \Pi(\theta)$, for some angles $\theta \in [-\pi/2, \pi/2]$. The angles used in Table II are chosen as follows:

$$(\alpha_0, \alpha_1, \beta_0, \beta_1) := \left(-\theta_1, \theta_2, \frac{\pi}{2} - \theta_2, \theta_1\right), \tag{32}$$

$$\theta_1 := \frac{1}{4}\arccos\left(\frac{121 + 52\sqrt{13}}{477}\right), \tag{33}$$

$$\theta_2 := \frac{1}{4}\arccos\left(\frac{-431 + 4\sqrt{13}}{477}\right). \tag{34}$$

The angles θ_1 and θ_2 satisfy $\cos(4\theta_1) = 12 + 13\cos(4\theta_2)$ and have the following explicit cosines:

$$\cos\theta_1 = \sqrt{\frac{1}{318}\left(159 + \sqrt{689(23 + 2\sqrt{13})}\right)}, \tag{35}$$

$$\cos\theta_2 = \sqrt{\frac{1}{318}\left(159 + \sqrt{53(23 + 2\sqrt{13})}\right)}. \tag{36}$$

Using a computer algebra system, one can verify that

$$\langle\sigma|_{\mathsf{A}'\mathsf{B}'}\left(\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) M_x(a) \otimes N_x(b)\right)|\sigma\rangle_{\mathsf{A}'\mathsf{B}'}$$
$$= \frac{16 + \sqrt{13}}{45} = t_*. \tag{37}$$

In fact, $|\sigma\rangle_{\mathsf{A}'\mathsf{B}'}$ is the principal eigenvector of the above operator.[2]

Next, let us prove that the above strategy is optimal if the shared entangled state has local dimension $d = 2$ and Alice and Bob use only projective measurements (we will later reduce the case of general measurements in any finite dimension d to this). For now, our goal is to show that

$$\sup_{\substack{\Pi:\mathscr{A}\to\mathrm{PM}(\mathbb{C}^2)\\ \Sigma:\mathscr{B}\to\mathrm{PM}(\mathbb{C}^2)}} \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) \Pi_x(a) \otimes \Sigma_x(b) \right\| \leqslant t_*. \tag{38}$$

First, by Proposition 3 we can assume that

$$\Pi_0(0) = \Pi_2(1) = \Sigma_2(0) = \Sigma_1(1) = 0 \tag{39}$$

since Alice should not guess 0 if $a = 0$ and 2 if $a = 1$, and Bob should not guess 2 if $b = 0$ and 1 if $b = 1$. The remaining operators form two 2-outcome projective measurements for each party:

$$\Pi(0) = \{\Pi_1(0), \Pi_2(0)\}, \quad \Pi(1) = \{\Pi_0(1), \Pi_1(1)\}, \tag{40}$$

$$\Sigma(0) = \{\Sigma_0(0), \Sigma_1(0)\}, \quad \Sigma(1) = \{\Sigma_0(1), \Sigma_2(1)\}. \tag{41}$$

To simplify notation, let us set $(A_0, A_1, B_0, B_1) := (\Pi_0(0), \Pi_0(1), \Sigma_0(0), \Sigma_0(1))$ so that

$$\Pi(0) = \{A_0, A_0^\perp\}, \quad \Pi(1) = \{A_1, A_1^\perp\}, \tag{42}$$

$$\Sigma(0) = \{B_0, B_0^\perp\}, \quad \Sigma(1) = \{B_1, B_1^\perp\}, \tag{43}$$

where $A_i^\perp := \mathbb{1} - A_i$ and $B_i^\perp := \mathbb{1} - B_i$. Our matrix of interest is then

$$\Omega := \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) \Pi_x(a) \otimes \Sigma_x(b) \tag{44}$$

$$= \frac{1}{5}[\Pi_0(1) \otimes \Sigma_0(0) + \Pi_0(1) \otimes \Sigma_0(1) + \Pi_1(0) \otimes \Sigma_1(0)$$
$$+ \Pi_1(1) \otimes \Sigma_1(0) + \Pi_2(0) \otimes \Sigma_2(1)] \tag{45}$$

$$= \frac{1}{5}(A_1 \otimes B_0 + A_1 \otimes B_1 + A_0 \otimes B_0^\perp$$
$$+ A_1^\perp \otimes B_0^\perp + A_0^\perp \otimes B_1^\perp). \tag{46}$$

[2] Indeed, one can check that its eigenvalues are $\frac{16+\sqrt{13}}{45}$, $\frac{25+\sqrt{13}}{90}$, $\frac{7+\sqrt{13}}{45}$, $\frac{19-5\sqrt{13}}{90}$.

We see from (43) that if any of the remaining Alice's measurement operators is 0, then all her operators commute. By Lemma 4 their winning probability cannot exceed the classical value $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \frac{2}{5}$. Hence, all remaining Alice's measurement operators are rank 1, and similarly for Bob.

By applying a local unitary change of basis on Alice and Bob's systems, we can assume without loss of generality that, for some angles $\alpha, \beta \in [0, 2\pi]$,

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_1 = \Pi\left(\frac{\alpha}{2}\right), \tag{47}$$

$$B_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B_1 = \Pi\left(\frac{\pi - \beta}{2}\right), \tag{48}$$

where $\Pi(\theta)$ is the projector defined in Eq. (31). With this choice, Ω from Eq. (46) can be written as

$$\Omega = \begin{pmatrix} -(a+1)(b-3) & (a+1)\sqrt{1-b^2} & -\sqrt{1-a^2}(b-3) & \sqrt{1-a^2}\sqrt{1-b^2} \\ (a+1)\sqrt{1-b^2} & ab - a + b + 7 & \sqrt{1-a^2}\sqrt{1-b^2} & \sqrt{1-a^2}(b-1) \\ -\sqrt{1-a^2}(b-3) & \sqrt{1-a^2}\sqrt{1-b^2} & ab - 3a + b + 5 & -(a+1)\sqrt{1-b^2} \\ \sqrt{1-a^2}\sqrt{1-b^2} & \sqrt{1-a^2}(b-1) & -(a+1)\sqrt{1-b^2} & -ab - b + a + 5 \end{pmatrix}, \tag{49}$$

where $a := \cos\alpha$ and $b := \cos\beta$. Our goal is to show that $\|\Omega\| \leqslant t_*$ over all $a, b \in [-1, 1]$. Using a computer algebra system we find that the characteristic polynomial of Ω in variable t is

$$\begin{aligned} f(t, a, b) = t^4 - t^3 &+ \frac{32 + (1+a)(1+b)}{100} t^2 \\ &- \frac{16 + 3(1+a)(1+b)}{500} t \\ &+ \frac{(1+a)(1+b)(4 - (1-a)(1-b))}{5000}. \end{aligned} \tag{50}$$

Since the largest eigenvalue of Ω is equal to the largest root of f, our goal is to show that f has no roots $t > t_*$. In Lemma 5 in Appendix C we find an exact sum of squares decomposition for f which shows that $f(t, a, b) > 0$ for any $t > t_*$ and $a, b \in [-1, 1]$. This implies that f has no roots larger than t_*.

It remains to show that $\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \leqslant t_*$. We will do this by reducing a general strategy to the above $d = 2$ problem. Let us fix any dimension $d \geqslant 2$ and consider arbitrary local quantum strategies for Alice and Bob. They are based on a shared state $|\sigma\rangle_{\mathsf{A}'\mathsf{B}'} \in \mathbb{C}^d \otimes \mathbb{C}^d$ and collections of measurements $M : \mathscr{A} \to \mathrm{M}(\mathbb{C}^d)$ and $N : \mathscr{B} \to \mathrm{M}(\mathbb{C}^d)$. By invoking Proposition 3 and then Corollary 5 we can reduce M and N to two two-outcome projective measurements that look the same as in Eq. (43), except that A_i and B_i are projectors in some finite-dimensional space $\mathbb{C}^{d'}$ where $d' \leqslant d \max\{|\mathscr{A}|, |\mathscr{B}|\}$.

For now, let us focus just on Alice's measurements. They are fully parametrized by two projectors A_0 and A_1. By Jordan's Lemma [17] (also known as *CS decomposition* [18]), there is a unitary change of basis on Alice's system that simultaneously block diagonalizes A_0 and A_1:

$$A_0 = \begin{pmatrix} \bigoplus_{j=1}^k \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & & & & \\ & \mathbb{1} & & & \\ & & \mathbb{1} & & \\ & & & 0 & \\ & & & & 0 \end{pmatrix}, \tag{51}$$

$$A_1 = \begin{pmatrix} \bigoplus_{j=1}^k \Pi(\theta_j) & & & & \\ & \mathbb{1} & & & \\ & & 0 & & \\ & & & \mathbb{1} & \\ & & & & 0 \end{pmatrix}. \tag{52}$$

Here the first k blocks are of size 2×2 and contain rank-1 projectors onto one-dimensional subspaces at angle θ_j between them [see (31)]. The remaining blocks are 1×1 and contain values (1,1), (1,0), (0,1), and (0,0) (the number of times each pair occurs is determined by the sizes of the identity and all-zeroes matrices). Note that $A_0^\perp$ and $A_1^\perp$ have similar block decompositions in the same basis.

We are interested in the largest eigenvalue of Ω defined in Eq. (46). Since all Alice's projectors are block diagonal, Ω is also block diagonal (each Alice's block gets tensored by Bob's operator). Since the largest eigenvalue of Ω must occur in one of these blocks, Alice might as well restrict her strategy to this single block. Since each of her blocks has size at most two, her strategy does not require more than two dimensions. By a similar argument, Bob's system can also be reduced to two dimensions. Since we already analyzed strategies based on orthogonal measurements on a shared state with local dimension two, the same upper bound t_* also applies to the general case. ■

In the following proposition, we show that the example presented in Theorem 1 is the "smallest" example illustrating a separation between the $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ and $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ in a sense that when $\mathscr{A}$ and $\mathscr{B}$ have cardinality two, three is the minimum cardinality of $\mathscr{X}$ such that there exists such a separation. We also upper bound the gap between $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ and $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ when $\mathscr{A}$ and $\mathscr{B}$ have cardinality two and $\mathscr{X}$ is arbitrary.

Proposition 1. Let P_{XAB} be such that $|\mathscr{A}| = |\mathscr{B}| = 2$. If $|\mathscr{X}| = 2$ then

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{53}$$

If $|\mathscr{X}| > 2$ then

$$\omega_{\rm ns}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \leqslant \min\left\{2\omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P + \tfrac{1}{8}\right\}. \tag{54}$$

Proof. To show Eq. (53), without loss of generality we assume that $\mathscr{A} = \mathscr{B} = \mathscr{X} = [2]$. By Lemma 1, it suffices to show that

$$\omega_{\rm c}(X|A;B)_P \geqslant \max_{f,g} \frac{1}{2}\Pr[f(A,X) - g(B,X) \bmod 2 = AB], \tag{55}$$

where the maximum is taken over all functions $f, g : [2] \times [2] \to [2]$. Note first that

$$\max_{f,g} \frac{1}{2}\Pr[f(A,X) - g(B,X) \bmod 2 = AB] \leqslant \frac{1}{2}. \tag{56}$$

Because $\mathscr{X}$ is of size two, we also have

$$\omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \geqslant \max_{x\in\mathscr{X}} P_{\mathsf{X}}(x) \geqslant \frac{1}{2}. \tag{57}$$

Therefore, we have Eq. (55) as desired.

When $\mathscr{X} = [d]$ for $d > 2$, we fix two functions $f, g : [2] \times [d] \to [d]$ such that for all $a, b \in [2]$, $f(a,\cdot) : [d] \to [d]$ and $g(b,\cdot) : [d] \to [d]$ are bijections. Let $f', g' : [2] \times [d] \to [d]$ be such that for all a, b, x, x', we have

$$f(a,x) = x' \iff f'(a,x') = x, \tag{58}$$

$$g(b,x) = x' \iff g'(b,x') = x. \tag{59}$$

Then,

$$\Pr[f(A,X) - g(B,X) \bmod k = AB] \tag{60}$$

$$\leqslant \sum_{i=0,1} \Pr[f(A,X) - g(B,X) \bmod k = i] \tag{61}$$

$$\leqslant \sum_{i=0,1}\sum_{j\in[k]} \Pr[f(A,X) = j, g(B,X) = (j+i) \bmod k] \tag{62}$$

$$\leqslant \sum_{i=0,1}\sum_{j\in[k]} \Pr\big[f'(A,j) = X, g'(B,(j+i) \bmod k) = X\big] \tag{63}$$

$$\leqslant 2k\omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{64}$$

Since f, g are arbitrary, we conclude by Lemma 1 that $\omega_{\rm ns}(X|A;B)_P \leqslant 2\omega_{\rm c}(X|A;B)_P$.

Next, with relabeling a and b we can always assume that $\Pr[AB = 1] \leqslant \frac{1}{4}$. Then

$$\Pr[f(A,X) - g(B,X) \bmod k = AB] \tag{65}$$

$$= \sum_{i=0,1} \Pr[f(A,X) - g(B,X) \bmod k = i \text{ and } AB = i]$$

$$\Pr[AB = i] \tag{66}$$

$$\leqslant \Pr[f(A,X) - g(B,X) \bmod k = 0] + \frac{1}{4}. \tag{67}$$

With the same argument as before,

$$\Pr[f(A,X) - g(B,X) \bmod k = 0] \leqslant k\omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{68}$$

Applying Lemma 1 again,

$$\omega_{\rm ns}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \leqslant \sup_{k\geqslant 2} \omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P + \frac{1}{4k} \leqslant \omega_{\rm c}(\mathsf{X}|\mathsf{A};\mathsf{B})_P + \frac{1}{8}, \tag{69}$$

as desired. ■

VI. MULTIPARTITE LSSD IS NP-HARD

One can naturally extend the LSSD setup to the case where $r \geqslant 2$ parties desire to simultaneously guess x. We study the computational complexity of finding the optimal simultaneous guessing probability in multipartite LSSD by investigating (again fully classical) problem instances based on hypergraphs. We reduce the NP-hard three-dimensional matching problem in a hypergraph [19] to finding the optimal winning probability of a three-party LSSD whose size is polynomial in the size of the hypergraph. Therefore, finding the optimal winning probability of a three-party LSSD is an NP-hard problem. In the following, we briefly review the definitions regarding hypergraphs.

A. Hypergraphs and (partial) matchings

A *hypergraph* $\mathcal{G}$ is a pair $(\mathscr{V}, \mathscr{E})$ where $\mathscr{V}$ is a set of vertices and $\mathscr{E}$ is a set of hyperedges, which are nonempty subsets of $\mathscr{V}$. A *matching* of a hypergraph $\mathcal{G} = (\mathscr{V}, \mathscr{E})$ is a subset $\mathscr{M} \subset \mathscr{E}$ of mutually disjoint hyperedges. We denote by $\nu(\mathcal{G})$ the maximum cardinality of a matching of $\mathcal{G}$. A *fractional matching* of a hypergraph $\mathcal{G} = (\mathscr{V}, \mathscr{E})$ is a function $g : \mathscr{E} \to [0, 1]$ such that $\sum_{e\in\mathscr{E}:v\in e} g(e) \leqslant 1$ for all $v \in \mathscr{V}$. We denote by $\nu_f(\mathcal{G})$ the maximum of $\sum_{e\in\mathscr{E}} g(e)$ for all fractional matchings g. For any matching $\mathscr{M}$, $g : e \mapsto \delta[e \in \mathscr{M}]$ is a fractional matching and therefore we always have $\nu(\mathcal{G}) \leqslant \nu_f(\mathcal{G})$.

We call a hypergraph $\mathcal{G} = (\mathscr{V}, \mathscr{E})$ *r-partite* if $\mathscr{V}$ can be partitioned into r parts such that each hyperedge contains precisely one vertex from each part. If we denote the r parts by $\mathscr{A}_1, \ldots, \mathscr{A}_r$, we can characterize a hyperedge e by $(a_1, \ldots, a_r) \in \mathscr{A}_1 \times \cdots \times \mathscr{A}_r$ where a_i is the unique vertex in $e \cap \mathscr{A}_i$. We can thus represent an r-partite hypergraph by $(\mathscr{A}_1, \ldots, \mathscr{A}_r, \tilde{\mathscr{E}})$ where $\tilde{\mathscr{E}} \subset \mathscr{A}_1 \times \cdots \times \mathscr{A}_r$.

B. Hypergraph games

For each hypergraph, we can introduce a probability distribution and a corresponding LSSD game. Note that we need to extend all definitions from Sec. III from two guessing parties to multiparty guessing, which can be done in a natural way.

Definition 1. Let $\mathcal{G} = (\mathscr{A}_1, \ldots, \mathscr{A}_r, \mathscr{E})$ be an r-partite hypergraph. We define a probability distribution over $\mathscr{E} \times \mathscr{A}_1 \times \cdots \times \mathscr{A}_r$ as

$$P^{\mathcal{G}}_{\mathbb{E}(\mathsf{A})_1\cdots\mathsf{A}_r}(e, a_1, \ldots, a_r) := \frac{1}{|\mathscr{E}|}\delta[e = (a_1, \ldots, a_r)]. \tag{70}$$

In other words, the random variable E is a uniformly chosen hyperedge of $\mathcal{G}$ and A_i is the vertex of E in $\mathscr{A}_i$.

Our main result of this section relates the optimal guessing probability of the game associated to a hypergraph to its maximum matching.

Theorem 2. For any r-partite hypergraph $\mathcal{G} = (\mathscr{A}_1, \dots, \mathscr{A}_r, \mathscr{E})$,

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\dots;\mathsf{A}_r)_{P^{\mathcal{G}}} = \frac{\nu(\mathcal{G})}{|\mathscr{E}|}, \tag{71}$$

$$\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\dots;\mathsf{A}_r)_{P^{\mathcal{G}}} \leqslant \frac{\nu_f(\mathcal{G})}{|\mathscr{E}|}. \tag{72}$$

We defer the proof to Appendix D and here state several consequences of this theorem.

Corollary 1. For a 3-partite hypergraph $\mathcal{G}$, finding $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}$ is an NP-hard problem.

Proof. According to Theorem 2, finding $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}$ is equivalent to finding the size of the maximum matching in $\mathcal{G}$, which is NP-hard [19]. ■

Corollary 2. Given the assumption P $\neq$ NP, there exists a 3-partite hypergraph $\mathcal{G}$ such that

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}} < \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}. \tag{73}$$

Proof. For the sake of contradiction, suppose that for all 3-partite hypergraphs $\mathcal{G}$,

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}} = \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}. \tag{74}$$

Since $\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}$ can be formulated as a linear program of size polynomial in $|\mathscr{A}_1||\mathscr{A}_2||\mathscr{A}_3|$, we can find $\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}$ in polynomial time. Therefore, by our assumption in Eq. (74), we can also find $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^{\mathcal{G}}}$ in polynomial time, which is in contradiction with corollary 1 and the assumption P $\neq$ NP. ■

Corollary 3. For any r-partite hypergraph $\mathcal{G} = (\mathscr{A}_1, \dots, \mathscr{A}_r, \mathscr{E})$,

$$\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\dots;\mathsf{A}_r)_{P^{\mathcal{G}}} \leqslant (r-1)\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\dots;\mathsf{A}_r)_{P^{\mathcal{G}}}. \tag{75}$$

Proof. For any r-partite hypergraph $\mathcal{G}$, we have $\nu_f(\mathcal{G}) \leqslant (r-1)\nu(\mathcal{G})$ [20]. Combining this with Theorem 2 completes the proof. ■

Corollary 4. For a bipartite graph $\mathcal{G}$,

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}} = \omega_{\mathrm{q}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}} = \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}}. \tag{76}$$

Proof. Applying Corollary 3 when $r = 2$, we have $\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}} \leqslant \omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}}$. On the other hand, $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}} \leqslant \omega_{\mathrm{q}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}} \leqslant \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^{\mathcal{G}}}$ by definition. Therefore, Eq. (76) holds. ■

VII. SYMMETRIC LSSDS

An LSSD problem is *symmetric* if the corresponding state ρ_{XAB} does not change when the registers A and B are swapped. A natural question is whether the optimal strategy for a symmetric LSSD is also symmetric (i.e., whether Alice and Bob share a symmetric resource state and perform the same measurement). When ρ_{XAB} is described by a classical distribution P_{XAB}, we present a symmetric example for which the optimal classical strategy is not symmetric. Let $\mathbb{Z}_5 := \{0, 1, 2, 3, 4\}$ denote the additive group of integers modulo 5 and P_{XAB} be the classical distribution defined as

$$P_{\mathsf{XAB}}(x, a, b) := \begin{cases} \frac{1}{10} & x = a = b - 1 \text{ or } x = a - 1 = b, \\ 0 & \text{otherwise} \end{cases} \tag{77}$$

for $x, a, b \in \mathbb{Z}_5$. P_{XAB} is symmetric with respect to registers A and B. Furthermore, if Alice outputs $\widehat{x}_A = a$ and Bob outputs $\widehat{x}_B = b - 1$, they win with probability $\frac{1}{2}$. However, one can show that the winning probability of any symmetric strategy is at most the size of a maximum matching in a cycle of length 5 divided by 5, which is $\frac{2}{5}$. This example rules out the possibility that symmetric LSSDs always have symmetric optimal strategy. Nevertheless, we shall show that under certain structure in a symmetric LSSD game, there exists a symmetric strategy in the following lemma.

Lemma 2. Let P_{XAB} be such that $P_{\mathsf{XAB}} = P_{\mathsf{X}}P_{\mathsf{A|X}}P_{\mathsf{B|X}}$, $\mathscr{A} = \mathscr{B}$, and $P_{\mathsf{A|X}} = P_{\mathsf{B|X}}$. We then have the following.

(1) There exists an optimal symmetric classical strategy, i.e.,

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_f \sum_{\substack{x\in\mathscr{X}\\ a,b\in\mathscr{A}}} P_{\mathsf{XAB}}(x, a, b)\, \delta[f(a) = x] \\ \delta[f(b) = x], \tag{78}$$

where $f : \mathscr{A} \to \mathscr{X}$ is a function.

(2) For any $d \geqslant 1$,

$$\omega_{\mathrm{q}}^d(\mathsf{X}|\mathsf{A};\mathsf{B})_P \\ = \sup_{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)} \left\| \sum_{\substack{x\in\mathscr{X}\\ a,b\in\mathscr{A}}} P_{\mathsf{XAB}}(x, a, b) M_x(a) \otimes M_x(b)^* \right\|, \tag{79}$$

where M is a collection of POVMs, i.e., $M(a) = \{M_x(a) : x \in \mathscr{X}\}$ forms a POVM for every input $a \in \mathscr{A}$.

We defer the proof to Appendix E.

VIII. IMPOSSIBILITY OF UNCLONABLE ENCRYPTION WITH PURE STATES

We discuss the connection of LSSD and unclonable cryptography. The general idea of using the no-cloning principle in cryptography dates back to Wiesner [21] who proposed a *quantum money* scheme where banknotes are quantum states, preventing copying. Later, quantum copy protection [14,22–24] and unclonable encryption [12,25] were introduced, which provide more sophisticated assets in an unclonable way. The quantification of cryptographic unclonability is naturally connected to LSSD: intuitively, any distributed decryption of a "cloned" quantum ciphertext leads to an LSSD where two parties attempt to guess the message based on their "clone."

We focus here on unclonable encryption. We formalize it following [12], and highlight its connection to LSSD by defining two ingredients: *quantum encryption of classical messages* (QECM) schemes and *cloning attacks*, which we describe in the following. We first define an encryption scheme that encrypts a classical message and a classical key to a quantum ciphertext, and then consider its unclonable security.

Definition 2 ([12], Definition 4). A *quantum encryption of classical messages* (QECM) scheme is a triple of algorithms $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ described as follows:

(i) The key generation algorithm KeyGen samples a classical key k from the key space $\mathscr{K}$ with distribution P_{K}.

(ii) The encryption algorithm $\mathsf{Enc}_k(m)$ takes as inputs the classical key k and classical message $m \in \mathscr{M}$, and produces a quantum ciphertext $\rho_{\mathsf{A}} \in \mathrm{D}(\mathcal{A})$.

(iii) The decryption algorithm $\mathsf{Dec}_k(\rho_{\mathsf{A}})$ takes as inputs the classical key k and a quantum ciphertext ρ_{A}, and returns the classical message $m \in \mathscr{M}$.

We note that our definition of a QECM differs slightly from [12]. In particular, we do not include a security parameter in our definition of a QECM because we only study information-theoretic security in this article and therefore do not impose any computational assumptions on the adversary. Our results hold for any fixed underlying security parameter of the scheme.

Correctness is defined in the natural way.

Definition 3. A QECM scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *(perfectly) correct* if for all k produced by KeyGen, and for all messages $m \in \mathscr{M}$, it holds that

$$\Pr[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] = 1. \tag{80}$$

As in [12], we define unclonable security, in which the adversary chooses a message $m_1 \in \mathscr{M}$ and the encrypted message is uniformly distributed over the set $\{m_0, m_1\}$ for a fixed $m_0 \in \mathscr{M}$.

Definition 4 (Cloning attack, [12], Definition 10). Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a QECM scheme and fix $m_0 \in \mathscr{M}$. A *cloning attack* against $\mathcal{E}$ and m_0 is a quadruple $\mathcal{A} = (m_1, \mathcal{N}_{\mathsf{A}\to\mathsf{BC}}, \{P_b(k)\}, \{Q_b(k)\})$ such that

(i) the message m_1 is in $\mathscr{M} \setminus \{m_0\}$,

(ii) the quantum channel $\mathcal{N}_{\mathsf{A}\to\mathsf{BC}}$ describes the adversary's cloning operation,

(iii) for every possible key k, $\{P_b(k) : b \in \{0,1\}\}$ is Bob's POVM on $\mathcal{B}$ to guess the message m_b,

(iv) for every possible key k, $\{Q_b(k) : b \in \{0,1\}\}$ is Charlie's POVM on $\mathcal{C}$ to guess the message m_b.

The success probability of a cloning attack $\mathcal{A}$ against encryption scheme $\mathcal{E}$ is

$$\begin{aligned} \mathrm{p}_{\text{win-ind}}(\mathcal{E};\mathcal{A}) := \frac{1}{2}\sum_{b\in\{0,1\}} \mathbb{E}_{k\leftarrow\mathsf{KeyGen}}\{\mathrm{tr}[(P_b(k)\otimes Q_b(k)) \\ \times \mathcal{N}_{A\to BC}(\mathsf{Enc}_k(m_b))]\}. \end{aligned} \tag{81}$$

Our main result in this section is the following lower bound on optimal probability of success of cloning attacks for any QECM scheme.

Theorem 3. For any correct (see Definition 3) QECM scheme $\mathcal{E}$ and arbitrary $m_0 \in \mathscr{M}$, there exists a cloning attack $\mathcal{A}$ against $\mathcal{E}$ as defined in Definition 4 and m_0 such that

$$\mathrm{p}_{\text{win-ind}}(\mathcal{E};\mathcal{A}) \geqslant \frac{1}{2} + \frac{\max_{m\in\mathscr{M}} \mathbb{E}_{k\leftarrow\mathsf{KeyGen}}(\|\mathsf{Enc}_k(m)\|)}{16}. \tag{82}$$

Proof. We define the "cloning operation"

$$V_{\mathsf{A}\to\mathsf{BC}} : |\phi\rangle \mapsto \frac{1}{\sqrt{2}}(|\bot\rangle_{\mathsf{B}}\otimes|\phi\rangle_{\mathsf{C}} + |\phi\rangle_{\mathsf{B}}\otimes|\bot\rangle_{\mathsf{C}}), \tag{83}$$

where $|\bot\rangle$ is a unit vector orthogonal to $\mathcal{A}$. Intuitively, $V_{\mathsf{A}\to\mathsf{BC}}$ distributes the input state to B and C "in superposition." Let ρ, σ be perfectly distinguishable states, for example, $\rho = |0\rangle\langle 0|$ and $\sigma = |1\rangle\langle 1|$. We now consider the task where for a random bit $X \in \{0,1\}$, Bob and Charlie have to simultaneously distinguish the following two cases:

(i) if $X = 0$: $V\rho V^\dagger$ is handed to Bob and Charlie,

(ii) if $X = 1$: $V\sigma V^\dagger$ is handed to Bob and Charlie.

The following lemma gives a nontrivial lower bound on their simultaneous guessing probability of X for this task. In particular, for pure states like $\rho = |0\rangle\langle 0|$ and $\sigma = |1\rangle\langle 1|$, we obtain a lower bound of $\frac{1}{2} + \frac{1}{16} = \frac{9}{16}$. At first sight, it seems counterintuitive that Bob and Charlie are able to succeed with probability strictly higher than $\frac{1}{2}$. One might think that after applying the cloning operation $V_{A\to BC}$, the state should be either with Bob or with Charlie, so the other party will succeed with probability at most $\frac{1}{2}$. However, as one can see from the explicit simultaneous guessing strategy that we construct in the proof of Lemma 3 below, Bob and Charlie can exploit the quantum coherence of the state after applying $V_{\mathsf{A}\to\mathsf{BC}}$ to achieve a simultaneous guessing probability strictly larger than $\frac{1}{2}$.

To complete the proof, let $m_1 := \mathrm{argmax}_{m\in\mathscr{M}\setminus\{m_0\}} \mathbb{E}_{k\leftarrow\mathsf{KeyGen}}(\|\mathsf{Enc}_k(m)\|)$. We consider the unclonable-indistinguishable attack $(m_1, V_{\mathsf{A}\to\mathsf{BC}}, \{\Pi^k, \mathbb{1} - \Pi^k\}, \{\Pi^k, \mathbb{1} - \Pi^k\})$ where the projector Π^k is Π defined in the proof of Lemma 3 for $\rho = \mathsf{Enc}_k(m_0)$ and $\sigma = \mathsf{Enc}_k(m_1)$. The claim then follows directly from the lemma below. ■

Lemma 3. Let $\rho, \sigma \in \mathrm{D}(\mathcal{A})$ such that $\rho\sigma = 0$, and define $\tau_{\mathsf{XBC}} := \frac{1}{2}|0\rangle\langle 0|_{\mathsf{X}} \otimes V\rho V^\dagger + \frac{1}{2}|1\rangle\langle 1|_{\mathsf{X}} \otimes V\sigma V^\dagger$. We have

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{B};\mathsf{C})_\tau \geqslant \frac{1}{2} + \frac{\max(\|\rho\|, \|\sigma\|)}{16}. \tag{84}$$

Proof. Let d denote the dimension of $\mathcal{A}$. We consider eigendecompositions

$$\rho = \sum_{i\in[d]} \lambda_i |a_i\rangle\langle a_i|, \qquad \sigma = \sum_{i\in[d]} \mu_i |b_i\rangle\langle b_i|, \tag{85}$$

such that $\lambda_0 \geqslant \cdots \geqslant \lambda_{d-1}$ and $\mu_0 \geqslant \cdots \geqslant \mu_{d-1}$. We set $|\phi\rangle := \sqrt{1-\alpha}|a_0\rangle + \sqrt{\alpha}|\bot\rangle$ for some parameter $\alpha \in [0,1]$ (to be determined below) and

$$\Pi := |\phi\rangle\langle\phi| + \sum_{i\in[d]\setminus\{0\}:\lambda_i>0} |a_i\rangle\langle a_i|. \tag{86}$$

Π is a projector and one can verify the following equalities by straightforward calculations:

$$\langle\bot|\Pi|\bot\rangle = \alpha, \tag{87}$$

$$\langle a_0|\Pi|a_0\rangle = 1-\alpha, \tag{88}$$

$$\langle a_0|\Pi|\bot\rangle = \langle\bot|\Pi|a_0\rangle = \sqrt{\alpha(1-\alpha)}, \tag{89}$$

$$\langle a_i|\Pi|a_i\rangle = 1 \quad \forall\, i \in [d]\setminus\{0\} \text{ such that } \lambda_i > 0, \tag{90}$$

$$\langle a_i|\Pi|\bot\rangle = \langle\bot|\Pi|a_i\rangle = 0 \quad \forall\, i \in [d]\setminus\{0\} \text{ such that } \lambda_i > 0. \tag{91}$$

It holds that $\lambda_i\mu_j|\langle a_i|b_j\rangle|^2 = 0$ for all i and j since $\rho\sigma = 0$. Hence, $\Pi|b_j\rangle = 0$ for all j with $\mu_j > 0$ and

$$\langle b_j|(\mathbb{1}-\Pi)|b_j\rangle = 1, \tag{92}$$

$$\langle b_j|(\mathbb{1}-\Pi)|\bot\rangle = \langle\bot|(\mathbb{1}-\Pi)|b_j\rangle = 0, \tag{93}$$

for all j with $\mu_j > 0$.

Bob and Charlie both use the POVM $\{\Pi, \mathbb{1} - \Pi\}$ as their local guessing strategies for X. By definition of $\omega_c(\mathsf{X}|\mathsf{B};\mathsf{C})_\tau$, we have

$$\omega_c(\mathsf{X}|\mathsf{B};\mathsf{C})_\tau \geqslant \tfrac{1}{2}(\mathrm{tr}((\Pi\otimes\Pi)V\rho V^\dagger) + \mathrm{tr}(((\mathbb{1}-\Pi) \otimes (\mathbb{1}-\Pi))V\sigma V^\dagger)). \tag{94}$$

The first term on the right-hand side of Eq. (94) is

$$\begin{aligned}
&\mathrm{tr}((\Pi\otimes\Pi)V\rho V^\dagger) && (95)\\
&= \sum_{i\in[d]} \lambda_i \mathrm{tr}((\Pi\otimes\Pi)V|a_i\rangle\langle a_i|V^\dagger) && (96)\\
&= \frac{1}{2}\sum_{i\in[d]} \lambda_i \mathrm{tr}((\Pi\otimes\Pi)(|a_i\rangle\langle a_i|\otimes|\perp\rangle\langle\perp| \\
&\quad +|\perp\rangle\langle\perp|\otimes|a_i\rangle\langle a_i| \\
&\quad +|a_i\rangle\langle\perp|\otimes|\perp\rangle\langle a_i| + |\perp\rangle\langle a_i|\otimes|a_i\rangle\langle\perp|)) && (97)\\
&\overset{(a)}{=} 2\lambda_1\alpha(1-\alpha) + \alpha \sum_{i\in[d]\setminus\{0\}} \lambda_i && (98)\\
&= \alpha + \lambda_0\alpha(1-2\alpha), && (99)
\end{aligned}$$

where (a) follows by using Eqs. (87)–(91). Similarly applying Eqs. (92) and (93) yields that

$$\mathrm{tr}(((\mathbb{1}-\Pi)\otimes(\mathbb{1}-\Pi))V\sigma V^\dagger) = 1-\alpha. \tag{100}$$

Combining Eqs. (94), (99), and (100) and setting $\alpha := 1/4$, we obtain that

$$\omega_c(\mathsf{X}|\mathsf{B};\mathsf{C})_\tau \geqslant \frac{1}{2} + \frac{\lambda_0}{16}. \tag{101}$$

Finally, without loss of generality we can assume that $\lambda_0 \geqslant \mu_0$, and therefore, $\lambda_0 = \max(\|\rho\|, \|\sigma\|)$. ■

Some related work and open problems

LSSD is a fascinating new problem in quantum information processing, and there are many associated open questions. Our results so far only treat the case where the referee uses classical states. How do the different success probabilities behave when distinguishing actual quantum states? Are there dimension constraints under which the classical and quantum values coincide?

Earlier work by Buscemi [26] studied "semiquantum" nonlocal games where a referee picks a bipartite quantum state and sends the registers as questions to two players, Alice and Bob. Their answers are classical bit strings. The subclass of quantum XOR games has been studied in depth by Regev and Vidick [27]. Here, the players' answers are classical bits, and the winning predicate only depends on their XOR. Our LSSD scenario involves a similar restriction, as the players simultaneously have to guess the referee's choice. It is a very interesting open problem to investigate whether some of the results from quantum XOR games carry over to the LSSD setting. For instance, does there exist a family of games that can only be won optimally with an ever-increasing amount of entanglement? Can we find efficiently computable lower or upper bounds on the various success probabilities?

Another line of related work [28–30] studies the relation between various distinguishability norms with the goal of maximizing the so-called data hiding ratio, i.e., how much worse restricted sets of measurements (such as local ones) perform in the task of state discrimination versus global measurements. In this setting, the "local operations" performed by the players can still be postprocessed by the referee (akin to some form of communication), whereas in our LSSD setting, the players simultaneously have to guess the referee's input using only local operations.

The authors of [31] study the LSSD problem for two bipartite quantum states that are in tensor product. It shows the same "two-regime behavior" as our Example 1 where depending on a parameter, it is better to use the locally optimal discrimination strategy in one regime, whereas in the other regime, it is better for the players to correlate their errors.

Concerning unclonable encryption, the followup work of [32] proves a new impossibility result. The authors improve our lower bound on the indistinguishably of any scheme whose ciphertexts are pure states. Nevertheless, one cannot extend their bound beyond pure states unlike our approach. In other followup work [33], we have investigated the behavior of LSSD games under parallel repetition, establishing interesting relations with error-correcting and list-decoding codes.

Note added. Recently, we have become aware of independent unpublished work by Chitambar and Mančinska [31] that also studies our scenario.

Our code is available at [34].

ACKNOWLEDGMENTS

We would like to thank L. Mančinska and E. Chitambar for useful discussions and for sharing a draft of [31] with us. C.M. was supported by an NWO Veni grant (Grant No. VI.Veni.192.159). M.O. was supported by an NWO Vidi grant (Grant No. VI.Vidi.192.109). C.S. and M.T. were supported by an NWO Vidi grant (Grant No. 639.022.519).

APPENDIX A: PROOF OF LEMMA 1

In the classical case, it is enough to consider only deterministic strategies. They can be described by functions $f : \mathscr{A} \to \mathscr{X}$ and $g : \mathscr{B} \to \mathscr{X}$ that locally map Alice and Bob's inputs to outputs. Their success probability is given by

$$\begin{aligned}
\omega_c(\mathsf{X}|\mathsf{A};\mathsf{B})_P &= \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A}, b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\delta[f(a)=x]\delta[g(b)=x] && (A1)\\
&= \sum_{a,b} P_{\mathsf{XAB}}(f(a),a,b)\delta[f(a)=g(b)]. && (A2)
\end{aligned}$$

There are two possibilities: Alice can either ignore her input and always produce a fixed output, or she can take her input into account.

In the first case, $f(0) = f(1) =: s$ and their success probability is

$$\sum_{a,b} P_{\mathsf{XAB}}(s,a,b)\delta[s=g(b)]. \tag{A3}$$

It is maximized when Bob also ignores his input and outputs the same fixed value s as Alice, i.e., $g(0) = g(1) = s$. This results in success probability

$$\sum_{a,b} P_{\mathsf{XAB}}(s, a, b) = P_{\mathsf{X}}(s), \tag{A4}$$

where $s \in \{0, 1\}$. This accounts for the first term in Eq. (24).

If Alice does *not* ignore her input, then $f(0) \neq f(1)$. We can assume that neither does Bob, i.e., $g(0) \neq g(1)$. Indeed, if Bob were to ignore his input, Alice could improve her strategy by outputting the same value as Bob and we would again arrive at Eq. (A4). To maximize the success probability in Eq. (A2), the strategies f and g should be coordinated so that $\{f(0), f(1)\} = \{g(0), g(1)\}$ as sets. In other words, either $f(0) = g(0)$ and $f(1) = g(1)$, or $f(0) = g(1)$ and $f(1) = g(0)$. These two cases result in success probabilities

$$P_{\mathsf{XAB}}(f(0), 0, 0) + P_{\mathsf{XAB}}(f(1), 1, 1), \tag{A5}$$

$$P_{\mathsf{XAB}}(f(0), 0, 1) + P_{\mathsf{XAB}}(f(1), 1, 0). \tag{A6}$$

Letting $\{s, t\} := \{f(0), f(1)\} \subseteq \mathscr{X}$ we recover the last two terms in (24).

We now prove Eq. (25). Recall from Eq. (16) that

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P := \sup_{Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x, x|a, b), \tag{A7}$$

where $Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ is a conditional probability distribution satisfying the no-signaling conditions in Eqs. (13) and (15). Since the objective function and all constraints are linear, an optimal $Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ is an extreme point of the set of all no-signaling conditional probability distributions. A *local* extreme point can achieve success probability at most $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$, corresponding to the first term in (25).

According to [35, Theorem 1], any *nonlocal* extreme point of the two-party no-signaling polytope where each party has two inputs and d outputs, is given by $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ in (26), for some $k \in \{2, \dots, d\}$, up to reversible local relabeling. Intuitively, Eq. (26) says that we choose $x_B \in [k]$ uniformly at random and set

$$x_A = \begin{cases} x_B + 1 \pmod{k} & \text{if } (a, b) = (1, 1), \\ x_B & \text{otherwise.} \end{cases} \tag{A8}$$

A reversible local relabeling means that each party can locally permute their input as well as output values, and the output permutation may depend on the local input value. The extreme distributions in Eq. (26) have the property that any local permutation of input values can be achieved by instead locally permuting outputs conditioned on inputs. For example, the input permutation $a \mapsto 1 - a$ for Alice can be achieved by first negating both variables (i.e., $x_A \mapsto -x_A$ and $x_B \mapsto -x_B$) and then Bob increasing his output by one (i.e., $x_B \mapsto x_B + 1$) whenever $b = 1$. Indeed, this will cause $x_A = x_B + 1$ whenever $(a, b) = (0, 1)$ and $x_A = x_B$ otherwise [see Eq. (A8)].

Since we only need to take into account local output permutations that may depend on local inputs, any nonlocal extreme point of the no-signaling polytope is of the form

$$\tilde{Q}^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A, x_B|a, b) = Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(f(x_A, a), g(x_B, b)|a, b), \tag{A9}$$

where $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ is given by Eq. (26) and $f : \mathscr{X} \times \mathscr{A} \to \mathscr{X}$ and $g : \mathscr{X} \times \mathscr{B} \to \mathscr{X}$ are functions such that $f(\cdot, a), g(\cdot, b) : \mathscr{X} \to \mathscr{X}$ are permutations for every $a \in \mathscr{A}$ and $b \in \mathscr{B}$. This establishes Eq. (25).

APPENDIX B: CONSTRAINTS ON OPTIMAL MEASUREMENTS

The following proposition shows that any measurement can be replaced by a projective measurement on a larger space.

Proposition 2. For any an n-outcome measurement $M = \{M_1, \dots, M_n\}$ on $\mathbb{C}^d$, there is a projective measurement $\{\Pi_1, \dots, \Pi_n\}$ on $\mathbb{C}^d \otimes \mathbb{C}^n$ and an isometry $U : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^n$ such that, for all $i = 1, \dots, n$,

$$M_i = U^\dagger \Pi_i U. \tag{B1}$$

Proof. Let $U := \sum_{i=1}^n \sqrt{M_i} \otimes |i\rangle$ and $\Pi_i := \mathbb{1} \otimes |i\rangle\langle i|$. Clearly, each Π_i is a projector and $\sum_{i=1}^n \Pi_i = \mathbb{1}$. Equation (B1) holds since

$$U^\dagger \Pi_i U = \left(\sum_{j=1}^n \sqrt{M_j} \otimes \langle j|\right) \Pi_i \left(\sum_{k=1}^n \sqrt{M_k} \otimes |k\rangle\right) \tag{B2}$$

$$= \sum_{j,k=1}^n \sqrt{M_j}\mathbb{1}\sqrt{M_k} \otimes \langle j|i\rangle\langle i|k\rangle \tag{B3}$$

$$= M_i. \tag{B4}$$

Finally, U is an isometry since $U^\dagger U = U^\dagger(\sum_{i=1}^n \Pi_i)U = \sum_{i=1}^n U^\dagger \Pi_i U = \sum_{i=1}^n M_i = \mathbb{1}$. ■

Using the above result, we can show that it suffices to consider only projective measurements when determining the optimal winning probability for quantum strategies assisted by an entangled state of an arbitrarily large dimension. Our argument is similar to [36, Lemma 9].

Corollary 5. If P_{XAB} is a probability distribution over $\mathscr{X} \times \mathscr{A} \times \mathscr{B}$ then

$$\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{d\geqslant 1} \omega^d_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{d\geqslant 1} \sup_{\substack{\Pi:\mathscr{A}\to\mathrm{PM}(\mathbb{C}^d)\\ \Sigma:\mathscr{B}\to\mathrm{PM}(\mathbb{C}^d)}} \times \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) \Pi_x(a) \otimes \Sigma_x(b) \right\|, \tag{B5}$$

where the last supremum is over collections of projective measurements.

Proof. The first equality in (B5) is by definition [see Eq. (8)]. For the second equality, recall from Eq. (11) that

$$\omega^d_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)\\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) M_x(a) \otimes N_x(b) \right\|. \tag{B6}$$

We need to show that, at the cost of increasing the dimension d, the optimization here can be restricted to just projective measurements. For convenience, let

$$\Omega_{\mathsf{A'B'}} := \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b), \tag{B7}$$

where M_x^a and N_x^b act on registers A' and B' of dimension d.

Let us fix a dimension $d \geqslant 1$ and set $\mathcal{A} = \mathbb{C}^{\mathscr{A}}$ and $\mathcal{B} = \mathbb{C}^{\mathscr{B}}$ as usual. Using Proposition 2, we can find collections of isometries $U_a : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathcal{A}$ and $V_b : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathcal{B}$ and projective measurements $\Pi(a) \in \mathrm{PM}(\mathbb{C}^d \otimes \mathcal{A})$ and $\Sigma(b) \in \mathrm{PM}(\mathbb{C}^d \otimes \mathcal{B})$ such that

$$M_x(a) = U_a^\dagger \Pi_x^a U_a, \quad N_x(b) = V_b^\dagger \Sigma_x^b V_b, \tag{B8}$$

for all $a \in \mathscr{A}$, $b \in \mathscr{B}$, and $x \in \mathscr{X}$. Then

$$\Omega_{\mathsf{A'B'}} = \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)(U_a\otimes V_b)^\dagger(\Pi_x(a)\otimes\Sigma_x(b)) (U_a\otimes V_b). \tag{B9}$$

Let $|\sigma\rangle_{\mathsf{A'B'}} \in \mathbb{C}^d \otimes \mathbb{C}^d$ denote its principal eigenvector.

Let us fix some arbitrary states $|\alpha\rangle \in \mathcal{A}$ and $|\beta\rangle \in \mathcal{B}$, and arbitrarily extend the isometries U_a and V_b to unitaries $\widetilde{U}_a \in \mathrm{U}(\mathbb{C}^d \otimes \mathcal{A})$ and $\widetilde{V}_b \in \mathrm{U}(\mathbb{C}^d \otimes \mathcal{B})$ so that

$$U_a = \widetilde{U}_a(\mathbb{1}_{\mathsf{A}'} \otimes |\alpha\rangle_{\mathsf{A}}), \quad V_b = \widetilde{V}_b(\mathbb{1}_{\mathsf{B}'} \otimes |\beta\rangle_{\mathsf{B}}). \tag{B10}$$

Furthermore, we promote $|\sigma\rangle_{\mathsf{A'B'}} \in \mathbb{C}^d \otimes \mathbb{C}^d$ to $|\widetilde{\sigma}\rangle_{\mathsf{A'A,B'B}} \in (\mathbb{C}^d \otimes \mathcal{A}) \otimes (\mathbb{C}^d \otimes \mathcal{B})$ by defining

$$|\widetilde{\sigma}\rangle_{\mathsf{A'A,B'B}} := |\sigma\rangle_{\mathsf{A'B'}} \otimes |\alpha\rangle_{\mathsf{A}} \otimes |\beta\rangle_{\mathsf{B}}, \tag{B11}$$

where the registers on the right-hand side should be rearranged accordingly. Then

$$(U_A \otimes V_b)|\sigma\rangle_{\mathsf{A'B'}} = (\widetilde{U}_a \otimes \widetilde{V}_b)|\widetilde{\sigma}\rangle_{\mathsf{A'A,B'B}} \tag{B12}$$

because of Eq. (B10). Substituting this in Eq. (B9),

$$\langle\sigma|\Omega|\sigma\rangle = \langle\widetilde{\sigma}|\left(\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)(\widetilde{\Pi}_x(a)\otimes\widetilde{\Sigma}_x(b))\right)|\widetilde{\sigma}\rangle, \tag{B13}$$

where $\widetilde{\Pi}_x(a) := \widetilde{U}_a^\dagger \Pi_x(a)\widetilde{U}_a$ and $\widetilde{\Sigma}_x(b) := \widetilde{V}_b^\dagger \Sigma_x(b)\widetilde{V}_b$ are projectors on $\mathbb{C}^d \otimes \mathcal{A}$ and $\mathbb{C}^d \otimes \mathcal{B}$.

Hence, we have promoted the original d-dimensional strategy to one in dimension $d\max\{|\mathscr{A}|, |\mathscr{B}|\}$ that uses only projective measurements and achieves the same success probability. Since $\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ in (B5) is defined as a supremum over all $d \geqslant 1$, this increase of dimension does not matter. Hence, we can obtain the optimal quantum value by optimizing only over projectors. ■

Intuitively, Alice and Bob should never guess values of x that cannot occur based on their local inputs. The following result shows that optimal measurements for Alice and Bob's quantum strategies can always be assumed to have this property.

Proposition 3. Let P_{XAB} be a probability distribution on $\mathscr{X} \times \mathscr{A} \times \mathscr{B}$ and $d \geqslant 1$ an integer. The supremum in

$$\omega_{\mathrm{q}}^d(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)\\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b) \right\| \tag{B14}$$

is achieved by collections of measurements $M(a) = \{M_x(a) : x \in \mathscr{X}\}$ and $N(b) = \{N_x(b) : x \in \mathscr{X}\}$ on $\mathbb{C}^d$ with

$$M_x(a) = 0 \quad \text{if } P_{\mathsf{XA}}(x,a) = 0 \text{ and } P_{\mathsf{A}}(a) > 0, \tag{B15}$$

$$N_x(b) = 0 \quad \text{if } P_{\mathsf{XB}}(x,b) = 0 \text{ and } P_{\mathsf{B}}(b) > 0. \tag{B16}$$

In particular, if the supremum can be achieved by projective measurements then it can also be achieved by projective measurements that satisfy Eqs. (B15) and (B16).

Proof. The set of all measurements on a finite-dimensional complex Euclidean space and with a finite output set $\mathscr{X}$ is compact. Since the objective function is continuous, the maximum is achieved by some collections of measurements $M(a)$ and $N(b)$. We can potentially improve Alice's measurement M^a by absorbing those measurement operators $M_{x'}(a)$ that correspond to pairs (x', a) that never occur into other operators. More specifically, for each $a \in \mathscr{A}$ with $P_{\mathsf{A}}(a) > 0$ there exists some $x_a \in \mathscr{X}$ with $P_{\mathsf{XA}}(x_a, a) > 0$, so we can absorb all $M_{x'}(a)$ with $P_{\mathsf{XA}}(x', a) = 0$ into $M_{x_a}(a)$:

$$\widetilde{M}_x^a := \begin{cases} 0 & \text{if } P_{\mathsf{XA}}(x,a) = 0 \text{ and } P_{\mathsf{A}}(a) > 0, \\ M_x(a) + \sum_{x':P_{\mathsf{XA}}(x',a)=0} M_{x'}(a) & \text{if } P_{\mathsf{A}}(a) > 0 \text{ and } x = x_a, \\ M_x(a) & \text{otherwise.} \end{cases} \tag{B17}$$

We can perform a similar procedure for Bob's measurements $N(b)$ to obtain $\widetilde{N}(b)$. It is clear that all $\widetilde{M}(a)$ and $\widetilde{N}(b)$ are still measurements, and that they satisfy (B15) and (B16). In particular, if $M(a)$ are projective measurements then so are $\widetilde{M}(a)$. Moreover,

$$P_{\mathsf{XAB}}(x,a,b)\widetilde{M}_x(a)\otimes\widetilde{N}_x(b) \succeq P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b), \tag{B18}$$

for all x, a, b. Indeed, if $P_{\mathsf{XAB}}(x,a,b) = 0$ then this holds trivially, and if $P_{\mathsf{XAB}}(x,a,b) > 0$ then $\widetilde{M}_x(a) \succeq M_x(a)$ and $\widetilde{N}_x(b) \succeq N_x(b)$, so $\widetilde{M}_x(a)\otimes\widetilde{N}_x(b) \succeq M_x(a)\otimes N_x(b)$. Since Eq. (B18) still holds when summing over all x, a, b,

$$\left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\widetilde{M}_x(a)\otimes\widetilde{N}_x(b) \right\| \geqslant \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b) \right\|, \tag{B19}$$

as desired. ■

Lemma 4. Let P_{XAB} be a joint probability distribution. We fix a quantum strategy consisting of a quantum bipartite state $\sigma_{\mathsf{A'B'}}$ with $\mathcal{A}' = \mathcal{B}' = \mathbb{C}^d$ and collections of measurement $M : \mathscr{A} \to \mathrm{M}(\mathbb{C}^d)$ and $N : \mathscr{B} \to \mathrm{M}(\mathbb{C}^d)$ with output on $\mathscr{X}$. Let M be such that $[M(a)_x, M(a')_{x'}] = 0$ for all $a, a' \in \mathscr{A}$ and for all $x, x' \in \mathscr{X}$. Then,

$$\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\mathrm{tr}[\sigma_{\mathsf{A'B'}}(M_x(a)\otimes N_x(b))]$$
$$\leqslant \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{B20}$$

Proof. Because Alice's measurement operators commute, she can jointly perform all measurements for all inputs $a \in \mathscr{A}$ *before* receiving her input to obtain a collection of random variables $\{X_a : a \in \mathscr{A}\}$ and use X_a as her output when her input is a. Let $\widetilde{\mathsf{X}}$ denote the register containing all $\{X_a : a \in \mathscr{A}\}$. Equivalently, Alice and Bob can share $\sigma_{\widetilde{\mathsf{X}}\mathsf{B'}}$ in the first place, which is a cq state and therefore separable. Let $\sigma_{\widetilde{\mathsf{X}}\mathsf{B'}} = \sum_i p_i\sigma^{(i)}_{\widetilde{\mathsf{X}}} \otimes \sigma^{(i)}_{\mathsf{B'}}$ where $\{p_i\}$ is a probability distribution. For any collection of measurements $\widetilde{M} : \mathscr{A} \to \mathrm{M}(\widetilde{\mathscr{X}})$,

$$\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\mathrm{tr}[\sigma_{\widetilde{\mathsf{X}}\mathsf{B'}}(\widetilde{M}_x(a)\otimes N_x(b))] \tag{B21}$$
$$= \sum_i p_i \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)$$
$$\times\mathrm{tr}\big[\big(\sigma^{(i)}_{\widetilde{\mathsf{X}}}\otimes\sigma^{(i)}_{\mathsf{B'}}\big)(\widetilde{M}_x(a)\otimes N_x(b))\big] \tag{B22}$$
$$= \sum_i p_i \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)$$
$$\times\mathrm{tr}\big[\sigma^{(i)}_{\widetilde{\mathsf{X}}}\widetilde{M}_x(a)\big]\mathrm{tr}\big[\sigma^{(i)}_{\mathsf{B'}}N_x(b)\big]. \tag{B23}$$

Therefore, for each i, Alice and Bob can use classical strategies $Q_{\mathsf{X}_A|\mathsf{A}}(x_a|a) := \mathrm{tr}[\sigma^{(i)}_{\widetilde{\mathsf{X}}}\widetilde{M}_x(a)]$ and $Q_{\mathsf{X}_B|\mathsf{B}}(x_b|b) := \mathrm{tr}[\sigma^{(i)}_{\mathsf{B'}}N_x(b)]$, respectively. Hence,

$$\sum_i p_i \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\mathrm{tr}\big[\sigma^{(i)}_{\widetilde{\mathsf{X}}}\widetilde{M}_x(a)\big]\mathrm{tr}\big[\sigma^{(i)}_{\mathsf{B'}}N_x(b)\big]$$
$$\leqslant \sum_i p_i\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \tag{B24}$$

as desired. ■

APPENDIX C: SOS REPRESENTATION

Lemma 5. For any $t > t_* = \frac{16+\sqrt{13}}{45}$ and $a, b \in [-1, 1]$, the polynomial

$$f(t,a,b) = t^4 - t^3 + \frac{32+(1+a)(1+b)}{100}t^2 - \frac{16+3(1+a)(1+b)}{500}t + \frac{(1+a)(1+b)(4-(1-a)(1-b))}{5000} \tag{C1}$$

is strictly positive.

Proof. Let us first establish that $f(t, a, b) \geqslant 0$ for all $t \geqslant t_*$ and $a, b \in [-1, 1]$. This would be evident if we managed to find a representation of f of the form

$$f(t,a,b) = v(t,a,b)^{\mathsf{T}}[Q_1 + (t-t_*)Q_2 + (1-a^2)Q_3 + (1-b^2)Q_4]v(t,a,b), \tag{C2}$$

where Q_i are fixed positive-semidefinite matrices and $v(t, a, b)$ is a vector whose entries depend on t, a, b (e.g., are monomials in them). Generally such "sums of squares" representations can be found using semidefinite programming (see lectures 10–14 of Fawzi [37] or Sec. 3.4.4 of [38]). In our case this is a semidefinite feasibility problem where the matrices Q_i are subject to $Q_i \succeq 0$ and a set of linear constraints obtained by comparing the coefficients of the polynomials in Eqs. (C1) and (C2).

We found the following exact solution of this problem:

$$v(a,b,t) = \begin{pmatrix} 1\\ a\\ b\\ ab\\ t\\ t^2 \end{pmatrix}, \tag{C3}$$

$$Q_1 = \begin{pmatrix} \alpha & \beta & \beta & \gamma & \delta & \varepsilon\\ \beta & \zeta & \eta & \theta & -\frac{3}{1000} & \frac{1}{200}\\ \beta & \eta & \zeta & \theta & -\frac{3}{1000} & \frac{1}{200}\\ \gamma & \theta & \theta & \iota & -\frac{3}{1000} & \frac{1}{200}\\ \delta & -\frac{3}{1000} & -\frac{3}{1000} & -\frac{3}{1000} & \kappa & -\frac{1}{2}\\ \varepsilon & \frac{1}{200} & \frac{1}{200} & \frac{1}{200} & -\frac{1}{2} & 1 \end{pmatrix}, \tag{C4}$$

$$Q_2 = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$Q_3 = \begin{pmatrix} \mu & 0 & \theta & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ \theta & 0 & \nu & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{C5}$$

$$Q_4 = \begin{pmatrix} \mu & \theta & 0 & 0 & 0 & 0\\ \theta & \nu & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{C6}$$

where the values of the missing matrix entries are as follows:

$$\alpha = \frac{973\,343 + 240\,821\sqrt{13}}{371\,790\,000}, \quad \beta = \frac{33\,139 - 617\sqrt{13}}{82\,620\,000}, \tag{C7}$$

$$\gamma = \frac{20-\sqrt{13}}{45\,000}, \quad \delta = -\frac{1721 + 62\sqrt{13}}{81\,000}, \tag{C8}$$

$$\varepsilon = \frac{25 - 2\sqrt{13}}{600}, \quad \zeta = \frac{21\,592 - 2903\sqrt{13}}{185\,895\,000}, \tag{C9}$$

$$\eta = \frac{-2+\sqrt{13}}{45\,000}, \quad \theta = \frac{-91+617\sqrt{13}}{82\,620\,000}, \tag{C10}$$

$$\iota = \frac{-47+127\sqrt{13}}{4\,590\,000}, \quad \kappa = \frac{37+\sqrt{13}}{150}, \tag{C11}$$

$$\lambda = \frac{91+31\sqrt{13}}{20\,250}, \quad \mu = \frac{8203-1325\sqrt{13}}{743\,580\,000}, \tag{C12}$$

$$\nu = \frac{871+127\sqrt{13}}{9\,180\,000}. \tag{C13}$$

The correctness of this decomposition can be verified by plugging these values into Eq. (C2) and comparing the resulting polynomial with Eq. (C1).

To verify that Q_i are positive semidefinite, we can simply compute their eigenvalues. The nonzero eigenvalues of Q_1 are

$$\begin{aligned} &1.255\,390\,507\ldots, \\ &0.020\,376\,547\ldots, \\ &0.000\,059\,985\ldots, \\ &0.000\,024\,167\ldots, \\ &0.000\,015\,112\ldots. \end{aligned} \tag{C14}$$

The remaining matrices Q_2, Q_3, Q_4 have rank one and their only nonzero eigenvalues are

$$\frac{91+31\sqrt{13}}{20\,250}, \quad \frac{39\,377+4481\sqrt{13}}{371\,790\,000}, \quad \frac{39\,377+4481\sqrt{13}}{371\,790\,000}. \tag{C15}$$

To prove that $f(a,b,t) > 0$ when $t > t_*$, expand Eq. (C2) to obtain

$$\begin{aligned} f(t,a,b) = {} & v^{\mathsf{T}}Q_1v + (t-t_*)v^{\mathsf{T}}Q_2v + (1-a^2)v^{\mathsf{T}}Q_3v \\ & + (1-b^2)v^{\mathsf{T}}Q_4v. \end{aligned} \tag{C16}$$

Note that all terms are non-negative when $t \geqslant t_*$ and $a, b \in [-1, 1]$. Since $\lambda > 0$, the second term

$$(t-t_*)v^{\mathsf{T}}Q_2v = (t-t_*)\lambda \tag{C17}$$

is strictly positive when $t > t_*$. ■

The above solution was found using *Mathematica*. First, we used the `SemidefiniteOptimization` function to find an initial solution. Then, for all sufficiently small matrix entries, we included additional linear constraints that force them to be exactly zero. This resulted in a preliminary solution with sufficiently many zeros. Our hope was to convert this to an exact algebraic solution using the `RootApproximant` function. However, this would work only if the solution is isolated (i.e., cannot be perturbed to other nearby solutions) and of sufficiently high accuracy. Unfortunately, the built-in `SemidefiniteOptimization` function cannot obtain high-accuracy solutions.

To overcome this, we had to rely on the generic `NMinimize` and `FindMinimum` routines that support `WorkingPrecision` option. However, since they do not support semidefinite constraints, we had to use the preliminary solution to choose a sufficiently simple ansatz matrix A_i and set $Q_i = A_i^{\mathsf{T}}A_i$. This automatically guarantees that all Q_i are positive semidefinite. By further tweaking the ansatz we managed to obtain an isolated solution.

To get an exact algebraic solution, we supplied this isolated numerical solution as an initial point to the `FindMinimum` routine and, by increasing the `WorkingPrecision` option, dialed up the accuracy to several hundreds of digits. Finally, applying `RootApproximant` to Q_i, followed by `ToRadicals`, produced the above exact algebraic solution.

APPENDIX D: PROOF OF THEOREM 2

Consider a matching $\mathscr{M}$ of $\mathcal{G}$. For a fixed $1 \leqslant i \leqslant r$ we define $h_i : \mathscr{A}_i \to \mathscr{E}$ as follows. Given $a \in \mathscr{A}_i$, there is at most one $e = (a_1, \ldots, a_r) \in \mathscr{M}$ such that $a_i = a$. We set $f_i(a) = e$ if there is such hyperedge e and set $f_i(a)$ to an arbitrary hyperedge otherwise. The probability of winning for this strategy is

$$\sum_{e,a_1,\ldots,a_r} P^{\mathcal{G}}_{\mathbb{E}(\mathsf{A})_1\cdots\mathsf{A}_r}(e, a_1, \ldots, a_r) \times\delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D1}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e,a_1,\ldots,a_r} \delta[e = (a_1, \ldots, a_r))] \times\delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D2}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}} \delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D3}$$

$$\leqslant \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\ldots,a_r)\in\mathscr{M}} \delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D4}$$

$$= \frac{|\mathscr{M}|}{|\mathscr{E}|}, \tag{D5}$$

which implies that $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^{\mathcal{G}}} \geqslant \frac{\nu(\mathcal{G})}{|\mathscr{E}|}$.

To show the other direction, consider an arbitrary classical strategy described by functions $h_1, \ldots, h_r$. Define the subset

$$\mathscr{M} := \{e = (a_1, \ldots, a_r) \in \mathscr{E} : h_1(a_1) = \cdots = h_r(a_r) = e\}. \tag{D6}$$

To show that $\mathscr{M}$ is a matching, let $e = (a_1, \ldots, a_r)$ and $e' = (a'_1, \ldots, a'_r)$ be two distinct hyperedges in $\mathscr{M}$. Also suppose that $a_i = a'_i$ for some i. From the definition of $\mathscr{M}$, we have $e = h_i(a_i) = h_i(a'_i) = e'$ which contradicts the distinctness of e and e'. Therefore, e and e' differ in all vertices and $\mathscr{M}$ is a matching. Next, note that

$$\sum_{e,a_1,\ldots,a_r} P^{\mathcal{G}}_{\mathbb{E}(\mathsf{A})_1\cdots\mathsf{A}_r}(e, a_1, \ldots, a_r) \times\delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D7}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e,a_1,\ldots,a_r} \delta[e = (a_1, \ldots, a_r)] \times\delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D8}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}} \delta[h_1(a_1) = \cdots = h_r(a_r) = e] \tag{D9}$$

$$= \frac{|\mathscr{M}|}{|\mathscr{E}|}. \tag{D10}$$

Therefore, $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^{\mathcal{G}}} \leqslant \frac{\nu(\mathcal{G})}{|\mathscr{E}|}$.

We now prove Eq. (72). Let $Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}$ be a no-signaling strategy. For $e=(a_1,\dots,a_r)\in\mathscr{E}$, we define

$$g(e) := Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\dots,e|a_1,\dots,a_r). \tag{D11}$$

We have $g(e)\in[0,1]$ and for any $a\in\mathscr{A}_i$

$$\sum_{e=(a_1,\dots,a_r)\in\mathscr{E}:a_i=a} g(e) \tag{D12}$$

$$= \sum_{e=(a_1,\dots,a_r)\in\mathscr{E}:a_i=a} Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\dots,e|a_1,\dots,a_r) \tag{D13}$$

$$\leqslant \sum_{e=(a_1,\dots,a_r)\in\mathscr{E}:a_i=a} \sum_{e_1,\dots,e_{i-1},e_{i+1},\dots,e_r} \times Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e_1,\dots,e_{i-1},e,e_{i+1},\dots,e|a_1,\dots,a_r) \tag{D14}$$

$$= \sum_{e=(a_1,\dots,a_r)\in\mathscr{E}:a_i=a} Q_{\mathsf{E}_i|\mathsf{A}_1,\dots,\mathsf{A}_r}(e|a_1,\dots,a_r) \tag{D15}$$

$$\overset{(a)}{=} \sum_{e=(a_1,\dots,a_r)\in\mathscr{E}:a_i=a} Q_{\mathsf{E}_i|\mathsf{A}_i}(e|a) \tag{D16}$$

$$\overset{(b)}{\leqslant} 1, \tag{D17}$$

where (a) follows since $Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}$ is nonsignaling and (b) follows since $Q_{\mathsf{E}_i|\mathsf{A}_i}$ is a conditional probability distribution. Therefore, g is a fractional matching. We can upper bound the probability of winning for the no-signaling strategy $Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}$ as

$$\sum_{e,a_1,\dots,a_r} P^{\mathcal{G}}_{\mathsf{EA}_1\cdots\mathsf{A}_r}(e,a_1,\dots,a_r) \times Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\dots,e|a_1,\dots,a_r) \tag{D18}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\dots,a_r)} Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\dots,e|a_1,\dots,a_r) \tag{D19}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\dots,a_r)} g(e) \tag{D20}$$

$$\leqslant \frac{\nu_f(\mathcal{G})}{|\mathscr{E}|}, \tag{D21}$$

which completes the proof of Eq. (72).

APPENDIX E: PROOF OF LEMMA 2

We only prove the second statement since the first statement is a special case of the second statement for $d=1$. Let us consider an arbitrary quantum strategy $(\sigma_{\mathsf{A}'\mathsf{B}'},M,N)$ where $\mathcal{A}'=\mathcal{B}'=\mathbb{C}^d$, $\sigma_{\mathsf{A}'\mathsf{B}'}\in\mathrm{D}(\mathbb{C}^d\otimes\mathbb{C}^d)$, and $M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)$ and $N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)$ are two collections of POVMs. It achieves winning probability

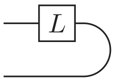
$$\sum_{x\in\mathscr{X},a\in\mathscr{A},b\in\mathscr{B}} P_{\mathsf{XAB}}(x,a,b)\mathrm{tr}[\sigma_{\mathsf{A}'\mathsf{B}'}M_x(a)\otimes N_x(b)]. \tag{E1}$$

Without loss of generality we can assume that $\sigma_{\mathsf{A}'\mathsf{B}'}$ is pure, i.e., there exists a unit vector $|\Psi\rangle_{\mathsf{A}'\mathsf{B}'}\in\mathbb{C}^d\otimes\mathbb{C}^d$ such that $\sigma_{\mathsf{A}'\mathsf{B}'}=|\Psi\rangle\langle\Psi|_{\mathsf{A}'\mathsf{B}'}$. Consider its Schmidt decomposition

$$|\Psi\rangle_{\mathsf{A}'\mathsf{B}'} = \sum_{i\in[d]}\sqrt{\lambda_i}|e_i\rangle\otimes|f_i\rangle, \tag{E2}$$

where $\lambda_0,\dots,\lambda_{d-1}$ are non-negative real numbers with $\sum_{i\in[d]}\lambda_i=1$, and $\{|e_i\rangle : i\in[d]\}$ and $\{|f_i\rangle : i\in[d]\}$ are orthonormal bases for $\mathbb{C}^d$. Alice and Bob can locally perform unitaries $U_{\mathsf{A}'}:|e_i\rangle\mapsto|i\rangle$ and $U_{\mathsf{B}'}:|f_i\rangle\mapsto|i\rangle$, respectively, prior to their measurement, where $|0\rangle,\dots,|d-1\rangle$ is the computational basis for $\mathbb{C}^d$. This operation does not change their probability of winning and, therefore, we can assume without loss of generality that

$$|\Psi\rangle_{\mathsf{A}'\mathsf{B}'} = \sum_{i\in[d]}\sqrt{\lambda_i}|i\rangle\otimes|i\rangle = \sum_{i\in[d]}L|i\rangle\otimes|i\rangle =$$



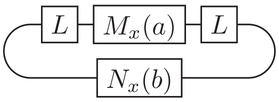
(E3)

where $L:=\sum_{i\in[d]}\sqrt{\lambda_i}|i\rangle\langle i|$ is the matrix whose vectorization is $|\Psi\rangle_{\mathsf{A}'\mathsf{B}'}$. We then have

$$\mathrm{tr}[|\Psi\rangle\langle\Psi|M_x(a)\otimes N_x(b)] \tag{E4}$$

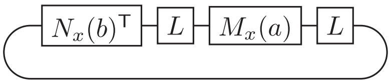
$$= \langle\Psi|(M_x(a)\otimes N_x(b))|\Psi\rangle \tag{E5}$$

$$=$$



(E6)

$$=$$



(E7)

$$= \mathrm{tr}[N_x(b)^\mathsf{T}LM_x(a)L] \tag{E8}$$

$$= \mathrm{tr}[\sqrt{L}N_x(b)^\mathsf{T}\sqrt{L}\sqrt{L}M_x(a)\sqrt{L}], \tag{E9}$$

where we used the cyclic property of trace and the "transpose trick" or "sliding" in graphical notation. Using Eq. (E9) and $P_{\mathsf{XAB}}=P_{\mathsf{X}}P_{\mathsf{A}|\mathsf{X}}P_{\mathsf{B}|\mathsf{X}}$, we can re-rewrite the probability of winning as

$$\sum_{x\in\mathscr{X},a\in\mathscr{A},b\in\mathscr{B}} P_{\mathsf{XAB}}(x,a,b)\mathrm{tr}[\sqrt{L}N_x(b)^\mathsf{T}\sqrt{L}\sqrt{L}M_x(a)\sqrt{L}]$$

$$= \sum_{x\in\mathscr{X}}P_{\mathsf{X}}(x)\times\mathrm{tr}\Bigg[\sqrt{L}\Bigg(\sum_{b\in\mathscr{B}}P_{\mathsf{B}|\mathsf{X}}(b|x)N_x(b)^\mathsf{T}\Bigg)\sqrt{L} \times\sqrt{L}\Bigg(\sum_{a\in\mathscr{A}}P_{\mathsf{A}|\mathsf{X}}(a|x)M_x(a)\Bigg)\sqrt{L}\Bigg]. \tag{E10}$$

Defining $Q_x:=\sum_{a\in\mathscr{A}}P_{\mathsf{A}|\mathsf{X}}(a|x)M_x(a)$ and $R_x:=\sum_{b\in\mathscr{B}}P_{\mathsf{B}|\mathsf{X}}(b|x)N_x(b)^*$, the winning probability is

$$\sum_{x\in\mathscr{X}}P_{\mathsf{X}}(x)\mathrm{tr}[\sqrt{L}R_x^\dagger\sqrt{L}\sqrt{L}Q_x\sqrt{L}]. \tag{E11}$$

The set $\mathcal{V}=\{F:\mathscr{X}\to L(\mathbb{C}^d)\}$ is a vector space and

$$\langle F,G\rangle := \sum_{x\in\mathscr{X}}P_{\mathsf{X}}(x)\mathrm{tr}[\sqrt{L}F(x)^\dagger\sqrt{L}\sqrt{L}G(x)\sqrt{L}], \quad \forall\, F,G\in\mathcal{V} \tag{E12}$$

defines an inner product on $\mathcal{V}$. Setting $F(x) := R_x$ and $G(x) := Q_x$, the probability of winning the game for distribution $P_{\mathsf{XAB}} = P_{\mathsf{X}} P_{\mathsf{A}|\mathsf{X}} P_{\mathsf{B}|\mathsf{X}}$ by using strategies N and M is $\langle F, G\rangle$. Note that $\langle F, F\rangle$ and $\langle G, G\rangle$ are the winning probabilities for quantum strategies $(\sigma_{\mathsf{A}'\mathsf{B}'}, M, M^*)$ and $(\sigma_{\mathsf{A}'\mathsf{B}'}, N^*, N)$, respectively. By Cauchy-Schwarz inequality, we have $|\langle F, G\rangle| \leqslant |\langle F, F\rangle|$ or $|\langle F, G\rangle| \leqslant |\langle G, G\rangle|$. Without loss of generality, assume that $|\langle F, G\rangle| \leqslant |\langle F, F\rangle|$. Then, the quantum strategy $(\sigma_{\mathsf{A}'\mathsf{B}'}, M, M^*)$ performs at least as well as an optimal strategy $(\sigma_{\mathsf{A}'\mathsf{B}'}, M, N)$, and satisfies the desired condition.

[1] C. W. Helstrom, J. Stat. Phys. **1**, 231 (1969).

[2] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).

[3] J. Bae and L.-C. Kwek, J. Phys. A: Math. Theor. **48**, 083001 (2015).

[4] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[6] S. Satyajit, K. Srinivasan, B. K. Behera, and P. K. Panigrahi, Quantum Inf. Proc. **17**, 212 (2018).

[7] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[9] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Commun. Math. Phys. **328**, 303 (2014).

[10] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).

[11] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, Commun. Math. Phys. **323**, 1121 (2013).

[12] A. Broadbent and S. Lord, in *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 158, edited by S. T. Flammia (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020), pp. 4:1–4:22.

[13] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[14] S. Aaronson, J. Liu, Q. Liu, M. Zhandry, and R. Zhang, in *Advances in Cryptology–Crypto 2021*, edited by T. Malkin and C. Peikert (Springer, Cham, 2021), pp. 526–555.

[15] A. Coladangelo, J. Liu, Q. Liu, and M. Zhandry, in *Advances in Cryptology–Crypto 2021*, edited by T. Malkin and C. Peikert (Springer, Cham, 2021), pp. 556–584.

[16] C. Majenz, C. Schaffner, and M. Tahmasbi, arXiv:2103.14510.

[17] C. Jordan, Bul. Soc. Math. France **3**, 103 (1873).

[18] J. Benítez and V. Rakočević, Appl. Math. Comput. **203**, 761 (2008).

[19] R. M. Karp, in *Proceedings of a Symposium on the Complexity of Computer Computations*, edited by R. E. Miller, J. W. Thatcher, and J. D. Bohlinger (Springer, Boston, 1972), pp. 85–103.

[20] Z. Füredi, Combinatorica **1**, 155 (1981).

[21] S. Wiesner, SIGACT News **15**, 78 (1983).

[22] S. Aaronson, in *24th Annual IEEE Conference on Computational Complexity* (IEEE, Piscataway, NJ, 2009), pp. 229–242.

[23] P. Ananth and R. L. La Placa, in *Advances in Cryptology–Eurocrypt 2021*, edited by A. Canteaut and F.-X. Standaert (Springer, Cham, 2021), pp. 501–530.

[24] A. Coladangelo, C. Majenz, and A. Poremba, arXiv:2009.13865.

[25] D. Gottesman, Quantum Inf. Comput. **3**, 581 (2003).

[26] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).

[27] O. Regev and T. Vidick, ACM Trans. Comput. Theory **7**, 1 (2015).

[28] W. Matthews, S. Wehner, and A. Winter, Commun. Math. Phys. **291**, 813 (2009).

[29] C. Lancien and A. Winter, Commun. Math. Phys. **323**, 555 (2013).

[30] L. Lami, C. Palazuelos, and A. Winter, Commun. Math. Phys. **361**, 661 (2018).

[31] E. Chitambar and L. Mančinska (private communication).

[32] P. Ananth, F. Kaleoglu, X. Li, Q. Liu, and M. Zhandry, in *Advances in Cryptology–CRYPTO 2022*, edited by Y. Dodis and T. Shrimpton (Springer, Cham, 2022), pp. 212–241.

[33] L. Escolà-Farràs, J. Has, M. Ozols, C. Schaffner, and M. Tahmasbi, arXiv:2211.06456.

[34] `https://github.com/mtahmasbi/lssd-codes`

[35] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[36] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, New J. Phys. **15**, 103002 (2013).

[37] H. Fawzi, Topics in convex optimisation, Lecture Notes at University of Cambridge (unpublished), https://www.damtp.cam.ac.uk/user/hf323/M18-OPT/index.html.

[38] G. Blekherman, P. A. Parrilo, and R. R. Thomas, *Semidefinite Optimization and Convex Algebraic Geometry* (Society for Industrial and Applied Mathematics, Philadelphia, 2012).