Entanglement-assisted guessing of complementary measurement outcomes

Mario Berta,[1] Patrick J. Coles,[2,3] and Stephanie Wehner[3,4]
[1]*Institute for Quantum Information and Matter, Caltech, Pasadena, California 91125, USA*
[2]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L3G1*
[3]*Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, 117543 Singapore*
[4]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands*
(Received 6 June 2013; published 22 December 2014)

Heisenberg's uncertainty principle implies that if one party (Alice) prepares a system and randomly measures one of two incompatible observables, then another party (Bob) cannot perfectly predict the measurement outcomes. This implication assumes that Bob does not possess an additional system that is entangled to the measured one; indeed, the seminal paper of Einstein, Podolsky, and Rosen (EPR) showed that maximal entanglement allows Bob to perfectly win this guessing game. Although not in contradiction, the observations made by EPR and Heisenberg illustrate two extreme cases of the interplay between entanglement and uncertainty. On the one hand, no entanglement means that Bob's predictions must display some uncertainty. Yet on the other hand, maximal entanglement means that there is no more uncertainty at all. Here we follow an operational approach and give an exact relation—an equality—between the amount of uncertainty as measured by the guessing probability and the amount of entanglement as measured by the recoverable entanglement fidelity. From this equality, we deduce a simple criterion for witnessing bipartite entanglement and an entanglement monogamy equality.

DOI: 10.1103/PhysRevA.90.062127 PACS number(s): 03.65.Ta, 03.65.Ud, 03.67.−a, 89.70.Cf

I. UNCERTAINTY RELATIONS

Heisenberg's uncertainty principle forms one of the fundamental elements of quantum mechanics. Originally proven for measurements of position and momentum, it is one of the most striking examples of the difference between a quantum and a classical world [1]. Uncertainty relations today are probably best known in the form given by Robertson [2], who extended Heisenberg's result to two arbitrary observables X and Z. More precisely, Robertson's relation states that when measuring the state $|\psi\rangle$ using either X or Z, one finds

$$\Delta X \Delta Z \geqslant \tfrac{1}{2}|\langle\psi|[X,Z]|\psi\rangle|, \tag{1}$$

where $\Delta Y = \sqrt{\langle\psi|Y^2|\psi\rangle - \langle\psi|Y|\psi\rangle^2}$ for $Y \in \{X,Z\}$ is the standard deviation resulting from measuring $|\psi\rangle$ with observable Y.

In the modern-day literature, uncertainty is usually measured in terms of entropies (starting with [3–5]; see [6] for a survey). One of the reasons this is desirable is that Eq. (1) makes no statement if $|\psi\rangle$ happens to give zero expectation on $[X,Z]$ [7]. To see how uncertainty can be quantified in terms of entropies, let us start with a simple example. Throughout, we let Alice (A) denote the system to be measured. For now, let us consider measuring a single qubit in the state ρ_A using two incompatible measurements given by the Pauli σ_x or σ_z eigenbases, and let K be the random variable associated with the measurement outcome. We have from [8] that for any state ρ_A,

$$H(K|\Theta) = \tfrac{1}{2}[H(K|\Theta=\sigma_x) + H(K|\Theta=\sigma_z)] \geqslant \tfrac{1}{2}, \tag{2}$$

where $H(K|\Theta=\theta) = -\sum_k p_{k|\Theta=\theta} \log p_{k|\Theta=\theta}$ is the Shannon entropy (all logarithms are base 2 in this article) of the probability distribution over measurement outcomes $k \in \{0,1\}$ when we perform the measurement labeled θ on the state ρ_A, and each measurement is chosen with probability $p_\theta = 1/2$. To see that this is an uncertainty relation, note that if one of the two entropies is zero, then (2) tells us that the other is necessarily nonzero, i.e., there is at least some amount of uncertainty. If we measure a d_A-dimensional system A in two orthonormal bases $\theta_0 = \{|x_0\rangle\}_{x=1}^{d_A}$ and $\theta_1 = \{|x_1\rangle\}_{x=1}^{d_A}$, then the right-hand side (r.h.s.) of (2) becomes $\log(1/c)$, where $c = \max_{x_0,x_1} |\langle x_0|x_1\rangle|^2$. The largest amount of uncertainty, i.e., the largest $\log(1/c)$, is thereby obtained when $|\langle x_0|x_1\rangle| = 1/\sqrt{d_A}$, that is, the two bases are mutually unbiased (MUB) [9].

When thinking about uncertainty, it is often illustrative to adopt an adversarial perspective and consider an "uncertainty game" [10], commonly used in quantum cryptography [11]. In particular, we will think about uncertainty from the perspective of an observer called Bob holding a second system (B) whose task is to guess the outcome of the measurement on Alice's system successfully. Bob thereby knows ahead of time what measurements could be made and the probability that a particular measurement setting is chosen. To help him win the game, Bob may even prepare ρ_A himself, and Alice tells him which measurement she performed before he has to make his guess. The amount of uncertainty as measured by entropies can be understood as a limit on how well Bob can guess Alice's measurement outcome—the more difficult it is for Bob to guess, the more uncertain Alice's measurement outcomes are. If Bob is not entangled with A but only keeps classical information about the state, such as for example a description of the density operator ρ_A, then (2) still holds even if we condition on Bob's classical information B [12]. More precisely, we have $H(K|\Theta B_{\text{classical}}) \geqslant 1/2$ for any states or distribution of states that Bob may prepare.

II. UNCERTAINTY AND ENTANGLEMENT

Another central element of quantum mechanics is the possibility of entanglement, and examples suggest that there

 ©2014 American Physical Society

is a strong interplay between entanglement and uncertainty. In particular, Einstein, Poldolsky, and Rosen (EPR) [13] observed that if Bob is maximally entangled with A, then his uncertainty can be reduced dramatically. To see this, imagine that $\rho_{AB} = |\Phi\rangle\langle\Phi|$ where $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is the maximally entangled state between A and B. Since $|\Phi\rangle$ is maximally correlated in both the σ_x and σ_z eigenbases, Bob can simply measure his half of the EPR pair in the same basis as Alice to predict her measurement outcome perfectly, winning the guessing game described above. This is precisely the effect observed in [13] and highlights that the uncertainty relations of (1) and (2) do not capture the interplay between entanglement and uncertainty in the general two-party guessing game. Fortunately, it is possible to extend the notion of uncertainty relations to take the possibility of entanglement into account [14]. Such relations are known as uncertainty relations with quantum side information (here B). More precisely, it was shown [10] that if we measure A in two bases labeled θ_0,θ_1, then

$$H(K|B\Theta) = \tfrac{1}{2}[H(K|B\Theta = \theta_0) + H(K|B\Theta = \theta_1)] \geqslant \log(1/c) + H(A|B), \quad (3)$$

where $H(A|B)$ is the conditional von Neumann entropy of A given B. If A and B are entangled, then $H(A|B)$ can be negative. Indeed, $H(A|B) = -\log d_A$ when ρ_{AB} is the maximally entangled state, in which case the lower bound in (3) becomes trivial. The uncertainty relation of (3) thus allows for the possibility that Bob's uncertainty could be reduced in the presence of entanglement. It also provides us with a first clue to the relation between entanglement and uncertainty in one direction, namely, that little uncertainty [i.e., $H(K|B\Theta)$ is small] implies that $H(A|B)$ must be negative and hence ρ_{AB} is entangled [15]. As such, (3) is useful for the task of witnessing entanglement [16,17].

Many more similar relations have since been proven for more than two measurements on Alice's system, and in terms of other forms of entropies. One entropy measure that is of central importance in cryptography is the conditional min-entropy $H_{\min}$, and it yields a more immediate link between uncertainty relations with quantum side information and the uncertainty game mentioned above. Specifically, it was shown [18] that if we measure A in one of $d_A + 1$ possible mutually unbiased bases chosen uniformly at random, then

$$H_{\min}(K|B\Theta) \gtrsim \log d_A + \min\{0, H_{\min}(A|B)\}. \quad (4)$$

[More precisely, smoothing of the entropies is required for (4) to hold, and hence the symbol $\gtrsim$ refers to an additional term that depends on the smoothing.] With K being a classical random variable, the conditional min-entropy $H_{\min}(K|B\Theta) = -\log P_{\text{guess}}(K|B\Theta)$ is simply derived from the maximum probability that Bob can guess K, averaged over the choice of basis θ [19]. That is, it captures exactly how well Bob can guess Alice's measurement outcome K by performing a measurement on B. The fully quantum conditional min-entropy $H_{\min}(A|B)$ has the operational interpretation $H_{\min}(A|B) = -\log[d_A F(A|B)]$, with

$$F(A|B) = \max_{\Lambda_{B\to A'}} F(\Phi_{AA'}, \mathcal{I}_A \otimes \Lambda_{B\to A'}(\rho_{AB})), \quad (5)$$

where $F(\rho,\sigma) = (\text{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2$ is Uhlmann's fidelity [20], $\Phi_{AA'} = |\Phi_{AA'}\rangle\langle\Phi_{AA'}|$, and $|\Phi_{AA'}\rangle = (1/\sqrt{d_A})\sum_{j=1}^{d_A} |j\rangle_A|j\rangle_{A'}$ is the maximally entangled state between A and A' [19]. In other words, the conditional min-entropy $H_{\min}(A|B)$ measures how close one can bring a bipartite quantum state ρ_{AB} to the maximally entangled state by performing an arbitrary operation Λ on the B system. Recall from the example above that Bob can win the uncertainty game perfectly if ρ_{AB} really is maximally entangled. Intuitively, the conditional min-entropy thus measures how far away Bob is from this scenario. Needless to say, one could write similar statements for Rényi entropies other than the min-entropy, but these are, in fact, equivalent up to small error terms.

Do these relations resolve the question of how uncertainty relates to entanglement? Note that the uncertainty relation (4) again provides us with a relation between entanglement and uncertainty in one direction. In particular, it tells us that if it is easy for Bob to guess Alice's measurement outcome [$H_{\min}(K|B\Theta)$ is small], then there really exists some map $\Lambda_{B\to A'}$ that Bob can use to bring ρ_{AB} at least somewhat close to being maximally entangled with A. That is, it tells us that a reduction in uncertainty implies the presence of entanglement. However, it does not tell us that the presence of entanglement really does lead to a significant reduction in uncertainty. Of course, if ρ_{AB} is close to the maximally entangled state, then uncertainty is reduced by at least some amount because two states which are close yield similar statistics when measured. Yet we will see below that this alone is insufficient for our purpose.

III. MAIN RESULT

Here, we prove the following finite-dimensional equality if we measure A in one of $d_A + 1$ possible mutually unbiased bases with uniformly random probability

$$H_2(K|B\Theta) = \log(d_A + 1) - \log\left(2^{-H_2(A|B)} + 1\right), \quad (6)$$

where

$$H_2(A|B) = -\log \text{Tr}[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}] \quad (7)$$

is the conditional Rényi 2-entropy used in quantum cryptography (see, e.g., [21,22]), and K is the classical measurement outcome obtained by measuring A in the basis labeled $\Theta = \theta$. Since K is a classical random variable, the Rényi 2-entropy $H_2(K|B\Theta)$ has an operational interpretation as given by the probability that Bob manages to guess Alice's measurement outcome K using the pretty good measurement [23,24] after he learns which measurement Θ was made: $H_2(K|B\Theta) = -\log P^{\text{pg}}_{\text{guess}}(K|B\Theta)$. For the fully quantum Rényi 2-entropy $H_2(A|B)$, we prove (see Appendix A) that

$$H_2(A|B) = -\log[d_A F^{\text{pg}}(A|B)], \quad (8)$$

with

$$F^{\text{pg}}(A|B) = F\left(\Phi_{AA'}, \mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'}(\rho_{AB})\right), \quad (9)$$

where Λ^{pg} is the pretty good recovery map [25]. [We denote by $\Phi_{AA'}$ the normalized maximally entangled state, and hence a factor d_A appears in (8).] Both the pretty good

measurement and the pretty good recovery map get very close to the performance of the optimal processes [24,25]. For the special case $\rho_{AB} = \rho_A \otimes \rho_B$, (6) becomes an equation relating unconditional entropies that was discussed in [26,27] and used to derive uncertainty relations for Shannon entropies (see [6] for an overview). Furthermore, the conditional Rényi 2-entropy also appears in the study of randomness extractors against quantum side information (see, e.g., [22,28]), and in its quantum counterpart decoupling (see, e.g., [29,30]).

We mention that the existence of a full set of MUBs is only known in prime power dimension [31,32], but we show in Appendix D 1 that our main result (6) also holds for informationally complete positive operator valued measures (SIC-POVMs) and unitary 2-designs. For the latter, efficient constructions are known in any dimension [33,34], and in particular the set of all bases defines a unitary 2-design.

Our relation (6) establishes an equivalence between uncertainty as measured by $H_2(K|B\Theta)$ and our ability to recover entanglement as given by $H_2(A|B)$. It is an operational way to merge the observations of EPR and Heisenberg into a single equation, demonstrating that both effects can be seen as flip sides of the same coin.

IV. DISCUSSION

A. Operational examples

To gain further intuition about (6), let us first return to the uncertainty game discussed earlier. Note that in terms of the operational interpretations of the conditional Rényi 2-entropy, we can rewrite (6) as

$$P^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta) = \frac{1}{d_A+1}\sum_{\theta} P^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta=\theta) = \frac{d_A F^{\mathrm{pg}}(A|B)+1}{d_A+1}. \tag{10}$$

In the game, Bob prepares a state ρ_{AB} and sends the A system to Alice. She measures A in one basis chosen uniformly at random from the complete set of d_A+1 MUBs, and announces the basis (the index θ) to Bob. Bob's task is to guess Alice's outcome using the pretty good measurement on B. Equation (10) says that Bob's ability to win or lose this game is quantitatively connected to the recoverable entanglement fidelity of ρ_{AB}, as measured by $F^{\mathrm{pg}}(A|B)$.

Let us consider a number of special cases that illustrate this concept. In what follows, we refer to $H_2(A|B) \geqslant 0$ as the Heisenberg-limited regime and $H_2(A|B) < 0$ as the enhanced regime. As we will see below, this terminology refers to two distinct regimes, one in which Bob's guessing probability is restricted by a Heisenberg-like uncertainty relation [see Eq. (11)], and the other in which his guessing probability can be enhanced beyond this restriction (although, of course, not in violation of the uncertainty principle). For example, if ρ_{AB} is the maximally entangled state, we have $F^{\mathrm{pg}}(A|B) = 1$ and Bob can guess Alice's measurement outcome perfectly regardless of which measurement she performs, i.e., $P^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta=\theta) = 1$ for all θ. That is, there is no uncertainty, as expected. If Bob prepares ρ_{AB} with less than maximal entanglement, then $F^{\mathrm{pg}}(A|B) < 1$ and there will be at least one basis for which Bob cannot perfectly guess the outcome. Thus, there is at least some amount of uncertainty expressed quantitatively as $H_2(K|B\Theta)$. If ρ_{AB} is separable, then Bob is stuck in the Heisenberg-limited regime ($F^{\mathrm{pg}} \leqslant 1/d_A$) and his ability to guess is very poor, constrained by the uncertainty relation

$$P^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta) \leqslant 2/(d_A+1). \tag{11}$$

This illustrates that entanglement is necessary for Bob to gain an advantage in the guessing game.

B. Uncertainty and certainty relations

One might ask why we formulate our uncertainty equality (6) using a full set of d_A+1 MUBs and not fewer measurements. To answer this, it is instructive to study what kind of relations our main result (6) implies. On the one hand, we can deduce regular uncertainty relations and, e.g., we get a relation in terms of the smooth conditional min-entropy similar to [18],

$$H^{\varepsilon}_{\min}(K|\Theta B) \geqslant \log(d_A+1) - \log(2^{-H_{\min}(A|B)}+1) - 1 - 2\log\frac{1}{\epsilon}, \tag{12}$$

where $\epsilon > 0$ denotes a small error term (see Appendix C 2 for details). Here, the left-hand side has the operation meaning of minus the logarithm of Bob's guessing probability (up to error ϵ) when Alice measures in one of d_A+1 possible MUBs chosen uniformly at random. But, on the other hand, we also get relations that upper bound the uncertainties of incompatible observables. In the literature, these are known as certainty relations [35,36], and here we give such relations that allow for quantum side information. For example, we get, in terms of the conditional min-entropy (again up to a small error term $\epsilon > 0$),

$$H_{\min}(K|\Theta B) \leqslant \log(d_A+1) - \log\left(2^{-H^{\epsilon}_{\min}(A|B)} + \frac{2}{\epsilon^2}\right) + 1 + 2\log\frac{1}{\epsilon}. \tag{13}$$

This says that Bob's certainty, i.e., his ability to guess Alice's measurement outcome, must be high if he is highly entangled to Alice as measured by the smooth conditional min-entropy. Like our main result, (13) implies that if Alice and Bob are maximally entangled, Bob has perfect certainty about Alice's outcomes regardless of which measurement she performs.

Now there is a simple argument that considering less than a complete set of MUBs, a so-called extendable set (where there exists an MUB that could be added to the set), implies that only trivial certainty relations can hold. As uncertainty equalities as in (6) imply nontrivial certainty relations, such equalities cannot hold for extendable sets. This is in sharp contrast to uncertainty relations, where nontrivial relations can be obtained for just two measurements. To see this, consider the case where ρ_A is just one qubit and we perform measurements in the σ_X and σ_Z eigenbases, respectively. Hence, B is trivial, $H_{\min}(K|\Theta B) = H_{\min}(K|\Theta)$, and we just consider the entropy of the outcome distribution of measuring ρ_A in one of the two bases. In terms of the uncertainty game discussed before, this means that Bob can only choose the state ρ_A in order to guess the outcome of the measurement on Alice's system (but is not

allowed to keep any quantum information B about A). Clearly, when ρ_A is an eigenstate of σ_Y, the outcome distribution for both σ_X and σ_Z is uniform and hence $H_{\min}(K|\Theta) = 1$, which is the maximum value. This argument generalizes to any extendable set of MUBs, since there exists a state (from another MUB) that has $H_{\min}(K|\Theta) = \log d_A$ which is the maximum value that it can take and hence only the trivial upper bound or certainty relation holds. It is thus clear that equalities such as (6) can only hold for sets of measurements that are sufficiently rich.

C. Bounds for fewer bases

Even though there does not exist an uncertainty equality for measuring in less than $d_A + 1$ MUBs, we can still give lower (and trivial upper) bounds for Bob's uncertainty about $1 \leqslant n \leqslant d_A$ MUBs on A in terms of the recoverable entanglement fidelity between A and B. Moreover, these inequalities are tight for all n; that is, fixing the set of measurements, there exist states that achieve the upper and lower bounds. Our relations are again in terms of the conditional Rényi 2-entropy. Using $P^{\text{pg}}_{\text{guess}}(n)$ as a shorthand to denote Bob's guessing probability $P^{\text{pg}}_{\text{guess}}(K|B\Theta)$ when Alice does measurements in a subset of size n of a complete set of MUBs, we find that the following bounds are tight in the Heisenberg-limited regime $[F^{\text{pg}}(A|B) \leqslant 1/d_A]$:

$$\frac{1}{d_A} \leqslant P^{\text{pg}}_{\text{guess}}(n) \leqslant \frac{d_A}{n} F^{\text{pg}}(A|B) + \frac{n-1}{nd_A}. \tag{14}$$

Moreover, the following bounds are tight in the enhanced regime $[F^{\text{pg}}(A|B) > 1/d_A]$:

$$F^{\text{pg}}(A|B) \leqslant P^{\text{pg}}_{\text{guess}}(n) \leqslant \frac{n-1}{n} F^{\text{pg}}(A|B) + \frac{1}{n}. \tag{15}$$

Here, the upper bounds (lower bounds) can be thought of as uncertainty relations (certainty relations). Note that we can derive these tight relations for all n directly from our main result. Taken together, (14) and (15) completely characterize the allowable range of values that $P^{\text{pg}}_{\text{guess}}(n)$ can attain. As an example, consider $d_A = 5$. Figure 1 plots the tight upper and lower bounds as a function of $F^{\text{pg}}(A|B)$. Notice that the (trivial) lower bound does not change as n varies from 1 to 5; it only increases when we include the sixth basis. This is consistent with our discussion in the previous section, where we noted that a nontrivial certainty relation, i.e., a relation stronger than the certainty relation one obtains for a single basis, requires sufficiently rich sets of measurements. In contrast, the tight upper bound steadily decreases with n, reflecting the complementarity between the different bases. Overall, as n increases from 1 to 6, the area of the allowed range monotonically shrinks towards zero, and the allowed area becomes zero for $n = 6$ since the two quantities $P^{\text{pg}}_{\text{guess}}(n)$ and $F^{\text{pg}}(A|B)$ are deterministically related by our main result.

From Fig. 1, one can also see that if Bob can guess two MUBs on A well, then he can also guess $d_A + 1$ MUBs on A fairly well. Conceptually, this follows from a two-step chain of reasoning: if Bob's uncertainty is low for two MUBs, then he must be entangled to Alice, which in turn implies that he must have a low uncertainty for all bases. So entanglement provides the key link, from two MUBs to all bases. From

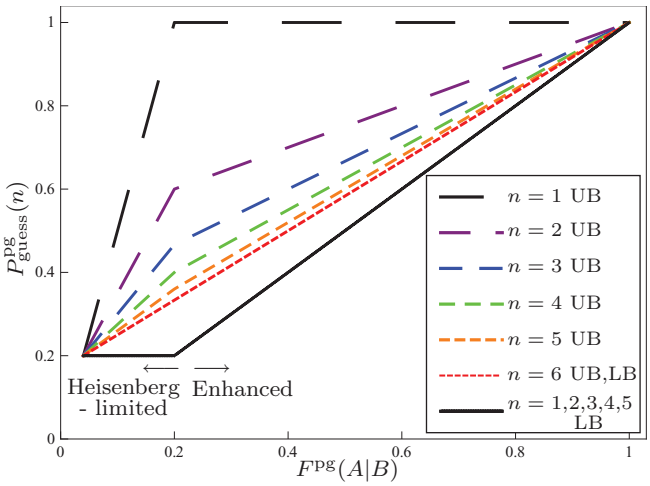


FIG. 1. (Color online) Upper bounds (UB) and lower bounds (LB) on $P^{\text{pg}}_{\text{guess}}(n)$ as a function of $F^{\text{pg}}(A|B)$ for $d_A = 5$, for various values of n. For $n = 1,2,3,4,5$, the (trivial) lower bound is given by the solid black line. The upper bounds for these values of n are, respectively, the black, purple, blue, green, and orange dashed lines. For $n = 6$, the upper and lower bounds coincide, i.e., the allowed values are confined to live on the red dashed line. The regions where $H_2(A|B) \geqslant 0$ and $H_2(A|B) < 0$ are labeled "Heisenberg-limited" and "enhanced," respectively.

the above results, it is straightforward to derive the following quantitative statement of this idea:

$$P^{\text{pg}}_{\text{guess}}(d_A + 1) \geqslant \frac{d_A\left[2P^{\text{pg}}_{\text{guess}}(2) - 1\right] + 1}{d_A + 1}, \tag{16}$$

which says that as $P^{\text{pg}}_{\text{guess}}(2) \to 1$, then $P^{\text{pg}}_{\text{guess}}(d_A + 1) \to 1$.

D. Applications in quantum information theory

We briefly discuss some applications of our main result to quantum information processing tasks. Because entanglement is crucial for several quantum information technologies, the experimenter often needs a method to verify that their source is indeed producing entangled pairs, i.e., an "entanglement witness." Following [10,37–39], our main result offers a simple strategy for witnessing entanglement since it connects entanglement to uncertainty, which is experimentally measurable. In particular, Alice and Bob (in their distant laboratories, receiving A and B, respectively) can sample from the source multiple times and communicate their results to gather statistics, say, regarding the K_θ observable on A and the L_θ observable on B. Suppose they do this for a set of n MUBs $\{K_\theta\}_{\theta=1}^n$ on A, with Bob measuring in some arbitrary set of n bases $\{L_\theta\}_{\theta=1}^n$ on B. They then estimate the joint probability distribution for each pair $\{K_\theta, L_\theta\}$, and hence they can evaluate the classical entropies $H_2(K_\theta|L_\theta)$. According to our main result, their source is necessarily entangled if

$$\sum_{\theta=1}^{n} 2^{-H_2(K_\theta|L_\theta)} > 1 + \frac{n-1}{d_A}. \tag{17}$$

Note that this method offers the flexibility of witnessing entanglement with $2 \leqslant n \leqslant d_A + 1$ observables (see also [40]

for a different approach). For $n = 2$, the same strategy based on the uncertainty relation (3) was implemented in [16,17].

Another application of our main result is to quantum error correction of noisy quantum channels. By viewing (6) from the dynamic perspective of Alice sending states through a quantum channel to Bob, and noting that the entanglement fidelity such as that appearing in (8) is a standard figure of merit for quantum error correction, we see from (6) that Bob's ability to error correct is quantitatively linked to his ability to guess which states Alice sends, when she is sending basis elements from a complete set of MUBs.

Our uncertainty equality (6) also gives insight for studying the monogamy of correlations. The basic idea of monogamy is that A's entanglement with B limits the degree to which A can be entangled with a third system, E. There have been several statements of monogamy in the literature; however, a nice aspect of our results is the potential to state monogamy as an equation rather than an inequality. We show that for any tripartite pure state ρ_{ABE},

$$\inf_{\sigma} D_{\frac{1}{2}}\left(\rho_{AE}\|\frac{\mathbb{1}_A}{d_A}\otimes\sigma_E\right) = \log d_A - \log\left[(d_A+1)P^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta)-1\right], \tag{18}$$

where the infimum is over all quantum states σ_E, and $D_{\frac{1}{2}}$ denotes the relative Rényi 1/2-entropy (see Appendix B 3 for details). This relation states that Bob's guessing probability for a complete set of Alice's MUBs is a quantitative measure of the distance of ρ_{AE} (Alice's and Eve's state) to a completely uncorrelated state. According to (18), Bob and Eve fight in a "zero-sum game" to be correlated to Alice, i.e., any gain of knowledge about Alice's system by Bob forces Eve's state to get closer to being uncorrelated with Alice, and conversely any gain of distance from the uncorrelated state by Eve forces Bob to lose knowledge.

Finally, we remark that the conditional Rényi 2-entropy is an important quantity in the study of classical and quantum randomness extractors against quantum side information (see, e.g., [28,29]). Since our uncertainty equality (6) connects the conditional Rényi 2-entropy of the premeasurement state to the conditional Rényi 2-entropy of the postmeasurement state, our main result (6) shines some light on the relation between classical and quantum extractors. It can be used to get a new perspective on the results in [18], where security of the noisy storage model [41] was first linked to the quantum capacity.

E. Conclusions

In summary, we considered a two-party guessing game, where Alice measures her system A in one of n possible complementary observables and Bob uses his system B to help him guess Alice's outcome. We showed that Bob's probability for winning this game, assuming he does the "pretty good measurement" on B, is connected through an equality for $n = d_A + 1$ (inequality for $n < d_A + 1$) to the prior entanglement between B and A. The latter is measured by the entanglement fidelity that can be recovered with the "pretty good recovery map," which we proved is given by the conditional Rényi 2-entropy. We therefore showed that our operationally motivated equality can be thought of as an entropic uncertainty relation and, as such, connects Heisenberg's uncertainty principle to EPR's guessing game via an equation. We expect our approach to inspire further quantitative relations capturing the connection between uncertainty and entanglement. In addition, it would be interesting to explore the connection between the guessing game considered here and other nonlocal uncertainty games that have been considered in the literature, e.g., in the context of Bell inequalities [42] and steering [43,44].

ACKNOWLEDGMENTS

P.J.C. thanks Jędrzej Kaniewski for helpful discussions. P.J.C. and S.W. acknowledge funding from the Ministry of Education (MOE) and National Research Foundation Singapore, as well as MOE Tier 3 Grant "Random numbers from quantum processes" (Grant No. MOE2012-T3-1-009).

APPENDIX A: QUANTITATIVE MEASURES

1. Entanglement

Despite not being monotonic under local operations and classical communication, conditional entropies play an important role in entanglement theory [45]. For example, the conditional von Neumann entropy $H(A|B)$ quantifies the asymptotic rate for distilling EPR pairs via a one-way hashing protocol [15]. Another important conditional entropy studied in cryptography is the min-entropy. It was originally defined in an abstract form [22], but was later given an intuitive operational meaning [19] in terms of the recoverable entanglement fidelity, i.e., $H_{\min}(A|B) = -\log[d_A F(A|B)]$ with

$$F(A|B) = \max_{\Lambda_{B\to A'}} F(\Phi_{AA'},(\mathcal{I}_A\otimes\Lambda_{B\to A'})(\rho_{AB})), \tag{A1}$$

where the maximum is over all quantum operations $\Lambda_{B\to A'}$ with A' a copy of A. (See, e.g., [46] for discussion of the importance of the entanglement fidelity in quantum information theory.)

A related entropy measure is the conditional Rényi 2-entropy, which is defined as

$$H_2(A|B) = -\log \mathrm{Tr}[\rho_{AB}(\mathbb{1}_A\otimes\rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A\otimes\rho_B)^{-1/2}]. \tag{A2}$$

Here we give an operational meaning for the conditional Rényi 2-entropy by showing that like the conditional min-entropy, it is linked to the recoverable entanglement fidelity in that $H_2(A|B) = -\log[d_A F^{\mathrm{pg}}(A|B)]$, with

$$F^{\mathrm{pg}}(A|B) = F\left(\Phi_{AA'},\mathcal{I}_A\otimes\Lambda^{\mathrm{pg}}_{B\to A'}(\rho_{AB})\right), \tag{A3}$$

and $\Lambda^{\mathrm{pg}}_{B\to A'}$ is the pretty good recovery map. To see this, we note that the pretty good recovery map can be written as

$$\Lambda^{\mathrm{pg}}_{B\to A'}(\cdot) = \frac{1}{d_A}\mathcal{E}^{\dagger}_{B\to A'}\left(\rho_B^{-1/2}(\cdot)\rho_B^{-1/2}\right), \tag{A4}$$

where $\mathcal{E}^{\dagger}_{B\to A'}$ denotes the adjoint of the Choi-Jamilkowski map of ρ_{AB},

$$\mathcal{E}_{A\to B}(\cdot) = d_A \mathrm{Tr}_A\{[(\cdot)^T\otimes\mathbb{1}_B]\rho_{AB}\}. \tag{A5}$$

Putting this in (A2), we arrive at (A3). The map $\Lambda^{\mathrm{pg}}_{B\to A'}$ is pretty good in the sense that it is close to optimal for recovering the

maximally entangled state, i.e., we have [25]

$$F^2(A|B) \leqslant F^{\mathrm{pg}}(A|B) \leqslant F(A|B). \tag{A6}$$

We also remark that both $F(A|B)$ and $F^{\mathrm{pg}}(A|B)$ are nonincreasing under the action of local quantum channels acting on system B and local unital (identity-preserving) quantum channels acting on system A (see, e.g., [21]).

2. Uncertainty

When measuring a bipartite quantum state ρ_{AB} on A in some basis $K = \{|k\rangle\}$, we arrive at a classical-quantum state,

$$\rho_{KB} = \sum_k (|k\rangle\langle k| \otimes \mathbb{1}_B)\rho_{AB}(|k\rangle\langle k| \otimes \mathbb{1}_B) \tag{A7}$$

$$= \sum_k |k\rangle\langle k| \otimes \rho_B^k. \tag{A8}$$

The conditional min-entropy of ρ_{KB}, using the formula for $F(K|B)$ from (A1), translates to $H_{\min}(K|B) = -\log P_{\mathrm{guess}}(K|B)$, with

$$P_{\mathrm{guess}}(K|B) = \max_{\{E_B^k\}} \sum_k \mathrm{Tr}\left[E_B^k \rho_B^k\right] \tag{A9}$$

the probability for guessing K correctly by performing the optimal measurement $\{E_B^k\}$ on the quantum side information B. The conditional min-entropy quantifies the uncertainty of K in the exact sense of the uncertainty game, namely, it quantifies the probability that Bob wins the uncertainty game.

The conditional Rényi 2-entropy of a classical-quantum state is again defined as in (A2). Furthermore, it was shown in [23] that its operational form (A3) is given by

$$H_2(K|B) = -\log P_{\mathrm{guess}}^{\mathrm{pg}}(K|B), \tag{A10}$$

where $P_{\mathrm{guess}}^{\mathrm{pg}}(K|B)$ denotes the probability of guessing K by performing the pretty good measurement [24]. For the classical-quantum state (A7), the pretty good measurement operators are defined as

$$\Pi_B^k = \rho_B^{-1/2}\rho_B^k\rho_B^{-1/2}. \tag{A11}$$

By calculating $P_{\mathrm{guess}}^{\mathrm{pg}}(K|B) = \sum_k \mathrm{Tr}[\Pi_B^k \rho_B^k]$, the equivalence of (A10) to the definition of the conditional Rényi 2-entropy in (A2) can be seen. Hence, the conditional Rényi 2-entropy corresponds to the probability that Bob wins the uncertainty game by using the pretty good measurement. It is known that the pretty good measurement performs close to optimal, i.e., analogous to (A6), we have [24]

$$P_{\mathrm{guess}}^2(K|B) \leqslant P_{\mathrm{guess}}^{\mathrm{pg}}(K|B) \leqslant P_{\mathrm{guess}}(K|B). \tag{A12}$$

In the following, we will not only measure in one fixed basis, but with equal probability in one of $d_A + 1$ MUBs. For that reason, we will work with the state

$$\rho_{KB\Theta} = \frac{1}{d_A+1}\sum_{\theta=1}^{d_A+1}\sum_{k=1}^{d_A}(|\theta_k\rangle\langle\theta_k| \otimes \mathbb{1}_B) \times \rho_{AB}(|\theta_k\rangle\langle\theta_k| \otimes \mathbb{1}_B) \otimes |\theta\rangle\langle\theta|_\Theta, \tag{A13}$$

where the elements of the $d_A + 1$ MUBs θ are denoted by $\{|\theta_k\rangle\}$. It is straightforward to see that

$$P_{\mathrm{guess}}^{\mathrm{pg}}(K|B\Theta) = \frac{1}{d_A+1}\sum_\theta P_{\mathrm{guess}}^{\mathrm{pg}}(K|B\Theta = \theta). \tag{A14}$$

APPENDIX B: PROOF OF MAIN RESULTS

1. Full set of mutually unbiased bases

Here we prove our main result, the uncertainty equality (6). For this, we define $\tilde{\rho}_{AB} = (\mathbb{1}_A \otimes \rho_B^{-1/4})\rho_{AB}(\mathbb{1}_A \otimes \rho_B^{-1/4})$ and rewrite the fully quantum conditional Rényi 2-entropy as $H_2(A|B) = -\log \mathrm{Tr}[\tilde{\rho}_{AB}^2]$. Similarly, we rewrite the classical-quantum conditional Rényi 2-entropy as

$$H_2(K|B\Theta) = -\log\left(\frac{1}{d_A+1}\sum_{\theta,k}\mathrm{Tr}_B\{\mathrm{Tr}_A[\tilde{\rho}_{AB}(|\theta_k\rangle\langle\theta_k| \otimes \mathbb{1}_B)]^2\}\right). \tag{B1}$$

Now we introduce the space $\mathcal{H}_{A'B'} \cong \mathcal{H}_{AB}$ as well as the state $\tilde{\rho}_{A'B'} \cong \tilde{\rho}_{AB}$. We have

$$(d_A+1)\times 2^{-H_2(K|B\Theta)} = \sum_{\theta,k}\mathrm{Tr}_B\{\mathrm{Tr}_A[(|\theta_k\rangle\langle\theta_k| \otimes \mathbb{1}_B)\tilde{\rho}_{AB}]\mathrm{Tr}_A[(|\theta_k\rangle\langle\theta_k| \otimes \mathbb{1}_B)\tilde{\rho}_{AB}]\} \tag{B2}$$

$$= \sum_{\theta,k}\mathrm{Tr}_{BB'}\mathrm{Tr}_{AA'}[(|\theta_k\rangle\langle\theta_k| \otimes |\theta_k\rangle\langle\theta_k|)(\tilde{\rho}_{AB} \otimes \tilde{\rho}_{A'B'})F_{BB'}] \tag{B3}$$

$$= \mathrm{Tr}_{BB'}\mathrm{Tr}_{AA'}[(I_{AA'} + F_{AA'})(\tilde{\rho}_{AB} \otimes \tilde{\rho}_{A'B'})F_{BB'}] \tag{B4}$$

$$= \mathrm{Tr}_{BB'}\mathrm{Tr}_{AA'}[(\tilde{\rho}_{AB} \otimes \tilde{\rho}_{A'B'})F_{BB'}] + \mathrm{Tr}_{BB'}\mathrm{Tr}_{AA'}[F_{AA'}(\tilde{\rho}_{AB} \otimes \tilde{\rho}_{A'B'})F_{BB'}] \tag{B5}$$

$$= \mathrm{Tr}_B[\mathrm{Tr}_A(\tilde{\rho}_{AB})\mathrm{Tr}_A(\tilde{\rho}_{AB})] + \sum_{t,s}\mathrm{Tr}_{BB'}\mathrm{Tr}_{AA'}[(|t\rangle\langle s| \otimes |s\rangle\langle t| \otimes \mathbb{1}_{BB'})(\tilde{\rho}_{AB} \otimes \tilde{\rho}_{A'B'})F_{BB'}] \tag{B6}$$

$$= 1 + \sum_{t,s}\mathrm{Tr}_B\{\mathrm{Tr}_A[(|t\rangle\langle s| \otimes \mathbb{1})\tilde{\rho}_{AB}]\mathrm{Tr}_A[(|s\rangle\langle t| \otimes \mathbb{1})\tilde{\rho}_{AB}]\} \tag{B7}$$

$$= 1 + \mathrm{Tr}\left[\tilde{\rho}_{AB}^2\right], \tag{B8}$$

where $F_{AA'} = \sum_{t,s}|t\rangle\langle s| \otimes |s\rangle\langle t|$ is the operator that swaps A and A' (similarly for $F_{BB'}$). The second line uses the "swap trick," for operators M and N, and swap operator F: $\mathrm{Tr}(MN) = \mathrm{Tr}[(M \otimes N)F]$. The third line invokes that a full set of MUBs generates

a complex projective 2-design [47], that is,

$$\sum_{\theta,k} |\theta_k\rangle\langle\theta_k| \otimes |\theta_k\rangle\langle\theta_k| = I_{AA'} + F_{AA'}. \tag{B9}$$

In Appendix D 1, we show that our result also holds for other measurements as long as they form a complex projective 2-design.

2. Fewer bases

Here, we derive the upper and lower bounds (14) and (15) on the uncertainty when Alice measures in $1 \leqslant n < d_A + 1$ MUBs. It is helpful to first analyze the case for one basis K.

Lemma 1. Let $K = \{|k\rangle\}$ be an orthonormal basis on some Hilbert space $\mathcal{H}_A$. Then, we have for any bipartite quantum state ρ_{AB} that

$$P^{\text{pg}}_{\text{guess}}(K|B) \geqslant F^{\text{pg}}(A|B), \tag{B10}$$

where $\rho_{KB} = \sum_k (|k\rangle\langle k| \otimes \mathbb{1}_B)\rho_{AB}(|k\rangle\langle k| \otimes \mathbb{1}_B)$.

Proof. We calculate

$$\begin{aligned}
P^{\text{pg}}_{\text{guess}}(K|B) &= \text{Tr}\big[\rho_{KB}\rho_B^{-1/2}\rho_{KB}\rho_B^{-1/2}\big] && \text{(B11)}\\
&= \text{Tr}\big[\rho_{AB}\rho_B^{-1/2}\rho_{KB}\rho_B^{-1/2}\big] && \text{(B12)}\\
&= d_A \text{Tr}\big[\Phi_{AA'}(\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'})(\rho_{KB})\big] && \text{(B13)}\\
&= F\big[\Phi_{AA'}, d_A(\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'})(\rho_{KB})\big] && \text{(B14)}\\
&\geqslant F\big[\Phi_{AA'}, (\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'})(\rho_{AB})\big] && \text{(B15)}\\
&= F^{\text{pg}}(A|B). && \text{(B16)}
\end{aligned}$$

The inequality step in this proof invoked the property that the fidelity decreases upon decreasing one of its arguments, and hence it remains to show

$$d_A\big(\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'}\big)(\rho_{KB}) \geqslant \big(\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'}\big)(\rho_{AB}). \tag{B17}$$

We denote the non-negative operator $\sigma_{AA'} = (\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'})(\rho_{AB})$, and note that the measurement in K on the A system commutes with $\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'}$. We get

$$\begin{aligned}
&d_A\big(\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'}\big)(\rho_{KB}) - \big(\mathcal{I}_A \otimes \Lambda^{\text{pg}}_{B\to A'}\big)(\rho_{AB})\\
&= d_A \sum_k (|k\rangle\langle k| \otimes \mathbb{1}_{A'})\sigma_{AA'}(|k\rangle\langle k| \otimes \mathbb{1}_{A'})\\
&\quad - \sum_{k,k'} (|k\rangle\langle k| \otimes \mathbb{1}_{A'})\sigma_{AA'}(|k'\rangle\langle k'| \otimes \mathbb{1}_{A'}) && \text{(B18)}\\
&= (d_A - 1)\left[\sum_k (|k\rangle\langle k| \otimes \mathbb{1})\sigma_{AA'}(|k\rangle\langle k| \otimes \mathbb{1})\right.\\
&\quad \left. - \frac{1}{d_A - 1}\sum_{k,k'\neq k} (|k\rangle\langle k| \otimes \mathbb{1})\sigma_{AA'}(|k'\rangle\langle k'| \otimes \mathbb{1})\right] && \text{(B19)}\\
&= (d_A - 1)(\mathcal{F} \otimes \mathcal{I})(\sigma_{AA'}), && \text{(B20)}
\end{aligned}$$

where we set in the last line

$$\mathcal{F}(\cdot) = \frac{1}{d_A - 1}\sum_{m=1}^{d_A-1} Z^m(\cdot)(Z^m)^\dagger, \quad Z = \sum_{k=0}^{d_A-1} \omega^k |k\rangle\langle k|, \quad \omega = e^{2\pi i/d_A}. \tag{B21}$$

Since $\mathcal{F}$ is a completely positive trace-preserving map, the claim follows. ■

Equation (B10) states that the entanglement fidelity quantified by $F^{\text{pg}}(A|B)$ lower bounds the guessing probability $P^{\text{pg}}_{\text{guess}}(K|B)$. By combining (B10) with our uncertainty equality (6), we get that for subset of size $1 \leqslant n < d_A + 1$ of a complete set of MUBs,

$$\sum_{\theta=1}^{n} P^{\text{pg}}_{\text{guess}}(K|B\Theta = \theta) = (n-1)F^{\text{pg}}(A|B) + 1 + \left[(d_A + 1 - n)F^{\text{pg}}(A|B) - \sum_{\theta=n+1}^{d_A+1} P^{\text{pg}}_{\text{guess}}(K|B\Theta = \theta)\right] \tag{B22}$$

$$\leqslant (n-1)F^{\text{pg}}(A|B) + 1, \tag{B23}$$

and this proves (15). Similarly, we can invoke the immediate relation $P^{\text{pg}}_{\text{guess}}(K|B) \geqslant 1/d_A$ to get

$$\sum_{\theta=1}^{n} P^{\text{pg}}_{\text{guess}}(K|B\Theta = \theta) = d_A F^{\text{pg}}(A|B) + \frac{n-1}{d_A} + \left[\frac{d_A + 1 - n}{d_A} - \sum_{\theta=n+1}^{d_A+1} P^{\text{pg}}_{\text{guess}}(K|B\Theta = \theta)\right] \tag{B24}$$

$$\leqslant d_A F^{\text{pg}}(A|B) + \frac{n-1}{d_A}, \tag{B25}$$

and this proves (14). The tightness of the bounds in (14) and (15) follows by construction. In the region $F^{\text{pg}}(A|B) \geqslant 1/d_A$, the upper bound is achieved by a bipartite pure state whose Schmidt basis is one of the Θ bases appearing in the sum of guessing probabilities under consideration, and the lower bound is achieved by a bipartite pure state whose Schmidt basis is one of the Θ bases that belongs to the same complete MUB set as the bases under consideration, but whose guessing probability was removed from the sum under consideration.

In the region $F^{\text{pg}}(A|B) \leqslant 1/d_A$, the upper bound is achieved by a tensor product state $\rho_A \otimes \rho_B$ such that ρ_A is diagonal in one of the Θ bases appearing in the sum of guessing probabilities under consideration, and the lower bound is similarly achieved by such a tensor product state where ρ_A is diagonal in one of the Θ bases that belongs to the same complete MUB set as the bases under consideration, but whose guessing probability was removed from the sum under consideration.

3. Monogamy of correlations

Here we show (18) from the main text. The precise statement is as follows.

Corollary 1. Let $\{\Theta\}_{\theta\in\Theta}$ be a complete set of MUBs on some Hilbert space $\mathcal{H}_A$, and denote $\theta = \{|\theta_k\rangle\}_{k=1}^{d_A}$. Then, we have for any tripartite pure quantum state ρ_{ABE} that

$$\inf_{\sigma} D_{\frac{1}{2}}\left(\rho_{AE}\|\frac{\mathbb{1}_A}{d_A}\otimes\sigma_E\right) = \log d_A - \log\left[(d_A+1)P^{\mathrm{pg}}_{\mathrm{guess}}(K|B\Theta)-1\right], \quad \text{(B26)}$$

where the infimum is over all quantum states σ_E, and the relative Rényi 1/2-entropy is given by

$$D_{\frac{1}{2}}\left(\rho_{AE}\|\frac{\mathbb{1}_A}{d_A}\otimes\sigma_E\right) = -\log\left\{\mathrm{tr}\left[\rho_{AE}^{1/2}\left(\frac{\mathbb{1}_A}{d_A}\otimes\sigma_E\right)^{1/2}\right]\right\}^2. \quad \text{(B27)}$$

Proof. For any conditional entropy that is invariant under local isometries on the conditioning system, one can define a dual entropy. For some generic entropy H_K, the dual entropy H_K^{dual} is defined by

$$H_K(A|B) = -H_K^{\mathrm{dual}}(A|E)_\rho, \quad \text{(B28)}$$

where E is a system that purifies ρ_{AB}. Since $H_2(A|B)$ is invariant under local isometries on B, the dual entropy is well defined, and it is known that [48]

$$-H_2^{\mathrm{dual}}(A|E) = \inf_{\sigma} D_{\frac{1}{2}}(\rho_{AE}\|\mathbb{1}_A\otimes\sigma_E). \quad \text{(B29)}$$

By the standard rewriting,

$$D_{\frac{1}{2}}(\rho_{AE}\|\mathbb{1}_A\otimes\sigma_E) = D_{\frac{1}{2}}\left(\rho_{AE}\|\frac{\mathbb{1}_A}{d_A}\otimes\sigma_E\right) - \log d_A, \quad \text{(B30)}$$

the claim follows from our main result (6). ■

APPENDIX C: APPLICATIONS

1. Witnessing entanglement

Here we show the origin of (17), our condition for witnessing entanglement. We will make use of the following lemma, which says that separable states cannot have a negative conditional entropy.

Lemma 2. Let ρ_{AB} be a separable quantum state. Then, we have

$$H_2(A|B) \geqslant H_{\min}(A|B) \geqslant 0. \quad \text{(C1)}$$

Proof. The inequality $H_2(A|B) \geqslant H_{\min}(A|B)$ holds for any quantum state ρ_{AB} since $\Lambda^{\mathrm{pg}}_{B\to A'}$ in (A3) is a particular map, and the conditional min-entropy involves an optimization over all maps $\Lambda_{B\to A'}$ in (A1).

To prove $H_{\min}(A|B) \geqslant 0$, note that any local operation on a separable state results in another separable state. Now suppose $\sigma_{AA'} = (\mathcal{I}_A\otimes\hat{\Lambda}_{B\to A'})(\rho_{AB})$ is the separable state that achieves the optimization when evaluating the conditional min-entropy for ρ_{AB} [i.e., $\hat{\Lambda}$ is the optimal channel in (A3)]. Then, we have

$$F(A|B) = F(\Phi_{AA'},\sigma_{AA'}) \leqslant F(\Phi_{AA'},\mathbb{1}_A\otimes\sigma_{A'}) \quad \text{(C2)}$$

$$= 1/d_A, \quad \text{(C3)}$$

which follows because the fidelity increases upon increasing one of its arguments, and because for separable $\sigma_{AA'}$ we have $\sigma_{AA'} \leqslant \mathbb{1}_A\otimes\sigma_{A'}$ with $\sigma_{A'} = \mathrm{Tr}_A(\sigma_{AA'})$. Using $H_{\min}(A|B) = -\log[d_A F(A|B)]$, the claim follows. ■

The following is our criterion for witnessing entanglement.

Lemma 3. Let ρ_{AB} be a separable quantum state. Let $\{K_\theta\}_{\theta=1}^n$ be a subset (of size n) of a complete set of MUBs on A, and let $\{L_\theta\}_{\theta=1}^n$ be an arbitrary set of n orthonormal bases on B. Then, we have

$$\sum_{\theta=1}^n 2^{-H_2(K_\theta|L_\theta)} \leqslant 1 + \frac{n-1}{d_A}, \quad \text{(C4)}$$

where

$$\rho_{K_\theta L_\theta} = \sum_{p,q}(|K_{\theta,p}\rangle\langle K_{\theta,p}|\otimes|L_{\theta,q}\rangle\langle L_{\theta,q}|)\rho_{AB} \times (|K_{\theta,p}\rangle\langle K_{\theta,p}|\otimes|L_{\theta,q}\rangle\langle L_{\theta,q}|). \quad \text{(C5)}$$

Proof. Since ρ_{AB} is separable, the previous lemma (Lemma 2) tells us that $F^{\mathrm{pg}}(A|B) \leqslant 1/d_A$. Combining this with the bound in (14), we have

$$\frac{n-1}{d_A} + 1 \geqslant (n-1)F^{\mathrm{pg}}(A|B) + 1 \quad \text{(C6)}$$

$$\geqslant \sum_{\theta=1}^n P^{\mathrm{pg}}_{\mathrm{guess}}(K_\theta|B) \quad \text{(C7)}$$

$$= \sum_{\theta=1}^n 2^{-H_2(K_\theta|B)} \quad \text{(C8)}$$

$$\geqslant \sum_{\theta=1}^n 2^{-H_2(K_\theta|L_\theta)}, \quad \text{(C9)}$$

where the last inequality follows because the conditional Rényi 2-entropy satisfies the data-processing inequality [21]. ■

2. Quantum cryptography

Here we show the uncertainty and certainty relations (12) and (13) in terms of the smooth conditional min-entropy. For a bipartite quantum state ρ_{AB} and smoothing parameter $\varepsilon \geqslant 0$, the smooth conditional min-entropy is defined as

$$H^{\varepsilon}_{\min}(A|B)_\rho = \sup_{\bar{\rho}_{AB}} H_{\min}(A|B)_{\bar{\rho}}, \quad \text{(C10)}$$

where the supremum is over all subnormalized states $\bar{\rho}_{AB}$ on AB that are ε close to ρ_{AB} in purified distance [49]. Now, the crucial point is that $H^{\varepsilon}_{\min}$ and H_2 are equivalent in the following sense: it holds for any bipartite quantum state ρ_{AB} and $\varepsilon > 0$ that (see, e.g., Lemma A.25 in [50])

$$H_{\min}(A|B) \leqslant H_2(A|B) \leqslant H^{\varepsilon}_{\min}(A|B) + \log\frac{2}{\varepsilon^2}. \quad \text{(C11)}$$

By combining (C11) with our main result (6), we obtain the uncertainty and certainty relation for the smooth conditional min-entropy as given in (12) and (13). We note that similar uncertainty relations have been derived in [18,51], and were used to analyze security in the noisy storage model.

APPENDIX D: EXTENSIONS OF MAIN RESULT

1. Complex projective 2-designs

We have seen in Appendix A that the proof of our uncertainty equality (6) crucially relies on the fact that a full set of MUBs generates a complex projective 2-design. In general, a complex projective 2-design is a set $\{|\psi_y\rangle\}_{y\in Y}$ (of size $|Y|$) of vectors $|\psi_y\rangle$ lying in a Hilbert space $\mathcal{H}_A$ such that

$$\frac{1}{|Y|}\sum_{y\in Y}|\psi_y\rangle\langle\psi_y|^{\otimes 2}=\frac{1}{d_A(d_A+1)}(\mathbb{1}_{AA'}+F_{AA'}), \tag{D1}$$

where $F_{AA'}$ denotes the swap operator, and A' is a copy of A. It turns out that there are other "informationally equivalent" measurements that generate a complex projective 2-design. As an example, we mention SIC-POVMs, such as the four states forming a tetrahedron on the Bloch sphere for qubits.

Corollary 2. Let $\{\frac{1}{d_A}|\psi_k\rangle\langle\psi_k|\}_{k=1}^{d_A^2}$ be a SIC-POVM on some Hilbert space $\mathcal{H}_A$. Then, we have for any bipartite quantum state ρ_{AB} that

$$H_2(K|B)=\log[d_A(d_A+1)]-\log(2^{-H_2(A|B)}+1), \tag{D2}$$

where

$$\rho_{KB}=\sum_{k=1}^{d_A^2}|k\rangle\langle k|\otimes \mathrm{Tr}_A\left[\left(\frac{1}{d_A}|\psi_k\rangle\langle\psi_k|\otimes\mathbb{1}_B\right)\rho_{AB}\right] \tag{D3}$$

is a classical-quantum state with $\{|k\rangle\}$ an orthonormal basis on $\mathcal{H}_K$.

Notice that the d_A-dependent term on the r.h.s. of (D2) is slightly different from the corresponding term appearing in our main result (6), and indeed (D2) implies that $\log d_A \leqslant H_2(K|B)\leqslant 2\log d_A$ for SIC-POVMs. Nevertheless, the proof of (D2) is identical to the proof of (6), with the appropriate version of (D1) substituted into the proof.

In addition, so-called unitary 2-designs are closely related to complex projective 2-designs. A set $\{U_y\}_{y\in Y}$ (of size $|Y|$) of unitaries U_y on some Hilbert space $\mathcal{H}_A$ forms a unitary 2-design if

$$\frac{1}{|Y|}\sum_{y\in Y}(U_y\otimes U_y^\dagger)^{\otimes 2}=\int_{U(d_A)}(U\otimes U^\dagger)^{\otimes 2}dU, \tag{D4}$$

where the integration is over all unitaries with respect to the Haar measure. Examples of unitary 2-designs are the full unitary group, or the Clifford group for qubit systems. In fact, unitary 2-designs generate complex projective 2-designs.

Lemma 4. Let $\{U_\theta\}_{\theta\in\Theta}$ be a unitary 2-design on some Hilbert space $\mathcal{H}_A$. Then, we have

$$\frac{1}{d_A|\Theta|}\sum_{k=1}^{d_A}\sum_{\theta\in\Theta}(U_\theta|k\rangle\langle k|U_\theta^\dagger)^{\otimes 2}=\frac{1}{d_A(d_A+1)}(\mathbb{1}_{AA'}+F_{AA'}), \tag{D5}$$

where $\{|k\rangle\}$ denotes some orthonormal basis of $\mathcal{H}_A$.

Hence, our main result also holds for unitary 2-designs.

Corollary 3. Let $\{U_\theta\}_{\theta\in\Theta}$ be a unitary 2-design on some Hilbert space $\mathcal{H}_A$. Then, we have for any bipartite quantum state ρ_{AB} that

$$H_2(K|B\Theta)=\log(d_A+1)-\log(2^{-H_2(A|B)}+1), \tag{D6}$$

where

$$\rho_{KB\Theta}=\frac{1}{|\Theta|}\sum_{\theta,k}(|\theta_k\rangle\langle\theta_k|\otimes\mathbb{1}_B)\rho_{AB}(|\theta_k\rangle\langle\theta_k|\otimes\mathbb{1}_B)\otimes|\theta\rangle\langle\theta|_\Theta, \tag{D7}$$

and $|\theta_k\rangle=U_\theta|k\rangle$ for some orthonormal basis $\{|k\rangle\}$ of $\mathcal{H}_A$.

2. More general entropies

Our main result (6) is in terms of the conditional Rényi 2-entropy. However, we can also prove it in terms of a more general continuous family of conditional 2-entropies. For $\nu\in[0,1]$ and bipartite quantum states ρ_{AB}, we define

$$H_{2,\nu}(A|B)=-\log\mathrm{Tr}[\rho_{AB,\nu}^\dagger\rho_{AB,\nu}], \tag{D8}$$

where

$$\rho_{AB,\nu}=\left(\mathbb{1}_A\otimes\rho_B^{-(1-\nu)/4}\right)\rho_{AB}\left(\mathbb{1}_A\otimes\rho_B^{-(1+\nu)/4}\right). \tag{D9}$$

It is easily seen that $\nu=0$ corresponds to the usual definition (A2) in the main text. We state the generalization of our uncertainty equality (6) for a full set of MUBs, but note that it also holds for all other "informationally equivalent" measurements (cf. Appendix D 1).

Corollary 4. Let $\{\Theta\}_{\theta\in\Theta}$ be a complete set of MUBs on some Hilbert space $\mathcal{H}_A$, and denote $\theta=\{|\theta_k\rangle\}_{k=1}^{d_A}$. Then, we have for any bipartite quantum state ρ_{AB} that

$$H_{2,\nu}(K|B\Theta)=\log(d_A+1)-\log(2^{-H_{2,\nu}(A|B)}+1), \tag{D10}$$

where

$$\rho_{KB\Theta}=\frac{1}{d_A+1}\sum_{\theta,k}(|\theta_k\rangle\langle\theta_k|\otimes\mathbb{1}_B)\times\rho_{AB}(|\theta_k\rangle\langle\theta_k|\otimes\mathbb{1}_B)\otimes|\theta\rangle\langle\theta|_\Theta. \tag{D11}$$

The proof is obvious by just taking the one for the conditional Rényi 2-entropy, and replacing $\tilde\rho_{AB}$ with $\rho_{AB,\nu}$. It is worth noting that (D10) applies to the variant (used in, e.g., [52,53]),

$$H_{2,1}(A|B)=-\log\mathrm{Tr}\left[\rho_{AB}^2\left(\mathbb{1}_A\otimes\rho_B^{-1}\right)\right]. \tag{D12}$$

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[2] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[3] W. Beckner, Ann. Math. **102**, 159 (1975).
[4] I. Białynicki-Birula and J. Mycielski, Commun. Math. Phys. **44**, 129 (1975).
[5] I. I. Hirschman, Am. J. Math. **79**, 152 (1957).

[6] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).
[7] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[8] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[9] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
[10] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
[11] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, *International Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, FOCS* (IEEE, Piscataway, NJ, 2005), pp. 449–458.
[12] M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1995).
[13] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[14] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
[15] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[16] C.-F. Li, J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, Nat. Phys. **7**, 752 (2011).
[17] R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, Nat. Phys. **7**, 757 (2011).
[18] M. Berta, O. Fawzi, and S. Wehner, IEEE Trans. Inf. Theor. **60**, 1168 (2014).
[19] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theor. **55**, 4337 (2009).
[20] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[21] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, J. Math. Phys. **54**, 122203 (2013).
[22] R. Renner, Ph.D. thesis, ETH Zurich, 2005.
[23] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Phys. Rev. A **78**, 022316 (2008).
[24] P. Hausladen and W. K. Wootters, J. Mod. Opt. **41**, 2385 (1994).
[25] H. Barnum and E. Knill, J. Math. Phys. **43**, 2097 (2002).
[26] C. Brukner and A. Zeilinger, Phys. Rev. Lett. **83**, 3354 (1999).
[27] I. D. Ivanovic, J. Phys. A **25**, L363 (1992).
[28] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theor. **57**, 5524 (2010).
[29] F. Dupuis, Ph.D. thesis, Université de Montréal, 2009.
[30] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, Commun. Math. Phys. **328**, 251 (2014).
[31] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[32] W. K. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).
[33] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).
[34] D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48**, 052104 (2007).
[35] W. Matthews, S. Wehner, and A. Winter, Commun. Math. Phys. **291**, 813 (2009).
[36] J. Sánchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
[37] V. Giovannetti, S. Mancini, D. Vitali, and P. Tombesi, Phys. Rev. A **67**, 022320 (2003).
[38] O. Gühne and M. Lewenstein, Phys. Rev. A **70**, 022316 (2004).
[39] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).
[40] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Phys. Rev. A **86**, 022311 (2012).
[41] R. König, W. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theor. **58**, 1962 (2012).
[42] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[43] D. H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White, Nat. Commun. **3**, 625 (2012).
[44] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[45] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[46] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 5th ed. (Cambridge University Press, Cambridge, 2000).
[47] A. Klappenecker and M. Rotteler, *International Proceedings of the Symposium on Information Theory, ISIT* (IEEE, Piscataway, NJ, 2005), pp. 1740–1744.
[48] M. Tomamichel, M. Berta, and M. Hayashi, J. Math. Phys. **55**, 082206 (2014).
[49] M. Tomamichel, Ph.D. thesis, ETH Zurich, 2012.
[50] M. Berta, Ph.D. thesis, ETH Zurich, 2013.
[51] F. Dupuis, O. Fawzi, and S. Wehner, IEEE Trans. Inf. Theor. **PP**, 1 (2014).
[52] M. Hayashi, *IEEE International Symposium on Information Theory Proceedings, ISIT* (IEEE, Piscataway, NJ, 2012), pp. 895–899.
[53] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theor. **55**, 5840 (2009).