






Maximal intrinsic randomness of a quantum stateShuyang Meng ¹, Fionnuala Curran ², Gabriel Senno ³, Victoria J. Wright^{2,4}, Máté Farkas ^{2,5}, Valerio Scarani ^{1,6} and Antonio Acín^{2,7}¹*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*²*ICFO–Institut de Ciències Fotòniques, Barcelona Institute of Science and Technology, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain*³*Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels, Barcelona, Spain*⁴*Quantinum, Terrington House, 13-15 Hills Road, Cambridge CB2 1NL, United Kingdom*⁵*Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom*⁶*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*⁷*ICREA–Institut de Recerca i Estudis Avançats, 08010 Barcelona, Spain*

(Received 6 September 2023; accepted 18 June 2024; published 8 July 2024)

One of the most counterintuitive aspects of quantum theory is its claim that there is “intrinsic” randomness in the physical world. Quantum information science has greatly progressed in the study of intrinsic, or secret, quantum randomness in the past decade. With much emphasis on device-independent and semi-device-independent bounds, one of the most basic questions has escaped attention: how much intrinsic randomness can be extracted from a given state ρ , and what measurements achieve this bound? We answer this question for three different randomness quantifiers: the conditional min-entropy, the conditional von Neumann entropy, and the conditional max-entropy. For the first, we solve the min-max problem of finding the projective measurement that minimizes the maximal guessing probability of an eavesdropper. The result is that one can guarantee an amount of conditional min-entropy $H_{\min}^* = -\log_2 P_{\text{guess}}^*(\rho)$ with $P_{\text{guess}}^*(\rho) = \frac{1}{d} (\text{tr} \sqrt{\rho})^2$ by performing suitable projective measurements. For the conditional von Neumann entropy, we find that the maximal value is $H^* = \log_2 d - S(\rho)$, with $S(\rho)$ the von Neumann entropy of ρ , while for the conditional max-entropy, we find the maximal value $H_{\max}^* = \log_2 d + \log_2 \lambda_{\max}(\rho)$, where $\lambda_{\max}(\rho)$ is the largest eigenvalue of ρ . Optimal values for H_{\min}^* , H^* and H_{\max}^* are achieved by measuring in any basis that is unbiased with respect to the eigenbasis of ρ , as well as by other, less intuitive, measurements.

DOI: [10.1103/PhysRevA.110.L010403](https://doi.org/10.1103/PhysRevA.110.L010403)

Introduction. One of the core differences between classical and quantum physics is the latter’s probabilistic character, which is irreducible to ignorance of underlying variables. This difference has fundamental implications for our worldview, but it is also attractive as a natural source of randomness for practical uses. Indeed, Geiger counting was already used as a source of physical randomness in the second half of the 20th century. In the past two decades, with the development of quantum information science, a large number of quantum random number generators (QRNGs) have been designed, and many have been implemented, usually with light (see [1,2] for comprehensive reviews). The *amount of randomness* is naturally captured by the *guessing probability* P_{guess} : the higher the probability that the random variable is guessed, the smaller the randomness. This intuitive characterization was found to have operational meaning: the *min-entropy* $H_{\min} = -\log_2 P_{\text{guess}}$ quantifies (informally) the fraction of perfect coin tosses that can be extracted from a string generated by the available source. But randomness is not an absolute notion: one has to specify *for whom* the source should be partly unpredictable. For mere sampling purposes, it might be sufficient to take the observed probabilities at face value; for cryptographic applications, however, one needs to estimate the probability that *an adversary, Eve*, guesses the outcomes. The

resulting randomness is called *secret randomness*, or *intrinsic randomness*.

The computation of intrinsic randomness using quantum resources and against a quantum adversary has been studied from different perspectives. When considering a user with classical data correlated with quantum information in the hands of an adversary, the min-entropy quantifies the amount of perfect random bits that the user can establish [3]. The question was also addressed for the task of quantum key distribution, which is the extraction of secret *shared* randomness. It was in this context that the idea of device-independent certification was born: the possibility of bounding the amount of randomness in a black-box setting, based on the observation of Bell-nonlocal correlations [4]. Next, it was noticed that device-independent certification can be performed for randomness as well [5,6], providing the first disruptive case for quantum randomness in a non-shared setting [7]. This breakthrough happened as the race to demonstrate loophole-free Bell tests was taking up speed. There followed an explosion of designs and implementations of QRNGs certifiable under various assumptions, from device-independent (disruptive, but hard to implement), to semi-device-independent in various forms, to fully characterized (practical and fast, but requiring a precise modeling

of the setups). For these developments, we refer to the reviews [1,2,8,9].

In this flurry of activity, one of the most basic questions was somehow left out: *how much secret randomness can be extracted from a known state ρ* . In this paper, we solve this problem for three of the most natural and operational measures of randomness: the conditional min-entropy, the conditional von Neumann entropy, and the conditional max-entropy. For the first, we show that the answer is $H_{\min}^* = -\log_2 P_{\text{guess}}^*(\rho)$, with

$$P_{\text{guess}}^*(\rho) = \frac{1}{d} (\text{tr} \sqrt{\rho})^2, \quad (1)$$

where d is the dimension of the Hilbert space of the system, assumed to be finite. We find a family of measurements that generate this amount of randomness, which is closely related to the concept of “pretty good measurements” [10], originally used as a close-to-optimal way to distinguish an ensemble of states. For the second, we find the maximal value

$$H^* = \log_2 d - S(\rho), \quad (2)$$

where $S(\rho) = -\text{tr}(\rho \log_2 \rho)$ is the von Neumann entropy of ρ , while for the third, we find

$$H_{\max}^* = \log_2 d + \log_2 \lambda_{\max}(\rho), \quad (3)$$

where $\lambda_{\max}(\rho)$ is the largest eigenvalue of ρ . Interestingly, for $d > 2$, we find that some measurements maximize one of H_{\min} , H and H_{\max} , but not the other two.

Qubit example. A case study will help to introduce the main ideas. Alice has a source that produces a qubit. She has characterized its state to the best of her knowledge and found it to be

$$\rho = \frac{1}{2}(\mathbb{1} + m\sigma_z) = \frac{1+m}{2}|0\rangle\langle 0| + \frac{1-m}{2}|1\rangle\langle 1| \quad (4)$$

for some $0 \leq m \leq 1$. If she measures σ_x , her observed statistics will be those of a perfect unbiased coin: $P_A(+1) = P_A(-1) = \frac{1}{2}$. Suppose now that what the source really does is produce a pure state in each round, specifically half of the rounds $|\chi_+\rangle$ and half of the rounds $|\chi_-\rangle$, with

$$|\chi_{\pm}\rangle = \sqrt{\frac{1 \pm \sqrt{1-m^2}}{2}}|+\rangle + \sqrt{\frac{1 \mp \sqrt{1-m^2}}{2}}|-\rangle \quad (5)$$

(indeed, $\frac{1}{2}|\chi_+\rangle\langle\chi_+| + \frac{1}{2}|\chi_-\rangle\langle\chi_-| = \rho$). If Eve knows the working of the source exactly, she will guess $i = +1$ ($i = -1$) in the rounds when the source sent out $|\chi_+\rangle$ ($|\chi_-\rangle$). Her guess will then be correct with probability

$$P_{\text{guess}} = \frac{1}{2}(1 + \sqrt{1-m^2}), \quad (6)$$

which is strictly larger than $\frac{1}{2}$ when $m < 1$ (i.e., when ρ is mixed). Thus, the intrinsic randomness of Alice’s protocol is less than her apparent perfect randomness. In particular, there is no secret randomness in the state $\rho = \frac{1}{2}\mathbb{1}$, since $P_{\text{guess}} = \frac{1}{2}$ for $m = 0$.

As will be expanded on in what follows, two things are already known about this case study and its generalization to higher dimensions. First: we presented this example with Eve having perfect classical information about the source, in the

sense that she knows at each instance which state has been prepared and accordingly makes her guess on Alice’s measurement outcome. However, the result is unchanged if Eve holds quantum side information. Eve then holds a purification of Alice’s state, and she measures her own system to guess Alice’s result. Since the two scenarios are equivalent in terms of the guessing probability, we will move from one to the other when convenient for the argumentation. Second: having fixed Alice’s protocol (both the state and the measurement), the maximization of P_{guess} over all decompositions of ρ is a known semidefinite program (SDP) [11]; in the case study, we have presented the optimal decomposition. What is not known is whether σ_x is the best measurement for Alice, even in the presence of Eve: could another measurement on the same state ρ decrease Eve’s guessing probability, at the expense of biasing the observed P_A ? We set out to solve this min-max problem, and thus determine the maximal amount of secret randomness that can be extracted from ρ .

Setting of the problem. Alice holds a quantum state ρ from a Hilbert space of dimension d . We want to determine how much intrinsic randomness she can extract from ρ and which measurement achieves this maximum. We consider only measurements $\mathcal{M} = \{M_i\}_i$ which are projective, i.e., $M_i M_j = \delta_{ij} M_i$, where δ_{ij} is the Kronecker delta (we discuss general POVMs at the end of this section). To quantify how intrinsically random, that is, how unpredictable, Alice’s measurement outcome is, one considers the existence of an eavesdropper, Eve, who has a more detailed knowledge than Alice about the process, but cannot actively influence it (she is “outside the laboratory”). Concretely, in every round, Eve knows the true state ρ_c produced by the source. Given this knowledge, she guesses the most likely outcome $i = i(c)$ for that round. Without loss of generality, we can group together all of Eve’s states that lead to the same guessed outcome, since Eve does not gain anything in treating them as distinct. We denote by ρ_i the states seen by Eve, subnormalized such that $q_i = \text{tr} \rho_i$ is the probability that Eve’s most likely outcome is i . These states must satisfy $\sum_i \rho_i = \rho$.

Having set this stage, Eve’s average guessing probability is $P_{\text{guess}}(\{\rho_i\}, \mathcal{M}) = \sum_i \text{tr}(M_i \rho_i)$. Since we don’t know the true states ρ_i , we need to consider the worst case scenario, i.e., the decomposition that maximizes Eve’s guessing probability,

$$P_{\text{guess}}(\rho, \mathcal{M}) = \max_{\{\rho_i\}} \sum_i \text{tr}(M_i \rho_i) \text{ s.t. } \rho_i \geq 0, \quad \sum_i \rho_i = \rho. \quad (7)$$

This optimization is an SDP, and so can be solved efficiently. In order to determine, *the maximal amount of secret randomness that can be extracted from the known state ρ* , one needs to optimize Eq. (7) over Alice’s measurement, i.e., compute

$$P_{\text{guess}}^*(\rho) = \min_{\mathcal{M} \in \Pi} P_{\text{guess}}(\rho, \mathcal{M}), \quad (8)$$

where Π is the set of all projective measurements. Our main result is to show that Eq. (1) is the solution to the optimization (8).

The search for an optimal measurement could have been extended to the larger set of positive operator-valued measures (POVMs), but the operational interpretation in our context is unclear. Recall that our goal is to quantify the secret

randomness in the state ρ . When implementing a POVM, however, the projective measurement acts on the given state ρ plus an auxiliary system, so part of the obtained randomness may come from the latter. In fact, for extremal measurements minimizing the guessing probability, the auxiliary system has to be in a pure state, say, $|a\rangle$, of dimension d_A [12]. It follows from our main result that the maximal amount of randomness obtained when implementing a projective measurement on the global state is $P_{\text{guess}}^*(\rho \otimes |a\rangle\langle a|)$. It is easy, however, to see that $P_{\text{guess}}^*(\rho \otimes |a\rangle\langle a|) = \frac{1}{d_A} P_{\text{guess}}^*(\rho)$, that is, the optimal guessing probability is equal to that obtained by performing the corresponding optimal projective measurements independently on the system and the auxiliary.

Thus, the extra randomness supplied by using the optimal POVM is exactly equal to the intrinsic randomness of the auxiliary system used to implement the POVM, so we view it as arising from the auxiliary rather than from ρ itself.

Main results. Theorem 1. The maximal amount of secret randomness that can be extracted from a quantum state ρ using a projective measurement is given by $H_{\text{min}}^* = -\log_2 P_{\text{guess}}^*(\rho)$ with $P_{\text{guess}}^*(\rho) = \frac{1}{d} (\text{tr} \sqrt{\rho})^2$.

Without loss of generality, one can restrict the optimization to rank-one projective measurements (see the Supplemental Material [13, Sec. II]). In what follows, we outline a proof that uses notions from state discrimination and the resource theory of coherence, with full details in the Supplemental Material [13, Sec. III] (see also Refs. [29–33] therein). An alternative proof using properties of the min-entropy and semidefinite programming is provided in [13, Sec. IV]. We prove the theorem by first proving the lower bound $P_{\text{guess}}^*(\rho) \geq \frac{1}{d} (\text{tr} \sqrt{\rho})^2$ (Lemma 1) and then showing that there exist measurements that achieve that bound (Lemma 2).

Lemma 1. The lower bound $P_{\text{guess}}^*(\rho) \geq \frac{1}{d} (\text{tr} \sqrt{\rho})^2$ holds for every state ρ .

Proof. Using the fact that rank-one measurements are optimal for Alice, from [14, Theorem 1, (iii)], we find

$$P_{\text{guess}}(\rho, \mathcal{M}) = \max_{\{\sigma \in \mathcal{I}_{\mathcal{M}}\}} F(\rho, \sigma), \quad (9)$$

where F is the Uhlmann fidelity and $\mathcal{I}_{\mathcal{M}}$ is the set of states that are diagonal in the measurement basis $\{|m_i\rangle\}$. Notice that $\mathbb{1}/d \in \mathcal{I}_{\mathcal{M}}$ for all $\mathcal{M} \in \Pi$, so $P_{\text{guess}}(\rho, \mathcal{M}) \geq F(\rho, \mathbb{1}/d) = \frac{1}{d} (\text{tr} \sqrt{\rho})^2$ for all \mathcal{M} . Hence, $P_{\text{guess}}^*(\rho)$ cannot be smaller than $\frac{1}{d} (\text{tr} \sqrt{\rho})^2$. ■

Lemma 2. A projective measurement \mathcal{M} in the basis $\{|m_i\rangle\}$ achieves the bound $P_{\text{guess}}(\rho, \mathcal{M}) = \frac{1}{d} (\text{tr} \sqrt{\rho})^2$ if and only if $\langle m_i | \sqrt{\rho} | m_i \rangle = \frac{1}{d} \text{tr} \sqrt{\rho}$ for all $i = 1, \dots, d$.

Proof. The details missing here are provided in [13, Sec. III A]. In the quantum side-information scenario, any k -outcome rank-one measurement, \mathcal{M} , by Alice steers k pure states on Eve. To optimize her guess, Eve has to measure her system to optimally discriminate among these k states. It is known [15] that the best discrimination of a set of pure states is obtained with rank-one measurements: thus, Eve will also perform a rank-one measurement. In turn, Eve's measurement defines an ensemble realizing the mixed state ρ . This ensemble consists of k pure states $\rho_i = |\tilde{\psi}_i\rangle\langle \tilde{\psi}_i|$. If \mathcal{M} is projective, we have $k = d$, and it follows from [16] that any

decomposition of ρ in d pure states is defined by the choice of an orthonormal basis $\{|i\rangle\}$ through

$$|\tilde{\psi}_i\rangle = \sqrt{\rho} |i\rangle \quad \text{with} \quad \langle i | i' \rangle = \delta_{ii'}, \quad i, i' = 1, \dots, d. \quad (10)$$

Inserting all these observations in (7), we obtain

$$P_{\text{guess}}(\rho, \mathcal{M}) = \max_{\{\tilde{i}\}} \sum_i |\langle m_i | \sqrt{\rho} | i \rangle|^2. \quad (11)$$

The r.h.s. has been called the geometric coherence of ρ [17] and was shown in [18] to be equivalent to $\max_{\{\sigma \in \mathcal{I}_{\mathcal{M}}\}} F(\rho, \sigma)$, with $\mathcal{I}_{\mathcal{M}}$ the set of states diagonal in the basis $\{|m_i\rangle\}$. If we rewrite (11) as

$$P_{\text{guess}}(\rho, \mathcal{M}) = \max_{\{\Pi_i\}} \sum_i \text{tr}(\Pi_i \tilde{\gamma}_i) \langle \tilde{\gamma}_i | \quad \text{s.t.} \quad \Pi_i \geq 0, \quad (12)$$

$$\sum_i \Pi_i = \mathbb{1},$$

the r.h.s. defines the optimal discrimination of the subnormalized states $|\tilde{\gamma}_i\rangle := \sqrt{\rho} |m_i\rangle$ with a projective measurement $\Pi_i = |i\rangle\langle i|$. One then checks (see [13, Sec. III B]) that, under the assumption that

$$\langle m_i | \sqrt{\rho} | m_i \rangle = \frac{1}{d} \text{tr} \sqrt{\rho} \quad \text{for all } i = 1, \dots, d, \quad (13)$$

the choice $|i\rangle = |m_i\rangle$ fulfills all the conditions for optimal discrimination of the $|\tilde{\gamma}_i\rangle$ [19–21]. Thus, for measurements satisfying (13), it holds that $P_{\text{guess}}(\rho, \mathcal{M}) = \sum_i |\langle m_i | \sqrt{\rho} | m_i \rangle|^2 = \frac{1}{d} (\text{tr} \sqrt{\rho})^2$. Furthermore, we prove (see [13, Sec. III C]) that the condition (13) is also necessary for a projective measurement to achieve the optimal guessing probability. What remains to be proven is that there exist measurements satisfying condition (13). An example of such a measurement valid for any state is the one defined by a basis $\{|m_i\rangle\}$ that is unbiased to the eigenbasis of ρ , that is, all moduli of inner products between elements of the two different bases equal $\frac{1}{\sqrt{d}}$. However, as we discuss in two case studies, one can find other measurements satisfying condition (13) when $d > 2$. ■

Notice that, when Alice uses measurements satisfying (13), the decomposition (10) that is optimal for Eve is $|\tilde{\psi}_i\rangle = \sqrt{\rho} |m_i\rangle$. If ρ is full rank, $M_i = \rho^{-1/2} \rho_i \rho^{-1/2}$ is the “pretty good measurement” [10] for the ensemble $\{q_i, \rho_i/q_i\}$ steered by Eve. This measurement is known to be optimal when special symmetries like (13) are present in the problem [22] (in the notation of that work, the Gram matrix has entries $G_{ij} = \langle m_i | \rho | m_j \rangle$). Moreover, when Alice's measurement satisfies (13) and when ρ is full-rank, we can show (see [13, Sec. III D]) that Eve's optimal measurement to discriminate her local states is also a “pretty good” measurement.

After solving the problem for the guessing probability, we now move to the von Neumann entropy of the measurement outcomes conditioned on Eve's side information, a quantity of relevance in the multiround setting [23–25].

Theorem 2. The maximal conditional entropy that can be extracted from a quantum state ρ using a projective measurement is $H^* = \log_2 d - S(\rho)$, where $S(\rho) = -\text{tr} \rho \log_2 \rho$ is the von Neumann entropy.

Proof. From [14, Theorem 1, (i)], we have that the entropy $H(Z|E)$ of Alice's measurement outcomes Z conditioned on

Eve's side information E is

$$H(Z|E) = D\left(\rho \parallel \sum_z M_z \rho M_z\right), \quad (14)$$

where $\{M_z\}_z$ is Alice's projective measurement and $D(\rho|\sigma)$ is the quantum relative entropy between the states ρ and σ ,

$$D(\rho|\sigma) = \text{tr}[\rho(\log_2 \rho - \log_2 \sigma)], \quad (15)$$

which is defined when the support of ρ is contained within the support of σ . In [13, Sec. II B], we show that (1) a rank-one measurement is optimal for Alice to maximize $H(Z|E)$ for a given ρ , and (2) that

$$D\left(\rho \parallel \sum_z M_z \rho M_z\right) = S\left(\sum_z M_z \rho M_z\right) - S(\rho). \quad (16)$$

In [26], the r.h.s. is shown to be equivalent to the relative entropy of coherence of ρ with respect to the measurement basis, which is used as a quantifier of randomness.

The maximum von Neumann entropy of a state of dimension d is $\log_2 d$ and is achieved only for maximally mixed states, so we can upper bound Eq. (16) with

$$H(Z|E) \leq \log_2 d - S(\rho), \quad (17)$$

with equality reached if and only if Alice's measurement basis $\{|m_z\rangle\}_z$ leaves her system in the maximally mixed state, i.e., if the condition

$$\langle m_z | \rho | m_z \rangle = \frac{1}{d} \quad \text{for all } z = 1, \dots, d \quad (18)$$

is satisfied. ■

As in the case for the condition (13) for H_{\min}^* , suitable measurements satisfying (18) include bases $\{|m_z\rangle\}$ that are unbiased to the eigenbasis of ρ , implying the tightness of (17). However, when $d > 2$ we can find other suitable measurements, as discussed in two case studies. The quantity $\log_2 d - S(\rho)$ is defined in [27] as the total information of ρ , and it is used in [28] as a measure of the objective information of ρ .

We now consider the conditional max-entropy of the measurement outcomes conditioned on Eve's side information. This quantity has been interpreted as the security of Alice's measurement outcomes when used as a secret key [3].

Theorem 3. The maximal conditional max-entropy that can be extracted from a quantum state ρ using a projective measurement is $H_{\max}^* = \log_2 d + \log_2 \lambda_{\max}(\rho)$, where $\lambda_{\max}(\rho)$ is the largest eigenvalue of ρ .

Proof. The details missing here are given in [13, Sec. V]. Without loss of generality, we restrict Alice to performing rank-one projective measurements (see [13, Sec. II B]). In the case where Alice makes a rank-one projective measurement, the conditional max-entropy of her outcomes conditioned on Eve can be formulated [3] as

$$H_{\max}(A|E) = \log_2 p_{\text{secre}}, \quad (19)$$

where

$$p_{\text{secre}} = \max_{\sigma} \left(\sum_x \sqrt{p_x \text{tr}(\sigma |\psi_x^E\rangle\langle\psi_x^E| \psi_x^E)} \right)^2, \quad (20)$$

$$\text{s.t. } \sigma \geq 0, \quad \text{tr} \sigma = 1, \quad (21)$$

where $\{|\psi_x^E\rangle\}$ are Eve's postmeasurement states and $p_x = \langle m_x | \rho | m_x \rangle$. By applying the Cauchy-Schwartz inequality and identifying the semidefinite optimization problem for the maximum eigenvalue of a quantum state, we find

$$p_{\text{secre}} \leq d \lambda_{\max}(\rho). \quad (22)$$

In the case where the largest eigenvalue of ρ is unique, the bound (22) is reached if and only if the condition

$$|\langle m_x | u_{\max} \rangle|^2 = \frac{1}{d} \quad \text{for all } x = 1, \dots, d \quad (23)$$

is satisfied, where $|u_{\max}\rangle$ is the eigenvector of ρ corresponding to its largest eigenvalue. The optimal measurements in the case where the maximum eigenvalue of ρ is degenerate are discussed in [13, Sec. V]. ■

As in the case of H_{\min}^* and H^* , suitable measurements satisfying (23) include bases $\{|m_x\rangle\}$ that are unbiased to the eigenbasis of ρ , but, as before, when $d > 2$ we can find other suitable measurements, as discussed in two case studies.

Two case studies. Let us now study measurements that satisfy (13), (18), or (23) but which are not unbiased to the eigenbasis of ρ . For one qubit, it is quickly verified that all measurements that satisfy (13) are unbiased, so our first case study is for *one qutrit*. Consider $\rho = \sum_{i=1}^3 \lambda_i |i\rangle\langle i|$ with $\lambda_1 \geq \lambda_2 \geq \lambda_3$, and the measurement basis $\{M_i = |m_i\rangle\langle m_i|\}_{i=1,2,3}$, with

$$\begin{aligned} |m_1\rangle &= \sqrt{\frac{1+a}{3}} |1\rangle + \sqrt{\frac{1+b}{3}} |2\rangle + \sqrt{\frac{1+c}{3}} |3\rangle, \\ |m_2\rangle &= \sqrt{\frac{1+a}{3}} e^{i\theta_1} |1\rangle + \sqrt{\frac{1+b}{3}} |2\rangle + \sqrt{\frac{1+c}{3}} e^{i\theta_2} |3\rangle, \end{aligned} \quad (24)$$

and $|m_3\rangle$ defined by the normalization condition $\sum_i M_i = \mathbb{1}$, where $a = -(\gamma_2 - \gamma_3)k$, $b = (\gamma_1 - \gamma_3)k$, $c = -(\gamma_1 - \gamma_2)k$, $k \in \mathbb{R}$ and each $\gamma_i \geq 0$ with $\gamma_1 \geq \gamma_2 \geq \gamma_3$. We show in [13, Sec. VI A] that suitable parameters θ_1 and θ_2 can always be chosen such that this is a valid rank-one projective measurement when k is in the range $-\frac{1}{2} \leq k \leq \frac{1}{2}$.

This measurement basis is not in general unbiased to the eigenbasis of ρ , except when ρ is maximally mixed. When we set $\{\gamma_i\} = \{\sqrt{\lambda_i}\}$, it is straightforward to show that the condition (18) for the measurement to maximize H_{\min} is satisfied. Similarly, if we set $\{\gamma_i\} = \{\lambda_i\}$, we see that the condition (18) for maximal H is satisfied. Finally, the condition (23) for maximal H_{\max} is satisfied when $\gamma_2 = \gamma_3$, so we see that, for qutrits at least, there exist nonunbiased measurements that achieve maximal randomness for every ρ for all three of our quantifiers of randomness. Interestingly, though, these three conditions are inequivalent in general, so one can choose parameters $\{\gamma_i\}$ such that the measurement maximizes any one of the entropies but not the other two.

The second case study uses *two qubits*. It is based on the observation (proved in [13, Sec. VI B]) that there is no product

basis unbiased to the basis

$$\begin{aligned}
 |\psi_1\rangle &= |00\rangle, \\
 |\psi_2\rangle &= \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + |11\rangle), \\
 |\psi_3\rangle &= \frac{1}{\sqrt{3}}(|01\rangle + \omega|10\rangle + \omega^2|11\rangle), \\
 |\psi_4\rangle &= \frac{1}{\sqrt{3}}(|01\rangle + \omega^2|10\rangle + \omega|11\rangle), \quad (25)
 \end{aligned}$$

where $\omega = e^{i2\pi/3}$. Consider a state $\rho = \sum_{k=1}^4 \lambda_k |\psi_k\rangle\langle\psi_k|$ diagonal in this basis. To extract the maximal randomness with an unbiased measurement, one must be able to perform entangled measurements. This is not a conceptual problem in our setting, since there is no reason why the two qubits should be far apart; nonetheless, such measurements may be more challenging to perform than basic single-qubit measurements. The question is: can one extract maximal randomness from ρ by using a product basis? The answer seems to be positive. While we do not have an analytical proof, for a large number of choices of λ , we performed a heuristic optimization over product bases, both general ($\{|a, b\rangle, |a, b^\perp\rangle, |a^\perp, c\rangle, |a^\perp, c^\perp\rangle\}$, with six free parameters) and restricted to proper product measurements ($\{|a, b\rangle, |a, b^\perp\rangle, |a^\perp, b\rangle, |a^\perp, b^\perp\rangle\}$, with four free parameters). In both cases and for all states that we probed, we numerically found measurements satisfying $\sum_i ((m_i|\sqrt{\rho}|m_i) - \frac{\text{tr}\sqrt{\rho}}{4})^2 \leq 10^{-15}$, $\sum_i ((m_i|\rho|m_i) - \frac{1}{4})^2 \leq 10^{-15}$ or $\sum_i (|\langle m_i|u_{\max}\rangle|^2 - \frac{1}{4})^2 \leq 10^{-15}$, which suggests that there exist product measurements satisfying the conditions (13), (18), and (23), respectively. In this family of examples, therefore, the freedom to choose a measurement basis that is not unbiased may

lead to a practical advantage: it allows one to obtain maximal randomness with product measurements.

Conclusion. It is well known that quantum physics contains an intrinsic form of randomness, but, somewhat surprisingly, given a quantum state, it is unknown what is the optimal measurement to extract from it the maximum amount of such randomness. In this work, we concentrate on three different quantifiers of the amount of randomness in a measurement's outcomes conditioned on an adversary's side information: the conditional min-entropy, the conditional von Neumann entropy, and the conditional max-entropy. As one might have expected, all measurements in a basis that is unbiased to the eigenbasis of ρ maximize all three of these conditional entropies. However, we also find other measurements that achieve the optimal values, providing a flexibility that may have practical implications, as in the second case study reported. In fact, beyond its fundamental motivation, our analysis is also relevant for the design of device-dependent QRNGs, for which the quantum state is fully characterized. Interestingly, we find measurements in the qutrit case that maximize one of the three conditional entropies considered, but which are not optimal for the other two.

Acknowledgments. We thank Siddhartha Das for pointing out to us the use of Eq. (2) in other contexts [27,28]. This work is supported by the National Research Foundation, Singapore, and A*STAR under its CQT Bridging Grant, the Government of Spain (Severo Ochoa CEX2019-000910-S, Torres Quevedo PTQ2021-011870, FUNQIP, and European Union NextGenerationEU PRTR-C17.I1), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA program), the European Union (QSNP, 101114043, and Quanteria project Veriqtas), the ERC AdG CERQUITE, the AXA Chair in Quantum Information Science, and the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant No. 754510.

-
- [1] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
- [2] A. P. Vaisakh Mannalath and S. Mishra, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness, *Quantum Inf. Process.* **22**, 439 (2023).
- [3] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, *IEEE Trans. Inf. Theory* **55**, 4337 (2009).
- [4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [5] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2006.
- [6] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
- [7] As long as *process randomness* requires characterized devices, classical and quantum RNGs compete on the same grounds for speed, stability, practicality, etc. But, given an alleged RNG as a black box, on classical devices, one can test product randomness only with statistical tests. While process randomness implies product randomness, the opposite is certainly not true: one could have recorded a long enough list of random numbers, and the device under study may just be reading deterministically from that record.
- [8] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology, *Rep. Prog. Phys.* **80**, 124001 (2017).
- [9] A. Acín and L. Masanes, Certified randomness in quantum physics, *Nature (London)* **540**, 213 (2016).
- [10] P. Hausladen and W. K. Wootters, A 'pretty good' measurement for distinguishing quantum states, *J. Mod. Opt.* **41**, 2385 (1994).
- [11] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, Quantum randomness extraction for various levels of characterization of the devices, *J. Phys. A: Math. Theor.* **47**, 424028 (2014).
- [12] G. Senno, T. Strohm, and A. Acín, Quantifying the intrinsic randomness of quantum measurements, *Phys. Rev. Lett.* **131**, 130202 (2023).
- [13] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevA.110.L010403> for the detailed proofs of all

- the technical results in the main text, which include Refs. [29–33].
- [14] P. J. Coles, Unification of different views of decoherence and discord, *Phys. Rev. A* **85**, 042103 (2012).
- [15] Y. C. Eldar, A. Megretski, and G. C. Verghese, Designing optimal quantum detectors via semidefinite programming, *IEEE Trans. Inf. Theory* **49**, 1007 (2003).
- [16] L. P. Hughston, R. Jozsa, and W. K. Wootters, A complete classification of quantum ensembles having a given density matrix, *Phys. Lett. A* **183**, 14 (1993).
- [17] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Measuring quantum coherence with entanglement, *Phys. Rev. Lett.* **115**, 020403 (2015).
- [18] C. Xiong and J. Wu, Geometric coherence and quantum state discrimination, *J. Phys. A: Math. Theor.* **51**, 414005 (2018).
- [19] A. S. Holevo, Statistical decision theory for quantum systems, *J. Multivariate Anal.* **3**, 337 (1973).
- [20] C. W. Helstrom, Quantum detection and estimation theory, *J. Stat. Phys.* **1**, 231 (1969).
- [21] H. Yuen, R. Kennedy, and M. Lax, Optimum testing of multiple hypotheses in quantum detection theory, *IEEE Trans. Inf. Theory* **21**, 125 (1975).
- [22] N. Dalla Pozza and G. Pierobon, Optimality of square-root measurements in quantum state discrimination, *Phys. Rev. A* **91**, 042334 (2015).
- [23] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, *IEEE Trans. Inf. Theory* **55**, 5840 (2009).
- [24] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, *Commun. Math. Phys.* **379**, 867 (2020).
- [25] H. Dai, B. Chen, X. Zhang, and X. Ma, Intrinsic randomness under general quantum measurements, *Phys. Rev. Res.* **5**, 033081 (2023).
- [26] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, Quantum coherence and intrinsic randomness, *Adv. Quantum Technol.* **2**, 1900053 (2019).
- [27] W. H. Zurek, Information transfer in quantum measurements: Irreversibility and amplification, in *Quantum Optics, Experimental Gravity, and Measurement Theory*, edited by P. Meystre and M. O. Scully, NATO Advanced Science Institutes Series Vol. 94 (Springer, Boston, MA, 1983), pp. 87–116.
- [28] M. Horodecki, P. Horodecki, and J. Oppenheim, Reversible transformations from pure to mixed states and the unique measure of information, *Phys. Rev. A* **67**, 062104 (2003).
- [29] R. Renner, Security of quantum key distribution, [arXiv:quant-ph/0512258](https://arxiv.org/abs/quant-ph/0512258).
- [30] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, The classical-quantum boundary for correlations: Discord and related measures, *Rev. Mod. Phys.* **84**, 1655 (2012).
- [31] M. Tomamichel, *Quantum Information Processing with Finite Resources* (Springer International Publishing, Cham, 2016).
- [32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [33] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science* (IOP Publishing, Bristol, UK, 2023), pp. 2053–2563.