Quantifying the Intrinsic Randomness of Quantum Measurements

Gabriel Senno,[1,2] Thomas Strohm,[3] and Antonio Acín[1,4]
[1]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
[2]Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels, Barcelona, Spain
[3]Corporate Research, Robert Bosch GmbH, 71272 Renningen, Germany
[4]ICREA-Institucio Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain

(Received 5 April 2022; accepted 31 August 2023; published 28 September 2023)

Intrinsic quantum randomness is produced when a projective measurement on a given basis is implemented on a pure state that is not an element of the basis. The prepared state and implemented measurement are perfectly known, yet the measured result cannot be deterministically predicted. In realistic situations, however, measurements and state preparation are always noisy, which introduces a component of stochasticity in the outputs that is not a consequence of the intrinsic randomness of quantum theory. Operationally, this stochasticity is modeled through classical or quantum correlations with an eavesdropper, Eve, whose goal is to make the best guess about the outcomes produced in the experiment. In this Letter, we study Eve's maximum guessing probability when she is allowed to have correlations with both the state and the measurement. We show that, unlike the case of projective measurements (as it was already known) or pure states (as we prove), in the setting of generalized measurements and mixed states, Eve's guessing probability differs depending on whether she can prepare classically or quantumly correlated strategies.

DOI: 10.1103/PhysRevLett.131.130202

Introduction.—Quantum theory contains a form of randomness that is not the result of ignorance or any stochastic behavior. For instance, according to the theory, the result of implementing a spin measurement along the x direction on a spin state pointing in the $+z$ direction is fully unpredictable. This is despite the fact that the description of the experiment within the theory is complete, in the sense that the prepared state and implemented measurement are perfectly known, without any stochastic component. This form of randomness is *intrinsic* to quantum theory and impossible in classical physics [1,2]. Beyond fundamental considerations, it is also the key element behind any quantum random-number generator (QRNG).

In real life implementations, however, measurements are never projective and states are never pure. Noise and imperfections introduce an unavoidable element of *stochasticity* that produces an apparent randomness that is not intrinsic to quantum theory. Therefore, it is a fundamental problem to design the tools to estimate the correct amount of intrinsic quantum randomness produced in a quantum experiment. This question is of relevance from a quantum foundations viewpoint, but also for the proper design of QRNGs. In fact, the natural and operational way to model the stochasticity in the components of the setup is through classical or quantum correlations with an external observer, Eve, who can also be interpreted as an eavesdropper and whose goal is to make the best *guess* about the outcomes produced in the experiment. The correlations with Eve are often named (classical or quantum) side information.

So far, the scenario that has mostly been considered in the literature is the one in which all the stochasticity comes from the prepared quantum state. That is, the state of the system is no longer pure, but the measurement is still assumed to be projective. The main goal of this work is to study *Eve's guessing probability* about the outcomes of a quantum measurement when she is allowed to have correlations with both the state and the measurement. We work in a completely *device-dependent* setting, where the state of the system and the measurement have been fully characterized, and consider two alternative formulations of this problem: a classical and a quantum one. In the classical picture, Eve can sample a random variable Λ given the value of which there is no stochasticity in her description of the experiment. For the quantum case, we consider the model of quantum side information involving a *generalized* Naimark dilation of the user's measurement, introduced by Frauchiger *et al.* [3]. In this model, Eve is allowed to have a quantum system E correlated with the system being measured and with the ancillary system in the dilation.

It is a well-known result that when the measurement is assumed to be projective (or, more generally, extremal), Eve's guessing probability in the classical and quantum pictures coincide. Our first result (Theorem 2) is that this is also the case when the measurement is arbitrary but the

TABLE I. Relationship between the classical and quantum guessing probabilities. Prior to this work, they were only known to be equivalent for projective measurements. In this work we proved (i) the equivalence for pure states and an arbitrary POVMs and (ii) that the quantum guessing probability can be strictly larger than the classical in the most general scenario.

	Projective measurement	General POVM
Pure state	$p^Q_{\text{guess}}(X\|E) = p^C_{\text{guess}}(X\|\Lambda)$	$p^Q_{\text{guess}}(X\|E) = p^C_{\text{guess}}(X\|\Lambda)$ [*This Letter*]
General state	$p^Q_{\text{guess}}(X\|E) = p^C_{\text{guess}}(X\|\Lambda)$	$p^Q_{\text{guess}}(X\|E) \geq p^C_{\text{guess}}(X\|\Lambda)$ [*This Letter*]
		$\exists \rho,\ \{M^x_S\}_x\ p^Q_{\text{guess}}(X\|E,\rho,\{M^x_S\}_x) > p^C_{\text{guess}}(X\|\Lambda,\rho,\{M^x_S\}_x)$ [*This Letter*]

state is pure. Then, we move to the more relevant case in which both the prepared state and the implemented measurement are subject to (in general, correlated) noise, and provide a framework to estimate the produced quantum randomness. For this general scenario, we first show that Eve's guessing probability in the quantum picture is always greater than or equal to the classical one (Theorem 3). Our main result, however, is that there exist states and measurements for which the inequality is strict (Theorem 4). In Table I we summarize the relative strengths of classical and quantum guessing probabilities for the different combinations of types of states and measurements. We finally illustrate the applicability of our approach by considering an experiment in which noisy single-photon detectors are applied to the two-mode state resulting from a single photon impinging into a balanced beam splitter. The bounds on the guessing probability we derive demonstrate that Eve could make a more informed guess on the obtained results than when using the measurement model in [3].

Noisy preparation.—Before presenting our contributions, it is worth reviewing the known results for the setting of a projective measurement (PVM) on a system in a mixed state. Let us start with a toy example. Consider that a measurement in the computational basis $\{|0\rangle, |1\rangle\}$ is conducted on a qubit S in the $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ state and that the outcome $+1$ is obtained. Suppose that this outcome was to be communicated to an interested user, Alice, but, before that, an eavesdropper, Eve, learns this outcome and then destroys any record of it. If Alice, knowing that the measurement was performed but ignoring the outcome, wants to describe the state of system S after the measurement, she has to associate to it the ensemble of states $\{p_X(x), |x\rangle\}$ with $p_X(0) = p_X(1) = 1/2$ and represent it with the maximally mixed state $(\mathbb{I}/2) = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|]$. Therefore, to the question of what would be the result of a second measurement on S in the computational basis, she can do no better than a uniformly random guess. Eve, on the other hand, having the additional *classical side information* of the first measurement's outcome, has a better (in fact, complete) description of the state of S and, therefore, can deterministically predict that the second outcome will be $+1$.

As this simple example shows, when a system S is in a mixed state ρ_S compatible with an ensemble $\{p_\Lambda(\lambda), |\varphi_\lambda\rangle_S\}$, in order to determine the predictability of the outcomes of a measurement $\{\Pi^x_S\}_x$ on S one has to consider the possibility of Eve having access to the random variable (or, the classical noise) Λ. In that case, after learning (or, sampling) a value λ for Λ, Eve knows that S is in the state $|\varphi_\lambda\rangle_S$ and, hence, her best prediction for the outcome of $\{\Pi^x_S\}_x$ would be $\text{argmax}_x \langle\varphi_\lambda|\Pi^x_S|\varphi_\lambda\rangle_S$. The probability that she guesses correctly is obtained averaging over Λ, i.e., $\sum_\lambda p(\lambda)\max_x \langle\varphi_\lambda|\Pi^x_S|\varphi_\lambda\rangle_S$. Finally, since for a given mixed state ρ_S there are infinitely many ensembles compatible with it, to assess the unpredictability of the outcomes of $\{\Pi^x_S\}_x$ one has to consider them all, as some might provide better predicting power to Eve than others. This rationale leads to defining Eve's *classical guessing probability* as

$$p^C_{\text{guess}}(X|\Lambda,\rho_S,\{\Pi^x_S\}_x) \coloneqq \max_{p(\lambda),|\varphi_\lambda\rangle_S} \sum_\lambda p(\lambda)\max_x \langle\varphi_\lambda|\Pi^x_S|\varphi_\lambda\rangle_S \quad \text{subject to} \sum_\lambda p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|_S = \rho_S. \tag{1}$$

Notice that when $\rho_S = |\psi\rangle\langle\psi|_S$ is pure, because of its extremality in the set of states, $p^C_{\text{guess}}(X|\Lambda,\rho_S,\{\Pi^x_S\}_x) = \max_x \langle\psi|\Pi^x_S|\psi\rangle_S$ and, hence, all the observed randomness is of a quantum origin.

One could have considered that Eve, rather than having access to some classical random variable Λ, has access to another quantum system E (or, to the environment) such that the global state $\rho_{SE} = |\psi\rangle\langle\psi|_{SE}$ is (without loss of generality) pure. A measurement of $\{\Pi^x_S\}$ on S produces the classical outcome x with probability $p(x) = \text{Tr}[\Pi^x_S\rho_S]$ and steers Eve's system E to the state $\rho^x_E = \text{Tr}_S[(\Pi^x_S \otimes \mathbb{I}_E)|\psi\rangle\langle\psi|_{SE}]/p(x)$. Knowing this, Eve would then look for a measurement $\{M^x_E\}_x$ on her system E that maximizes the probability that its outcome (her guess) is x when the state steered on her system was ρ^x_E—in other words, a measurement maximizing $\sum_x p(x)\text{Tr}[M^x_E\rho^x_E]$, the average probability to distinguish the states ρ^x_E occurring with probability $p(x)$. Eve's *quantum guessing probability* [4] is then given by

$$p^Q_{\text{guess}}(X|E,\rho_S,\{\Pi^x_S\}_x) \coloneqq \max_{\{M^x_E\}_x} \sum_x p(x)\text{Tr}[M^x_E\rho^x_E] = \max_{\{M^x_E\}_x} \sum_x \langle\psi|\Pi^x_S \otimes M^x_E|\psi\rangle_{SE}, \tag{2}$$

where $|\psi\rangle_{SE}$ is any fixed purification of ρ_S (they are all equivalent up to a unitary in E, which can be absorbed in the optimization over $\{M_E^x\}_x$). Given that the states ρ_E^x are, in general, not diagonal in the same basis, we say that Eve holds *quantum side information* about the random variable X.

Theorem 1 states the well-known result that these two different ways of quantifying Eve's predicting power are equivalent. In other words, entanglement does not provide Eve with an advantage in the task of guessing the outcomes of a PVM on a mixed state.

Theorem 1.—For every state ρ_S and every PVM $\{\Pi_S^x\}_x$,

$$p^C_{\text{guess}}(X|\Lambda,\rho_S,\{\Pi_S^x\}_x) = p^Q_{\text{guess}}(X|E,\rho_S,\{\Pi_S^x\}_x).$$

This result, which in fact holds for any extremal measurement, is often assumed (see, e.g., [[5], Section 8.2]) but, to our knowledge, no explicit proof of it appears on the literature. It follows from the fact that any measurement on Eve's system E defines a convex decomposition of the state ρ_S of system S, and that any decomposition (in particular, the optimal) can be steered in this way. In the following, we prove a more general result (Theorem 3) from which Theorem 1 follows as a corollary.

Noisy measurement.—Before studying the most general scenario, let us first consider the case in which a general measurement, represented by a positive-operator valued measure (POVM) $\{M_S^x\}_x$, is measured on a system S in a pure state $|\phi\rangle_S$. Given that the set of POVMs is, just like the set of quantum states, convex [6], we can proceed via analogy with the case of a mixed state and assume that Eve can now sample a random variable Λ such that $M_S^x = \sum_\lambda p(\lambda) M_S^{x,\lambda}$ with $\{M_S^{x,\lambda}\}_x$ POVMs for all λ. With her knowledge of λ, her best prediction for the outcome of the measurement on S is $\text{argmax}_x \langle\phi|M_S^{x,\lambda}|\phi\rangle$ and this is correct with probability $\sum_\lambda p(\lambda)\max_x \langle\phi|M_S^{x,\lambda}|\phi\rangle$. Finally, by letting Eve optimize over all possible convex combinations, her *classical guessing probability* is

$$\begin{aligned} &p^C_{\text{guess}}(X|\Lambda,|\phi\rangle_S,\{M_S^x\}_x) \\ &:= \max_{p(\lambda),\{M_S^{x,\lambda}\}_x} \sum_\lambda p(\lambda)\max_x \langle\phi|M_S^{x,\lambda}|\phi\rangle_S \\ &\quad \text{subject to} \sum_\lambda p(\lambda) M_S^{x,\lambda} = M_S^x \quad \text{for all } x. \end{aligned} \tag{3}$$

Analogously to the case of a pure state, when $\{M_S^x\}_x$ is extremal (but not necessarily projective [6]) we have completely intrinsic quantum randomness, that is $p^C_{\text{guess}}(X|\Lambda,|\phi\rangle_S,\{M_S^x\}_x) = \max_x \langle\phi|M_S^x|\phi\rangle_S$.

A notion of a quantum guessing probability for the case of general POVMs was given in [3]. One assumes that what is seen as a POVM $\{M_S^x\}_x$ on system S is, in fact, a PVM $\{\Pi_{SA}^x\}$ on S and an ancillary system A. In fact, $\{\Pi_{SA}^x\}_x$ is a Naimark extension of $\{M_S^x\}_x$ and the correlations with Eve are modeled via a mixed state σ_A on A, of which she holds a purification $|\psi_{AE}\rangle$. See Fig. 1 for a schematic description of this model of quantum side information. Then, as in the case studied in the previous section, Eve optimizes over measurements $\{M_E^x\}_x$ on her system E trying to maximize on average the correlation $\langle\phi,\psi|\Pi_{SA}^x \otimes M_E^x|\phi,\psi\rangle_{SAE}$. Eve's quantum guessing probability is thus given by

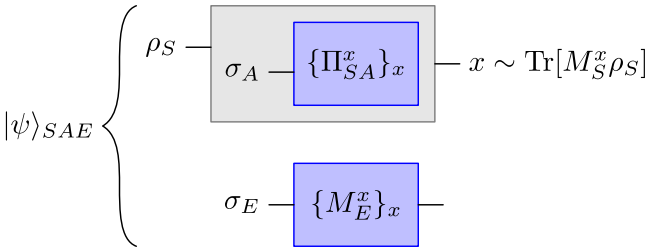

FIG. 1. Schematic description of our model for quantum side information. Eve chooses a projective implementation $(\{\Pi_{SA}^x\}_x, \sigma_A)$ of the user's POVM $\{M_S^x\}_x$ and she is allowed to be entangled with both the system S and the ancilla A. With this, she optimizes over measurements on her subsystem maximizing the correlation with the user's measurement outcomes [see Eq. (6)].

$$\begin{aligned} &p^Q_{\text{guess}}(X|E,|\phi\rangle_S,\{M_S^x\}_x) \\ &:= \max_{\{\Pi_{SA}^x\}_x,|\psi\rangle_{AE},\{M_E^x\}_x} \sum_x \langle\phi,\psi|\Pi_{SA}^x \otimes M_E^x|\phi,\psi\rangle_{SAE} \\ &\quad \text{subject to} \\ &\quad \text{Tr}_A[\Pi_{SA}^x(\mathbb{I}_S \otimes \text{Tr}_E[|\psi\rangle\langle\psi|_{AE}])] = M_S^x \quad \text{for all } x. \end{aligned} \tag{4}$$

There is an important difference between Eq. (4) and the analogous in the framework introduced in [3]. In the latter, the particular projective implementation $(\{\Pi_{SA}^x\}_x, \sigma_A)$ for a given POVM $\{M_S^x\}_x$ has to be specified by the user. In this work, we let it be chosen, in fact optimized, by Eve. This is more natural when quantifying randomness, especially in adversarial scenarios. Our first result, Theorem 2, is the analogous of Theorem 1, now for noisy measurements and pure states, instead of noisy states and PVMs.

Theorem 2.—For every pure state $|\phi\rangle_S$ and every POVM $\{M_S^x\}_x$,

$$p^C_{\text{guess}}(X|\Lambda,|\phi\rangle_S,\{M_S^x\}_x) = p^Q_{\text{guess}}(X|E,|\phi\rangle_S,\{M_S^x\}_x).$$

Theorem 2, in fact, follows as a corollary of a theorem for the most general scenario, which we state in the following section.

Noisy preparation and measurement.—We arrive, now, at the most general setting. Let us consider that a POVM $\{M_S^x\}_x$ is measured on a system S in a state ρ_S. When considering classical side information, we now let Eve choose convex decompositions of both the state and the

measurement. Her classical guessing probability is thus given by

$$p^{C}_{\text{guess}}(X|\Lambda,\rho_S,\{M^x_S\}_x) \coloneqq \max_{p(i,j),|\varphi_i\rangle_S,\{M^{x,j}_S\}_x} \sum_{i,j} p(i,j)\max_x \langle\varphi_i|M^{x,j}_S|\varphi_i\rangle_S$$

subject to

$$\sum_{i,j} p(i,j)|\varphi_i\rangle\langle\varphi_i| = \rho_S$$
$$\sum_{i,j} p(i,j)M^{x,j}_S = M^x_S \quad \text{for all } x$$
$$\sum_{i,j} p(i,j)\langle\varphi_i|M^{x,j}_S|\varphi_i\rangle = \text{Tr}[M^x_S\rho_S]. \tag{5}$$

The last condition in this optimization problem states that Eve's strategy, although potentially correlating the choices of pure state and extremal measurement, cannot be arbitrary, as it must reproduce the observed statistics on S. In the restricted cases of the previous sections, we do not need to explicitly impose this because it follows immediately from the convex decomposition requirement.

In the case of quantum side information, we let Eve hold a purification of the joint state ρ_{SA} of the system S plus the ancillary system used for her choice of a projective implementation $(\{\Pi^x_{SA}\},\sigma_A)$ of $\{M^x_S\}_x$. Notice that we do not assume that $\rho_{SA}=\rho_S\otimes\sigma_A$. Eve's quantum guessing probability is thus given by

$$p^{Q}_{\text{guess}}(X|E,\rho_S,\{M^x_S\}_x) \coloneqq \max_{\{\Pi^x_{SA}\}_x,|\psi\rangle_{SAE},\{M^x_E\}_x} \sum_x \langle\psi|\Pi^x_{SA}\otimes M^x_E|\psi\rangle_{SAE}$$

subject to

$$\text{Tr}_{AE}[|\psi\rangle\langle\psi|_{SAE}] = \rho_S$$
$$\text{Tr}_A[\Pi^x_{SA}(\mathbb{I}_S\otimes\text{Tr}_{SE}[|\psi\rangle\langle\psi|_{SAE}])] = M^x_S \quad \text{for all } x$$
$$\langle\psi|\Pi^x_{SA}\otimes\mathbb{I}_E|\psi\rangle_{SAE} = \text{Tr}[M^x_S\rho_S]. \tag{6}$$

As a warm up for our main result, we first state Theorem 3, whose proof we defer to the Supplemental Material [7]. Its first part says that, as expected, any general strategy involving classical side information can be implemented in the quantum picture. Its second part is a sufficient condition for there to be an equality between the classical and the quantum guessing probabilities in this general scenario.

Theorem 3.—Let ρ_S be a state, $\{M^x_S\}$ a POVM, and $p^{C}_{\text{guess}}(X|\Lambda,\rho_S,\{M^x_S\}_x)$ and $p^{Q}_{\text{guess}}(X|E,\rho_S,\{M^x_S\}_x)$ as defined in Eqs. (5) and (6), respectively. Then, (1) $p^{C}_{\text{guess}}(X|\Lambda,\rho_S,\{M^x_S\}_x) \le p^{Q}_{\text{guess}}(X|E,\rho_S,\{M^x_S\}_x)$; (2) if $p^{Q}_{\text{guess}}(X|E,\rho_S,\{M^x_S\}_x)$ has an optimal solution $\langle\{\Pi^x_{SA}\}_x, |\psi\rangle_{SAE},\{M^x_E\}_x\rangle$ such that the postmeasurement states on SA

$$\rho^x_{SA} = \frac{\text{Tr}_E[(\mathbb{I}_{SA}\otimes M^x_E)|\psi\rangle\langle\psi|_{SAE}]}{\langle\psi|\mathbb{I}_{SA}\otimes M^x_E|\psi\rangle_{SAE}}$$

are all separable, then $p^{Q}_{\text{guess}}(X|E,\rho_S,\{M^x_S\}_x) \le p^{C}_{\text{guess}}(X|\Lambda,\rho_S,\{M^x_S\}_x)$.

It is straightforward to see that Theorems 1 and 2 immediately follow as a corollaries of Theorem 3. For example, if $\rho_S=|\phi\rangle\langle\phi|_S$, then the postmeasurement states on SA after any measurement on E are necessary separable (in fact, product), implying then, by Theorem 3, that $p^{C}_{\text{guess}}(X|\Lambda,|\phi\rangle_S,\{M^x_S\}_x) = p^{Q}_{\text{guess}}(X|E,|\phi\rangle_S,\{M^x_S\}_x)$. Same reasoning holds for Theorem 1.

From the second part of Theorem 3 it follows that, if there is to be an advantage for Eve in the quantum scenario, it must come from her preparing an entangled state between S and A via her measurement. Building on this fact, our main result, Theorem 4 below, is the construction of a 4-outcome qubit measurement (in fact, a family of these) for which Eve's quantum guessing probability is perfect and strictly greater than the classical one.

Theorem 4.—There exists a 4-outcome qubit POVM $\{M^x_S\}_x$ such that

$$1 = p^{Q}_{\text{guess}}\left(X|E,\frac{\mathbb{I}_S}{2},\{M^x_S\}_x\right) > p^{C}_{\text{guess}}\left(X|\Lambda,\frac{\mathbb{I}_S}{2},\{M^x_S\}_x\right).$$

Proof sketch.—The proof of Theorem 4 can be found in the Supplemental Material [7]. Here, we sketch the main parts. Let $\{|\Phi^\theta_x\rangle\}^4_{x=1}$ be the parametric family, indexed by $\theta\in[0,\pi/2]$, of entangled bases for a space of two qubits defined in [[8], Eq. (3)]. We set

$$\{\Pi^{x,\theta}_{SA}\}_x = \{|\Phi^\theta_x\rangle\langle\Phi^\theta_x|\}_x \quad \text{and} \quad \rho_{SA} = \frac{\mathbb{I}_{SA}}{4},$$

and, therefore,

$$\{M^{x,\theta}_S\}_x = \left\{\text{Tr}_A\left[\Pi^{x,\theta}_{SA}\cdot\frac{\mathbb{I}_{SA}}{2}\right]\right\}_x \quad \text{and} \quad \rho_S = \frac{\mathbb{I}_S}{2}.$$

It is straightforward to see that Eve can achieve $p^{Q}_{\text{guess}}(X|E,\rho_S,\{M^{x,\theta}_S\}_x)=1$ if she steers the ensemble $\{1/4,|\Phi^\theta_x\rangle\}_x$ on SA by measuring her share of $|\psi\rangle_{SAE} = \sum_x 1/2|\Phi^\theta_x\rangle_{SA}|x\rangle_E$ in the $\{|x\rangle\}$ basis. As for the classical guessing probability being strictly below 1, this follows from two technical results that we prove in the Supplemental Material [7]. The first one states that for the settings in which extremal measurements are necessarily rank one (e.g., d^2-outcome measurements, where d is the dimension of S), having $p^{C}_{\text{guess}}(X|\Lambda,\rho,\{M^x_S\}_x)=1$ implies that $\{M^x_S\}_x$ is a convex combination of PVMs. In [[9], Eq. (56)], the class of 4-outcome qubit POVMs that are convex combinations of PVMs was shown to be definable with an semidefinite program. We numerically

checked that for values of $\theta \in [0, \pi/10]$, the POVMs $\{M_S^{x,\theta}\}_x$ are not a convex combination of PVMs [10]. To end the proof, and for concreteness, we set $\{M_S^x\}_x = \{M_S^{x,\theta}\}_x$ for $\theta = 0$. ∎

We conclude this section with a corollary to Theorem 3, which applies to a restricted adversarial setting. Consider the case in which the quantum adversary Eve is restricted to having two separate systems E_1 and E_2, one purifying ρ_S and the other one purifying σ_A, which she cannot measure jointly. Corollary 1 below states that, in this restricted setting, every quantum strategy is classically simulable.

Corollary 1.—Let $\tilde{p}^Q_{\text{guess}}(X|E, \rho_S, \{M_S^x\}_x)$ be as in Eq. (6) with the additional restriction that $|\psi\rangle_{SAE} = |\psi_1\rangle_{SE_1}|\psi_2\rangle_{AE_2}$ and $M_E^x = M_{E_1}^x \otimes M_{E_2}^x$. Then,

$$\tilde{p}^Q_{\text{guess}}(X|E, \rho_S, \{M_S^x\}_x) \leq p^C_{\text{guess}}(X|\Lambda, \rho_S, \{M_S^x\}_x).$$

It is unclear to us whether, on the other hand, every general classical strategy of Eq. (5) can be reproduced by these restricted quantum strategies. Notice that the quantum strategies that we build from classical strategies in the proof of the first part of Theorem 3 fall outside this restricted set. We leave this question for future research.

Application to a QRNG.—In [[3], Examples 1–3], the following simple model of an imperfect QRNG based on a beam splitter (BS) with inefficient detectors is considered. Let $|\psi\rangle_{12} := (1/\sqrt{2})(|10\rangle + |01\rangle)$ be the two-mode state obtained after sending a single photon onto an ideal BS. Let there be detectors with efficiency $\mu \in [0, 1]$ at each of two output paths of the BS and let $M_D^1 = \mu|1\rangle\langle 1|_D$ be the operator of a two-outcome POVM $\{M_D^0, M_D^1\}$ representing the detection of 1 photon on path $D \in \{1, 2\}$. If we measure each path separately, the overall measurement can be represented by the POVM

$$M_\mu = \{M_1^0 \otimes M_2^0, M_1^0 \otimes M_2^1, M_1^1 \otimes M_2^0, M_1^1 \otimes M_2^1\}.$$

As we noted before, in order to use the framework in [3] to quantify the unpredictability of this QRNG's outcomes one has to decide on a particular projective implementation of $\{M_S^x\}$. In [[3], Example 3], the authors consider the projective implementation $(\{\Pi_{11'}^x \otimes \Pi_{22'}^y\}_{x,y}, \sigma_{1'} \otimes \sigma_{2'})$ of M_μ with

$$\Pi_{DD'}^1 = |1\rangle\langle 1|_D \otimes |1\rangle\langle 1|_{D'} \quad \text{and}$$
$$\sigma_{D'} = (1-\mu)|0\rangle\langle 0|_{D'} + \mu|1\rangle\langle 1|_{D'}. \tag{7}$$

In Fig. 2, we plot Eve's guessing probability for this particular projective implementation

$$f(\mu) := \max_{\{M_E^{x,y}\}_{x,y}} \sum_{x,y} \langle\psi|\Pi_{11'}^x \otimes \Pi_{22'}^y \otimes M_E^{x,y}|\psi\rangle_{11'22'E}, \tag{8}$$

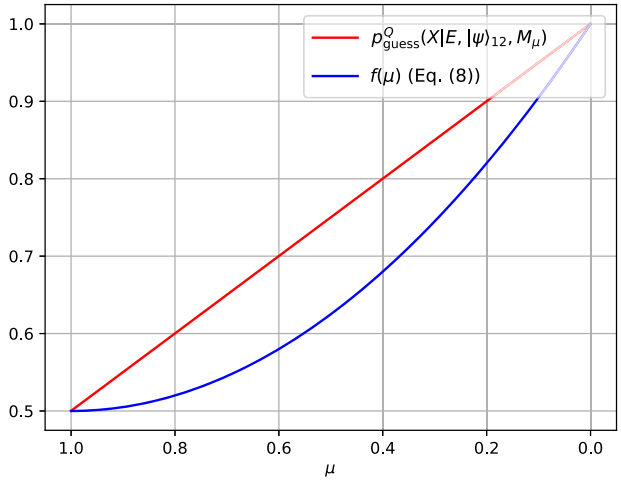

FIG. 2. Comparison between our work and [3]. In this plot we show that if, rather than assuming the particular projective implementation of inefficient detectors on the outputs of an ideal BS used in [3] and reproduced in Eq. (7), we let it be chosen by Eve, her guessing probability is strictly bigger for every value of the efficiency $\mu \in (0, 1)$.

with $|\psi\rangle_{11'22'E}$ a fixed purification of $|\psi\rangle\langle\psi|_{12} \otimes \sigma_{1'} \otimes \sigma_{2'}$ and compare it to $p^Q_{\text{guess}}(X|E, |\psi\rangle_{12}, M_\mu)$, as a function of the (decreasing) efficiency μ of the detectors [10].

We see that, for every value of the efficiency $\mu \in (0, 1)$, fixing the particular projective extension in Eq. (7) strictly decreases Eve's maximal guessing probability. In other words, the projective implementation in Eq. (7) leads to an underestimation of Eve's guessing probability for every $\mu \in (0, 1)$.

Conclusions.—In this Letter, we have studied the unpredictability of the outcomes of a general quantum measurement from the point of view of an eavesdropper holding side information correlated to both the state of the system and the measurement. We have shown that, while the quantum and classical guessing probabilities coincide in the case of extremal states (i.e., pure) or extremal measurements, equivalence does not hold in general.

The classical and quantum guessing probabilities not coinciding in the general scenario has immediate consequences for the design of device-dependent QRNGs, as proper justifications should be issued regarding which of the two pictures is assumed. However, being the characterization of intrinsic randomness is quite a general quantum mechanical problem, our result might find applicability beyond QRNGs.

As for future research directions, it would be interesting to characterize the set of states and measurements for which there is a quantum advantage in the guessing probability. Last but not least, from a practical perspective, it is important to come up with ways to compute (or, at least, computably approximate from above) these quantities.

We thank Máté Farkas for fruitful discussions. We acknowledge financial support from the ERC AdG CERQUTE, the EU project QRANGE (Grant No. 820405), the AXA Chair in Quantum Information Science, the Government of Spain (FIS2020-TRANQI, NextGen Recovery Funds and Severo Ochoa CEX2019-000910-S, Torres Quevedo PTQ2021-011870), Fundació Cellex, Fundació Mir-Puig and Generalitat de Catalunya (CERCA, AGAUR SGR 1381).

Note added.—While completing this work we became aware of a recent work [11] in which a similar approach to characterize the intrinsic randomness under quantum measurements is introduced.

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[2] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[3] D. Frauchiger, R. Renner, and M. Troyer, True randomness from realistic quantum devices, arXiv:1311.4547.

[4] R. König, R. Renner, and C. Schaffner, The operational meaning of min-and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[5] V. Scarani, *Bell Nonlocality* (Oxford University Press, New York, 2019).

[6] G. M. D'Ariano, P. Lo Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A **38**, 5979 (2005).

[7] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.130202 for the proofs of Theorems 3 and 4.

[8] A. Tavakoli, N. Gisin, and C. Branciard, Bilocal Bell Inequalities Violated by the Quantum Elegant Joint Measurement, Phys. Rev. Lett. **126**, 220401 (2021).

[9] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Simulating Positive-Operator-Valued Measures with Projective Measurements, Phys. Rev. Lett. **119**, 190501 (2017).

[10] For the code used in all the numerical simulations, see https://github.com/gsenno/quantifying-randomness.

[11] H. Dai, B. Chen, X. Zhang, and X. Ma, Intrinsic randomness under general quantum measurements, Phys. Rev. Res. **5**, 033081 (2023).