





Intrinsic randomness under general quantum measurements

Hao Dai ^{1,2}, Boyang Chen ¹, Xingjian Zhang ¹, and Xiongfeng Ma ^{1,*}
¹Center for Quantum Information, Institute for Interdisciplinary Information Sciences,
 Tsinghua University, Beijing 100084, People's Republic of China
²Hefei National Laboratory, University of Science and Technology of China,
 Hefei, Anhui 230088, People's Republic of China



(Received 20 March 2022; revised 28 February 2023; accepted 8 July 2023; published 4 August 2023)

Quantum measurements can produce unpredictable randomness arising from the uncertainty principle. When measuring a state with von Neumann measurements, the intrinsic randomness can be quantified by the quantum coherence of the state on the measurement basis. Unlike projection measurements, there are additional and possibly hidden degrees of freedom in an apparatus for generic measurements. We propose an adversary scenario to characterize the intrinsic randomness of general measurements with arbitrary input states. Interestingly, we discover that certain measurements, including symmetric and information-complete ones, generate nonzero randomness for all states, which suggests a new approach for designing source-independent random number generators without state characterization. Furthermore, our results reveal that intrinsic randomness can quantify coherence under general measurements, which generalizes the result in the standard resource theory of state coherence.

DOI: [10.1103/PhysRevResearch.5.033081](https://doi.org/10.1103/PhysRevResearch.5.033081)

I. INTRODUCTION

Randomness is a critical resource in cryptography and scientific simulation. In classical physics, the deterministic nature of Newtonian physics cannot provide intrinsically unpredictable randomness. This poses a significant challenge to the security of cryptosystems, which rely on the unpredictability of random numbers for information-theoretic security. Fortunately, the uncertainty principle in quantum physics offers a promising solution for generating intrinsic randomness [1]. Quantum random number generators (QRNGs) harness this quantum feature and provide a strong foundation for the security of cryptographic systems [2,3].

A QRNG is typically composed of a source and a detector, each of which plays a critical role in generating truly random numbers. The source is characterized by a quantum state [4,5], while the detector is calibrated by a quantum measurement [6,7]. After obtaining outcomes from the quantum measurement, the legitimate user, Alice, must analyze the amount of randomness in the raw data to ensure the output unpredictability. This analysis can be put in an adversary scenario, as shown in Fig. 1. The adversary, Eve, may have a correlation with the system that could allow her to obtain information about the measurement outcomes. To remove the information leakage, we can separate the entropy of outcomes

into intrinsic randomness, which Eve cannot access, and extrinsic randomness, which Eve may know. The essential task in randomness analysis is to quantify the intrinsic randomness given an input state and a measurement. It is worth noting that in the (semi-)device-independent scenarios, Alice might skip some of these steps. For instance, in source-independent schemes [8–10], the source is assumed to be uncalibrated or even untrusted, and therefore, there is no need for Alice to calibrate the source.

As for the intrinsic randomness quantification, let us start with a well-studied special case with the detection calibrated as a von Neumann measurement, $\{|i\rangle\langle i|\}$. If the input is in a superposition state, $|\psi\rangle = \sum_i a_i |i\rangle$ with normalized complex coefficients $a_i \in \mathbb{C}$ and $\sum_i |a_i|^2 = 1$, the measurement outcome is intrinsically random and the probability of obtaining outcome i is $|a_i|^2$ according to Born's rule [1]. In this case, intrinsic randomness of the outcomes arises from breaking superposition [11] and is given by the Shannon entropy of the probability distribution, $\{|a_i|^2\}$. In resource theory, superposition is quantified by quantum coherence with respect to the measurement basis, $\{|i\rangle\}$ [12,13]. In fact, for a generic input state described by a density matrix, the link between output intrinsic randomness and state coherence has been established [14–17].

A projection measurement is an idealized model for detection devices. In reality, noise is inevitable, or equivalently, part of instrument information is missing from the user's point of view. Then, the detection is generally characterized by a positive-operator-valued measure (POVM) through tomography. How to quantify intrinsic randomness of the outcomes from a generic measurement is an important yet unsettled problem. Given a set of POVM elements, as many degrees of freedom in measurement instruments are hidden from Alice,

*xma@tsinghua.edu.cn

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

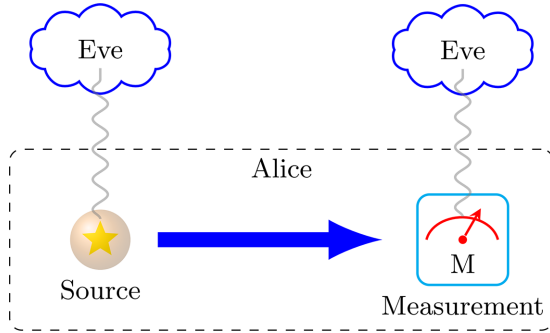


FIG. 1. Illustration of a typical QRNG. The source sends quantum signals in the state of ρ to the measurement device, which outputs a sequence of random numbers. Eve could have a certain correlation with the devices, where she could possess the purification of ρ on the source side and know the construction of the detection on the measurement side. Eve might even have entanglement with the internal apparatus.

there is an infinite number of ways to construct the detection instrument [18–20]. This hidden information makes it very challenging to characterize the amount of information leaked to Eve. In the literature, there are some attempts on randomness evaluation [21,22] and coherence measures [23,24] under POVMs, as listed in Table I. Unfortunately, the existing measures cannot properly quantify randomness or coherence under the most general measurements. Let us take an example to illustrate this issue. Consider a two-outcome POVM, $\mathbf{M} = \{\mathbf{1}/2, \mathbf{1}/2\}$; the outcome is independent of input states. Then, it can be seen as a classical random variable taking values 0 and 1 with an equal probability. We expect this measurement to be of a classical nature. Thus, all states should have zero randomness or coherence under this measurement. This can also be understood from the resource theory of measurement informativeness [25]. Yet for this seemingly simple example, the existing measures either fail to accord with our intuition or suffice only for the qubit case.

In this work, we provide a generic adversary scenario where the detection is correlated with Eve as shown in Fig. 1. The adversary scenario is a generalized version of Naimark extension, with the difference that the ancillary system, which includes hidden variables and missing information, is not necessarily in a pure state as in the conventional one [19,27]. Then, we can apply the results of intrinsic randomness quantification for projection measure-

TABLE I. Existing randomness evaluation and coherence measures. In the last column, we show a simple example of a specific POVM, under which no randomness or coherence should be generated. A measure cannot quantify randomness or coherence properly for general measurements if it gives a nonzero evaluation result for some states.

Ref.	Randomness	Coherence	Measurement	$\{\mathbf{1}/2, \mathbf{1}/2\}$
[14,16]	✓	✓	von Neumann	not applicable
[21]	✓	×	POVM	failed
[22]	✓	×	POVM	qubit only [26]
[23,24]	×	✓	POVM	failed

TABLE II. Notations.

Notation	Description
\mathcal{H}	Hilbert space
\mathbf{M}	POVM
M_i	element of POVM \mathbf{M}
\mathbf{P}	PVM
$\Delta_{\mathbf{P}}$	block-dephasing operation defined by \mathbf{P}
$\mathcal{L}_{\mathbf{P}}$	the set of block-incoherent states
H	Shannon entropy
S	von Neumann entropy
R	randomness function
$[m]$	the set $\{1, \dots, m\}$
$\mathcal{P}(m)$	the set of POVMs with at most m outcomes
\mathcal{P}	the set of POVMs with discrete outcomes
$\{\mathbf{P}, \sigma\}$	generalized Naimark extension
\log	logarithm based 2
ρ	state to be measured and held by Alice ρ^A

ments, while we need to optimize over all possible extensions. For a special type of measurement, extremal POVM [28], we show that all generalized Naimark extensions give the same amount of randomness. Surprisingly, for some extremal measurements, such as the symmetric and information-complete (SIC) measurement [29,30], their outcomes have nonzero randomness for any input states. Then, we can design a new source-independent QRNG using these measurements. The key advantage over the existing source-independent schemes [8,9] is that we do not need any state characterization in the new design. Inspired by the relation between mixed states and pure states, we take the extremal POVMs as the starting point for the study of general POVMs and construct a convex-roof-type intrinsic randomness measure. Besides, we can also regard the randomness quantification as a state coherence measure under POVMs, which reduce to the ones in the standard state-coherence-measure framework for the special case of von Neumann measurements.

The rest of the paper is organized as follows. In Sec. II, we review quantum measurement, extremal measurement, and Naimark extension. In Sec. III, we show the randomness and coherence quantification for general projection measurements, resulting in block randomness and coherence, respectively. In addition, we derive the additivity and unitary-invariant properties of the intrinsic randomness. In Sec. IV, we derive the intrinsic randomness for general POVMs and characterize the set of nonrandom states. In Sec. V, we establish a resource theory framework for POVM coherence. In Sec. VI, we present a numerical approach to evaluate the intrinsic randomness function. All the proofs are presented in appendices.

II. PRELIMINARIES: MEASUREMENT

In this section, we briefly review quantum measurement and Naimark extension. The main notations used in following discussions are listed in Table II.

A. General measurement

For a d -dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$, a POVM on \mathcal{H} is a set of positive-semidefinite Hermitian operators

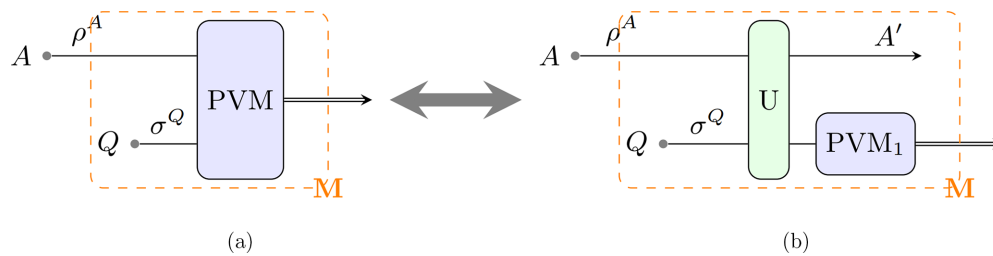


FIG. 2. Two equivalent pictures of Naimark extensions of the POVM \mathbf{M} depicted as the dashed box. (a) PVM on the joint system AQ . (b) Joint preprocessing unitary operation on system AQ followed by a rank-1 PVM on some subsystem.

$\mathbf{M} = \{M_1, \dots, M_m\}$, where $\sum_{i=1}^m M_i = \mathbf{1}$. When two POVMs are the same, $\forall i, M_i = N_i$, we denote by $\mathbf{M} = \mathbf{N}$. Each element can be expressed as $M_i = A_i A_i^\dagger$, where A_i is called a POVM operator and generally not a square matrix. When measuring a state ρ , the probability of obtaining the outcome i is given by $\text{tr}(M_i \rho)$ and the corresponding postmeasurement state is $A_i \rho A_i^\dagger / \text{tr}(M_i \rho)$. The set of operators $\{A_i\}$ uniquely determines the implementation of the measurement—the instrument. In an experiment, Alice can determine the POVM elements of M_i via measurement tomography. On the other hand, a POVM generally corresponds to many possible implementations or different sets of operators, $\{A_i\}$, which are often intractable. This is the challenging part for the randomness quantification of POVMs.

The projection measurement, also called the projection-valued measure (PVM), is a special case of a POVM when $\{M_i\}$ are projection operators, $M_i^2 = M_i = A_i$. As a special case, when every PVM element is rank 1, we call it von Neumann measurement. For a PVM, the implementation is unique. This is why the randomness analyses are simple for von Neumann measurements [16] and PVMs.

B. Extremal POVM

The POVM set is convex and some of the POVMs can be treated as a mixture of others,

$$\mathbf{M} = \sum_j r_j \mathbf{N}^j, \tag{1}$$

which is equivalent to the existence of a hidden variable in some sense. Those indecomposable POVMs are extreme points of the convex set and play a similar role to that of pure states [28,31,32]. Similarly to the case for mixed states, general POVMs can be decomposed into a mixture of extremal ones. Here, we introduce the definition and some important properties of extremal POVMs.

Denote the set of POVMs with at most m outcomes and the one with discrete outcomes as $\mathcal{P}(m)$ and \mathcal{P} , respectively. For $m \leq n$, $\mathcal{P}(m) \subseteq \mathcal{P}(n) \subseteq \mathcal{P}$, since one can let the $n - m$ additional elements be 0. The sets $\mathcal{P}(m)$ and \mathcal{P} are both convex. Clearly, the extremal points in $\mathcal{P}(m)$ are also extremal in \mathcal{P} and the extremal points of \mathcal{P} are called extremal POVMs [28,33].

Definition 1 (extremal POVM). A POVM \mathbf{M} in \mathcal{P} is said to be extremal if, for every expression

$$\mathbf{M} = \lambda \mathbf{M}' + (1 - \lambda) \mathbf{M}'' \tag{2}$$

with $0 < \lambda < 1$ and $\mathbf{M}', \mathbf{M}'' \in \mathcal{P}$, it holds that $\mathbf{M} = \mathbf{M}' = \mathbf{M}''$.

As an example, a PVM is extremal. Next, we give a property of extremal POVMs and leave its proof to Appendix A.

Lemma 1 (linear independence of extremal POVM elements [28,34]). A POVM is extremal; then its elements are linearly independent. A rank-1 POVM is extremal iff its elements are linearly independent.

From this lemma, we can see that the symmetric and information-complete (SIC) POVM is extremal, which is composed of d^2 rank-1 operators, $|\phi_i\rangle\langle\phi_i|/d$, with normalized vectors $|\phi_i\rangle$ satisfying [29,30], $\forall i \neq j$,

$$|\langle\phi_j|\phi_i\rangle|^2 = \frac{1}{d+1}. \tag{3}$$

C. Naimark extension

It has been shown that a POVM can be realized by a PVM in a proper extended Hilbert space, which is called Naimark extension [19]. Concretely, as shown in Fig. 2(a), the measurement is described by POVM \mathbf{M} . When a state ρ^A is input, classical output is obtained. The POVM can be implemented by a PVM with an ancillary state σ^Q . In particular, when σ^Q is pure, it becomes the conventional Naimark extension as introduced in Definition 2. The POVM and the extended PVM should give the same probability distribution [35]; hence, we have the following consistency condition.

Lemma 2 (consistency condition). A Naimark extension should satisfy the consistency condition, $\forall \rho^A$, $\text{tr}(M_i \rho^A) = \text{tr}[P_i(\rho^A \otimes \sigma^Q)]$, which is equivalent to

$$M_i = \text{tr}_Q[P_i(\mathbf{1}^A \otimes \sigma^Q)]. \tag{4}$$

Proof. $\forall \rho^A$,

$$\begin{aligned} \text{tr}(M_i \rho^A) &= \text{tr}[P_i(\mathbf{1}^A \otimes \sigma^Q)(\rho^A \otimes \mathbf{1}^Q)] \\ &= \text{tr}_A\{\rho^A \text{tr}_Q[P_i(\mathbf{1}^A \otimes \sigma^Q)]\}, \end{aligned} \tag{5}$$

which concludes Eq. (4). ■

One can also view the extended PVM as a unitary followed by a von Neumann measurement, also called a rank-1 PVM—a set of rank-1 projectors, as shown in Fig. 2(b). Now, the extended PVM $\mathbf{P} = \{P_1, \dots, P_m\}$ can be written as

$$P_i = U^\dagger(\mathbf{1}^{A'} \otimes |i\rangle\langle i|)U, \tag{6}$$

where system A' is generally different from A . The unitary operation is sometimes called preprocessing [36,37].

Lemma 3 (equivalence between two forms of Naimark extensions). For any generalized Naimark extension of a POVM,

$\{\tilde{\mathbf{P}}, \sigma^Q\}$, we can find an equivalent extension, $\{\mathbf{P}, \sigma^Q\}$, in the form of Eq. (6), as shown in Fig. 2. That is, $\forall i, \rho^A$,

$$P_i(\rho^A \otimes \sigma^Q)P_i = \tilde{P}_i(\rho^A \otimes \sigma^Q)\tilde{P}_i, \quad (7)$$

where we ignore a trivial zero subspace.

From Eq. (6), we can see that all the PVM elements, P_i , in this extension have the same ranks. The key point to prove the equivalence between the two forms of extensions, Figs. 2(a) and 2(b), is to show that any extension is equivalent to an extension with the same rank PVM elements.

Proof. For an extended PVM $\tilde{\mathbf{P}} = \{\tilde{P}_1, \dots, \tilde{P}_m\}$, denote the maximum rank of the elements as r , and assume s is an integer satisfying $(s-1)d < r \leq sd$. Consider a larger space \mathcal{H}' with dimension msd and embed \mathcal{H}_{AQ} into \mathcal{H}' . For each $\text{rank}(\tilde{P}_i) < sd$, we can further extend \tilde{P}_i to rank sd by adding additional rank-1 projectors $\{|\varphi\rangle\langle\varphi|\}$, where $\{|\varphi\rangle\}$ are normalized basis states chosen from the complement space of \mathcal{H}_{AQ} , $\mathcal{H}' \ominus \mathcal{H}_{AQ}$. In the end, we can have a set of m new extended PVM elements, $\mathbf{P} = \{P_1, \dots, P_m\}$, whose ranks are sd in \mathcal{H}' and $\dim(\mathcal{H}') = msd$. Note that these newly added complement projectors, $\{|\varphi\rangle\langle\varphi|\}$, are orthogonal to the state space $\mathcal{D}(\mathcal{H}_A) \otimes \sigma^Q$, so, they have no influence on the measurement outcomes. Now, all the elements have the same ranks; the extended PVM is unitarily equivalent to $\{|1\rangle\langle 1| \otimes \mathbf{1}, \dots, |m\rangle\langle m| \otimes \mathbf{1}\}$, i.e., $P_i = U^\dagger(|i\rangle\langle i| \otimes \mathbf{1})U$, as given in Eq. (6). ■

Now, we can introduce canonical Naimark extension, where systems A and A' are the same in Fig. 2(b) and the dimension of the ancillary system is the same as the number of POVM elements.

Definition 2 (canonical Naimark extension [19]). For POVM $\mathbf{M} = \{M_1, \dots, M_m\}$ in \mathcal{H}_A , the canonical Naimark extension results in a PVM $\mathbf{P} = \{P_1, \dots, P_m\}$ in a larger Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_Q$, where \mathcal{H}_Q is an m -dimensional ancillary space. Assume $\{|1\rangle, \dots, |m\rangle\}$ is an orthonormal basis of ancillary space \mathcal{H}_Q . The ancillary state is $|1\rangle\langle 1|$. Then, each P_i has the form of

$$P_i = U^\dagger(\mathbf{1}^A \otimes |i\rangle\langle i|^Q)U, \quad (8)$$

with U being a suitable unitary operator to satisfy the consistency condition

$$M_i = \text{tr}_Q[P_i(\mathbf{1}^A \otimes |1\rangle\langle 1|^Q)]. \quad (9)$$

III. RANDOMNESS AND COHERENCE IN PVM

Here, we calculate the intrinsic randomness under projection-valued measures (PVMs), prove several useful properties, and link randomness with block coherence. We shall derive two widely used types of block randomness and their properties in detail.

A. Block randomness

Definition 3 (dephasing operation [12]). For a projection measurement, $\mathbf{P} = \{P_1, \dots, P_m\}$, acting on a d -dimensional Hilbert space \mathcal{H} , the corresponding block-dephasing operation is defined as

$$\Delta_{\mathbf{P}}(\rho) = \sum_{i=1}^m P_i \rho P_i. \quad (10)$$

In the following, we shall consider the Shannon limit to simplify the discussion. That is, we consider the case where Alice measures infinitely many copies of a state with the same measurement independently and identically (i.i.d.), and evaluate the average amount of randomness generated per round.

Consider a general PVM; when Alice's input state is pure, Born's rule together with Shannon's source coding theorem [38] tells us that the randomness of the outcomes is equal to $S(\Delta_{\mathbf{P}}(|\psi\rangle\langle\psi|))$, where $S(\rho) = -\text{tr}(\rho \log \rho)$ is the von Neumann entropy function.

For a general mixed input state, ρ , without loss of generality, an adversary, Eve, holds the purification system in the beginning, $|\Psi\rangle^{AE}$. In this case, we have two ways to extend the results from the pure-state case depending on different adversarial scenarios. In a general scenario, Eve can collect all the purification states over the rounds and perform a joint measurement. The intrinsic randomness should be quantified by the conditional min-entropy [39]. Nevertheless, using the fully quantum asymptotic equipartition property, the intrinsic randomness per round is characterized by the von Neumann entropy of the postmeasurement state of Alice conditioned on Eve [40]. Alice obtains the classical outcomes and stores them in system A' , which is m -dimensional. After Alice's measurement, the classical-quantum state is given by

$$\tilde{\rho}^{A'E} = \sum_i p_i |i\rangle\langle i|^{A'} \otimes \rho_i^E, \quad (11)$$

where $p_i = \text{tr}(P_i \rho)$ is the probability obtaining output i and $\rho_i^E = \frac{1}{p_i} \text{tr}_A[|\Psi\rangle\langle\Psi|^{AE}(P_i^A \otimes \mathbf{1}^E)]$. As Alice's measurement should not change the state of Eve's system, we have

$$\text{tr}_A(|\Psi\rangle\langle\Psi|^{AE}) = \rho^E = \text{tr}_A(\tilde{\rho}^{A'E}) = \sum_i p_i \rho_i^E. \quad (12)$$

The intrinsic randomness of Alice's measurement result, defined by the quantum entropy conditioned on Eve, is

$$\begin{aligned} R_q(\rho, \mathbf{P}) &= S(A'|E)_{\tilde{\rho}^{A'E}} \\ &= S(\tilde{\rho}^{A'E}) - S(\rho^E) \\ &= H(\{p_i\}) + \sum_i p_i S(\rho_i^E) - S(\rho) \\ &= H(\{p_i\}) + \sum_i p_i S\left(\frac{P_i \rho P_i}{p_i}\right) - S(\rho) \\ &= S\left(\sum_i P_i \rho P_i\right) - S(\rho) \\ &= S(\rho \|\Delta_{\mathbf{P}}(\rho)), \end{aligned} \quad (13)$$

where ρ denotes Alice's initial state, $H(\{p_i\}) = -\sum_i p_i \log p_i$ is the Shannon entropy function, and $S(\rho \|\sigma) = \text{tr}(\rho \log \rho - \rho \log \sigma)$ is the quantum relative entropy function. The fourth equality is due to the fact that ρ_i^E is a reduced part of the pure state $(P_i^A \otimes \mathbf{1}^E)|\Psi\rangle^{AE}$. The result is consistent with Eq. (29).

In another scenario, we assume Eve measures each purification system, $\rho^E = \text{tr}_A(|\Psi\rangle\langle\Psi|^{AE})$, with an optimal i.i.d. measurement, and hence the state held by Alice has a related decomposition, $\rho^A = \sum_j q_j^E |\psi_j\rangle\langle\psi_j|^A$, where $\sum_j q_j = 1$ and

$q_j \geq 0, \forall j$. Since Eve can optimize her measurement, one should minimize over all possible decompositions of ρ in randomness evaluation. The randomness of the PVM outcomes is quantified by the convex-roof measure,

$$R_c(\rho, \mathbf{P}) = \min_{\{q_j, |\psi_j\rangle\}} \sum_j q_j S(\Delta_{\mathbf{P}}(|\psi_j\rangle\langle\psi_j|)). \quad (14)$$

This randomness measure is of practical interest, where due to current technology limitations, it is often reasonable to assume that the adversary has a limited memory.

The randomness function R_c is always larger than R_q since the assumption of the adversary in the first case is stronger than in the second case. Similarly to the case of a von Neumann measurement, the difference between two randomness function is quantified by the discord between A' and E [16],

$$\begin{aligned} R_c(\rho, \mathbf{P}) - R_q(\rho, \mathbf{P}) &= D_E(\tilde{\rho}^{A'E}) \\ &= \min_{\{q_j^E\}} S(A'|\{q_j^E\})_{\tilde{\rho}^{A'E}} - S(\tilde{\rho}^{A'E}) + S(\rho^E), \end{aligned} \quad (15)$$

where $\{q_j^E\}$ is a probability distribution given by measurement on system E . The equality holds since the measurement on E corresponds to a decomposition $\rho^A = \sum_j q_j^E |\psi_j\rangle\langle\psi_j|$ and $S(A'|\{q_j^E\})_{\tilde{\rho}^{A'E}} = \sum_j q_j^E S(\Delta_{\mathbf{P}}(|\psi_j\rangle\langle\psi_j|))$. It is straightforward to check that both randomness functions, Eqs. (14) and (13), satisfy the convexity condition,

$$\begin{aligned} R_c\left(\sum_j r_j \rho_j, \mathbf{P}\right) &\leq \sum_j r_j R_c(\rho_j, \mathbf{P}), \\ R_q\left(\sum_j r_j \rho_j, \mathbf{P}\right) &\leq \sum_j r_j R_q(\rho_j, \mathbf{P}). \end{aligned} \quad (16)$$

As for the additivity condition for block-diagonal states, it is less obvious.

Definition 4 (block-diagonal state with respect to \mathbf{P}). A state is called block-diagonal with respect to \mathbf{P} , denoted by $\rho = \sum_j r_j \rho_j \equiv \oplus_j r_j \rho_j$ with $\sum_j r_j = 1$ and $r_j \geq 0, \forall j$, if $\forall P_i, j \neq k$,

$$\text{tr}(P_i \rho_j P_i \rho_k) = 0. \quad (17)$$

For a block-diagonal state, each PVM element projects diagonal decomposed state ρ_j into density operators with different orthogonal supports. From the definition, we can show that the diagonal decomposed states are orthogonal, $\forall j \neq k, \text{tr}(\rho_j \rho_k) = 0$. Consider the spectral decomposition of $\rho_j = \sum_a \lambda_a |\alpha_a\rangle\langle\alpha_a|$ and $\rho_k = \sum_b \mu_b |\beta_b\rangle\langle\beta_b|$, where $\lambda_a > 0$ and $\mu_b > 0$, by Eq. (17),

$$\begin{aligned} \text{tr}(P_i \rho_j P_i \rho_k) &= \text{tr}\left[P_i \left(\sum_a \lambda_a |\alpha_a\rangle\langle\alpha_a|\right) P_i \left(\sum_b \mu_b |\beta_b\rangle\langle\beta_b|\right)\right] \\ &= \sum_{a,b} \lambda_a \mu_b \text{tr}(P_i |\alpha_a\rangle\langle\alpha_a| P_i |\beta_b\rangle\langle\beta_b|) \\ &= \sum_{a,b} \lambda_a \mu_b |\langle\alpha_a| P_i |\beta_b\rangle|^2 = 0. \end{aligned} \quad (18)$$

Hence, $\forall a, b, \langle\alpha_a| P_i |\beta_b\rangle = 0$, and $\forall P_i$,

$$\sum_{a,b} |\alpha_a\rangle\langle\alpha_a| P_i |\beta_b\rangle\langle\beta_b| = 0. \quad (19)$$

Moreover, there is

$$\begin{aligned} \text{tr}(\rho_j \rho_k) &= \text{tr}\left[\rho_j \left(\sum_i P_i\right) \rho_k\right] = \sum_i \text{tr}(\rho_j P_i \rho_k) \\ &= \sum_i \sum_{a,b} \lambda_a \mu_b \langle\alpha_a| P_i |\beta_b\rangle\langle\beta_b| \alpha_a\rangle = 0. \end{aligned} \quad (20)$$

The two random functions characterize the intrinsic randomness under different adversarial scenarios and both satisfy the following two properties with the proofs given in Appendices B and C.

Lemma 4 (additivity of randomness functions). For a block-diagonal state $\rho = \oplus_j r_j \rho_j$ with respect to \mathbf{P} , the randomness functions satisfy the additivity condition,

$$\begin{aligned} R_c(\oplus_j r_j \rho_j, \mathbf{P}) &= \sum_j r_j R_c(\rho_j, \mathbf{P}), \\ R_q(\oplus_j r_j \rho_j, \mathbf{P}) &= \sum_j r_j R_q(\rho_j, \mathbf{P}). \end{aligned} \quad (21)$$

Lemma 5 (randomness-invariant unitary). For two PVMs $\mathbf{P} = \{P_1, \dots, P_m\}$ and $U^\dagger \mathbf{P} U = \{U^\dagger P_1 U, \dots, U^\dagger P_m U\}$ connected by a unitary operator U , if for any pure state $|\psi\rangle$ in the support of an input state $\rho, \forall i$,

$$\langle\psi| P_i |\psi\rangle = \langle\psi| U^\dagger P_i U |\psi\rangle, \quad (22)$$

then the randomness of ρ with respect to these two PVMs is the same,

$$R(\rho, \mathbf{P}) = R(\rho, U^\dagger \mathbf{P} U). \quad (23)$$

B. Block coherence

The randomness functions developed in Eqs. (14) and (13) can also be used for the block coherence measures, which was introduced by Åberg [12] and was put in a resource theory framework later [23]. Here, we adopt a slightly reformulated framework. For a PVM \mathbf{P} , the set of block-incoherent states is defined as

$$\mathcal{I}_{\mathbf{P}} = \{\Delta_{\mathbf{P}}(\rho) \mid \rho \in \mathcal{D}(\mathcal{H})\}, \quad (24)$$

with $\mathcal{D}(\mathcal{H})$ being the set of all the density matrices defined on the Hilbert space.

There are different ways to define free operations. For example, we can consider block-incoherent operations (IOs),

$$\Lambda_{\text{IO}}(\rho) = \sum_n K_n \rho K_n^\dagger, \quad (25)$$

with Kraus operators satisfying

$$K_n \mathcal{I}_{\mathbf{P}} K_n^\dagger \subseteq \mathcal{I}_{\mathbf{P}}. \quad (26)$$

A block coherence measure should satisfy the criteria presented in Box 1, which are essentially the same as the coherence-measure criteria for von Neumann measurements [41]. These criteria are not independent. In fact, criteria (C3) and (C4) for incoherent operations defined in Eq. (25) can be

Box 1: Criteria for block-coherence measures for PVMs.

- (C1) Non-negativity: $C(\rho) \geq 0$, and $C(\sigma) = 0$ iff $\sigma \in \mathcal{I}_{\mathbf{P}}$.
- (C2) Monotonicity: for any incoherent map Λ_I , $C(\rho) \geq C(\Lambda_I(\rho))$.
- (C3) Strong monotonicity: for any IO map defined in Eq. (25), $C(\rho) \geq \sum_n p_n C(\rho_n)$, where $p_n = \text{tr}(K_n \rho K_n^\dagger)$ and $\rho_n = K_n \rho K_n^\dagger / p_n$.
- (C4) Convexity: $C(\sum_j \lambda_j \rho_j) \leq \sum_j \lambda_j C(\rho_j)$ with $\lambda_j > 0$ and $\sum \lambda_j = 1$.
- (C5) Uniqueness for pure states: $C(|\psi\rangle\langle\psi|) = S(\Delta_{\mathbf{P}}(|\psi\rangle\langle\psi|))$.
- (C6) Additivity for a tensor state, $C(\rho \otimes \delta, \mathbf{P}_1 \otimes \mathbf{P}_2) = C(\rho, \mathbf{P}_1) + C(\delta, \mathbf{P}_2)$, where the joint projection measurement on $\rho \otimes \delta$ takes the tensor form of local projectors on ρ and δ .

replaced by the additivity for the block-diagonal state defined in Definition 4, $C(\oplus_j \lambda_j \rho_j) = \sum_j \lambda_j C(\rho_j)$ [41,42]. Here, we omit PVM \mathbf{P} from the coherence measure $C(\rho, \mathbf{P})$ for simplicity when there is no confusion.

With criterion (C5), we can employ the convex-roof construction for a block coherence measure. Not surprisingly, the same as the von Neumann measurement case, the measure is given by the randomness function R_c defined in Eq. (14).

We can also define block coherence measure $C(\rho)$ via the relative entropy, which, again, is the same as the randomness function Eq. (13),

$$\begin{aligned} C(\rho) &= \min_{\sigma \in \mathcal{I}_{\mathbf{P}}} S(\rho \| \sigma) = -\max_{\sigma \in \mathcal{I}_{\mathbf{P}}} \text{tr}(\rho \log \sigma) - S(\rho) \\ &= -\max_{\sigma \in \mathcal{I}_{\mathbf{P}}} \text{tr}[\Delta_{\mathbf{P}}(\rho) \log \sigma] - S(\rho) \\ &= S(\Delta_{\mathbf{P}}(\rho)) - S(\rho) + \min_{\sigma \in \mathcal{I}_{\mathbf{P}}} S(\Delta_{\mathbf{P}}(\rho) \| \sigma) \\ &= S(\Delta_{\mathbf{P}}(\rho)) - S(\rho) = R_q(\rho, \mathbf{P}), \end{aligned} \quad (27)$$

where the third equality holds because any incoherent state σ in Eq. (24) is diagonal with respect to \mathbf{P} .

C. Rank-1 case: von Neumann measurement

For von Neumann measurement $\{|i\rangle\langle i|\}$, the intrinsic randomness via measuring a state ρ is well studied in the literature [14–17]. This is a special case of block randomness since a von Neumann measurement is a rank-1 PVM. Here we briefly review this special case. For a pure state $|\psi\rangle$, the randomness of its measurement outcomes is directly given by Born’s rule, $S(\Delta_{\{|i\rangle\langle i|\}}(|\psi\rangle\langle\psi|))$. For the general cases of mixed states, there are also two ways to quantify the amount of randomness by measuring a mixed state.

First, if Eve measures the purification system, ρ_E , on an optimal basis for her, the randomness of the PVM outcomes is quantified by the convex-roof measure,

$$R_c(\rho, \{|i\rangle\langle i|\}) = \min_{\{q_j, |\psi_j\rangle\}} \sum_j q_j S(\Delta_{\{|i\rangle\langle i|\}}(|\psi_j\rangle\langle\psi_j|)). \quad (28)$$

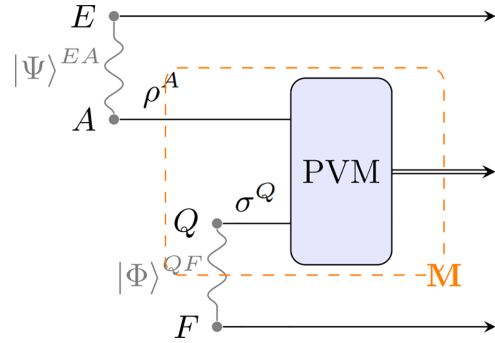


FIG. 3. The adversary scenario for a generalized Naimark extension: a PVM on the joint system AQ . From Alice’s perspective, the measuring process is described by POVM \mathbf{M} , depicted as the dashed box. Alice inputs state ρ^A and obtains classical outputs from the box. The ancillary system is generally in a mixed state σ^Q . If σ^Q is pure, it becomes the conventional Naimark extension. Both the source and the ancillary system could be entangled with Eve. There is no signaling from input A to Eve’s purification F .

Second, Eve performs a joint measurement on the independent purification systems, and the randomness is quantified by [16,43]

$$R_q(\rho, \{|i\rangle\langle i|\}) = S(\rho \| \Delta_{\{|i\rangle\langle i|\}}(\rho)). \quad (29)$$

The intrinsic randomness functions, Eqs. (28) and (29), directly give coherence measures for both R_c [14] and R_q [15,16] of von Neumann measurements.

IV. RANDOMNESS CHARACTERIZATION FOR GENERAL POVMs

Here, we describe the adversary scenario for general cases, which is a generalized Naimark extension, and then we quantify the intrinsic randomness for general POVMs based on the block randomness. As a special case, we characterize the set of states without randomness.

A. Quantification of intrinsic randomness

To quantify the amount of intrinsic randomness, we need to consider an adversarial perspective and examine what side information Eve may use in eavesdropping. In a QRNG, Alice first prepares a state, ρ^A , and then measures it with the POVM, \mathbf{M} . Apart from her knowledge of the form of these operators, Eve may correlate her system to ρ^A and \mathbf{M} as well. For ρ^A , the best Eve can achieve is to hold the purified system [44]. Similarly, for \mathbf{M} , Eve can also hold a “purified” process which means that the measurement on the joint system is a PVM. In the most general scenario, Eve puts a state σ^Q in the measurement device and holds the purification of σ^Q . Then, Alice’s device actually performs an extended measurement on both ρ^A and σ^Q , as shown in Fig. 3.

Note that from Alice’s viewpoint, the measurement is calibrated to act on system A ; in other words, Alice is unaware of σ^Q hidden in her measurement device. Generally, as Alice can change her input state, one would expect the measurement device to enjoy a consistent condition:

$$M_i = \text{tr}_Q[P_i(\mathbf{1}^A \otimes \sigma^Q)], \quad \forall i. \quad (30)$$

For simplicity, we shall omit the superscript A and Q when there is no confusion in the following discussions and denote the states ρ and σ as Alice’s state and the ancillary state, respectively.

Before we commence, let us briefly remark on the problem formulation. By posing the consistency condition, we assume that Eve does not target on a specific input state of Alice in eavesdropping. Intuitively, once Eve gives the measurement device to the user, she cannot access the apparatus anymore. Hence, there is a no-signaling relation between the input state and Eve’s system. In the common Naimark extension, σ^Q is restricted to a pure state, which corresponds to the assumption that Eve learns no further than the form of the POVM elements of the measurement device. In the analysis, we need to consider the most general case where system Q is in a general mixed state.

Now, we can see that in the most general scenario, Eve has the freedom to choose an extended PVM, \mathbf{P} , and the corresponding ancillary state σ . In the randomness analysis, we need to minimize over all possible Eve’s strategies. With the randomness quantification of PVMs, we have

$$R(\rho, \mathbf{M}) = \min_{\mathbf{P}, \sigma} R(\rho \otimes \sigma, \mathbf{P}),$$

$$\text{such that } \forall i, M_i = \text{tr}_Q[P_i(\mathbf{1}^A \otimes \sigma^Q)], \quad (31)$$

where the constraint is given by the consistency condition in Eq. (30). For the special case of von Neumann measurements, the randomness quantification $R(\varrho, \mathbf{P})$ is well studied in the literature under different adversary scenarios [16,43]. As the starting point of our randomness quantification of POVMs, we generalize the results to the general PVM case and give two widely used measures in the preliminary part,

$$R_c(\varrho, \mathbf{P}) = \min_{\{q_j, |\psi_j\rangle\}} \sum_j q_j S(\Delta_{\mathbf{P}}(|\psi_j\rangle\langle\psi_j|)),$$

$$R_q(\varrho, \mathbf{P}) = S(\varrho \parallel \Delta_{\mathbf{P}}(\varrho)). \quad (32)$$

The difference between R_c and R_q lies in whether Eve performs measurements on each copy of system E in Fig. 3 and the two functions coincide when ϱ is pure. Since a classical mixture of quantum states should not increase the output intrinsic randomness on average, the randomness function $R(\varrho, \mathbf{P})$ satisfies the convexity condition,

$$R\left(\sum_j r_j \varrho_j, \mathbf{P}\right) \leq \sum_j r_j R(\varrho_j, \mathbf{P}), \quad (33)$$

for arbitrary coefficients $\sum_j r_j = 1$ and $r_j \geq 0$. A state $\varrho = \sum_j r_j \varrho_j \equiv \oplus_j r_j \varrho_j$ is *block-diagonal* with respect to \mathbf{P} , when $\forall j \neq j'$ and $\forall P_i \in \mathbf{P}$, there is $\text{tr}(P_i \varrho_j P_i \varrho_{j'}) = 0$. Intuitively, different block subspaces should have no interference with each other when measuring. This indicates that the randomness function should also satisfy the additivity condition for the block-diagonal states,

$$R(\oplus_j r_j \varrho_j, \mathbf{P}) = \sum_j r_j R(\varrho_j, \mathbf{P}). \quad (34)$$

Note that the two aforementioned randomness functions for PVMs meet these criteria. With the convexity condition on

the randomness function, we can see that the randomness defined in Eq. (31) satisfies the convexity condition for both ρ and \mathbf{M} . From the resource theory point of view, these two conditions stem from the convexity [13] and the additivity on block-diagonal states [42] of coherence measures.

Let us check out a special case where the POVM is extremal, which cannot be decomposed into a linear mixture of other POVMs [28]. This is an analog to a pure state, which is often considered to be decoupled from the environment. An extremal POVM can also be treated as a measurement decoupled from the environment. In the adversary scenario, there is no hidden variable for a pure state or an extremal POVM. That is, in Fig. 3, system F is trivial. To put this intuition in a rigorous manner, we show that for an extremal POVM, the intrinsic randomness is independent of the extension $\{\mathbf{P}, \sigma\}$. We leave the proof to Appendix D.

Theorem 1. For an extremal POVM \mathbf{M} and a fixed input state ρ , all the generalized Naimark extensions give the same amount of randomness.

Then, we can skip the minimization problem in Eq. (31) and employ any extension for the randomness function. In practice, we can take a canonical extension of \mathbf{M} [19], denoted by \mathbf{P}_c ,

$$R(\rho, \mathbf{M}) = R(\rho \otimes |0\rangle\langle 0|, \mathbf{P}_c). \quad (35)$$

A general POVM can be decomposed to extremal ones, just like that a mixed state can be decomposed to pure states. The decomposition of a POVM is generally not unique, which is controlled by a hidden variable from Alice’s point of view. In the generalized Naimark extension as shown in Fig. 3, the following proposition connects the decomposition of the POVM with that of the ancillary state.

Proposition 1 (correspondence between ancillary state and measurement decomposition). In a generalized Naimark extension of a POVM, \mathbf{M} , if the ancillary state has a pure-state decomposition, $\sigma = \sum_j r_j |\varphi_j\rangle\langle\varphi_j|$ with $\sum_j r_j = 1$ and $r_j > 0$, then there exists a measurement decomposition $\mathbf{M} = \sum_j r_j \mathbf{N}^j$, and vice versa.

The proof is presented in Appendix E. Here, we need to emphasize that the correspondence between the state and measurement decomposition is not unique in general. That is, different $|\varphi_j\rangle\langle\varphi_j|$ might correspond to the same \mathbf{N}^j .

If Eve performs a local measurement on her system F , without loss of generality, the measurement can be restricted to be rank 1. Otherwise, the measurement can be viewed as a rank-1 measurement followed by coarse graining. Then, the ancillary state is chosen from a pure-state ensemble and the POVM degenerates into a mixture of corresponding POVMs according to Proposition 1. The intrinsic randomness of Alice’s outcomes is a weighted average of the randomness for each pure input ancillary state. So, the minimization problem of Eq. (31) becomes minimizing the value $\sum_j r_j R(\rho \otimes |\varphi_j\rangle\langle\varphi_j|, \mathbf{P})$ over all possible Naimark extensions and pure-state decompositions of the ancillary state.

Denote the solution to the minimization problem after Eve’s measurement to be \mathbf{P}^* and $\sigma^* = \sum_j r_j^* |\varphi_j^*\rangle\langle\varphi_j^*|$. We show that the corresponding measurement decomposition, $\mathbf{M} = \sum_j r_j^* \mathbf{N}^{*j}$, is extremal—indicating that $\{\mathbf{N}^{*j}\}$ are all extremal. The intrinsic randomness for the POVM outcomes is given by $\sum_j r_j^* R(\rho, \mathbf{N}^{*j})$. As a result, we can minimize over

all possible extremal decompositions for the POVM to evaluate Eq. (31) and give a convex-roof construction of intrinsic randomness, as presented in the following theorem with its proof in Appendix F.

Theorem 2. When Eve performs a measurement on her system F , the intrinsic randomness of POVM outcomes is given by

$$R^{cf}(\rho, \mathbf{M}) = \min_{\{\mathbf{N}^j, r_j\}} \sum_j r_j R(\rho, \mathbf{N}^j),$$

such that $\mathbf{M} = \sum_j r_j \mathbf{N}^j$, (36)

where the decomposed POVMs $\{\mathbf{N}^j\}$ are all extremal and the randomness function $R(\rho, \mathbf{N}^j)$ is given by Eq. (35).

Note that similarly to the case of pure states, when a POVM \mathbf{M} is extremal, there is $R(\rho, \mathbf{M}) = R^{cf}(\rho, \mathbf{M})$.

B. States without randomness

After quantifying randomness for the measurement outcomes with respect to a given POVM, it is interesting to consider the set of states that have no randomness, called *nonrandom states*. For the special case of a von Neumann measurement, a nonrandom state is diagonal in the measurement basis [13,14]. For a general PVM, a nonrandom state has a pure-state decomposition such that each decomposed state is a +1 eigenstate of a measurement projector. Here, we give necessary and sufficient conditions for the nonrandom states under a generic measurement in the following two corollaries with proofs in Appendices G and H.

Corollary 1 (necessary and sufficient condition for nonrandom states). Given a POVM \mathbf{M} , a state ρ is nonrandom, $R^{cf}(\rho, \mathbf{M}) = 0$, iff the measurement has an extremal decomposition, $\mathbf{M} = \sum_j r_j \mathbf{N}^j$, satisfying one of the following two equivalent conditions:

- (1) $\forall j, i \neq i', N_i^j \rho N_{i'}^j = 0$.
- (2) For each \mathbf{N}^j , the state has a corresponding spectral decomposition, $\rho = \sum_k q_k^j |\psi_k^j\rangle\langle\psi_k^j|$, such that $\forall k, N_i^j |\psi_k^j\rangle = |\psi_k^j\rangle$ for some element N_i^j .

For the special case of pure state $|\psi\rangle$, we can derive the necessary and sufficient condition for the general randomness quantification given in Eq. (31).

Corollary 2. Given a POVM \mathbf{M} , a pure state $|\psi\rangle$ is nonrandom, $R(|\psi\rangle\langle\psi|, \mathbf{M}) = 0$, iff $|\psi\rangle$ is a common eigenstate of all measurement elements.

For extremal POVMs, according to Corollary 1, the necessary and sufficient condition for zero randomness is that ρ has a corresponding spectral decomposition, $\sum_k q_k |\psi_k\rangle\langle\psi_k|$, such that each term $|\psi_k\rangle$ is a +1 eigenstate of some element. Intriguingly, there exist particular extremal POVMs; all measurement elements do not have +1 eigenvalue. For example, the SIC measurement is extremal and each POVM element only has 0 or $1/d$ as eigenvalues. Hence, there is no nonrandom state for the SIC measurement.

Observation 1. For some POVMs, such as SIC measurements, there does not exist a nonrandom state.

This observation can help us design source-independent QRNGs. Given a calibrated measurement, if Alice figures that nonrandom states do not exist, she can be sure that there is a

positive amount of randomness in the outcomes even without any source characterization. In this case, the lower bound of outcome randomness is given by

$$R(\mathbf{M}) = \min_{\rho} R(\rho, \mathbf{M}), \quad (37)$$

where the randomness function $R(\rho, \mathbf{M})$ is given in Eq. (31). The quantity $R(\mathbf{M})$ gives the source-independent randomness of the QRNG. This kind of source-independent QRNG designs is stronger than the existing ones [8,9], where at least partial source tomography is required. This observation can also help us design other device-independent QRNGs [45]. We illustrate this with an example. For the above-mentioned SIC measurement, since a nonrandom state does not exist, we can design a corresponding QRNG and the following theorem gives the lower bound of the outcome randomness.

Theorem 3. For a SIC measurement \mathbf{M} , a lower bound of intrinsic randomness is given by

$$R(\mathbf{M}) > \log\left(\frac{d+1}{2}\right), \quad (38)$$

where d is the dimension of the corresponding space.

The proof is presented in Appendix I. When $R = R_q$, to evaluate how tight our lower bound is, let us examine the special case of the maximally mixed input state. The amount of randomness from a general POVM has an upper bound

$$R_q(\mathbf{1}/d, \mathbf{M}) = S(\Delta_{\mathbf{P}}(\mathbf{1}/d \otimes |1\rangle\langle 1|)) - S(\rho) \leq \log d^2 - \log d = \log d. \quad (39)$$

This indicates $R_q(\mathbf{M}) \leq \log d$. The difference between our lower bound $\log[(d+1)/2]$ and this upper bound is less than 1 bit.

It is worth mentioning that for a SIC measurement with an arbitrary input state, if we take the additional assumption that Eve does not know the ancillary state of detection devices, a previous result shows that the amount of randomness in terms of min-entropy is lower bounded by $2 \log d - 1$ [46].

V. INTRINSIC RANDOMNESS AS A POVM COHERENCE MEASURE

Due to the close relation between randomness and coherence in the case of PVMs, we naturally regard the intrinsic randomness R as a coherence measure under general POVMs. Following a standard resource-theoretic approach, we define the set of incoherent states and incoherent operations for a general measurement. Given a POVM, the set of incoherent states is defined as the set of nonrandom states,

$$\mathcal{I}_{\mathbf{M}} = \{\rho \mid R(\rho, \mathbf{M}) = 0\}. \quad (40)$$

Corollary 2 gives the characterization of pure POVM-incoherent states. If we take the convex-roof construction in Theorem 2, $R^{cf}(\rho, \mathbf{M})$, Corollary 1 would give a full description of this POVM-incoherent state set. The set of POVM-incoherent states, $\mathcal{I}_{\mathbf{M}}$, is convex and can be empty for some special POVMs. With these definitions, we can show that the coherence measure given by the intrinsic randomness R in Eqs. (31) and (36) satisfies the coherence-measure criteria, as shown in Box 2. Besides, in the special case of PVMs, the definitions for coherence measures and incoherent

Box 2: Criteria for POVM coherence measures.

- (C1) Non-negativity: $C(\rho, \mathbf{M}) \geq 0$, and $C(\delta, \mathbf{M}) = 0$ iff $\delta \in \mathcal{I}_{\mathbf{M}}$.
- (C2) Monotonicity: for any POVM-incoherent operation Λ , $C(\Lambda(\rho), \mathbf{M}) \leq C(\rho, \mathbf{M})$.
- (C3) Strong monotonicity: for any POVM-incoherent operation Λ with Kraus operators K_i , $\sum_i p_i C(\rho_i, \mathbf{M}) \leq C(\rho, \mathbf{M})$ with $p_i = \text{tr}(K_i \rho K_i^\dagger)$ and $\rho_i = K_i \rho K_i^\dagger / p_i$.
- (C4) Convexity: $C(\sum_j \lambda_j \rho_j, \mathbf{M}) \leq \sum_j \lambda_j C(\rho_j, \mathbf{M})$ with $\lambda_j > 0$ and $\sum_j \lambda_j = 1$.

states are identical with their corresponding part in the block-coherence theory. In the previous section, we have shown that this set is empty for some special POVMs, like SIC POVMs. This is different from the PVM case, where the incoherent state set is always nonempty.

Though the set of POVM-incoherent states might be empty, incoherent operations always exist for any POVM. For example, the identity map is a trivial POVM-incoherent operation. Here, we give a definition of the POVM-incoherent operations.

Definition 5. For POVM \mathbf{M} , operation Λ is called incoherent, if for any generalized Naimark extension (\mathbf{P}, σ) on a larger space \mathcal{H}' , Λ has a corresponding extended operation Λ' on \mathcal{H}' that satisfies the following two conditions,

- (i) $\Lambda'(\rho \otimes \sigma) = \Lambda(\rho) \otimes \sigma$.
- (ii) $K'_i \mathcal{I}_{\mathbf{P}} K_i'^\dagger \subseteq \mathcal{I}_{\mathbf{P}}$, where $\mathcal{I}_{\mathbf{P}}$ is the set of incoherent states of \mathbf{P} , and K'_i 's are the Kraus operators of Λ' .

Under this definition, the coherence measures C defined by intrinsic randomness R and R^{cf} both satisfy the following criteria.

Besides the POVM-incoherent operation in Definition 5, we can also consider other sets of incoherent operations. For example, we can define the set of maximally POVM-incoherent operations. For an operation in this set, we also require item (i) in Definition 5. Differently from item (ii), we require the extended map Λ' to be a maximally block-incoherent operation satisfying $\Lambda'(\mathcal{I}_{\mathbf{P}}) \subset \mathcal{I}_{\mathbf{P}}$.

As a supplement to the above criteria, the coherence measures defined by R and R^{cf} satisfy the double-convexity condition for both states and measurements. That is, in addition to the criterion (C4), the coherence measures C also satisfy the convexity condition for measurements,

$$C\left(\rho, \sum_j \lambda_j \mathbf{M}^j\right) \leq \sum_j \lambda_j C(\rho, \mathbf{M}^j), \quad (41)$$

where $\{\mathbf{M}^j\}$ are all POVMs. It should be noticed that the previously defined coherence measure from the direct application of conventional Naimark extension does not satisfy the property [23].

Now we use this double-convexity property to examine the example mentioned in the introduction part, where we claim that all states under POVM $\{\mathbf{1}/2, \mathbf{1}/2\}$ should have no randomness. Consider a more general POVM \mathbf{M} with ele-

ment $M_i = a_i \mathbf{1}$, $a_i > 0$, and $\sum_i a_i = 1$; there is $\mathbf{M} = \sum_i a_i \mathbf{P}^i$, where each PVM \mathbf{P}^i has one element equal to $\mathbf{1}$ and the rest are 0. Then, $\forall \rho$,

$$0 \leq C(\rho, \mathbf{M}) \leq \sum_i a_i C(\rho, \mathbf{P}^i) = 0. \quad (42)$$

Thus, $C(\rho, \mathbf{M}) = 0$.

VI. NUMERICAL EVALUATION

In this section, for the convex-roof-type randomness measure defined by the optimization in Eq. (36), we present a numerical approach to evaluate intrinsic randomness under a general POVM and consider an example.

A. Numerical approach

The objective function is biconvex in its arguments, namely, the probability distribution $\{r_j\}$ and decomposed extremal POVMs $\{\mathbf{N}^j\}$. Also, the constraints form a convex set. For such optimization problems, a global optimal value can be obtained in principle [47]. Nevertheless, there are two difficulties: (1) the characterization of the set of extremal POVMs is relatively complex [28]; (2) the dimension of the probability distribution $\{r_j\}$ is not fixed.

To tackle the first problem, we can remove the constraint that $\{\mathbf{N}^j\}$ are all extremal. To see why this is the case, suppose the optimal value to Eq. (36) is given by the tuple $\{r_j^*, \mathbf{N}^{*j}\}$. In Theorem 2, we show that for any probability distribution $\{\tilde{r}_k\}$ and POVMs $\{\tilde{\mathbf{N}}^k\}$ such that $\mathbf{M} = \sum_k \tilde{r}_k \tilde{\mathbf{N}}^k$, the following inequality holds,

$$\begin{aligned} \sum_k \tilde{r}_k R(\rho \otimes |0\rangle\langle 0|, \tilde{\mathbf{P}}^k) &\geq \sum_j r_j^* R(\rho \otimes |0\rangle\langle 0|, \mathbf{P}^{*j}) \\ &= \sum_j r_j^* R(\rho, \mathbf{N}^{*j}), \end{aligned} \quad (43)$$

where $\tilde{\mathbf{P}}^k, \mathbf{P}^{*j}$ represent the canonical Naimark extension of $\tilde{\mathbf{N}}^k, \mathbf{N}^j$, respectively. With a slight abuse of notation, we also write $R(\rho \otimes |0\rangle\langle 0|, \tilde{\mathbf{P}}^k)$ as $R(\rho, \tilde{\mathbf{N}}^k)$ for a general POVM $\tilde{\mathbf{N}}^k$. Therefore, the optimization in Eq. (36) is equivalent to the following problem,

$$\begin{aligned} R^{cf}(\rho, \mathbf{M}) &= \min_{\{r_j, \mathbf{N}^j\}} \sum_j r_j R(\rho, \mathbf{N}^j), \\ \text{such that } \mathbf{M} &= \sum_j r_j \mathbf{N}^j, \\ \mathbf{N}^j &\in \mathcal{P}, \forall j, \\ r_j &\geq 0, \forall j, \\ \sum_j r_j &= 1, \end{aligned} \quad (44)$$

where \mathcal{P} is the set of POVMs.

To tackle the second problem that the dimension of $\{r_j\}$ is not fixed, we can apply Carathéodory's theorem for convex hulls. Suppose \mathbf{M} is a POVM acting on a d -dimensional Hilbert space with m elements. After considering the positive-semidefinite property and completeness, it can be parametrized by $(md^2 - 1)$ real parameters. Then, according

to Carathéodory’s theorem, the optimal value to Eq. (44) can be attained by a probability distribution $\{r_j\}$ with at most md^2 terms. Consequently, we can restrict the dimension of $\{r_j\}$ to be md^2 in Eq. (44) without loss of generality.

With the above results, the global optimum to Eq. (44) can now be efficiently solved numerically. In particular, for a fixed probability distribution $\{r_j\}$, the problem becomes a semidefinite programming optimization in the arguments $\{\mathbf{N}^j\}$.

B. Example

Here, we give a simple example and demonstrate the numerical evaluation results. In practice, von Neumann measurements, mutually unbiased bases, and SIC measurements are three widely used measurements. In a qubit system, we consider these three types of POVMs that are free of noise,

$$\mathbf{M}_{\text{vn}} = \{|+\rangle\langle +|, |-\rangle\langle -|, 0, 0\},$$

$$\mathbf{M}_{\text{mub}} = \{\frac{1}{2}|0\rangle\langle 0|, \frac{1}{2}|1\rangle\langle 1|, \frac{1}{2}|+\rangle\langle +|, \frac{1}{2}|-\rangle\langle -|\},$$

$$\mathbf{M}_{\text{sic}} = \{\frac{1}{2}|0\rangle\langle 0|, \frac{1}{2}|\phi_0\rangle\langle \phi_0|, \frac{1}{2}|\phi_1\rangle\langle \phi_1|, \frac{1}{2}|\phi_2\rangle\langle \phi_2|\}, \quad (45)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|\phi_k\rangle = \sqrt{1/3}|0\rangle + e^{2k\pi i/3}\sqrt{2/3}|1\rangle$, $k = 0, 1, 2$. Now, add a trivial POVM $\mathbf{I}_4 = \{a\mathbf{1}, b\mathbf{1}, c\mathbf{1}, (1 - a - b - c)\mathbf{1}\}$, $a, b, c \geq 0$, as noise. Then, we obtain three noisy POVMs,

$$\begin{aligned} \mathbf{M}_{\text{vn}}^\mu &= (1 - \mu)\mathbf{M}_{\text{vn}} + \mu\mathbf{I}_4, \\ \mathbf{M}_{\text{mub}}^\mu &= (1 - \mu)\mathbf{M}_{\text{mub}} + \mu\mathbf{I}_4, \\ \mathbf{M}_{\text{sic}}^\mu &= (1 - \mu)\mathbf{M}_{\text{sic}} + \mu\mathbf{I}_4, \end{aligned} \quad (46)$$

where $0 \leq \mu \leq 1$.

To evaluate randomness under these noisy measurements, first note the following fact. For an arbitrary state ρ and an arbitrary POVM \mathbf{M} , when the noise of a particular trivial POVM $\mathbf{I}_{(1)} = (1, 0, 0, 0)$ is added to \mathbf{M} , the amount of generated randomness changes,

$$R(\rho, (1 - \mu)\mathbf{M} + \mu\mathbf{I}_{(1)}) = (1 - \mu)R(\rho, \mathbf{M}). \quad (47)$$

The equality holds since for any extremal decomposition of the noised POVM $(1 - \mu)\mathbf{M} + \mu\mathbf{I}_{(1)}$, it must include $\mathbf{I}_{(1)}$ as a part. Therefore, for our cases,

$$R(\rho, (1 - \mu)\mathbf{M} + \mu\mathbf{I}_4) = (1 - \mu)R(\rho, \mathbf{M}). \quad (48)$$

If we input a pure state $|0\rangle$, then $R_c^{cf} = R_q^{cf}$ and hence we can briefly write the randomness measure as R^{cf} . The state coherences under these three POVMs are compared in Fig. 4. We can see that the randomness under a noisy SIC measurement, $R^{cf}(|0\rangle, \mathbf{M}_{\text{sic}}^\mu)$, remains larger than 1 even under a relatively strong deterministic noise, while $R^{cf}(\rho, \mathbf{M}_{\text{mub}}^\mu) \leq 1$ and $R^{cf}(\rho, \mathbf{M}_{\text{vn}}^\mu) \leq 1$ hold for arbitrary states. This simulation result demonstrates the advantage of the SIC measurement in the design of quantum random number generators.

VII. CONCLUSION AND DISCUSSION

In this work, we characterize intrinsic randomness for general states under general measurements. For some special cases such as extremal POVMs, we also provide a method for solving the optimization problem in Eq. (31), which defines the randomness evaluation problem under general POVMs.

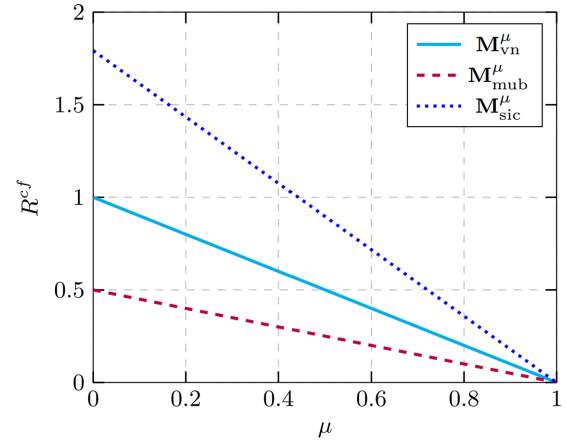


FIG. 4. Comparison among coherence measures of the qubit state $|0\rangle$ with respect to three specific POVMs.

We conjecture that the solution to the optimization for the most general case is a fixed Naimark extension in a finite-dimensional space, independent of the input state.

Our results also shed light on the information-theoretic analysis of quantum measurement processes [37,48–50]. In quantum mechanics, we know that any measurement that extracts information out of a state would inevitably introduce disturbance. One would expect a quantitative relation between intrinsic randomness and state disturbance. In the configuration of Fig. 3, quantum disturbance can be formulated as the decrease of mutual information between system E and system A after measurement [37,49]. However, when input states are pure, system E becomes trivial and the definition is not applicable. We leave it for future research on how to properly quantify the notion of disturbance and relate it to the randomness generation framework in this work.

ACKNOWLEDGMENTS

We acknowledge Junjie Chen, Zhenhuan Liu, Xiao Yuan, and Pei Zeng for the insightful discussions. This work is supported by the National Natural Science Foundation of China Grant No. 12174216 and Innovation Program for Quantum Science and Technology Grant No. 2021ZD0300804.

APPENDIX A: PROOF OF LEMMA 1

Assume elements of the extremal POVM \mathbf{M} are linearly dependent,

$$a_1M_1 + \dots + a_mM_m = 0, \quad (A1)$$

where not all the coefficients a_i are 0. Without loss of generality, we can assume $a_1 \geq \dots \geq a_n$. Each element M_i is a nonzero, positive-semidefinite operator, so $a_1 > 0$, $a_m < 0$. Define two new POVMs \mathbf{M}' and \mathbf{M}'' with, $\forall i \in [m] = \{1, \dots, m\}$,

$$\begin{aligned} M'_i &= (1 - a_i/a_1)M_i, \\ M''_i &= (1 - a_i/a_m)M_i, \end{aligned} \quad (A2)$$

where $M'_1 = 0$ and $M''_m = 0$. Hence, $\mathbf{M}' \neq \mathbf{M}$ and $\mathbf{M}'' \neq \mathbf{M}$. Meanwhile,

$$\mathbf{M} = \frac{a_1}{a_1 - a_m} \mathbf{M}' + \frac{-a_m}{a_1 - a_m} \mathbf{M}''. \quad (\text{A3})$$

This contradicts Definition 1.

Next, we prove in the case of rank-1 POVM, the reverse is also true. Assume \mathbf{M} is not extremal and then it can be decomposed to

$$\mathbf{M} = \lambda \mathbf{M}' + (1 - \lambda) \mathbf{M}'', \quad (\text{A4})$$

with $0 < \lambda < 1$ and $\mathbf{M}' \neq \mathbf{M}''$. Since \mathbf{M} is rank 1, it implies that $\forall i$, $M'_i = M''_i = M_i$, $M'_i = 0$, or $M''_i = 0$. Without loss of generality, assume for $i \leq n_1$, $M'_i = M''_i = M_i$; for $n_1 < i \leq n_2$, $M'_i = 0$; and for $i > n_2$, $M'_i = 0$; where $n_1 < n_2 < m$. Then, we have

$$\begin{aligned} \sum_{i=n_1+1}^{n_2} M_i &= \lambda \sum_{i=n_1+1}^{n_2} M'_i = \lambda \left(\mathbf{1} - \sum_{i=1}^{n_1} M_i \right), \\ \sum_{i=n_2+1}^m M_i &= (1 - \lambda) \sum_{i=n_2+1}^m M''_i = (1 - \lambda) \left(\mathbf{1} - \sum_{i=1}^{n_1} M_i \right), \end{aligned} \quad (\text{A5})$$

and hence,

$$\frac{1}{\lambda} \sum_{i=n_1+1}^{n_2} M_i - \frac{1}{1 - \lambda} \sum_{i=n_2+1}^m M_i = 0, \quad (\text{A6})$$

which contradicts the linear independence of M_i .

APPENDIX B: PROOF OF LEMMA 4

Without loss of generality, we consider the two-block case, $\rho = r\rho_1 \oplus (1 - r)\rho_2$.

Let us first prove for the case of R_c . Denote Π_1 as the projector onto the support of ρ_1 , $\Pi_1 = \sum_a |\alpha_a\rangle\langle\alpha_a|$ with $\{|\alpha_a\rangle\}$ being the set of nonzero eigenstates of ρ_1 . Similarly, denote Π_2 as the projector onto the support of state ρ_2 . In this proof, only the support of ρ is under consideration, $\Pi_1 + \Pi_2 = \mathbf{1}$. Then, $\Pi_1 \rho \Pi_1 = r\rho_1$ and $\Pi_2 \rho \Pi_2 = (1 - r)\rho_2$.

For arbitrary pure state $|\phi\rangle$ in the support space of ρ , let $|\phi_1\rangle = \Pi_1|\phi\rangle/\sqrt{p_1}$ and $|\phi_2\rangle = \Pi_2|\phi\rangle/\sqrt{p_2}$ with $p_1 = \langle\phi|\Pi_1|\phi\rangle$ and $p_2 = 1 - p_1 = \langle\phi|\Pi_2|\phi\rangle$, and from Eq. (19),

$$\langle\phi|\Pi_1 P_i \Pi_1|\phi\rangle + \langle\phi|\Pi_2 P_i \Pi_2|\phi\rangle = \langle\phi|P_i|\phi\rangle. \quad (\text{B1})$$

The quantum entropies,

$$\begin{aligned} S(\Delta_{\mathbf{P}}(|\phi_1\rangle\langle\phi_1|)) &= H\left(\left\{\frac{\langle\phi|\Pi_1 P_i \Pi_1|\phi\rangle}{p_1}\right\}\right), \\ S(\Delta_{\mathbf{P}}(|\phi_2\rangle\langle\phi_2|)) &= H\left(\left\{\frac{\langle\phi|\Pi_2 P_i \Pi_2|\phi\rangle}{p_2}\right\}\right), \end{aligned} \quad (\text{B2})$$

satisfy the concavity condition,

$$\begin{aligned} p_1 S(\Delta_{\mathbf{P}}(|\phi_1\rangle\langle\phi_1|)) + p_2 S(\Delta_{\mathbf{P}}(|\phi_2\rangle\langle\phi_2|)) &\leq H(\{\langle\phi|P_i|\phi\rangle\}) \\ &= S(\Delta_{\mathbf{P}}(|\phi\rangle\langle\phi|)). \end{aligned} \quad (\text{B3})$$

Now, consider an arbitrary decomposition $\rho = \sum_j q_j |\psi_j\rangle\langle\psi_j|$,

$$\begin{aligned} \Pi_1 \rho \Pi_1 &= r\rho_1 = \sum_j q_j p_{1j} |\psi_{1j}\rangle\langle\psi_{1j}|, \\ \Pi_2 \rho \Pi_2 &= (1 - r)\rho_2 = \sum_j q_j p_{2j} |\psi_{2j}\rangle\langle\psi_{2j}|, \end{aligned} \quad (\text{B4})$$

where $p_{1j} = \langle\psi_j|\Pi_1|\psi_j\rangle$, $p_{2j} = \langle\psi_j|\Pi_2|\psi_j\rangle$, $|\psi_{1j}\rangle = \Pi_1|\psi_j\rangle/\sqrt{p_{1j}}$, and $|\psi_{2j}\rangle = \Pi_2|\psi_j\rangle/\sqrt{p_{2j}}$. Combining with Eq. (B3),

$$\begin{aligned} \sum_j q_j p_{1j} S(\Delta_{\mathbf{P}}(|\psi_{1j}\rangle\langle\psi_{1j}|)) + \sum_j q_j p_{2j} S(\Delta_{\mathbf{P}}(|\psi_{2j}\rangle\langle\psi_{2j}|)) \\ \leq \sum_j q_j S(\Delta_{\mathbf{P}}(|\psi_j\rangle\langle\psi_j|)). \end{aligned} \quad (\text{B5})$$

Note that $\{|\psi_{1j}\rangle\}$ and $\{|\psi_{2j}\rangle\}$ are the pure-state decompositions of ρ_1 and ρ_2 , respectively. According to the randomness function defined in Eq. (14), we have $rR_c(\rho_1, \mathbf{P}) + (1 - r)R_c(\rho_2, \mathbf{P}) \leq R_c(\rho, \mathbf{P})$. Therefore, by combining it with the convexity condition, Eq. (16), the additivity condition can be obtained.

For the case of R_q , first, from the definition in Eq. (17), ρ_1 and ρ_2 have different orthogonal supports,

$$\begin{aligned} S(\rho) &= S(r\rho_1 + (1 - r)\rho_2) \\ &= h(r) + rS(\rho_1) + (1 - r)S(\rho_2), \end{aligned} \quad (\text{B6})$$

where $h(r) = -r \log r - (1 - r) \log(1 - r)$ is the binary entropy function. Second, the dephasing state is given by

$$\begin{aligned} \sum_i P_i \rho P_i &= \sum_i r P_i \rho_1 P_i + (1 - r) P_i \rho_2 P_i \\ &= r \Delta_{\mathbf{P}}(\rho_1) + (1 - r) \Delta_{\mathbf{P}}(\rho_2). \end{aligned} \quad (\text{B7})$$

From the definition in Eq. (17), we can see that $\Delta_{\mathbf{P}}(\rho_1)$ and $\Delta_{\mathbf{P}}(\rho_2)$ have orthogonal supports, and hence,

$$S\left(\sum_i P_i \rho P_i\right) = h(r) + rS(\Delta_{\mathbf{P}}(\rho_1)) + (1 - r)S(\Delta_{\mathbf{P}}(\rho_2)). \quad (\text{B8})$$

By substituting Eqs. (B6) and (B8) into the fifth equality of Eq. (13), we can prove the claim.

APPENDIX C: PROOF OF LEMMA 5

According to the unitary invariance of the randomness functions, we always have $R(\rho, U^\dagger \mathbf{P} U) = R(U \rho U^\dagger, \mathbf{P})$ and need to prove $R(\rho, \mathbf{P}) = R(U \rho U^\dagger, \mathbf{P})$.

(i) Consider $R = R_c$,

$$\begin{aligned} R_c(\rho, \mathbf{P}) &= \min_{\{q_j, |\psi_j\rangle\}} \sum_j q_j R_c(|\psi_j\rangle\langle\psi_j|, \mathbf{P}) \\ &= \min_{\{q_j, |\psi_j\rangle\}} \sum_j q_j R_c(U|\psi_j\rangle\langle\psi_j|U^\dagger, \mathbf{P}) \\ &= R_c(U \rho U^\dagger, \mathbf{P}). \end{aligned} \quad (\text{C1})$$

(ii) Consider the case $R = R_q$ and suppose $\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ is the spectral decomposition; its purification

can be taken as $|\Psi^{AE}\rangle = \sum_j \sqrt{\lambda_j} |\psi_j\rangle^A |j\rangle^E$. Denote $\sigma = U\rho U^\dagger$ and $(U^A \otimes \mathbf{1}^E)|\Psi^{AE}\rangle$ is its purification. Write the two classical-quantum states after Alice's measurement as given in Eq. (11),

$$\begin{aligned}\tilde{\rho}^{A'E} &= \sum_i p_i |i\rangle\langle i|^{A'} \otimes \rho_i^E, \\ \tilde{\sigma}^{A'E} &= \sum_i p_i |i\rangle\langle i|^{A'} \otimes \sigma_i^E,\end{aligned}\quad (\text{C2})$$

where from Eq. (22), p_i and the classical measurement outcome system A' are the same in the two equations, $\rho_i^E = \text{tr}_A[|\Psi\rangle\langle\Psi|^{AE}(P_i^A \otimes \mathbf{1}^E)]/p_i$ and $\sigma_i^E = \text{tr}_A[|\Psi\rangle\langle\Psi|^{AE}((U^\dagger P_i U)^A \otimes \mathbf{1}^E)]/p_i$.

For any two different eigenstates $|\psi_j\rangle$ and $|\psi_{j'}\rangle$, consider a pure state $|\psi\rangle = a|\psi_j\rangle + b|\psi_{j'}\rangle$, with $|a|^2 + |b|^2 = 1$. According to Eq. (22),

$$\begin{aligned}|a|^2 p_{ij} + |b|^2 p_{i'j'} + 2\text{Re}(a^* b \langle \psi_j | P_i | \psi_{j'} \rangle) \\ = |a|^2 p_{ij} + |b|^2 p_{i'j'} + 2\text{Re}(a^* b \langle \psi_j | U^\dagger P_i U | \psi_{j'} \rangle),\end{aligned}\quad (\text{C3})$$

where $p_{ij} = \langle \psi_j | P_i | \psi_j \rangle$ and $p_{i'j'} = \langle \psi_{j'} | P_i | \psi_{j'} \rangle$. Since a, b are arbitrary, it can be obtained $\langle \psi_j | P_i | \psi_{j'} \rangle = \langle \psi_j | U^\dagger P_i U | \psi_{j'} \rangle, \forall j, j'$. Combined with the fact

$$\begin{aligned}\rho_i^E &= \frac{1}{p_i} \sum_{jj'} \sqrt{\lambda_j \lambda_{j'}} \langle \psi_{j'} | P_i | \psi_j \rangle |j\rangle\langle j|^{j'E}, \\ \sigma_i^E &= \frac{1}{p_i} \sum_{jj'} \sqrt{\lambda_j \lambda_{j'}} \langle \psi_{j'} | U^\dagger P_i U | \psi_j \rangle |j\rangle\langle j|^{j'E},\end{aligned}\quad (\text{C4})$$

we have $\rho_i^E = \sigma_i^E$. Then, from Eq. (C2), we get $\tilde{\rho}^{A'E} = \tilde{\sigma}^{A'E}$. Moreover, due to Eq. (C1) and the relation between two randomness functions Eq. (15), we have $R_q(\rho, \mathbf{P}) = R_q(\rho, U^\dagger \mathbf{P} U)$.

APPENDIX D: PROOF OF THEOREM 1

To prove Theorem 1, we need the following lemma.

Lemma 6. For any two Naimark extensions with pure ancillary state, $\{\mathbf{P}_1, |\varphi_1\rangle\langle\varphi_1|\}$ and $\{\mathbf{P}_2, |\varphi_2\rangle\langle\varphi_2|\}$, for arbitrary input state ρ , $R(\rho \otimes |\varphi_1\rangle\langle\varphi_1|, \mathbf{P}_1) = R(\rho \otimes |\varphi_2\rangle\langle\varphi_2|, \mathbf{P}_2)$.

Proof. By inserting necessary zero subspace, we can link \mathbf{P}_1 and \mathbf{P}_2 with a unitary matrix, according to Lemma 3. With the freedom to choose a unitary transformation, we can assume $|\varphi_1\rangle = |\varphi_2\rangle = |1\rangle$. By the consistency condition in Eq. (4) and Lemma 5, we can obtain $R(\rho \otimes |\varphi_1\rangle\langle\varphi_1|, \mathbf{P}_1) = R(\rho \otimes |\varphi_2\rangle\langle\varphi_2|, \mathbf{P}_2)$. ■

With this Lemma, we prove Theorem 1.

Proof. We need to show that the mixture of ancillary states would not affect the intrinsic randomness. Consider a generalized Naimark extension to be $\{\mathbf{P}, \sigma\}$. Without loss of generality, suppose the ancillary state is rank 2 and has the spectral decomposition $\sigma = r|\varphi_1\rangle\langle\varphi_1| + (1-r)|\varphi_2\rangle\langle\varphi_2|$ and $0 < r < 1$. Then, according to Proposition 1 and Definition 1, we know that $\{\mathbf{P}, |\varphi_1\rangle\langle\varphi_1|\}$ and $\{\mathbf{P}, |\varphi_2\rangle\langle\varphi_2|\}$ are also Naimark extensions of \mathbf{M} .

Consider a pure state $|\varphi\rangle = a|\varphi_1\rangle + b|\varphi_2\rangle$ with $|a|^2 + |b|^2 = 1$ and $a, b \in \mathbb{C}$; we have

$$M_i = \text{tr}_Q[P_i(\mathbf{1}^A \otimes |\varphi\rangle\langle\varphi|^Q)] = M_i + ab^* W_i + a^* b W_i^\dagger, \quad (\text{D1})$$

where $W_i = \text{tr}_Q[P_i(\mathbf{1}^A \otimes |\varphi_1\rangle\langle\varphi_1|)]$. The coefficients a, b are arbitrary; thus, $W_i = 0$. For any pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, we have

$$\begin{aligned}\text{tr}(P_i |\psi_1\rangle\langle\psi_1| \langle\psi_1| P_i |\psi_2\rangle\langle\psi_2|) \\ = |\langle\psi_1| P_i |\psi_2\rangle|^2\end{aligned}\quad (\text{D2})$$

$$= |\langle\psi_1| W_i |\psi_2\rangle|^2 = 0. \quad (\text{D3})$$

This implies that the global state $\rho \otimes \sigma = r\rho \otimes |\varphi_1\rangle\langle\varphi_1| + (1-r)\rho \otimes |\varphi_2\rangle\langle\varphi_2|$ is always block-diagonal in Definition 4 and according to the additivity condition of the randomness functions in Lemma 4,

$$\begin{aligned}R(\rho \otimes \sigma, \mathbf{P}) &= rR(\rho \otimes |\varphi_1\rangle\langle\varphi_1|, \mathbf{P}) \\ &\quad + (1-r)R(\rho \otimes |\varphi_2\rangle\langle\varphi_2|, \mathbf{P}).\end{aligned}\quad (\text{D4})$$

Combine this equation with Lemma 6; then the randomness for extremal POVM is given by a canonical Naimark extension

$$R(\rho, \mathbf{M}) = R(\rho \otimes |1\rangle\langle 1|, \mathbf{P}_c). \quad (\text{D5})$$

■

APPENDIX E: PROOF OF PROPOSITION 1

Denote a generalized Naimark extension to be $\{\mathbf{P}, \sigma\}$.

⇒: The ancillary state has decomposition of $\sigma = \sum_j r_j |\varphi_j\rangle\langle\varphi_j|$. Then, the consistency condition becomes

$$\begin{aligned}M_i &= \text{tr}_Q[P_i(\mathbf{1}^A \otimes \sigma^Q)] \\ &= \sum_j r_j \text{tr}_Q[P_i(\mathbf{1}^A \otimes |\varphi_j\rangle\langle\varphi_j|^Q)].\end{aligned}\quad (\text{E1})$$

Denote $N_i^j = \text{tr}_Q[P_i(\mathbf{1}^A \otimes |\varphi_j\rangle\langle\varphi_j|^Q)]$ and hence

$$M_i = \sum_j r_j N_i^j. \quad (\text{E2})$$

Here, $\mathbf{N}^j = \{N_1^j, \dots, N_m^j\}$ forms a POVM on system A for each j . Thus, this gives a decomposition of POVM $\mathbf{M} = \sum_j r_j \mathbf{N}^j$. Note that each \mathbf{N}^j has an extended PVM of \mathbf{P} , independent of j .

⇐: The POVM has decomposition of $\mathbf{M} = \sum_{j=1}^l r_j \mathbf{N}^j$. According to the canonical Naimark extension, for each POVM \mathbf{N}^j , there exists an ancillary system Q_1 with an orthonormal basis $\{|1\rangle, \dots, |m\rangle\}$ and a unitary operator $U_j^{AQ_1}$ on global system $\mathcal{H}^A \otimes \mathcal{H}^{Q_1}$ such that

$$N_i^j = \text{tr}_{Q_1}[(U_j^{AQ_1})^\dagger (\mathbf{1}^A \otimes |i\rangle\langle i|^{Q_1}) U_j^{AQ_1} (\mathbf{1}^A \otimes |1\rangle\langle 1|^{Q_1})]. \quad (\text{E3})$$

Add another ancillary system Q_2 with an orthonormal basis $\{|\varphi_1\rangle, \dots, |\varphi_l\rangle\}$ and $Q_1 Q_2$ forms the total ancillary system Q in Fig. 2(b). Let the input ancillary state be $\sigma^Q = \sum_{j=1}^l r_j |1\rangle\langle 1|^{Q_1} \otimes |\varphi_j\rangle\langle\varphi_j|^Q$, which is in a form of pure-state decomposition. The unitary operator and the extended PVM are

$$\begin{aligned}U^{AQ} &= \sum_{j=1}^l U_j^{AQ_1} \otimes |\varphi_j\rangle\langle\varphi_j|^Q, \\ P_i &= (U^{AQ})^\dagger (\mathbf{1}^{AQ_2} \otimes |i\rangle\langle i|^{Q_1}) U^{AQ}.\end{aligned}\quad (\text{E4})$$

We need to show the consistency condition,

$$\begin{aligned}
& \text{tr}_Q[P_i(\mathbf{1}^A \otimes \sigma^Q)] \\
&= \text{tr}_Q[(U^{AQ})^\dagger(\mathbf{1}^{AQ_2} \otimes |i\rangle\langle i|^{Q_1})U^{AQ}(\mathbf{1}^A \otimes \sigma^Q)] \\
&= \sum_{j=1}^l r_j \text{tr}_Q(\mathbf{1}^A \otimes |1\varphi_j\rangle\langle 1\varphi_j|^Q) \\
&\quad \times (U^{AQ})^\dagger(\mathbf{1}^{AQ_2} \otimes |i\rangle\langle i|^{Q_1})U^{AQ}(\mathbf{1}^A \otimes |1\varphi_j\rangle\langle 1\varphi_j|^Q) \\
&= \sum_{j=1}^l r_j \text{tr}_{Q_1}(\mathbf{1}^A \otimes |1\rangle\langle 1|^{Q_1})(U_j^{AQ_1})^\dagger \\
&\quad \times (\mathbf{1}^A \otimes |i\rangle\langle i|^{Q_1})U_j^{AQ_1}(\mathbf{1}^A \otimes |1\rangle\langle 1|^{Q_1}) \\
&= \sum_{j=1}^l r_j N_i^j = M_i. \tag{E5}
\end{aligned}$$

APPENDIX F: PROOF OF THEOREM 2

Consider a generalized Naimark extension $\{\mathbf{P}, \sigma\}$. After Eve's measurement, the ancillary state can be treated as a pure-state ensemble, $\sigma = \sum_j r_j |\varphi_j\rangle\langle \varphi_j|$. Then, the randomness of ρ is given by

$$R^{cf}(\rho, \mathbf{M}) = \sum_j r_j R(\rho \otimes |\varphi_j\rangle\langle \varphi_j|, \mathbf{P}). \tag{F1}$$

The state decomposition corresponds to a POVM decomposition, $\mathbf{M} = \sum_j r_j \mathbf{N}^j$, from Proposition 1. To prove the theorem, we only need to prove that all \mathbf{N}^j are extremal; otherwise, we can find a smaller randomness value with a different extension.

Suppose one of the decomposed POVM, \mathbf{N}^0 , is not extremal and can be decomposed into $\mathbf{N}^0 = \lambda \mathbf{N}^{00} + (1 - \lambda) \mathbf{N}^{01}$, $0 < \lambda < 1$. Then, there is another decomposition of \mathbf{M} ,

$$\mathbf{M} = \lambda r_0 \mathbf{N}^{00} + (1 - \lambda) r_0 \mathbf{N}^{01} + \sum_{j \neq 0} r_j \mathbf{N}^j. \tag{F2}$$

From Eq. (E4), we can construct another Naimark extension $\{\mathbf{P}', \sigma'\}$ with ancillary state

$$\sigma' = \lambda r_0 |\varphi_{00}\rangle\langle \varphi_{00}| + (1 - \lambda) r_0 |\varphi_{01}\rangle\langle \varphi_{01}| + \sum_{j \neq 0} r_j |\varphi'_j\rangle\langle \varphi'_j|, \tag{F3}$$

where $\forall i$, the operator on system A , $\langle \varphi_{00} | P'_i | \varphi_{01} \rangle = 0$. After Eve's measurement, the randomness is given by

$$\begin{aligned}
& \lambda r_0 R(\rho \otimes |\varphi_{00}\rangle\langle \varphi_{00}|, \mathbf{P}') + (1 - \lambda) r_0 R(\rho \otimes |\varphi_{01}\rangle\langle \varphi_{01}|, \mathbf{P}') \\
&+ \sum_{j \neq 0} r_j R(\rho \otimes |\varphi'_j\rangle\langle \varphi'_j|, \mathbf{P}') \\
&= r_0 R(\rho \otimes [\lambda |\varphi_{00}\rangle\langle \varphi_{00}| + (1 - \lambda) |\varphi_{01}\rangle\langle \varphi_{01}|], \mathbf{P}') \\
&+ \sum_{j \neq 0} r_j R(\rho \otimes |\varphi_j\rangle\langle \varphi_j|, \mathbf{P}), \tag{F4}
\end{aligned}$$

where the equality comes from the additivity condition of the randomness functions for PVMs and Lemma 6.

Now, we only need to prove that

$$\begin{aligned}
& \lambda R(\rho \otimes |\varphi_{00}\rangle\langle \varphi_{00}|, \mathbf{P}') + (1 - \lambda) R(\rho \otimes |\varphi_{01}\rangle\langle \varphi_{01}|, \mathbf{P}') \\
&\leq R(\rho \otimes |\varphi_0\rangle\langle \varphi_0|, \mathbf{P}), \tag{F5}
\end{aligned}$$

for the randomness functions R_c in Eq. (14) and R_q in Eq. (13).

First, we consider the case of R_c . For pure input state $|\psi\rangle$, the consistency condition implies

$$\begin{aligned}
& \lambda \langle \psi | \varphi_{00} | P'_i | \psi \varphi_{00} \rangle + (1 - \lambda) \langle \psi | \varphi_{01} | P'_i | \psi \varphi_{01} \rangle \\
&= \langle \psi | \varphi_0 | P_i | \psi \varphi_0 \rangle. \tag{F6}
\end{aligned}$$

Due to the concavity of the Shannon entropy, we have

$$\begin{aligned}
& \lambda H(\{\langle \psi | \varphi_{00} | P'_i | \psi \varphi_{00} \rangle\}) + (1 - \lambda) H(\{\langle \psi | \varphi_{01} | P'_i | \psi \varphi_{01} \rangle\}) \\
&\leq H(\{\langle \psi | \varphi_0 | P_i | \psi \varphi_0 \rangle\}). \tag{F7}
\end{aligned}$$

Then Eq. (F5) for a general mixed state ρ can be obtained directly.

Now we consider the case of R_q . Suppose $|\Phi\rangle^{QF}$ is a purification of state $\tilde{\sigma} = \lambda |\varphi_{00}\rangle\langle \varphi_{00}| + (1 - \lambda) |\varphi_{01}\rangle\langle \varphi_{01}|$. Combine the consistency condition with Lemma 5 and Lemma 6; then

$$\begin{aligned}
& S(\rho^A \otimes |\Phi\rangle\langle \Phi|^{QF} \| \Delta_{\mathbf{P}^A \otimes \mathbf{1}^F}(\rho^A \otimes |\Phi\rangle\langle \Phi|^{QF})) \\
&= S(\rho \otimes |\varphi_0\rangle\langle \varphi_0| \| \Delta_{\mathbf{P}}(\rho \otimes |\varphi_0\rangle\langle \varphi_0|)). \tag{F8}
\end{aligned}$$

Take the partial trace tr_F on the left-hand side of the above equality; from the monotonicity of relative entropy, there is

$$\begin{aligned}
& S(\rho \otimes \tilde{\sigma} \| \Delta_{\mathbf{P}'}(\rho \otimes \tilde{\sigma})) \leq S(\rho \otimes |\varphi_0\rangle\langle \varphi_0| \| \\
&\quad \times \Delta_{\mathbf{P}}(\rho \otimes |\varphi_0\rangle\langle \varphi_0|)). \tag{F9}
\end{aligned}$$

Combine the inequality with the additivity condition and Eq. (F5) holds.

APPENDIX G: PROOF OF COROLLARY 1

We first prove that item 2 is a sufficient and necessary condition for $R^{cf}(\rho, \mathbf{M}) = 0$.

Sufficiency (\Rightarrow): For each extremal POVM \mathbf{N}^j , there exists a Naimark extension $\{\mathbf{P}^j, |\varphi_j\rangle\langle \varphi_j|\}$. According to the condition, for $\forall k$, we can find a POVM element N_i^j such that

$$\begin{aligned}
& \langle \psi_k^j | \varphi_j | P_i^j | \psi_k^j \varphi_j \rangle = \text{tr}\{\langle \psi_k^j | \langle \psi_k^j |^A \text{tr}_Q[P_i^j(\mathbf{1}^A \otimes |\varphi_j\rangle\langle \varphi_j|^Q)]\} \\
&= \text{tr}(N_i^j | \psi_k^j \rangle \langle \psi_k^j |) = 1. \tag{G1}
\end{aligned}$$

It follows that $P_i^j | \psi_k^j \varphi_j \rangle = | \psi_k^j \varphi_j \rangle$, and moreover, $R^{cf}(\rho, \mathbf{M}) = \sum_j r_j R(\rho, \mathbf{N}^j) = 0$.

Necessity (\Leftarrow): If $R^{cf}(\rho, \mathbf{M}) = 0$, there exists an extremal decomposition $\mathbf{M} = \sum_j r_j \mathbf{N}^j$, such that $\forall j$, $R(\rho, \mathbf{N}^j) = R(\rho \otimes |\varphi_j\rangle\langle \varphi_j|, \mathbf{P}^j) = 0$. Therefore, $\rho \otimes |\varphi_j\rangle\langle \varphi_j|$ does not change after the associated block-dephasing operation. We write the dephased state into its spectral decomposition,

$$\rho \otimes |\varphi_j\rangle\langle \varphi_j| = \sum_i P_i^j(\rho \otimes |\varphi_j\rangle\langle \varphi_j|)P_i^j = \sum_k q_k^j |u_k^j\rangle\langle u_k^j|. \tag{G2}$$

The eigenstate of $\rho \otimes |\varphi_j\rangle\langle \varphi_j|$ must be the product state. Thus, $|u_k^j\rangle = | \psi_k^j \varphi_j \rangle$ is also an eigenstate of some PVM element P_i^j . From Eq. (G1), we can obtain $N_i^j | \psi_k^j \rangle = | \psi_k^j \rangle$.

The sufficiency and necessity of item 1 can be deduced from the fact that $N_i^j \rho N_i^j = 0, i \neq i',$ is the sufficient and necessary condition for $R(\rho \otimes |\varphi_j\rangle\langle\varphi_j|, \mathbf{P}^j) = 0$ [23].

APPENDIX H: PROOF OF COROLLARY 2

To prove Corollary 2, we need the following definition and two lemmas.

Definition 6 (grouping/coarse-graining process [34]). Give two POVMs $\mathbf{M} = \{M_1, \dots, M_m\}$ and $\mathbf{N} = \{N_1, \dots, N_n\}$ with $m \leq n.$ A grouping is determined by a mapping $f : [n] \rightarrow [m].$ Concretely, the elements of two POVMs have the relation

$$M_i = \sum_{j \in f^{-1}(i)} N_j, \tag{H1}$$

where f^{-1} represents the inverse mapping.

Lemma 7. For a POVM, $\mathbf{M} = \{M_1, \dots, M_m\},$ if $|\psi_1\rangle, \dots, |\psi_l\rangle$ are pairwise orthogonal states and each $|\psi_k\rangle$ is a common eigenstate of all elements $M_i,$ then there exists a decomposition

$$\mathbf{M} = \sum_j r_j \mathbf{N}^j, \tag{H2}$$

such that for an arbitrary pure state $|\psi_k\rangle,$ each \mathbf{N}^j contains an element N_i^j satisfying $N_i^j |\psi_k\rangle = |\psi_k\rangle.$

Proof. From the condition, each POVM element has an eigendecomposition

$$M_i = \sum_{i'=1}^d \lambda_{i i'} |\psi_{i'}\rangle\langle\psi_{i'}|, \tag{H3}$$

where $|\psi_{i1}\rangle = |\psi_1\rangle, \dots, |\psi_{il}\rangle = |\psi_l\rangle$ and $\lambda_{i i'} \geq 0, \sum_{i'} \lambda_{i i'} = 1.$ All rank-1 terms form a new POVM denoted as $\mathbf{A} = \{\lambda_{i i'} |\psi_{i'}\rangle\langle\psi_{i'}|, i \in [m], i' \in [d]\}.$ Via the method that decomposes a POVM into a mixture of extremal POVMs in the proof of Lemma 1, the rank-1 POVM \mathbf{A} can be decomposed into a mixture of extremals. From the description of the algorithm, the elements of extremal POVMs inherit the elements of the POVM \mathbf{A} with only a difference in coefficients. As a consequence, each extremal POVM has elements $\{c_1 |\psi_1\rangle\langle\psi_1|, \dots, c_l |\psi_l\rangle\langle\psi_l|\}$ and other elements are in an orthogonal space; thus, $c_1 = \dots = c_l = 1.$ Write the decomposition as

$$\mathbf{A} = \sum_j r_j \mathbf{B}^j, \tag{H4}$$

and each POVM $\mathbf{B}^j = \{B_{i'}^j, i \in [m], i' \in [d]\}$ contains elements $\{|\psi_1\rangle\langle\psi_1|, \dots, |\psi_l\rangle\langle\psi_l|\}.$ Define $\mathbf{N}^j = \{N_1^j, \dots, N_m^j\}$ as a grouping of $\mathbf{B}^j,$

$$N_i^j = \sum_{i'=1}^d B_{i'}^j. \tag{H5}$$

Therefore, $\mathbf{M} = \sum_j r_j \mathbf{N}^j;$ in addition, for each \mathbf{N}^j and each $|\psi_k\rangle,$ there exists a related N_i^j such that $N_i^j |\psi_k\rangle = |\psi_k\rangle. \blacksquare$

Lemma 8. If $R(\rho, \mathbf{M}) = 0,$ then $[\rho, M_i] = \rho M_i - M_i \rho = 0, \forall i.$

Proof. Since $R(\rho, \mathbf{M}) = 0,$ there exists a Naimark extension $\{\mathbf{P}, \sigma\}$ such that the global input state has a spectral decomposition

$$\rho \otimes \sigma = \Delta_{\mathbf{P}}(\rho \otimes \sigma) = \sum_k \lambda_k |u_k\rangle\langle u_k|, \tag{H6}$$

where $\forall i, P_i |u_k\rangle = |u_k\rangle,$ or $P_i |u_k\rangle = 0.$ In either case, we can obtain $P_i(\rho \otimes \sigma) = (\rho \otimes \sigma) P_i.$ Take partial trace $\text{tr}_{\mathcal{Q}}$ on both sides of the equality,

$$\text{tr}_{\mathcal{Q}}[P_i(\mathbf{1}^{\mathcal{A}} \otimes \sigma^{\mathcal{Q}})(\rho^{\mathcal{A}} \otimes \mathbf{1}^{\mathcal{Q}})] = \text{tr}_{\mathcal{Q}}[(\rho^{\mathcal{A}} \otimes \mathbf{1}^{\mathcal{Q}})(\mathbf{1}^{\mathcal{A}} \otimes \sigma^{\mathcal{Q}})P_i]. \tag{H7}$$

Combined with the consistency condition, there is $M_i \rho = \rho M_i. \blacksquare$

Now, we give proof of Corollary 2.

Proof. From Lemma 8, the sufficiency is apparent. The two randomness functions have the relation $R(\rho, \mathbf{M}) \leq R^{cf}(\rho, \mathbf{M});$ therefore, the necessity can be directly obtained by Corollary 1 and Lemma 7. \blacksquare

APPENDIX I: PROOF OF THEOREM 3

For SIC POVM $\mathbf{M} = \{|\phi_1\rangle\langle\phi_1|/d, \dots, |\phi_{d^2}\rangle\langle\phi_{d^2}|/d\},$ let $\{\mathbf{P}, |1\rangle\langle 1|\}$ be a canonical Naimark PVM.

(i) When $R = R_c,$ the minimum randomness is achieved by some pure states from the expression Eq. (14). The randomness for pure state $|\psi\rangle$ is equal to Shannon entropy $H(\{p_i\})$ with $p_i = |\langle\phi_i|\psi\rangle|^2/d.$ For any state ρ and $p_i = \text{tr}(\rho|\phi_i\rangle\langle\phi_i|/d),$ the entropy of the distribution has a state-independent lower bound [51],

$$H(\{p_i\}) \geq \log \left(\frac{d(d+1)}{\text{tr}(\rho^2) + 1} \right). \tag{I1}$$

As a result,

$$R_c(\mathbf{M}) \geq \log \left(\frac{d(d+1)}{2} \right) > \log \left(\frac{d+1}{2} \right). \tag{I2}$$

(ii) When $R = R_q(\rho \otimes |1\rangle\langle 1|, \mathbf{P}) = S(\Delta_{\mathbf{P}}(\rho \otimes |1\rangle\langle 1|)) - S(\rho),$ assume $P_i(\rho \otimes |1\rangle\langle 1|)P_i = \sum_k q_{ik} |u_{ik}\rangle\langle u_{ik}|$ is a spectral decomposition and $\sum_k q_{ik} = \text{tr}(\rho|\phi_i\rangle\langle\phi_i|/d) = p_i.$ The entropy of probability distribution $\{q_{ik}/p_i\}$ is

$$\begin{aligned} 0 &\leq - \sum_k \frac{q_{ik}}{p_i} \log \left(\frac{q_{ik}}{p_i} \right) \\ &= - \frac{1}{p_i} \left[\sum_k (q_{ik} \log q_{ik}) - p_i \log p_i \right]. \end{aligned} \tag{I3}$$

Hence, $-\sum_k q_{ik} \log q_{ik} \geq -p_i \log p_i.$ Then the term $S(\Delta_{\mathbf{P}}(\rho \otimes |1\rangle\langle 1|)) = S[\sum_i P_i(\rho \otimes |1\rangle\langle 1|)P_i] \geq H(\{p_i\})$ and the equality holds only if ρ is pure. Combine this with Eq. (I1) and there is

$$\begin{aligned} R_q(\rho, \mathbf{M}) &\geq H(\{p_i\}) - S(\rho) \geq \log \left(\frac{d(d+1)}{\text{tr}(\rho^2) + 1} \right) - S(\rho) \\ &> \log \left(\frac{d+1}{2} \right). \end{aligned} \tag{I4}$$

Then, $R_q(\mathbf{M}) > \log[(d+1)/2].$

- [1] M. Born, Quantenmechanik der stoßvorgänge, *Z. Phys.* **37**, 863 (1926).
- [2] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).
- [3] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
- [4] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Efficient quantum state tomography, *Nat. Commun.* **1**, 149 (2010).
- [5] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, Sample-optimal tomography of quantum states, *IEEE Trans. Inf. Theory* **63**, 5628 (2017).
- [6] G. M. D'Ariano, L. Maccone, and P. Lo Presti, Quantum Calibration of Measurement Instrumentation, *Phys. Rev. Lett.* **93**, 250407 (2004).
- [7] J. Lundeen, A. Feito, H. Coldenstrodt-Ronge, K. Pregnell, C. Silberhorn, T. Ralph, J. Eisert, M. Plenio, and I. Walmsley, Tomography of quantum detectors, *Nat. Phys.* **5**, 27 (2009).
- [8] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, *Phys. Rev. X* **6**, 011020 (2016).
- [9] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, *Phys. Rev. Lett.* **118**, 060503 (2017).
- [10] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified Quantum Random Numbers from Untrusted Light, *Phys. Rev. X* **10**, 041048 (2020).
- [11] W. H. Zurek, Quantum Darwinism, *Nat. Phys.* **5**, 181 (2009).
- [12] J. Åberg, Quantifying superposition, [arXiv:quant-ph/0612146](https://arxiv.org/abs/quant-ph/0612146).
- [13] T. Baumgratz, M. Cramer, and M. B. Plenio, Quantifying Coherence, *Phys. Rev. Lett.* **113**, 140401 (2014).
- [14] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Intrinsic randomness as a measure of quantum coherence, *Phys. Rev. A* **92**, 022124 (2015).
- [15] M. Hayashi and H. Zhu, Secure uniform random-number extraction via incoherent strategies, *Phys. Rev. A* **97**, 012302 (2018).
- [16] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, Quantum coherence and intrinsic randomness, *Adv. Quantum Technol.* **2**, 1900053 (2019).
- [17] M. Hayashi, K. Fang, and K. Wang, Finite block length analysis on quantum coherence distillation and incoherent randomness extraction, *IEEE Trans. Inf. Theory* **67**, 3926 (2021).
- [18] M. Dušek and V. Bužek, Quantum-controlled measurement device for quantum-state discrimination, *Phys. Rev. A* **66**, 022112 (2002).
- [19] A. Peres, Neumark's theorem and quantum inseparability, *Found. Phys.* **20**, 1441 (1990).
- [20] D. N. Biggerstaff, R. Kaltenbaek, D. R. Hamel, G. Weihs, T. Rudolph, and K. J. Resch, Cluster-State Quantum Computing Enhanced by High-Fidelity Generalized Measurements, *Phys. Rev. Lett.* **103**, 240504 (2009).
- [21] Y. Z. Law, J.-D. Bancal, V. Scarani *et al.*, Quantum randomness extraction for various levels of characterization of the devices, *J. Phys. A: Math. Theor.* **47**, 424028 (2014).
- [22] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New J. Phys.* **17**, 125011 (2015).
- [23] F. Bischof, H. Kampermann, and D. Bruß, Resource Theory of Coherence Based on Positive-Operator-Valued Measures, *Phys. Rev. Lett.* **123**, 110402 (2019).
- [24] J. Xu, L.-H. Shao, and S.-M. Fei, Coherence measures with respect to general quantum measurements, *Phys. Rev. A* **102**, 012411 (2020).
- [25] P. Skrzypczyk and N. Linden, Robustness of Measurement, Discrimination Games, and Accessible Information, *Phys. Rev. Lett.* **122**, 140403 (2019).
- [26] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Simulating Positive-Operator-Valued Measures with Projective Measurements, *Phys. Rev. Lett.* **119**, 190501 (2017).
- [27] M. Neumark, On a representation of additive operator set functions, *C. R. (Dokl.) Acad. Sci. U.R.S.S. (N.S.)* **41**, 359 (1943).
- [28] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, *J. Phys. A: Math. Gen.* **38**, 5979 (2005).
- [29] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* **45**, 2171 (2004).
- [30] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, The SIC question: History and state of play, *Axioms* **6**, 21 (2017).
- [31] G. Chiribella, G. M. D'Ariano, and D. Schlingemann, How Continuous Quantum Measurements in Finite Dimensions Are Actually Discrete, *Phys. Rev. Lett.* **98**, 190403 (2007).
- [32] G. Sentís, B. Gendra, S. D. Bartlett, and A. C. Doherty, Decomposition of any quantum measurement into extremals, *J. Phys. A: Math. Theor.* **46**, 375302 (2013).
- [33] G. Chiribella and G. M. D'Ariano, Extremal covariant positive operator valued measures, *J. Math. Phys.* **45**, 4435 (2004).
- [34] E. Haapasalo, T. Heinosaari, and J.-P. Pellonpää, Quantum measurements on finite dimensional systems: Relabeling and mixing, *Quantum Inf. Process.* **11**, 1751 (2012).
- [35] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement* (Springer, Berlin, 1996).
- [36] M. Ozawa, Quantum measuring processes of continuous observables, *J. Math. Phys.* **25**, 79 (1984).
- [37] F. Buscemi, M. Hayashi, and M. Horodecki, Global Information Balance in Quantum Measurements, *Phys. Rev. Lett.* **100**, 210504 (2008).
- [38] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.* **27**, 379 (1948).
- [39] R. Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **06**, 1 (2008).
- [40] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, *IEEE Trans. Inf. Theory* **55**, 5840 (2009).
- [41] A. Streltsov, G. Adesso, and M. B. Plenio, Colloquium: Quantum coherence as a resource, *Rev. Mod. Phys.* **89**, 041003 (2017).
- [42] X.-D. Yu, D.-J. Zhang, G. F. Xu, and D. M. Tong, Alternative framework for quantifying coherence, *Phys. Rev. A* **94**, 060302(R) (2016).
- [43] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. London A* **461**, 207 (2005).
- [44] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).

- [45] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, and J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments, *Sci. Adv.* **7**, eabc3847 (2021).
- [46] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Unbounded randomness from uncharacterized sources, *Commun. Phys.* **5**, 273 (2022).
- [47] J. Gorski, F. Pfeuffer, and K. Klamroth, Biconvex sets and optimization with biconvex functions: A survey and extensions, *Math. Methods Oper. Res.* **66**, 373 (2007).
- [48] A. Winter, Extrinsic and intrinsic data in quantum measurements: Asymptotic convex decomposition of positive operator valued measures, *Commun. Math. Phys.* **244**, 157 (2004).
- [49] S. Luo, Information conservation and entropy change in quantum measurements, *Phys. Rev. A* **82**, 052103 (2010).
- [50] M. M. Wilde, P. Hayden, F. Buscemi, and M.-H. Hsieh, The information-theoretic costs of simulating quantum measurements, *J. Phys. A: Math. Theor.* **45**, 453001 (2012).
- [51] A. E. Rastegin, Uncertainty relations for MUBs and SIC-POVMs in terms of generalized entropies, *Eur. Phys. J. D* **67**, 269 (2013).