Information leak and incompatibility of physical context: A modified approach

Arindam Mitra ,[*] Gautam Sharma,[†] and Sibasish Ghosh[‡]

Optics and Quantum Information Group, The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India and Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai 400094, India

(Received 26 February 2021; accepted 3 September 2021; published 29 September 2021)

A beautiful idea about the incompatibility of physical context (IPC) was introduced in Phys. Rev. A **102**, 050201(R) (2020). Here, a context is defined as a set of a quantum state and two sharp rank-one measurements, and the incompatibility of physical context is defined as the leakage of information while implementing those two measurements successively in that quantum state. In this work, we show the limitations in their approach. The three primary limitations are that (i) their approach is not generalized for positive operator-valued measurements; (ii) they restrict information theoretic agents Alice, Eve, and Bob to specific quantum operations and do not consider most general quantum operations, i.e., quantum instruments; and (iii) their measure of IPC can take negative values in specific cases in a more general scenario, which implies the limitation of their information measure. Thereby, we have introduced a generalization and modification to their approach in a more general and convenient way, such that this idea is well defined for generic measurements, without these limitations. We also present a comparison of the measure of the IPC through their and our methods. Lastly, we show, how the IPC reduces in the presence of memory using our modification, which further validates our approach.

DOI: 10.1103/PhysRevA.104.032225

I. INTRODUCTION

Measurement incompatibility is a key feature of quantum theory, which distinguishes it from the classical world [1]. A pair of observables are incompatible if they are not measurable simultaneously, i.e., their outcomes can not be obtained jointly via a single joint measurement. Today, the connections among incompatibility, nonlocality, and steering are well known [2,3]. Nonclassical features such as Bell inequality violation as well as steering can be demonstrated only using incompatible measurements [4,5]. It is also well known that incompatible measurements provide an advantage over compatible measurements in several information-theoretic tasks in quantum information theory [6,7]. Measurement compatibility can be characterized as the existence of a common (i.e., constructed using same ancilla state and Hilbert space) commuting Naimark extensions [8–10]. It has been recently shown that there are several layers of classicality inside the compatibility of measurement [11,12].

Recently, a novel idea was presented in Ref. [13] to get a better understanding of nonclassicality associated with incompatibility. The authors of Ref. [13] introduced the concept of incompatibility of the physical context (IPC), which is a function of a given context, where a context is comprised of a quantum state and two measurements. In a way their measure of IPC captures the notion of nonclassicality associated with the context, as it vanishes when the state is a maximally mixed state or the measurements are commuting with each other. It was defined as the difference between the information remaining in a quantum state after the first sharp measurement and after the second sharp measurement. Moreover, the IPC is also linked with the information leakage when an eavesdropper performs a measurement on the state being transferred in a QKD-like game [14].

However, as we will show, the approach of Ref. [13] has several limitations. First, the authors of Ref. [13] restricted information theoretic agents Alice, Eve, and Bob to specific quantum operations and did not consider most general quantum operations, i.e., quantum instruments. Second, if we do not restrict Alice, Eve, and Bob to specific quantum operations, which they did, then their measure of IPC can take negative value, which implies that the state after second measurement by eavesdropper Eve has more information than the state after first measurement, which physically does not make sense. Third, it is not possible to extend this idea to a generic POVM measurements through their approach and without introducing quantum instruments. Fourth, in the presence of memory, IPC can increase, which is against the intuition that incompatibility is nonincreasing as we add memory.

In this work, we have generalized the idea of IPC for POVMs and modified the corresponding information measure. Our measure of the IPC can never be negative and it is nonincreasing on addition of memory. We also demonstrate the usefulness of the modified IPC measure through a QKD-like scenario as an example. In this way our approach has a wider applicability.

The rest of this paper is organized as follows. In Sec. II, we discuss the preliminary concepts necessary for this paper. Then, we discuss the limitations of the approach given in Ref. [13] and discuss our main results in Sec. III. Further, in Sec. IV, we include the effect of presence of memory in

[*]amitra@imsc.res.in; arindammitra143@gmail.com
[†]gautam.oct@gmail.com
[‡]sibasish@imsc.res.in

our analysis. Finally, in Sec. V we summarize our work and discuss future direction.

II. PRELIMINARIES

A. Observables and channels

An observable A with outcome set Ω_A in quantum mechanics is a collection of positive hermitian matrices $\{A(x) \mid x \in \Omega_A\}$ such that $\sum_x A(x) = \mathbb{I}$. A pair of observables (A, B) acting on same d-dimensional Hilbert space $\mathcal{H}$ and with outcome sets Ω_A and Ω_B, respectively, is compatible if there exists a joint observable $\mathcal{G}$ acting on same Hilbert space $\mathcal{H}$ and outcome set $\Omega_A \times \Omega_B$ such that for all $\rho \in \mathcal{S}(\mathcal{H}), x \in \Omega_A$ and $y \in \Omega_B$

$$A(x) = \sum_y \mathcal{G}(x, y); B(y) = \sum_x \mathcal{G}(x, y), \tag{1}$$

where $\mathcal{S}(\mathcal{H})$ is the state space. Only for PVMs, compatibility implies commutativity. We denote the set of all observables as $\mathcal{O}$.

On the other hand, a quantum channel is a CPTP map from one state space $\mathcal{S}(\mathcal{H}_1)$ to another state space $\mathcal{S}(\mathcal{H}_2)$, where $\mathcal{H}_1$ and $\mathcal{H}_2$ are two Hilbert spaces. We denote the concatenation of two quantum channels Λ_1 and Λ_2 as $\Lambda_1 \circ \Lambda_2$. Therefore, for all $\rho \in \mathcal{S}(\mathcal{H})$, $(\Lambda_1 \circ \Lambda_2)(\rho) = \Lambda_1(\Lambda_2(\rho))$. Consider two quantum channels $\Gamma : \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}_2)$ and $\Lambda : \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}'_1)$. If there exists a quantum channel $\Theta : \mathcal{S}(\mathcal{H}'_1) \to \mathcal{S}(\mathcal{H}_2)$ such that $\Gamma = \Theta \circ \Lambda$ holds, we denote it as $\Gamma \preceq \Lambda$. If both $\Gamma \preceq \Lambda$ and $\Lambda \preceq \Gamma$ hold, we denote it as $\Gamma \simeq \Lambda$ and we call it as Γ and Λ are concatenation equivalent. We denote the set of all concatenation equivalent channels to Λ by $[\Lambda]$.

There exists a special type of channel known as a completely depolarizing channel, which we will use in the following section. A channel Σ is called a completely depolarizing channel if for all $T \in \mathcal{L}^+(\mathcal{H})$, $\Sigma(T) = \mathrm{Tr}(T)\eta$ for some fixed $\eta \in \mathcal{S}(\mathcal{H})$, where $\mathcal{L}^+(\mathcal{H})$ is set of positive linear operators on Hilbert space $\mathcal{H}$. We denote the set of all channels as $\mathcal{C}$.

B. Quantum instruments and measurement models

In quantum measurements, there are two equivalent concepts, namely measurement models and quantum instruments [15,16]. Measurement models are descriptions of measurement process, whereas instruments are the concise version of it. Consider a measured system S associated with a Hilbert space $\mathcal{H}_S$ and with density matrix ρ and an ancilla system associated with another Hilbert space $\mathcal{H}_a$ and with density matrix σ_a. To perform a measurement on a measured system, at first a joint unitary U has to be applied on the composite system where U is acting on Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_a$. Then, a pointer observable A' with outcome set Ω'_A has to be measured on the ancilla system. Now in this process if the observable A with same outcome set as A' has is measured on the system S then for all $x \in \Omega_A$ and $\rho \in \mathcal{H}_S$ we have

$$\mathrm{Tr}[\rho A(x)] = \mathrm{Tr}[U(\rho \otimes \sigma_a)U^\dagger(\mathbb{I} \otimes A'(x))]. \tag{2}$$

The average postmeasurement state is given by

$$\Lambda(\rho) = \mathrm{Tr}_{\mathcal{H}_a}[U(\rho \otimes \sigma_a)U^\dagger]. \tag{3}$$

Here, Λ is a quantum channel. This measurement model is specified by the quadruple $(\mathcal{H}_a, \sigma_a, U, A')$.

A quantum instrument $\mathcal{I}$ through, which the measurement of an observable A can be implemented, is a collection of CP trace nonincreasing maps $\{\Phi_x\}$ such that for all $x \in \Omega_A$ and $\rho \in \mathcal{H}_S$ we have

$$\mathrm{Tr}[\rho A(x)] = \mathrm{Tr}[\Phi_x(\rho)] \tag{4}$$

and

$$\sum_x \Phi_x(\rho) = \Lambda(\rho), \tag{5}$$

where Λ is a quantum channel. We call such an instrument an A-compatible instrument. If $\mathcal{I} = \{\Phi_x\}$ is an A-compatible instrument, then another instrument $\Theta \circ \mathcal{I} = \{\Theta \circ \Phi_x\}$ is also an A-compatible instrument [17], where $(\Theta \circ \Phi_x)(\rho) = \mathrm{Tr}[\Phi_x(\rho)]\Theta(\frac{\Phi_x(\rho)}{\mathrm{Tr}[\Phi_x(\rho)]})$. We denote the set of all A-compatible instruments as $\mathcal{J}_A$.

Therefore, given a measurement model $(\mathcal{H}_a, \sigma_a, U, A')$, one can associate a quantum instrument $\mathcal{I}$ such that for all $x \in \Omega_A$ and $\rho \in \mathcal{H}_S$ we have

$$\mathrm{Tr}[\Phi_x(\rho)] = \mathrm{Tr}[U(\rho \otimes \sigma_a)U^\dagger(\mathbb{I} \otimes A'(x))]. \tag{6}$$

Similarly, given a quantum instrument it is possible to find out a measurement model such that Eq. (6) holds [18]. This implies that these two concepts are equivalent.

C. Observable-channel compatibility

A quantum channel Λ is compatible with an observable A if there exists a quantum instrument $\mathcal{I} = \{\Phi_x\}$ such that Eqs. (4) and (5) together hold. Otherwise, they are incompatible. If a channel Λ and an observable A are compatible, we denote it as $\Lambda \multimap A$ [19]. We call Λ as A-compatible channel. It is well known that completely depolarizing channels are compatible with any observable [16]. For a quantum channel $\Lambda \in \mathcal{C}$ and an observable $A \in \mathcal{O}$, the following sets are introduced in Ref. [19]:

$$\tau_c(\Lambda) = \{X \in \mathcal{O} \mid \Lambda \multimap X\}; \tag{7}$$

$$\sigma_c(A) = \{\Gamma \in \mathcal{C} \mid \Gamma \multimap A\}. \tag{8}$$

Let us now write down the following theorem, which was originally proved in Ref. [17]:

Theorem 1. Suppose $A \in \mathcal{O}$ is an observable acting on the state space $\mathcal{S}(\mathcal{H})$) and $(V, \mathcal{K}, \hat{A})$ is its Naimark extension, i.e., $\mathcal{K}$ is a Hilbert space, $V : \mathcal{H} \to \mathcal{K}$ is an isometry and $\hat{A} = \{\hat{A}(x)\}$ is a PVM such that $V^\dagger \hat{A}(x) V = A(x)$ for all $x \in \Omega_A$. Then,

$$\sigma_c(A) = \{\Lambda \in \mathcal{C} \mid \Lambda \preceq \Lambda_A\}, \tag{9}$$

where for any state ρ, $\Lambda_A(\rho) = \sum_x \hat{A}(x) V \rho V^\dagger \hat{A}(x)$.

We call Λ_A as parent channel of $\sigma_c(A)$ and we also call the corresponding A-compatible instrument $\mathcal{I}_A$ a parent instrument in $\mathcal{J}_A$. Clearly, Λ_A depends on the choice of the Naimark extension. But any two parent channels are concatenation equivalent. Therefore, we have freedom to choose it.

D. Holevo bound

The Holevo bound captures the maximum classical information that can be extracted from an ensemble of quantum states [20]. Suppose we have an ensemble $\mathcal{E} = \{p_X(x), \rho_x\}$, and our task is to determine the classical index x by doing some measurements. The density matrix operator corresponding to this ensemble has the form $\rho = \sum_x p_X(x)\rho_x$. Now, we can do a measurement Λ_y so that the information gain after doing the measurement is given by the mutual information $I = I(X;Y)$ after the measurement, where Y is the random variable corresponding to the outcome of measurement. It is known that the maximum value of this mutual information is given by the Holevo bound [20,21], given by

$$\chi(\mathcal{E}) = S(\rho) - \sum_x p_X(x)S(\rho_x), \tag{10}$$

where $S(\rho)$ is the von Neumann entropy of the state ρ. It is interesting to note that the Holevo bound χ is also the mutual information of a classical-quantum state of the form $\rho_{CQ} = \sum_x p_X(x)\,|x\rangle\langle x| \otimes \rho_x$. Under the action of a channel Λ the ensemble transforms as $\mathcal{E} \to \mathcal{E}' = \{p_X(x), \rho'_x\}$. But we know that the mutual information is nonincreasing under the action of channels [21], which implies that the Holevo information is also nonincreasing under the action of quantum channels, i.e.,

$$\chi(\mathcal{E}) \geqslant \chi(\mathcal{E}'). \tag{11}$$

E. Incompatibility of physical context

In a recent work [13], the concept of IPC was introduced, which was further used to show quantum resource covariance [22]. To define this idea, we need the notion of context. A context is defined as $\mathbb{C} = \{\rho, X, Y\}$, where ρ is an arbitrary quantum state. Also, $X = \{X_i\}$ and $Y = \{Y_j\}$ are two observables, with X_i and Y_j as the respective eigenprojectors.

Other than the definition of context, we also need a game, using which we define the incompatibility of a context $\mathbb{C}$. The game goes like this. Alice prepares the quantum state ρ, and of course it has some information content, which can be quantified by using any known measure. The authors in Ref. [13] quantify the information of ρ using the following:

$$I(\rho) = \ln d - S(\rho), \tag{12}$$

where $S(\rho) = -\mathrm{Tr}(\rho \ln \rho)$ is the von Neumann entropy of ρ and d is the dimension of the Hilbert space. This information is non-negative, i.e., $I(\rho) \geqslant 0$, is ensured because $S(\rho) \leqslant \ln d$. After state preparation, Alice performs a noisy measurement with X on the prepared state, so that ρ transforms as

$$\rho \to \mathcal{N}_X(\rho) = \sum_{i=1}^{d} X_i \rho X_i. \tag{13}$$

So, after this operation the information content in the state $\mathcal{N}_X(\rho)$ is $I_1 = I(\mathcal{N}_X(\rho))$. This state $\mathcal{N}_X(\rho)$ is then delivered to Bob, who verifies the information content of the state. In case Bob finds that there is no loss of information, Alice and Bob will agree that the channel is free from information leakage.

But it might happen that there is an eavesdropper, Eve, who performs a noisy measurement Y on the state $\mathcal{N}_X(\rho)$, before it is delivered to Bob. The state is then transformed as

$$\mathcal{N}_X(\rho) \to (\mathcal{N}_Y \circ \mathcal{N}_X)(\rho) = \mathcal{N}_{YX}(\rho) = \sum_{j=1}^{d} Y_j \mathcal{N}_X(\rho) Y_j. \tag{14}$$

Thus, the information content in the state $\mathcal{N}_{XY}(\rho)$ is $I_2 = I(\mathcal{N}_{YX}(\rho))$. And therefore, the leakage in the information content is given by

$$\begin{aligned} \mathscr{I}_C &= I_1 - I_2 = I(\mathcal{N}_X(\rho)) - I(\mathcal{N}_{YX}(\rho)), \\ &= S(\mathcal{N}_{YX}(\rho)) - S(\mathcal{N}_X(\rho)). \end{aligned} \tag{15}$$

Hence, only if $\mathscr{I}_C > 0$, Alice and Bob will know that there is information leakage from the channel. Notice that $\mathscr{I}_C = 0$ in two kinds of scenarios: (i) If X and Y commute with each other and (ii) if ρ is a maximally mixed state. In the first scenario $\mathcal{N}_X(\rho) = \mathcal{N}_{YX}(\rho)$ because the two operators are compatible with each other. And in the second type of scenario, $I_1 = 0$ and there is no information to lose, which results in $I_1 = I_2$. Thus, we require the incompatibility I_C to be nonzero for Bob to detect any leakage of information.

Hence, the concept of IPC can be defined as

Definition 1. Context incompatibility is the resource encoded in a context $\mathbb{C} = \{\rho, X, Y\}$ that allows one to test the safety of a communication channel against information leakage. It is quantified as $\mathscr{I}_C = I_1 - I_2 = I(\mathcal{N}_X(\rho)) - I(\mathcal{N}_{YX}(\rho))$. It is operationally related to the amount of information lost from the system under an external measurement.

III. MAIN RESULTS

A. Limitations of incompatibility of physical context

In this section, we discuss the limitations of the approach given in Ref. [13].

(1) First of all, according to the approach given in Ref. [13], the postmeasurement state after measuring a sharp observable $X \in \mathcal{O}$ on a quantum state ρ is $\mathcal{N}_X(\rho)$. Therefore, to measure an observable X, Alice and Eve both are restricted to use a particular channel $\mathcal{N}_X \in \mathcal{C}$, or equivalently, they are restricted to use a particular quantum instrument $\mathcal{I}_X = \{\Phi_X(x)\}$ such that $\sum_x \Phi_X(x) = \mathcal{N}_X$. Since, we have no control at least over eavesdropper Eve, there is no reason to assume such a restriction.

(2) Second, to generalize it, suppose we remove such restriction, i.e., to measure an observable, now Alice and Eve can use all possible instruments that are compatible with that observable. Then to measure the observable X if Alice uses an arbitrary instrument $\mathcal{I}'_X = \{\Phi'_X(x)\}$ such that $\Lambda' = \sum_x \Phi'_X(x)$ and to measure Y, Eve uses a special instrument $\mathcal{I}_Y^{\mathrm{depo}} = \{\Phi_Y^{\mathrm{depo}}(y)\}$ such that for all $\rho \in \mathcal{S}(\mathcal{H})$ and a fixed pure state η, $\Lambda_\eta^{\mathrm{depo}}(\rho) = \sum_y \Phi_Y^{\mathrm{depo}}(y)(\rho) = \eta$ is a completely depolarizing channel. Now, as $S(\eta) = 0$, from Eq. (15) we have

$$\begin{aligned} \mathscr{I}_C &= I(\Lambda'(\rho)) - I\big((\Lambda_\eta^{\mathrm{depo}} \circ \Lambda')(\rho)\big) \\ &= -S(\Lambda'(\rho)) \\ &\leqslant 0. \end{aligned} \tag{16}$$

The negativity of IPC implies that the postmeasurement state of Eve has more information than the postmeasurement state of Alice, which does not make sense. This is because the information that Alice sends to Bob, can not be increased by the eavesdropper. Such a problem is occurring because von Neumann entropy is not monotonically nonincreasing under action of a quantum channel. Therefore, in this general context, their information measure is not a proper information measure.

(3) Third, as we know that for any POVM, the postmeasurement state depends on the quantum instrument used to implement that POVM, their results can not be generalized for POVMs without introducing quantum instruments or equivalently, without introducing measurement models.

Therefore, in our attempt to generalize the idea of IPC for POVMs, we need to modify the idea and present it in a different way, which we describe in following sections.

B. Modified measure of information leakage

In this section we present a generalization of the game presented in Sec. II E. Now, in the game, after the state preparation of ρ, instead of only doing a sharp measurement we allow Alice to perform a more generic measurement. Now, Alice performs her measurement with the POVM measurement A on the quantum state $\rho \in \mathcal{S}(\mathcal{H})$ using the A-compatible instrument $\mathcal{I}'_A = \{\Phi_{A,x}\}$ such that $\Lambda'_A = \sum_x \Phi_{A,x}$ and generates the ensemble $\mathcal{E}_A = \{p_x, \rho_x\}$, where $p_x = \mathrm{Tr}[\Phi_{A,x}(\rho)]$ and $\rho_x = \frac{\Phi_{A,x}(\rho)}{\mathrm{Tr}[\Phi_{A,x}(\rho)]}$. Here, Λ'_A is the quantum channel such that $\Lambda'_A : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$. Furthermore, we quantify the information content of the ensemble $\mathcal{E}_A$ via the Holevo bound as:

$$\chi(\rho, \mathcal{I}'_A) = S(\Lambda'_A(\rho)) - \sum_x p_x S(\rho_x).$$

This measure of information has been previously used to quantify information gain in Ref. [23]. Similarly, the eavesdropper Eve performs the POVM measurement B on the quantum state $\Lambda'_A(\rho) \in \mathcal{S}(\mathcal{K})$ using the B-compatible instrument $\mathcal{I}'_B = \{\Phi_{B,y}\}$ such that $\Lambda'_B = \sum_y \Phi_{B,y}$ and generates the ensemble $\mathcal{E}_B = \{p_x, \Lambda'_B(\rho_x)\}$. Here, Λ'_B is the quantum channel such that $\Lambda'_B : \mathcal{S}(\mathcal{K}) \to \mathcal{S}(\mathcal{K}')$. It should be noted that Alice and Bob do not have access to Eve's measurement outcomes, her measurement can be represented using a channel. Now, the information remaining in the state $(\Lambda'_B \circ \Lambda'_A)(\rho)$ is given by its Holevo bound, i.e.,

$$\chi(\rho, \mathcal{I}'_A, \mathcal{I}'_B) = S((\Lambda'_B \circ \Lambda'_A)(\rho)) - \sum_x p_x S(\Lambda'_B(\rho_x)).$$

Therefore, Bob, who was expecting to receive an ensemble with information $\chi(\rho, \mathcal{I}'_A)$, would receive a different ensemble with information content $\chi(\rho, \mathcal{I}'_A, \mathcal{I}'_B)$. Thus, the new form of information leakage of the channel is

$$\begin{aligned} I_c^H(\rho, \mathcal{I}'_A, \mathcal{I}'_B) &= \chi(\rho, \mathcal{I}'_A) - \chi(\rho, \mathcal{I}'_A, \mathcal{I}'_B) \\ &= S(\Lambda'_A(\rho)) - S((\Lambda'_B \circ \Lambda'_A)(\rho)) \\ &\quad + \sum_x p_x S(\Lambda'_B(\rho_x)) - \sum_x p_x S(\rho_x). \end{aligned} \tag{17}$$

As Holevo bound is monotonically nonincreasing under the action of quantum channels, $I_c^H(\rho, \mathcal{I}'_A, \mathcal{I}'_B) \geqslant 0$. When $I_c^H(\rho, \mathcal{I}'_A, \mathcal{I}'_B) > 0$, Alice and Bob will be able to detect the information leakage in the channel.

Now, if Eve is rational, her goal will be to minimize leakage along with collecting information. Therefore, to measure B, she will choose an instrument such that $\mathcal{I}_c^H(\rho, \mathcal{I}'_A, \mathcal{I}'_B)$ takes the minimum value. Now, let Λ_B be a parent channel in $\sigma_c(B)$ and corresponding B-compatible instrument be $\mathcal{I}_B$. Then, as for any other channel $\Lambda'_B \in \sigma_B$, $\Lambda'_B \preceq \Lambda_B$ holds and Holevo bound is monotonically decreasing under action of a quantum channel,

$$\chi(\rho, \mathcal{I}'_A, \mathcal{I}'_B) \leqslant \chi(\rho, \mathcal{I}'_A, \mathcal{I}_B)\ \forall \mathcal{I}_B. \tag{18}$$

Therefore, implementation of a parent instrument keeps maximum amount of accessible information or equivalently, maximum Holevo bound. Therefore, for a given instrument of Alice the minimum leakage of information is

$$\begin{aligned} I_c^H(\rho, \mathcal{I}'_A, B) &= \min_{\mathcal{I}'_B} I_c^H(\rho, \mathcal{I}'_A, \mathcal{I}'_B) \\ &= \chi(\rho, \mathcal{I}'_A) - \max_{\mathcal{I}'_B} \chi(\rho, \mathcal{I}'_A, \mathcal{I}'_B) \\ &= \chi(\rho, \mathcal{I}'_A) - \chi(\rho, \mathcal{I}'_A, \mathcal{I}_B) \\ &= I_c^H(\rho, \mathcal{I}'_A, \mathcal{I}_B). \end{aligned} \tag{19}$$

Note that the choice of B depends on output state space $\mathcal{S}(\mathcal{K})$ of the quantum channel Λ'_A and in that sense, it is arbitrary.

Now, if Alice is also rational and she does not know the presence of Eve, she will try to create an ensemble with most accessible information such that the receiver, i.e., Bob can get the best amount of information, or equivalently, she will use an A-compatible instrument for which $\chi(\rho, \mathcal{I}'_A)$ is maximum. Let Λ_A be a parent channel in $\sigma_c(A)$ and corresponding A-compatible parent instrument be $\mathcal{I}_A$. Then, using arguments as above

$$\chi(\rho, \mathcal{I}'_A) \leqslant \chi(\rho, \mathcal{I}_A)\ \forall \mathcal{I}'_A. \tag{20}$$

Therefore, if Alice uses the instrument $\mathcal{I}_A$, in this case the information leakage will be minimum when Alice uses a parent channel from $\sigma_c(A)$, and is given by:

$$I_c^H(\rho, A, B) = I_c^H(\rho, \mathcal{I}_A, \mathcal{I}_B). \tag{21}$$

Clearly, if Eve uses any other quantum instrument (e.g., dimension preserving instrument) $\mathcal{I}'_B$, then $I_c^H(\rho, \mathcal{I}_A, \mathcal{I}'_B) \geqslant I_c^H(\rho, A, B)$. Therefore, assuming both Alice and Eve to be rational, $I_c^H(\rho, A, B)$ is the appropriate amount of information leak when the parent instruments are used.

C. Incompatibility of physical context: A modified version

First of all we modify the notion of context so that, $\mathbb{C} = \{\rho, \mathbb{X}, \mathbb{Y}\}$, where $\mathbb{X}$ and $\mathbb{Y}$ are POVM measurements acting on $\mathcal{S}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H}')$, respectively. Since, $\mathbb{X}$ and $\mathbb{Y}$ are given, to define IPC, we restrict Alice's instrument $\mathcal{I}'^{,\mathcal{H}'}_{\mathbb{X}} = \{\Phi'^{,\mathcal{H}'}_{\mathbb{X},x}\}$ such that $\Lambda'_{\mathbb{X}} = \sum_x \Phi'^{,\mathcal{H}'}_{\mathbb{X},x}$ and $\Lambda'_{\mathbb{X}} : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}')$. We denote the set of all such $\mathbb{X}$-compatible instruments as $\mathcal{J}^{\mathcal{H}'}_{\mathbb{X}}$. With this restriction also, being rational, Alice's goal will be to maximize $\chi(\rho, \mathcal{I}'^{,\mathcal{H}'}_{\mathbb{X}})$. Let, for some $\mathcal{I}^{\mathcal{H}'}_{\mathbb{X},\max} \in \mathcal{J}^{\mathcal{H}'}_{\mathbb{X}}$,

$$\max_{\mathcal{I}^{\mathcal{H}'}_{\mathbb{X}}} \chi\big(\rho, \mathcal{I}^{\mathcal{H}'}_{\mathbb{X}}\big) = \chi\big(\rho, \mathcal{I}^{\mathcal{H}'}_{\mathbb{X},\max}\big). \tag{22}$$

Therefore, similar to Sec. III B, in this case the appropriate amount of information leak is

$$\mathfrak{I}(\mathbb{C}) = I_c^H\big(\rho, \mathcal{I}_{\mathbb{X},\max}^{\mathcal{H}'}, \mathcal{I}_{\mathbb{Y}}\big). \tag{23}$$

For the special case of, $\mathcal{H}' = \mathcal{H}$, we have

$$\mathfrak{I}(\mathbb{C}) = I_c^H\big(\rho, \mathcal{I}_{\mathbb{X},\max}^{\mathcal{H}}, \mathcal{I}_{\mathbb{Y}}\big). \tag{24}$$

Therefore, we can define the generalized version of IPC as:

Definition 2. Context incompatibility is the resource encoded in a context $\mathbb{C} = \{\rho, \mathbb{X}, \mathbb{Y}\}$ that allows one to test the safety of the channel against information leakage. This resource is quantified via $\mathfrak{I}(\mathbb{C}) = I_c^H(\rho, \mathcal{I}_{\mathbb{X},\max}^{\mathcal{H}}, \mathcal{I}_{\mathbb{Y}})$, where $\mathcal{I}_{\mathbb{X},\max}^{\mathcal{H}}$ is the $\mathbb{X}$-compatible instrument that maximizes $\chi(\rho, \mathcal{I}_{\mathbb{X}}^{\mathcal{H}})$. Operationally, it is the proper information leakage in the channel caused by an external measurement on the state.

Clearly, if Eve uses any other quantum instrument (e.g., dimension preserving instrument) $\mathcal{I}'_{\mathbb{Y}}$, then $I_c^H(\rho, \mathcal{I}_{\mathbb{X},\max}^{\mathcal{H}}, \mathcal{I}'_{\mathbb{Y}}) \geqslant \mathfrak{I}(\mathbb{C})$. Moreover, if Alice performs a sharp measurement $X = \{X_i\}$, from Theorem 1, choosing $V = \mathbb{I}$ or equivalently choosing $\mathcal{H} = \mathcal{K}$ and $X_i = \hat{X}_i$ we get a parent channel $\Lambda_A = \mathcal{N}(X) : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$. Let $\mathcal{I}_X = \{\Phi_X\}$ be a corresponding X-compatible parent instrument. As, implementation of a parent channel keeps maximum amount of accessible information or, equivalently maximum Holevo bound, we have $\mathcal{I}_{\mathbb{X},\max}^{\mathcal{H}} = \mathcal{I}_X$. Then the proper information leakage will have the following form:

$$\begin{aligned}\mathfrak{I}(\mathbb{C}) &= \chi(\rho, \mathcal{I}_X) - \chi(\rho, \mathcal{I}_X, \mathcal{I}_{\mathbb{Y}}),\\ &= S(\mathcal{N}_X(\rho)) - S((\Lambda_{\mathbb{Y}} \circ \mathcal{N}_X)(\rho))\\ &\quad + \sum_x p_x S(\Lambda_{\mathbb{Y}}(\rho_x)) - \sum_x p_x S(\rho_x),\end{aligned} \tag{25}$$

where $\Lambda_{\mathbb{Y}}$ is the $\mathbb{Y}$-compatible parent channel corresponding to the $\mathbb{Y}$-compatible parent instrument $\mathcal{I}_{\mathbb{Y}}$.

D. Relation between two definitions

Our generalization of the measure of IPC, gives a simplified form when we demand that both Alice and Eve perform rank-one sharp measurements X and Y using parent instruments $\mathcal{I}_X \in \mathcal{J}_X$ and $\mathcal{I}_Y \in \mathcal{J}_Y$, where $\mathcal{N}_X \in \sigma_c(X)$ and $\mathcal{N}_Y \in \sigma_c(Y)$ are the corresponding channels respectively. In this case $\mathfrak{I}(\mathbb{C})$ reads as

$$\mathfrak{I}(\mathbb{C}) = \sum_x p_x S(\mathcal{N}_Y(\rho_x)) - \mathscr{I}_C. \tag{26}$$

The above equation relates our generalized measure of IPC with the measure of IPC $\mathscr{I}_C$ defined in Ref. [13]. To compare the two measures of the IPC, we remind the reader that $\mathscr{I}_C$ is zero when (i) X and Y commute or (ii) ρ is a maximally mixed state (see Sec. II E). Coming to the new measure of IPC we find that $\mathfrak{I}(\mathbb{C}) = 0$ whenever X and Y commute, because then $\mathcal{N}_Y(\rho_x)$ are pure states. However, $\mathfrak{I}(\mathbb{C})$ is not necessarily equal to zero when ρ is a maximally mixed state [as in Eq. (26), $\mathscr{I}_C$ is zero but $S(\mathcal{N}_Y(\rho_x))$'s are not zero].

This implies that our measure captures the incompatibility of a context even when the state (belonging to the context) is a maximally mixed state. This is unlike the previous measure of IPC $\mathscr{I}_C$ given in Ref. [13], which says that the context is compatible if the state is a maximally mixed state. This difference arises from the fact that the Holevo quantity [unlike the information measure in Eq. (15)], which represents the extractable information, can be nonzero for an ensemble created from measurement on a maximally mixed state. We show the importance of the new IPC measure through the following example.

Example 1. Consider a scenario in which Alice is randomly implementing σ_x and σ_z measurements on the single-qubit maximally mixed state with equal probabilities and generates ensemble $\{\{\frac{1}{2}, |0\rangle\langle 0|\}, \{\frac{1}{2}, |1\rangle\langle 1|\}\}$ and $\{\{\frac{1}{2}, |+\rangle\langle +|\}, \{\frac{1}{2}, |-\rangle\langle -|\}\}$, respectively, for Bob. This is a QKD-like situation. Now, the possible bases of measurements are known for eavesdropper Eve. But she does not know which measurement is exactly implemented in a particular run. Therefore, she is randomly measuring σ_x and σ_z on the ensemble created by Alice. In this case, if we use the measure of IPC from Eq. (15), we get the following as the average IPC:

$$\begin{aligned}\mathscr{I}_{\text{avg}} &= \frac{1}{4}\mathscr{I}\left(\frac{\mathbb{I}}{2}, \sigma_z, \sigma_z\right) + \frac{1}{4}\mathscr{I}\left(\frac{\mathbb{I}}{2}, \sigma_z, \sigma_x\right)\\ &\quad + \frac{1}{4}\mathscr{I}\left(\frac{\mathbb{I}}{2}, \sigma_x, \sigma_z\right) + \frac{1}{4}\mathscr{I}\left(\frac{\mathbb{I}}{2}, \sigma_x, \sigma_x\right)\\ &= 0.\end{aligned} \tag{27}$$

Therefore, according to this analysis, the information leakage is not detectable. But it is a well-established fact that if Alice and Bob declare the basis of their measurements Eve will be detected since her operation disturbs the ensemble. Therefore, this measure of IPC is not very useful here. Instead, if we use the modified measure of IPC, we get

$$\begin{aligned}\mathfrak{I}_{\text{avg}} &= \frac{1}{4}\mathfrak{I}\left(\frac{\mathbb{I}}{2}, \sigma_z, \sigma_z\right) + \frac{1}{4}\mathfrak{I}\left(\frac{\mathbb{I}}{2}, \sigma_z, \sigma_x\right)\\ &\quad + \frac{1}{4}\mathfrak{I}\left(\frac{\mathbb{I}}{2}, \sigma_x, \sigma_z\right) + \frac{1}{4}\mathfrak{I}\left(\frac{\mathbb{I}}{2}, \sigma_x, \sigma_x\right)\\ &= \frac{1}{4}\mathfrak{I}\left(\frac{\mathbb{I}}{2}, \sigma_z, \sigma_x\right) + \frac{1}{4}\mathfrak{I}\left(\frac{\mathbb{I}}{2}, \sigma_x, \sigma_z\right)\\ &= \frac{1}{2}\ln 2\\ &\neq 0,\end{aligned} \tag{28}$$

where we have used Eq. (26) to arrived at the last line. This nonzero value suggests that information leakage can be detected, as expected. Hence, the modified IPC measure is useful in this scenario.

In this example we have considered that Eve is using a parent instrument for her measurement. If she uses any instrument other than the parent instrument the average information leakage will be higher than $\mathfrak{I}_{\text{avg}}$.

IV. INCOMPATIBILITY OF PHYSICAL CONTEXT IN THE PRESENCE OF MEMORY

Motivated by the work in Ref. [24], where it was shown that in the presence of memory the total uncertainty of two measurements gets reduced, we ask the question: How will the IPC change in the presence of memory? To accommodate the presence of memory, we modify our game slightly, for the scenario where we perform only rank-one projective measurements X and Y.

In the modified game, our initial state σ_{in} is the subsystem of the bipartite state $\sigma_{\text{in},M}$, where M acts as the memory. After the X measurement on the subsystem state σ_{in}, Alice produces the bipartite ensemble $\rho_{AM} = \sum_x p_x \rho_{AM}^x$, where $\rho_M^x = \text{Tr}_A[\rho_{AM}^x]$ acts as the memory and Bob receives the subsystem A prepared in the state $\rho_A = \text{Tr}_M[\rho_{AM}]$. On this ensemble, if we use the approach in Ref. [13], the information content of ρ_A conditioned on memory ρ_M is given by

$$I_1^{\text{mem}} = \ln d - S(A|M) = \ln d - S(\rho_{AM}) + S(\rho_M),$$

where $S(A|M) = S(\rho_{AM}) - S(\rho_M)$ is the conditional entropy [21]. After the Y measurement by Eve on ρ_A, the ensemble transforms as $\sum_x p_x \rho_{AM}^x \rightarrow \sum_x p_x (\mathcal{N}_Y \otimes \mathbb{I})(\rho_{AM}^x) = \sum_x p_x \rho_{A'M}^x$, so that the remaining information content of the state $\rho_{A'}$ is

$$I_2^{\text{mem}} = \ln d - S(A'|M) = \ln d - S(\rho_{A'M}) + S(\rho_M),$$

where $\mathbb{I}$ is the identity channel acting on the memory. Therefore, in the presence of memory, the expression of IPC takes the following form:

$$\begin{aligned} \mathscr{I}_C^{\text{mem}} &= I_1^{\text{mem}} - I_2^{\text{mem}} \\ &= S(\rho_{A'M}) - S(\rho_{AM}). \end{aligned} \tag{29}$$

To compare the IPC with and without memory, we compare Eq. (15) with Eq. (29), which gives the following:

$$\begin{aligned} \mathscr{I}_C - \mathscr{I}_C^{\text{mem}} &= [S(\rho_{A'}) - S(\rho_{A'M})] - [S(\rho_A) - S(\rho_{AM})] \\ &= I^{\text{coh}}(M\rangle A') - I^{\text{coh}}(M\rangle A) \leqslant 0. \end{aligned} \tag{30}$$

Here, $I^{\text{coh}}(M\rangle A) = S(\rho_A) - S(\rho_{AM})$ is the coherent information that is nonincreasing under the action of quantum channels [21,25,26]. This analysis tells us that the IPC is increasing in the presence of memory, which seems contrary to the intuition that memory reduces the incompatibility.

Next, we compute the IPC in the modified game with our approach. In our case, after the X measurement, the extractable classical information from ρ_A is the mutual information of the quantum-classical ensemble $\rho_{CA} = \sum_x |x\rangle_C \langle x| \otimes \rho_A^x$ (see Sec. II D). However, now it is conditioned on the memory ρ_M. Therefore, in the presence of memory the extractable information will be the mutual information between $\rho_C = \sum_x |x\rangle_C \langle x|$ and ρ_A, conditioned on the memory ρ_M via the tripartite classical-quantum state $\rho_{CAM} = \sum_x p_x |x\rangle_C \langle x| \otimes \rho_{AM}^x$, i.e.,

$$\begin{aligned} \mathcal{X}_1^{\text{mem}} &= S(A:C|M) \\ &= S(A|M) + S(C|M) - S(AC|M) \\ &= S(\rho_{AM}) - S(\rho_M) + S(\rho_{CM}) - S(\rho_{CAM}). \end{aligned}$$

Here, we have simply expanded the conditional entropies to get the final form. Also, after Eve performs her measurement Y on the subsystem ρ_A, the remaining mutual information between $\rho_{A'}$ and ρ_C conditioned on the memory ρ_M, via the classical-quantum ensemble $\sum_x p_x |x\rangle_C \langle x| \otimes \rho_{A'M}^x$ is given by

$$\begin{aligned} \mathcal{X}_2^{\text{mem}} &= S(A':C|M) \\ &= S(A'|M) + S(C|M) - S(A'C|M) \\ &= S(\rho_{A'M}) - S(\rho_M) + S(\rho_{CM}) - S(\rho_{CA'M}). \end{aligned}$$

Therefore the IPC, using our approach in presence of memory, takes the following form:

$$\begin{aligned} \mathfrak{I}^{\text{mem}}(\mathbb{C}) &= \mathcal{X}_1^{\text{mem}} - \mathcal{X}_2^{\text{mem}} \\ &= S(\rho_{AM}) - S(\rho_{A'M}) - S(\rho_{ACM}) + S(\rho_{A'CM}) \\ &= S(\rho_{AM}) - S(\rho_{A'M}) - \sum_x S(\rho_{AM}^x) + \sum_x S(\rho_{A'M}^x) \\ &= S(\rho_{AM}) - S(\rho_{A'M}) + \sum_x S(\rho_{A'}^x). \end{aligned} \tag{31}$$

In the above calculations we have used the fact that ρ_A^x are pure states so that ρ_{AM}^x and $\rho_{A'M}^x$ are bipartite product states. Now, if we compare the IPC without and with memory in from Eq. (26) and Eq. (31), respectively, we have

$$\begin{aligned} &\mathfrak{I}(\mathbb{C}) - \mathfrak{I}^{\text{mem}}(\mathbb{C}) \\ &\quad = [S(\rho_A) - S(\rho_{AM})] - [S(\rho_{A'}) - S(\rho_{A'M})] \\ &\quad = I^{\text{coh}}(M\rangle A) - I^{\text{coh}}(M\rangle A') \geqslant 0. \end{aligned} \tag{32}$$

Thus, we find that using our approach, the IPC is nonincreasing in the presence of memory. It follows the intuition that the presence of memory should reduce the incompatibility, as the memory can be utilized to recover the lost information. On comparing Eq. (30) with Eq. (32), we find that $\mathscr{I}_C - \mathscr{I}_C^{\text{mem}} = -[\mathfrak{I}(\mathbb{C}) - \mathfrak{I}^{\text{mem}}(\mathbb{C})]$. This relation strongly indicates that the information leakage content $\mathscr{I}_C$ envisaged in Ref. [13], is not capable of fully capturing the problems we face in a typical quantum information processing scenarios. This analysis also validates our approach for quantifying the IPC.

Example 2 (Comparison of incompatibilities of a physical context with two different memories). Suppose $\sigma_{\text{in}} = \alpha |\lambda_1\rangle\langle\lambda_1| + \beta |\lambda_2\rangle\langle\lambda_2|$ is a qubit state and $S_x = \{|+\rangle\langle+|, |-\rangle\langle-|\}$ and $S_z = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ are the sharp spin measurements along x and z directions, respectively, where $\{|\lambda_1\rangle, |\lambda_2\rangle\}$ is the eigenbasis of σ_{in}. Here $0 \leqslant \alpha, \beta \leqslant 1$ and $\alpha + \beta = 1$. Now, we take our physical context as $\mathbb{C}_1 = (\sigma_{\text{in}}, S_z, S_x)$. We will consider the following case where Alice is using memories M keeping input state σ_{in} fixed.

Suppose Alice is using a qubit memory M such that $\sigma_{\text{in},M} = p|\psi_{\text{in},M}\rangle\langle\psi_{\text{in},M}| + \frac{1-p}{4}\mathbb{I}_{\text{in}}$, where $0 \leqslant p \leqslant 1$, $|\psi\rangle_{\text{in},M} = \sqrt{\alpha'}|\lambda_1\rangle|\lambda_1'\rangle + \sqrt{\beta'}|\lambda_2\rangle|\lambda_2'\rangle$, $\mathbb{I}_{AM} = \mathbb{I}_{4\times 4}$, $0 \leqslant \alpha', \beta' \leqslant 1$, $\alpha' + \beta' = 1$, $\{|\lambda_1\rangle', |\lambda_2\rangle'\}$ is the eigenbasis of σ_M and $\sigma_M = \text{Tr}_{\text{in}}[\sigma_{\text{in},M}]$. Alice chooses α', β' and p such that

$$\alpha = p\alpha' + \frac{1-p}{2} \tag{33}$$

$$\beta = p\beta' + \frac{1-p}{2} \tag{34}$$

hold. Then, $\text{Tr}_M[\sigma_{\text{in},M}] = \sigma_{\text{in}}$. For example, when $\alpha = \frac{1}{4}$ and $\beta = \frac{3}{4}$, one possible choice is $p = \frac{3}{4}$, $\alpha' = \frac{1}{6}$ and $\beta' = \frac{5}{6}$. The state of the memory is $\sigma_M = \text{Tr}_{\text{in}}(\sigma_{\text{in},M}) = \alpha|\lambda_1'\rangle\langle\lambda_1'| + \beta|\lambda_2'\rangle\langle\lambda_2'|$. Let, $q_{xy} = \langle x|\lambda_y\rangle$ where $x \in \{0, 1, +, -\}$ and $y \in \{1, 2\}$. The bipartite ensemble, created by the S_z measurement of Alice, is $\{p_i', \sigma_{AM}^i\}$ where, $p_i' = \text{Tr}[(|i\rangle\langle i| \otimes \mathbb{I})\sigma_{\text{in},M}] = p[\alpha' \mid q_{i1} \mid^2 + \beta' \mid q_{i2} \mid^2] + \frac{1-p}{2}$

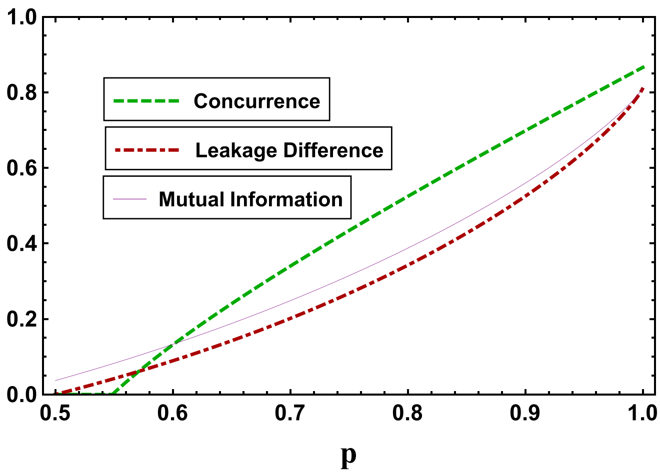

FIG. 1. Plot of concurrence and mutual information of $\sigma_{\text{in},M}$ and the leakage difference vs the parameter p. It can be seen that concurrence and mutual information of $\sigma_{\text{in},M}$ and the leakage difference is monotonically increasing with respect to the parameter p. All quantities are normalized i.e., all of them have been divided by their maximum values.

and $\sigma^i_{AM} = \frac{(|i\rangle\langle i|\otimes\mathbb{I})\sigma_{\text{in},M}(|i\rangle\langle i|\otimes\mathbb{I})}{\text{Tr}[(|i\rangle\langle i|\otimes\mathbb{I})\sigma_{\text{in},M}]}$ and $i \in \{0, 1\}$. Now it can be easily checked that $\sigma^i_{AM} = |i\rangle\langle i| \otimes [p\,|\phi'_i\rangle\langle\phi'_i| + \frac{1-p}{2p'_i}\frac{\mathbb{I}}{2}]$ where $|\phi_i\rangle = \frac{1}{\sqrt{p_i}}(\sqrt{\alpha'}q_{i1}\,|\lambda_1\rangle + \sqrt{\beta'}q_{i2}\,|\lambda_2\rangle)$. The postmeasurement average bipartite state is $\sigma_{AM} = \sum_i p'_i\sigma^i_{AM}$. Clearly, $\sigma_A = \text{Tr}_M\sigma_{AM} = p\sum_i p'_i\,|i\rangle\langle i| + (1-p)\frac{\mathbb{I}}{2}$. After, Eve's S_x measurement on A part, the average bipartite state will become $\sigma_{A'M} = \frac{\mathbb{I}}{2}\otimes\sigma_M$ where $\sigma_M = [p\sum_i p_i\,|\phi'_i\rangle\langle\phi'_i| + (1-p)\frac{\mathbb{I}}{2}] = \sigma_M$ and the average state of A part becomes $\sigma_{A'} = \frac{\mathbb{I}}{2}$. So, the reduction in information leak is given as

$$\begin{aligned}\mathfrak{I}(\mathbb{C}_1) - \mathfrak{I}^M(\mathbb{C}_1) &= [S(\sigma_A) - S(\sigma_{AM})] - [S(\sigma'_A) - S(\sigma_{A'M})]\\ &= [S(\sigma_A) - S(\sigma_{AM})] - [S(\sigma'_A) - S(\sigma_{A'}) - S(\sigma_M)]\\ &= S(\sigma_M) + S(\sigma_A) - S(\sigma_{AM}) = I(A:M)_{\sigma_{AM}}. \qquad (35)\end{aligned}$$

Now, consider a special case where $|\lambda_1\rangle, |\lambda_2\rangle$ are the eigenbasis of σ_y, $\alpha = \frac{1}{4}$ and $\beta = \frac{3}{4}$. In this case, $|q_{ij}|^2 = \frac{1}{2}$ $\forall i \in \{0, 1\}$ and $\forall j \in \{1, 2\}$. Also, from Eq. (33) we get $\alpha' = \frac{2p-1}{4p}$. Clearly, $\alpha' \geqslant 0$ only for $p \geqslant \frac{1}{2}$. We plot the leakage difference $\mathfrak{I}(\mathbb{C}_1) - \mathfrak{I}^M(\mathbb{C}_1)$ with respect to p in Fig. 1. To quantify the amount of memory we use the concurrence measure [27] and the mutual information of the initial bipartite state $\sigma_{\text{in},M}$. From Fig. 1 we get that with increment of p, concurrence and mutual information of $\sigma_{\text{in},M}$ and the leakage difference, are monotonically increasing with p. We can also say that the information leakage difference is a monotonically increasing function of both concurrence and mutual information in the state $\sigma_{\text{in},M}$. Equivalently, we can say that the leakage with memory is monotonically decreasing with increasing value concurrence and mutual information. It can be observed from Fig. 1, the leakage difference is nonzero for the region $p \lessapprox 0.548$ where the concurrence is vanishing. In this region the nonzero leakage difference can be attributed to the nonvanishing mutual information.

Example 2 suggests us to write down the following conjecture:

Conjecture 1. With increment of correlation between the memory and the input state, information leakage monotonically decreases.

Therefore, we conclude based on the validity of the conjecture, that the presence of more memory correlation helps in reducing the leakage.

V. CONCLUSION

In this work, we have derived the measure of an appropriate information leakage in all QKD-like games. Moreover, introducing quantum instruments, we have generalized the notion of IPC for POVMs. We have shown the relation between previous and our approaches for sharp measurements. Our approach always leads to a non-negative measure of IPC. We have also shown that the modified IPC measure is more useful compared to the earlier IPC measure in Eq. (15), in a QKD-like scenario as an example. Also, on including memory, our measure of IPC can never increase. In fact, in Example 2, we have shown that information leakage monotonically decreases with increment of correlation between input state and memory. Thus, we have successfully modified the notion of IPC for generic measurements.

Our work opens up several future directions. First, it would be useful to construct the resource theory of IPC using our measure. Further, our measure can be a useful tool for generic information-theoretic tasks, which involve transmission of classical information over quantum channels. We would like to explore how our generalized version of IPC can be related to incompatibility of POVMs.

[1] T. Heinosaari, T. Miyadera, and M. Ziman, An invitation to quantum incompatibility, J. Phys. A: Math. Theor. **49**, 123001 (2016).
[2] M. T. Quintino, T. Vértesi, and N. Brunner, Joint Measurability, Einstein-Podolsky-Rosen Steering, and Bell Nonlocality, Phys. Rev. Lett. **113**, 160402 (2014).
[3] N. Stevens and P. Busch, Steering, incompatibility, and bell-inequality violations in a class of probabilistic theories, Phys. Rev. A **89**, 022123 (2014).
[4] W. Son, E. Andersson, S. M. Barnett, and M. S. Kim, Joint measurements and bell inequalities, Phys. Rev. A **72**, 052116 (2005).
[5] R. Uola, C. Budroni, O. Gühne, and J.-P. Pellonpää, One-To-One Mapping Between Steering and Joint Measurability Problems, Phys. Rev. Lett. **115**, 230402 (2015).
[6] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-Level Systems, Phys. Rev. Lett. **88**, 127902 (2002).

[7] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. (NY) **191**, 363 (1989).

[8] A. Mitra, S. Ghosh, and P. Mandayam, Characterizing incompatibility of quantum measurements via their Naimark extensions, arXiv:2011.11364.

[9] C. Heunen, T. Fritz, and M. L. Reyes, Quantum theory realizes all joint measurability graphs, Phys. Rev. A **89**, 032121 (2014).

[10] R. Beneduci, Joint measurability through Naimark's dilation theorem, Rep. Math. Phys. **79**, 197 (2017).

[11] T. Heinosaari, Simultaneous measurement of two quantum observables: Compatibility, broadcasting, and in-between, Phys. Rev. A **93**, 042118 (2016).

[12] A. Mitra, Layers of classicality in the compatibility of measurements, Phys. Rev. A **104**, 022206 (2021).

[13] E. Martins, M. F. Savi, and R. M. Angelo, Quantum incompatibility of a physical context, Phys. Rev. A **102**, 050201(R) (2020).

[14] In earlier works, QKD games and measurement disturbance relations have been studied mostly using Ludër's instruments (or measurements), while our treatment in this work is valid for general quantum instruments [28–34].

[15] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement* (Springer, Berlin, 1991).

[16] T. Heinosaari, D. Reitzner, T. Rybár, and M. Ziman, Incompatibility of unbiased qubit observables and pauli channels, Phys. Rev. A **97**, 022112 (2018).

[17] T. Heinosaari and T. Miyadera, Qualitative noise-disturbance relation for quantum measurements, Phys. Rev. A **88**, 042117 (2013).

[18] M. Ozawa, Quantum measuring processes of continuous observables, J. Math. Phys. **25**, 79 (1984).

[19] C. Carmeli, T. Heinosaari, T. Miyadera, and A. Toigo, Noise-disturbance relation and the galois connection of quantum measurements, Found. Phys. **49**, 492 (2019).

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).

[21] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013).

[22] M. F. Savi and R. M. Angelo, Quantum resource covariance, Phys. Rev. A **103**, 022220 (2021).

[23] Z. Xi, Information gain and information leak in quantum measurements, Phys. Rev. A **93**, 052308 (2016).

[24] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).

[25] B. Schumacher and M. A. Nielsen, Quantum data processing and error correction, Phys. Rev. A **54**, 2629 (1996).

[26] B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channels, Phys. Rev. A **56**, 131 (1997).

[27] S. Hill and W. K. Wootters, Entanglement of a Pair of Quantum Bits, Phys. Rev. Lett. **78**, 5022 (1997).

[28] P. Bej, A. Ghosal, D. Das, A. Roy, and S. Bandyopadhyay, Information-disturbance trade-off in generalized entanglement swapping, Phys. Rev. A **102**, 052416 (2020).

[29] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy, Phys. Rev. A **56**, 1163 (1997).

[30] L. Knips, J. Dziewior, A.-L. K. Hashagen, J. D. A. Meinecke, H. Weinfurter, and M. M. Wolf, arXiv:1808.07882.

[31] L. Maccone, Information-disturbance tradeoff in quantum measurements, Phys. Rev. A **73**, 042307 (2006).

[32] P. Mandayam and M. D. Srinivas, Disturbance trade-off principle for quantum measurements, Phys. Rev. A **90**, 062128 (2014).

[33] L. Seveso and M. G. A. Paris, Trade-off between information and disturbance in qubit thermometry, Phys. Rev. A **97**, 032129 (2018).

[34] J. Zhang, Y. Zhang, and C.-S. Yu, The measurement-disturbance relation and the disturbance trade-off relation in terms of relative entropy, Int. J. Theor. Phys. **55**, 3943 (2016).