Joint measurability, steering, and entropic uncertainty

H. S. Karthik,[1,*] A. R. Usha Devi,[2,3,†] and A. K. Rajagopal[3,4,5,‡]
[1]*Raman Research Institute, Bangalore 560 080, India*
[2]*Department of Physics, Bangalore University, Bangalore-560 056, India*
[3]*Inspire Institute Inc., Alexandria, Virginia, 22303, USA*
[4]*Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai, 600113, India*
[5]*Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India*

(Received 10 October 2014; published 22 January 2015)

There has been a surge of research activity recently on the role of joint measurability of unsharp observables in nonlocal features, *viz*., violation of Bell inequality and EPR steering. Here, we investigate the entropic uncertainty relation for a pair of noncommuting observables (of Alice's system) when an entangled quantum memory of Bob is restricted to record outcomes of jointly measurable positive operator valued measures. We show that with this imposed constraint of joint measurability at Bob's end, the entropic uncertainties associated with Alice's measurement outcomes—conditioned by the results registered at Bob's end—obey an entropic steering inequality. Thus, Bob's nonsteerability is intrinsically linked to his inability to predict the outcomes of Alice's pair of noncommuting observables with better precision, even when they share an entangled state. As a further consequence, we prove that in the joint measurability regime, the quantum advantage envisaged for the construction of security proofs in quantum key distribution is lost.

DOI: 10.1103/PhysRevA.91.012115 PACS number(s): 03.65.Ta, 03.65.Ca

I. INTRODUCTION

In the classical domain physical observables commute with each other and they can all be jointly measured. In contrast, measurements of observables, which do not commute, are usually declared to be incompatible in the quantum scenario. However, the notion of *compatibility* of measurements is captured entirely by *commutativity* of the observables if one is restricted to sharp projective valued (PV) measurements. In an extended framework, which includes measurements of unsharp generalized observables, comprised of positive operator valued measures (POVMs), the concept of *joint measurability* gets delinked from that of commutativity [1–10]. Though noncommuting observables do not admit simultaneous sharp values through their corresponding PV measurements, it is possible to assign unsharp values jointly to compatible positive operator valued (POV) observables. Active research efforts are dedicated [1,3–5,7,12–15] to exploring clear, operationally significant criteria of joint measurability for two or more POVMs and also to determining whether incompatible measurements, which cannot be implemented jointly, are necessary to bring out nonclassical features. In this context, it is recognized [1,3–5,7,12,14,15] that if one is confined to local compatible POVMs on parts of an entangled quantum system, it is not possible to witness nonlocal quantum features such as steering (the ability to nonlocally alter the states of one part of a composite system by performing measurements on another spatially separated part [16]) and violation of Bell inequality. More specifically, incompatible measurements are instrumental in revealing violations of various no-go theorems in the quantum world.

In this work, we investigate the entropic uncertainty relation associated with Alice's measurements of a pair of noncommuting discrete observables with d outcomes, in the presence of Bob's quantum memory [17]—by restricting to compatible (jointly measurable) POVMs at Bob's end. We first establish that the sum of entropies of Alice's measurement results, when conditioned by the outcomes of compatible unsharp POVMs recorded in Bob's quantum memory, is constrained to obey an entropic steering inequality derived in Refs. [18] and [19]. This essentially brings out the intrinsic equivalence between the violation of an entropic steering inequality and the possibility of reducing the entropic uncertainty bound of a pair of noncommuting observables with the help of an entangled quantum memory. And as violation of a steering inequality requires [14,15] that (i) the parties share a steerable entangled state and, also, that (ii) the measurements by one of the parties (Bob) [23] are incompatible, it becomes evident that information stored in Bob's entangled quantum memory is of no use in reducing the uncertainty of Alice's pair of noncommuting observables when Bob can measure only compatible POVMs. Consequently, we prove that the quantum advantage of the construction of security proofs in quantum key distribution (QKD) [17] is lost in the joint measurability regime.

The paper is organized as follows. In Sec. II we give an overview of generalized POV observables and their joint measurability. The entropic uncertainty relation for Alice's pair of discrete observables in the presence of Bob's quantum memory is discussed in Sec. III. It is shown that when Bob is restricted to employing only jointly measurable POVMs, it is not possible to achieve enhanced precision in predicting Alice's measurement outcomes, even if an entangled state is shared between them. Implications of this identification for security proofs in QKD are also outlined. Section IV reports our concluding remarks.

II. JOINT MEASURABILITY

We begin by giving an outline of generalized measurement of observables in terms of POVMs. A POVM is a set

[*] karthik@rri.res.in
[†] arutth@rediffmail.com
[‡] attipat.rajagopal@gmail.com

$\mathbb{E} = \{E(x)\}$ of positive self-adjoint operators $0 \leqslant E(x) \leqslant 1$, called *effects*, satisfying $\sum_x E(x) = \mathbb{1}$; $\mathbb{1}$ denotes the identity operator. When a quantum system is prepared in state ρ, measurement of $\mathbb{E}$ gives an outcome x with probability $p(x) = \mathrm{Tr}[\rho\, E(x)]$. If $\{E(x)\}$ is a set of complete, orthogonal projectors, then the measurement reduces to the special case of PV measurement.

Let us consider a collection of POV observables $\mathbb{E}_i = \{E_i(x_i)\}$. They are jointly measurable if there exists a *grand* POVM $\mathbb{G} = \{G(\lambda);\ 0 \leqslant G(\lambda) \leqslant \mathbb{1}, \sum_\lambda G(\lambda) = \mathbb{1}\}$ from which the observables $\mathbb{E}_i$ can be constructed as follows. Suppose a measurement of the generalized observable $\mathbb{G}$ is carried out in state ρ and the probability of obtaining the outcome λ is denoted $p(\lambda) = \mathrm{Tr}[\rho\, G(\lambda)]$. If the elements of the POVMs $\mathbb{E}_i = \{E_i(x_i)\}$ can be constructed as *marginals* of the grand POVM $\mathbb{G} = \{G(\lambda),\ \lambda = \{x_1,x_2,\ldots\}\}$, i.e., $E_1(x_1) = \sum_{x_2,x_3,\ldots} G(x_1,x_2,\ldots)$, $E_2(x_2) = \sum_{x_1,x_3,\ldots} G(x_1,x_2,\ldots)$, and so on, the set $\{\mathbb{E}_i\}$ of POVMs is jointly measurable [1].

In general, if the effects $E_i(x_i)$ can be constructed in terms of $G(\lambda)$ as [15,20]

$$E_i(x_i) = \sum_\lambda p(x_i|i,\lambda)\, G(\lambda)\ \forall\ i, \tag{1}$$

where $0 \leqslant p(x_i|i,\lambda) \leqslant 1$ are positive numbers satisfying $\sum_{x_i} p(x_i|i,\lambda) = 1$, then the POVMs $\mathbb{E}_i$ are jointly measurable [21]. For all jointly measurable POVMs, the probability $p(x_i|i)$ of outcome x_i in the measurement of $\mathbb{E}_i$ can be postprocessed based on the results of measurement of the grand POV observale $\mathbb{G}$:

$$p(x_i|i) = \mathrm{Tr}[\rho\, E_i(x_i)] = \sum_\lambda p(\lambda)\, p(x_i|i,\lambda). \tag{2}$$

More specifically, measurements of compatible POVMs $\mathbb{E}_i$ can be interpreted in terms of a single grand POVM $\mathbb{G}$ [i.e., given the positive numbers $p(x_i|i,\lambda)$, one can construct the probabilities of measuring compatible POVMs $\mathbb{E}_i$ based solely on the results of measurement of $\mathbb{G}$]. An important feature to be highlighted here is that the generalized POV observables are jointly measurable even if they do not commute with each other.

Reconciling to joint measurability within quantum theory results in subsequent manifestation of classical features [15]. In particular, as measurement of a single grand POVM can be used to construct results of measurements of all compatible POVMs, joint measurability entails a joint probability distribution for all compatible observables (though for unsharp values of the observables) in *every* quantum state. The existence of joint probabilities in turn implies that the set of all Bell inequalities is satisfied [22] when only compatible measurements are employed. Wolf *et al.* [7] have shown that incompatible measurements of a pair of POVMs with dichotomic outcomes are necessary and sufficient for violation of Clauser-Horne-Shimony-Holt (CHSH) Bell inequality. Further, Quintino *et al.* [14] and Uola *et al.* [15] have established that a set of POVMs (with arbitrarily many outcomes) is not jointly measurable if and only if they are useful for nonlocal quantum steering. It is of interest to explore the limitations imposed by joint measurability on quantum information tasks. In the following, we study the implications of joint measurability on the entropic uncertainty relation in the presence of quantum memory.

III. ENTROPIC UNCERTAINTY RELATION IN THE PRESENCE OF QUANTUM MEMORY

The Shannon entropies $H(\mathbb{X}) = -\sum_x p(x)\log_2 p(x)$ and $H(\mathbb{Z}) = -\sum_z p(z)\log_2 p(z)$, associated with the probabilities $p(x) = \mathrm{Tr}[\rho E_{\mathbb{X}}(x)]$ and $p(z) = \mathrm{Tr}[\rho E_{\mathbb{Z}}(z)]$ of measurement outcomes x and z of a pair of POV observables $\mathbb{X} \equiv \{E_{\mathbb{X}}(x)|0 \leqslant E_{\mathbb{X}} \leqslant \mathbb{1};\ \sum_x E_{\mathbb{X}} = \mathbb{1}\}$ and $\mathbb{Z} \equiv \{E_{\mathbb{Z}}(z)|0 \leqslant E_{\mathbb{Z}} \leqslant \mathbb{1};\ \sum_z E_{\mathbb{Z}} = \mathbb{1}\}$, quantify the uncertainties of predicting the measurement outcomes in a quantum state ρ. Trade-off between the entropies of observables $\mathbb{X}$ and $\mathbb{Z}$ in a finite-level quantum system is quantified by the entropic uncertainty relation [24,25],

$$H(\mathbb{X}) + H(\mathbb{Z}) \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}), \tag{3}$$

where $\mathcal{C}(\mathbb{X},\mathbb{Z}) = \max_{x,z}||\sqrt{E_{\mathbb{X}}(x)}\sqrt{E_{\mathbb{Z}}(z)}||$. Here, $||A|| = \mathrm{Tr}[\sqrt{A^\dagger A}]$.

Consider the following uncertainty game [17]: two players, Alice and Bob, agree to measure a pair of observables $\mathbb{X}$ and $\mathbb{Z}$. Bob prepares a quantum state of his choice and sends it to Alice. Alice measures $\mathbb{X}$ or $\mathbb{Z}$ randomly and communicates her choice of measurements to Bob. To win the game, Bob's initial preparation of the quantum state should be such that he is able to predict Alice's measurement outcomes of the chosen pair of observables $\mathbb{X}$ and $\mathbb{Z}$ with as much precision as possible when Alice announces which of the pair of observables is measured. In other words, Bob's task is to minimize the uncertainties in the measurements of a pair of observables $\mathbb{X}$ and $\mathbb{Z}$ that were agreed upon initially, with the help of an optimal quantum state. The uncertainties of $\mathbb{X}$, and $\mathbb{Z}$ are bounded as in (3) when Bob has only classical information about the state. On the other hand, with the help of a quantum memory (where Bob prepares an entangled state and sends one part of the state to Alice), Bob can beat the uncertainty bound of (3).

The entropic uncertainty relation, when Bob possesses a quantum memory, was put forth by Berta *et al.* [17],

$$S(\mathbb{X}|B) + S(\mathbb{Z}|B) \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}) + S(A|B), \tag{4}$$

where $S(\mathbb{X}|B) = S(\rho_{AB}^{(\mathbb{X})}) - S(\rho_B)$ and $S(\mathbb{Z}|B) = S(\rho_{AB}^{(\mathbb{Z})}) - S(\rho_B)$ are the conditional von Neumann entropies of the post measured states $\rho_{AB}^{(\mathbb{X})} = \sum_x |x\rangle\langle x| \otimes \rho_B^{(x)}$ with $\rho_B^{(x)} = \mathrm{Tr}_A[\rho_{AB}(E_{\mathbb{X}}(x) \otimes \mathbb{1}_B)]$ and $\rho_{AB}^{(\mathbb{Z})} = \sum_z |z\rangle\langle z| \otimes \rho_B^{(z)}$ with $\rho_B^{(z)} = \mathrm{Tr}_A[\rho_{AB}(E_{\mathbb{Z}}(z) \otimes \mathbb{1}_B)]$, obtained after Alice's measurements of $\mathbb{X}$ and $\mathbb{Z}$ on her system. [Here, the measurement outcomes of the effects $E_{\mathbb{X}}(x)$ $[E_{\mathbb{Z}}(z)]$ are encoded in an orthonormal basis $\{|x\rangle\}$ ($\{|z\rangle\}$) and the probability of measurement outcome x (z) is given by $p(x) = \mathrm{Tr}[\rho_B^{(x)}]$ ($p(z) = \mathrm{Tr}[\rho_B^{(z)}]$); $S(A|B) = S(\rho_{AB}) - S(\rho_B)$ is the conditional von Neumann entropy of state ρ_{AB}.]

When Alice's system is in a maximally entangled state with Bob's quantum memory, the second term on the right-hand side of (4) takes the value $S(A|B) = -\log_2 d$, and as $-2\log_2 C(\mathbb{X},\mathbb{Z}) \leqslant \log_2 d$ (which can be realized when Alice employs pairs of unbiased projective measurements [26]), a trivial lower bound of 0 is obtained in the entropic uncertainty relation. In other words, by sharing an entangled state with

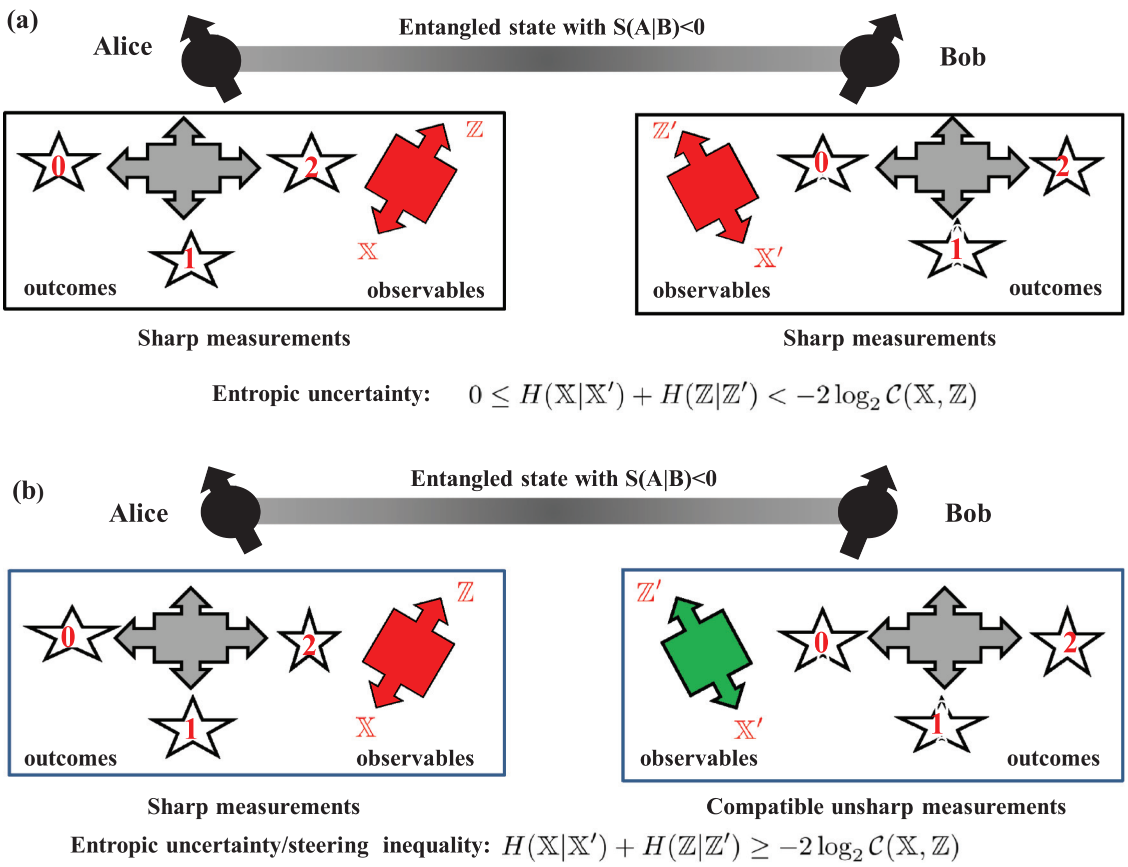
(a)
Alice
Entangled state with S(A|B)<0
Bob
0
2
1
$\mathbb{Z}$
$\mathbb{X}$
outcomes
observables
$\mathbb{Z}'$
$\mathbb{X}'$
0
2
1
observables
outcomes
Sharp measurements
Sharp measurements
Entropic uncertainty: $0 \leq H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') < -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z})$
(b)
Alice
Entangled state with S(A|B)<0
Bob
0
2
1
$\mathbb{Z}$
$\mathbb{X}$
outcomes
observables
$\mathbb{Z}'$
$\mathbb{X}'$
0
2
1
observables
outcomes
Sharp measurements
Compatible unsharp measurements
Entropic uncertainty/steering inequality: $H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geq -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z})$

FIG. 1. (Color online) Alice and Bob decide on the pair of noncommuting observables $\mathbb{X}$ and $\mathbb{Z}$. Bob prepares an entangled state ρ_{AB} and sends the subsystem A to Alice. Then Alice measures $\mathbb{X}$ or $\mathbb{Z}$ randomly and conveys her choice to Bob. At his end, Bob measures $\mathbb{X}'$ or $\mathbb{Z}'$ and predicts Alice's outcomes. (a) Alice and Bob both perform sharp measurements. In this case, Bob can predict Alice's outcomes with an enhanced precision, as the entropic uncertainty bound [see (5)] can be smaller than $-2\log_2 C(\mathbb{X},\mathbb{Z})$ when the conditional von Neumann entropy $S(A|B)$ of the entangled state ρ_{AB} is negative. (b) Alice performs sharp measurements of the chosen observable $\mathbb{X}$ or $\mathbb{Z}$, while Bob correspondingly records the outcomes of compatible unsharp measurements of $\mathbb{X}'$ or $\mathbb{Z}'$. In the joint measurability range of $\mathbb{X}'$ and $\mathbb{Z}'$, Bob's quantum memory fails to predict Alice's outcomes more precisely because the sum of entropies $H(\mathbb{X}|\mathbb{X}')$ and $H(\mathbb{Z}|\mathbb{Z}')$ is constrained to obey an entropic steering inequality: $H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geqslant -2\log_2 C(\mathbb{X},\mathbb{Z})$.

Alice, Bob can beat the uncertainty bound given by (3) and can predict the outcomes of a pair of observables $\mathbb{X}$ and $\mathbb{Z}$ with improved precision by performing suitable measurements on his part of the state.

Let us denote $\mathbb{X}'$ or $\mathbb{Z}'$ as the POVM which Bob chooses to measure when Alice announces her choice of measurements of the observable $\mathbb{X}$ or $\mathbb{Z}$. The uncertainty relation, (4), can be recast in terms of the conditional entropies [27] $H(\mathbb{X}|\mathbb{X}')$ and $H(\mathbb{Z}|\mathbb{Z}')$ of Alice's measurement outcomes of the observables $\mathbb{X}$ and $\mathbb{Z}$, conditioned by Bob's measurements of $\mathbb{X}'$ and $\mathbb{Z}'$. As measurements always increase the entropy, i.e., $H(\mathbb{X}|\mathbb{X}') \geqslant S(\mathbb{X}|B)$ and $H(\mathbb{Z}|\mathbb{Z}') \geqslant S(\mathbb{Z}|B)$, the entropic uncertainty relation in the presence of quantum memory can be expressed in the form [17]

$$H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}) + S(A|B). \quad (5)$$

On the other hand, the conditional entropies $H(\mathbb{X}|\mathbb{X}')$ and $H(\mathbb{Z}|\mathbb{Z}')$ are constrained to obey the *entropic steering inequality* [18,19],

$$H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}), \quad (6)$$

if Bob is unable to remotely steer Alice's state by his local measurements. And, as proven recently [14,15], measurements at Bob's end can result in the violation of any steering inequality if and only if they are incompatible (and, in addition, the state shared between Alice and Bob is entangled so as to be steerable). In other words, the entropic inequality, (6), can never be violated if Bob's measurements of $\mathbb{X}'$ and $\mathbb{Z}'$ are compatible. Violation of the steering inequality, (6), would in turn correspond to a reduced bound in the entropic uncertainty relation, (5), in the presence of quantum memory [a reduction in the bound is realized when Alice and Bob share an entangled state with $S(A|B) < 0$]. If Bob is constrained to perform compatible measurements on his system, he cannot beat the uncertainty bound of (3) and win the *uncertainty game* by predicting the outcomes as precisely as possible, even when he shares a maximally entangled state with Alice (see Fig. 1).

A. An example

We illustrate the entropic uncertainty relation, (4), for a pair of qubit observables $\mathbb{X} = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $\mathbb{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$, when Alice and Bob share a maximally entangled two-qubit state, $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0_A,1_B\rangle - |1_A,0_B\rangle)$. Alice performs one of the sharp PV measurements,

$$\Pi_{\mathbb{X}}(x) = \tfrac{1}{2}(\mathbb{1} + x\,\mathbb{X}), \quad x = \pm 1,$$
$$\Pi_{\mathbb{Z}}(z) = \tfrac{1}{2}(\mathbb{1} + z\,\mathbb{Z}), \quad z = \pm 1, \tag{7}$$

of the observable $\mathbb{X}$ or $\mathbb{Z}$ randomly on her qubit and announces her choice of measurement, while Bob tries to predict Alice's outcomes by performing unsharp compatible measurements of the POVMs $\{E_{\mathbb{X}'}(x'), x' = \pm 1\}$ or $\{E_{\mathbb{Z}'}(z'), z' = \pm 1\}$ on his qubit. The effects $E_{\mathbb{X}'}(x')$ and $E_{\mathbb{Z}'}(z')$ (corresponding to binary unsharp measurements of the observables $\mathbb{X}'$ and $\mathbb{Z}'$) are given by

$$E_{\mathbb{X}'}(x') = \tfrac{1}{2}(\mathbb{1} + \eta\, x'\,\mathbb{X}'),$$
$$E_{\mathbb{Z}'}(z') = \tfrac{1}{2}(\mathbb{1} + \eta\, z'\,\mathbb{Z}'), \tag{8}$$

where x' and z' are the measurement outcomes and $0 \leqslant \eta \leqslant 1$ denotes the unsharpness of the fuzzy measurements. Clearly, when $\eta = 1$, the POVM elements $E_{\mathbb{X}'}(x')$ and $E_{\mathbb{Z}'}(z')$ reduce to their corresponding sharp PV versions [see (7)], $\Pi_{\mathbb{X}'}(x')$ and $\Pi_{\mathbb{Z}'}(z')$.

The joint probabilities $p(x,x')$ [or $p(z,z')$] of Alice's sharp outcome x (or z) and Bob's unsharp outcome x' (or z'), when they both choose to measure the same observable $\mathbb{X}$ (or $\mathbb{Z}$) at their ends, is obtained as

$$\begin{aligned} p(x,x') &= \langle\psi_{AB}|\Pi_{\mathbb{X}}(x) \otimes E_{\mathbb{X}}(x')|\psi_{AB}\rangle \\ &= \tfrac{1}{4}(1 - \eta\, x\, x')), \\ p(z,z') &= \langle\psi_{AB}|\Pi_{\mathbb{Z}}(z) \otimes E_{\mathbb{Z}}(z')|\psi_{AB}\rangle \\ &= \tfrac{1}{4}(1 - \eta\, z\, z')). \end{aligned} \tag{9}$$

While the right-hand side of the entropic uncertainty relation, (5), reduces to 0 in this case, the left-hand side can be simplified (see [27]) to obtain

$$\begin{aligned} H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') &= -\sum_{x,x'=\pm 1} p(x,x')\log_2 p(x|x') \\ &\quad - \sum_{z,z'=\pm 1} p(z,z')\log_2 p(z|z') \\ &= 2\,H[(1+\eta)/2], \end{aligned} \tag{10}$$

where $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy. As the binary entropy function $H[(1+\eta)/2] = 0$ only when $\eta = 1$, the trivial lower bound of the uncertainty relation, (5), can be reached if Bob too performs sharp PV measurements of the observables $\mathbb{X}$ and $\mathbb{Z}$ at his end. In other words, Bob can predict the outcomes of Alice's measurements of $\mathbb{X}$ and $\mathbb{Z}$ precisely when he employs sharp PV measurements of the same observables. But sharp measurements of $\mathbb{X}$ and $\mathbb{Z}$ are not compatible. The joint measurability of the unsharp POVMs $\{E_{\mathbb{X}}(x')\}$ and $\{E_{\mathbb{Z}}(z')\}$ sets the limitation [1,5] $\eta \leqslant 1/\sqrt{2}$ on the unsharpness parameter.

If Bob is confined to the joint measurability range $0 \leqslant \eta \leqslant 1/\sqrt{2}$, the entropic steering inequality, (6),

$$H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geqslant 1, \tag{11}$$

is always satisfied [28]. In turn, this implies that Bob cannot beat the entropic uncertainty bound of (3)—even with the help of an entangled state he shares with Alice—if he is constrained to employ jointly measurable POVMs.

The result demonstrated here in the specific example of $d = 2$ (qubits) holds, in principle, for any d-dimensional POVMs. An illustration in the d-dimensional example, however, requires that the compatibility or incompatibility range of the unsharpness parameter η is known. However, optimal values of the unsharpness parameter (η) of a set of POVMs is known only for qubits.

B. Joint measurability and QKD

The entropic uncertainty relation in the presence of quantum memory, (4), provides a quantification for the connection between entanglement and uncertainty. Moreover, it has been shown [17] to be useful to derive a lower bound on the secret key rate that can be generated by Alice and Bob in a QKD against collective attacks by an adversary, Eve. Subsequently, a tighter finite-key bound on the discrete variable QKD was derived based on generalized uncertainty relations for smooth min and max entropies [29]. Entropic uncertainty relations have also proved to be of practical use in identifying security proofs of device-independent QKDs [30]. Recently Branciard *et al.* [31] showed for the first time that the steering and security of one-sided device independent QKDs are related. In the following, we focus on the implications of joint measurability for the secret key rate in a QKD against collective attacks by an adversary, Eve.

Suppose that Eve prepares a three-party quantum state ρ_{ABE} and gives the A and B parts to Alice and Bob, keeping part E with her. Alice measures the observables $\mathbb{X}$ and $\mathbb{Z}$ randomly on the state she receives and Bob tries to predict Alice's results by his measurements of $\mathbb{X}'$ and $\mathbb{Z}'$. In order to generate a key, Alice communicates her choice of measurements to Bob. Even if this communication is overheard by Eve, Alice and Bob can generate a secure key—provided the correlations between their measurement outcomes fare better than those between Eve and Alice. More specifically, if the difference between the mutual information $S(\mathbb{X}:B) = S(\rho_A^{\mathbb{X}}) + S(B) - S(\rho_{AB}^{\mathbb{X}}) = S(\rho_A^{\mathbb{X}}) - S(\mathbb{X}|B)$ and $S(\mathbb{X}:E) = S(\rho_A^{\mathbb{X}}) + S(E) - S(\rho_{AE}^{\mathbb{X}}) = S(\rho_A^{\mathbb{X}}) - S(\mathbb{X}|E)$ (corresponding to the measurement of $\mathbb{X}$ at Alice's end) is positive, Alice and Bob can always generate a secure key.

The amount of key K that Alice and Bob can generate per state is lower bounded by [32]

$$K \geqslant S(\mathbb{X}:B) - S(\mathbb{X}:E) = S(\mathbb{X}|E) - S(\mathbb{X}|B). \tag{12}$$

It may be noted that when Alice's measurement outcomes of $\mathbb{X}$ and $\mathbb{Z}$ are simultaneously stored in the quantum memories of Eve and Bob, respectively, the following trade-off relation for the entropies $S(\mathbb{X}|E)$ and $S(\mathbb{Z}|B)$ ensues [17,33,34]:

$$S(\mathbb{X}|E) + S(\mathbb{Z}|B) \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}). \tag{13}$$

And, employing (13) in (12), one obtains

$$\begin{aligned} K &\geqslant S(\mathbb{X}|E) + S(\mathbb{Z}|B) - [S(\mathbb{X}|B) + S(\mathbb{Z}|B)] \\ &\geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}) - [S(\mathbb{X}|B) + S(\mathbb{Z}|B)]. \end{aligned} \tag{14}$$

As $H(\mathbb{X}|\mathbb{X}') \geqslant S(\mathbb{X}|B)$ and $H(\mathbb{Z}|\mathbb{Z}') \geqslant S(\mathbb{Z}|B)$, the lower bound of inequality (14) can be simplified to obtain [17]

$$K \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}) - [H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}')]. \quad (15)$$

It is clear that when Bob is constrained to performing measurements of compatible POVMs $\mathbb{X}'$ and $\mathbb{Z}'$, the conditional entropies $H(\mathbb{X}|\mathbb{X}')$ and $H(\mathbb{Z}|\mathbb{Z}')$ satisfy the entropic steering inequality, $H(\mathbb{X}|\mathbb{X}') + H(\mathbb{Z}|\mathbb{Z}') \geqslant -2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z})$ [see (6)], in which case the key rate is not ensured to be positive. Bob must be equipped to perform incompatible measurements at his end [so that it is possible to witness violation of the steering inequality by beating the bound $-2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z})$ on entropic uncertainties and attain the refined bound of $-2\log_2 \mathcal{C}(\mathbb{X},\mathbb{Z}) + S(A|B)$ as in (5)] in order for a positive key rate to ensue. In other words, a quantum advantage for security in a QKD against collective attacks by Eve is not envisaged when Bob is constrained to performing compatible measurements only.

IV. CONCLUSIONS

Measurement outcomes of a pair of noncommuting observables reveal a trade-off, which is quantified by uncertainty relations. The entropic uncertainty relation [24] constrains the sum of entropies associated with the probabilities of outcomes of a pair of observables. An extended entropic uncertainty relation [17] brought out that it is possible to beat the lower bound on uncertainties when the system is entangled with a quantum memory. In this paper we have explored the entropic uncertainty relation when the entangled quantum memory is restricted to recording the outcomes of jointly measurable POVMs only. With this constraint on the measurements, the entropies satisfy an entropic steering inequality [18]. Thus, we identify that an entangled quantum memory, which is limited to recording results of compatible POVMs, cannot assist in beating the entropic uncertainty bound. As a consequence, we show that the quantum advantage in ensuring security in a key distribution against collective attacks is lost, even though a suitable entangled state is employed—but with the joint measurability constraint.

[1] P. Busch, Phys. Rev. D **33**, 2253 (1986).

[2] P. Lahti, Int. J. Theor. Phys. **42**, 893 (2003).

[3] E. Andersson, S. M. Barnett, and A. Aspect, Phys. Rev. A **72**, 042104 (2005).

[4] W. Son, E. Andersson, S. M. Barnett, and M. S. Kim, Phys. Rev. A **72**, 052116 (2005).

[5] T. Heinosaari, D. Reitzner, and P. Stano, Found. Phys. **38**, 1133 (2008).

[6] P. Busch, P. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement. Environmental Engineering*, Vol. 2 (Springer, New York, 1996).

[7] M. M. Wolf, D. Perez-Garcia, and C. Fernandez, Phys. Rev. Lett. **103**, 230402 (2009).

[8] S. Yu, N.-L. Liu, L. Li, and C. H. Oh, Phys. Rev. A **81**, 062116 (2010).

[9] T. Heinosaari and M. M. Wolf, J. Math. Phys. **51**, 092201 (2010).

[10] Y. C. Liang, R. W. Spekkens, and H. M. Wiseman, Phys. Rep. **506**, 1 (2011).

[11] D. Reeb, D. Reitzner, and M. M. Wolf, J. Phys. A: Math. Theor. **46**, 462002 (2013).

[12] M. Banik, Md. R. Gazi, S. Ghosh, and G. Kar, Phys. Rev. A **87**, 052125 (2013).

[13] R. Kunjwal, C. Heunen, and T. Fritz, Phys. Rev. A **89**, 052126 (2014).

[14] M. T. Quintino, T. Vértesi, and N. Brunner, Phys. Rev. Lett. **113**, 160402 (2014).

[15] R. Uola, T. Moroder, and O. Gühne, Phys. Rev. Lett. **113**, 160403 (2014).

[16] The concept of *nonlocal steering* was originally put forth by E. Schrödinger, Proc. Cambr. Philos. Soc. **31**, 555 (1935). A formal modern approach to steering was initiated by M. D. Reid [Phys. Rev. A **40**, 913 (1989)], who proposed the first experimentally testable criteria of nonlocal steering. Reid's criteria brought out that steering and the Einstein-Podolsky-Rosen paradox are equivalent notions of nonlocality. Further, H. M. Wiseman *et al.* [Phys. Rev. Lett. **98**, 140402 (2007)] showed that steering constitutes a different class of nonlocality, which lies between entanglement and Bell nonlocality. Manifestation of steering in the form of different types of steering inequalities is presented by E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

[17] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Phys. **6**, 659 (2010).

[18] J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, Phys. Rev. A **87**, 062103 (2013).

[19] The first entropic criterion of steering was formulated for position and momentum by S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011). Entropic steering inequalities for discrete observables were developed more recently in Ref. [18].

[20] S. T. Ali, C. Carmeli, T. Heinosaari, and A. Toigo, Found. Phys. **39**, 593 (2009).

[21] The effects $E_i(x_i)$ are positive by construction [see Eq. (1)] and they obey $\sum_{x_i} E_i(x_i) = \sum_\lambda [\sum_{x_i} p(x_i|i,\lambda)] G(\lambda) = \sum_\lambda G(\lambda) \equiv \mathbb{1}$. In particular, choosing $p(x_i|i,\lambda) = \delta_{x_i,x_i'}$ and expressing λ as a collective index, $\lambda = \{x_1', x_2', \ldots\}$, the elements of compatible POVMs are obtained as $E_i(x_i) = \sum_{\lambda=\{x_1',x_2',\ldots\}} \delta_{x_i',x_i} G(\lambda) = \sum_{x_1',x_2',\ldots,x_{i-1}',x_{i+1}'\ldots} G(x_1',x_2',\ldots,x_{i-1}',x_i,x_{i+1}'\ldots)$; i.e., they are the *marginals* of $\mathbb{G}$.

[22] A. Fine, Phys. Rev. Lett. **48**, 291 (1982); J. Math. Phys. **23**, 1306 (1982).

[23] The roles played by Alice and Bob in a nonlocal steering task (where, conventionally, Alice is an untrusted party and Bob needs to check violation or nonviolation of a steering inequality to verify if Alice's claim—that they share an entangled state—is true or false) are interchanged here so as to be consistent with the convention of Ref. [17].

[24] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[25] M. Krishna and K. R. Parthasarathy, Sankhya **64**, 842 (2002).

[26] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).

[27] Note that $H(\mathbb{X}|\mathbb{X}') = -\sum_{x,x'} p(x|x')\log_2 p(x|x')$, where $p(x,x') = \mathrm{Tr}[\rho_{AB} E_{\mathbb{X}}(x) \otimes E_{\mathbb{X}'}(x')]$ and $p(x|x') = p(x,x')/p(x')$, is the conditional Shannon entropy associated with the probabilities of Alice finding the outcome x of the POVM $\mathbb{X}$ when Bob has obtained the outcome x' in the measurement of $\mathbb{X}'$ and $p(x') = \mathrm{Tr}[\rho_B E_{\mathbb{X}'}(x')] = \sum_x p(x,x')$ is the probability of Bob's outcome x' in the measurement of $\mathbb{X}'$.

[28] The entropic steering inequality, (11), is violated when the unsharpness parameter $\eta > 0.78$, whereas the POVMs of (8) are incompatible for $\eta > 1/\sqrt{2} \approx 0.707$. In order to obtain the necessary and sufficient condition that the POVMs of (8) are useful for steering in the entire range of incompatibility, $1/\sqrt{2} < \eta \leqslant 1$, one must either examine the set of all pure entangled states for the task of steering or develop an appropriate steering inequality to capture the efficacy of the incompatible measurements [14, 15]. For instance, we find that the two-qubit maximally entangled state shared between Alice and Bob violates a linear steering inequality with two measurement settings [Eq. (64) in E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009)] for the *entire* range of incompatibility, $1/\sqrt{2} < \eta \leqslant 1$, of the unsharpness parameter when Bob (who claims to steer Alice's by measurements at his end) measures the pairs of POVMs of (8).

[29] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[30] E. Hänggi and R. Renner, arXiv:1009.1833.

[31] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).

[32] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[33] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).

[34] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **83**, 062338 (2011).