Fine-grained Einstein-Podolsky-Rosen–steering inequalities

Tanumoy Pramanik,[1,*] Marc Kaplan,[1,†] and A. S. Majumdar[2,‡]
[1]*LTCI, Télécom ParisTech, 23 Avenue d'Italie, 75214 Paris CEDEX 13, France*
[2]*S. N. Bose National Centre for Basic Sciences, Salt Lake, Kolkata 700 098, India*

We derive a steering inequality based on a fine-grained uncertainty relation to capture Einstein-Podolsky-Rosen steering for bipartite systems. Our steering inequality improves over previous ones since it can experimentally detect all steerable two-qubit Werner state with only two measurement settings on each side. According to our inequality, pure entangled states are maximally steerable. Moreover, by slightly changing the setting, we can express the amount of violation of our inequality as a function of their violation of the Clauser-Horne-Shimony-Holt inequality. Finally, after deriving a monogamy relation we prove that the amount of violation of our steering inequality is, up to a constant factor, a lower bound on the key rate of a one-sided device-independent quantum key distribution protocol secure against individual attacks.

PACS number(s): 03.67.Mn, 03.65.Ud, 03.67.Dd

Quantum information distinguishes three forms of nonlocal correlations [1–6]. These are entanglement, steering, and Bell nonlocal correlations. Einstein, Podolsky, and Rosen introduced entangled quantum states in an attempt to show the incompleteness of quantum physics, known as the Einstein-Podolsky-Rosen (EPR) paradox [1]. In the same year, Schrödinger reexpressed the EPR paradox as the possibility of steering, also known as EPR steering, i.e., when Alice and Bob share an entangled state, Alice can affect Bob's state through her own measurement. More precisely, a state exhibits EPR steering if it cannot be modeled as Bob holding an unknown yet definite state, a description known as a local hidden state (LHS) model [4]. Bell-type inequalities can be used to rule out local hidden variable models. Similarly, steering inequalities are used to rule out the existence of any LHS model and thus demonstrate steerability.

Wiseman *et al.* showed that the three forms of nonlocal correlations, viz., entanglement, steering, and Bell nonlocality, are also tightly related to the experimental settings required to test them [4]. To test entanglement, both parties need to trust that they perform quantum operations and also trust their measurement devices. In the case of EPR steering, only one party assumes that he applies a quantum measurement and that his device is not controlled by a third party. Finally, Bell nonlocality can be tested without assuming quantum theory and trusting measurement devices. This leads to a hierarchy in which EPR steering lies between Bell nonlocality and entanglement.

Experimental demonstration of Bell's nonlocality has been achieved by several experiments [7]. To test EPR steering, Reid proposed a testable formulation for continuous-variable systems based on a position-momentum uncertainty relation [5]. Later, Reid's criterion for steering was experimentally tested by Ou *et al.* [8]. Since Reid's criterion is based on variances, it fails to capture EPR steering for Bell nonlocal states whose correlation appears in higher than second order [9]. Walborn *et al.* [10] have improved the situation by introducing an entropic steering inequality. According to this criterion, states admitting LHS models satisfy

$$H(\mathcal{P}_B|\mathcal{P}_A) + H(\mathcal{Q}_B|\mathcal{Q}_A) \geqslant \ln \pi e, \tag{1}$$

where $\mathcal{P}$ and $\mathcal{Q}$ are two noncommuting observables and subscripts A and B label Alice's observable and Bob's observable, respectively. The intuition behind inequality (1) is that if the state has a LHS model, then Alice's choice of measurement does not affect Bob's state in a way that would violate the entropic uncertainty relation

$$H(\mathcal{P}_B) + H(\mathcal{Q}_B) \geqslant \ln \pi e. \tag{2}$$

Steering allows one to reduce the uncertainty of noncommuting measurements conditioned on Alice's measurement outcome. The violation of inequality (1) thus demonstrates EPR steering.

For discrete-variable systems, EPR-steering theory has been developed by Wiseman *et al.* [4]. In their proposal, Alice and Bob both choose observables among n possible ones. Alice sends A_k to Bob, a random variable that she obtained by operating on her share. Bob then measures the Pauli observable $\hat{\sigma}_k^B$. For LHS models, the average correlation of outcomes satisfies

$$\frac{1}{n}\sum_{k=1}^{n}\langle A_k\hat{\sigma}_k\rangle \leqslant C_n = \max_{A_k}\left(\frac{\lambda_{\max}}{n}\sum_{k=1}^{n}\langle A_k\hat{\sigma}_k\rangle\right). \tag{3}$$

A violation of inequality (3) demonstrates that the state shared by Alice and Bob is steerable. Based on this criterion, Saunders *et al.* experimentally demonstrated the steerability of a two-qubit Bell local state (which does not violate any Bell inequality) [11].

In the present work, we improve the coarse-grained steering criteria of Refs. [10,11]. While Reid's criterion was based on Heisenberg's uncertainty relation and that of Walborn *et al.* on the entropic uncertainty relation, our steering inequality is based on fine-grained uncertainty relations (FURs). The derivation of our steering inequality is in two parts. We first introduce a game played between Alice and Bob to characterize steering. We then use a FUR to upper bound the winning probability when played with states admitting LHS models.

*Pramanik@telecom-paristech.fr
†kaplan@telecom-paristech.fr
‡archan@bose.res.in

Fine-grained uncertainty relations were first introduced by Oppenheim and Wehner [12] and later generalized to tripartite systems in both the unbiased [13] and biased [14] cases. In their work [12] Oppenheim and Wehner show that the amount of nonlocality measured by the Clauser-Horne-Shimony-Holt (CHSH) inequality is bounded by the uncertainty as measured by some FUR. We extend this approach to steering, showing that the uncertainty between measurement quantified by FURs induces constraints (modeled as a game) on states admitting LHS models. Violation of these constraints thus demonstrates steering.

In the following, Alice is the supplier of the state and tries to convince Bob that the state she has prepared is steerable. We consider two different scenarios based on Alice's knowledge about Bob's set of observables before she sends the state. Depending on Alice's knowledge, our steering inequality has two different bounds. Then we discuss the steerability of pure bipartite entangle states and two-qubit Werner states [15] given by

$$\rho_{AB}^{W} = p\rho_S + \frac{1-p}{4} I, \tag{4}$$

where ρ_S is the density matrix of $(|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$. Using our steering inequality, one can experimentally test the steerability of ρ_{AB}^{W} for any mixing parameter chosen from the range $\frac{1}{2} < p \leqslant 1$, with only two measurement settings for each party. Prior to our work, two measurement settings only allowed demonstration of steerability of ρ_{AB}^{W} for $p > \frac{1}{\sqrt{2}}$ [11,16].

Finally, we study the relation between our inequality and a one-sided device-independent quantum key distribution (1SDIQKD) [17]. It is known that getting a positive key rate in a 1SDIQKD protocol implies the violation of some steering inequality of the state that is used [18]. We prove that, conversely, the violation of our steering inequality implies the security of a certain 1SDIQKD protocol. We also prove a quantitative relation between the amount of violation of our inequality and the key rate against individual attacks.

In the single-qubit case, a FUR can be described by the following game. Let Alice receive a binary question $s \in \{0,1\}$ with probability $p(s) = \frac{1}{2}$. When she receives the question $s = 0$ (resp. $s = 1$) Alice measures observable σ_z (resp. σ_x) on the state ρ_A. She gets outcome a_s. Alice wins the game if she gets a spin-up outcome, i.e, $a_s = 0$, for both questions $s = 0$ and $s = 1$. The winning probability of the above game is given by

$$P_{\text{game}} = \sum_s p(s)p(a_s = 0)_{\rho_A} \leqslant P_{\text{game}}^{\max} = \max_{\rho_A} P_{\text{game}}, \tag{5}$$

where $p(a_s = 0)_{\rho_A}$ is the probability of obtaining a spin-up outcome for the measurement corresponding to the question s on the state ρ_A and $P_{\text{game}}^{\max}$ is the maximum winning probability over all possible strategies, i.e., the choice of the single-qubit state ρ_A in this game. In the above situation, $P_{\text{game}}^{\max} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$ occurs for the eigenstates of $\frac{\sigma_x+\sigma_z}{\sqrt{2}}$, which are known as maximally certain states [12]. For the spin-down winning condition, i.e., $a_s = 1$, the maximum winning probability is the same and is achieved using eigenstates of $\frac{\sigma_x-\sigma_z}{\sqrt{2}}$. Further, FURs has been extended for bipartite systems [12] and tripartite systems [13,14]. In these cases, by considering a special kind of nonlocal retrieval game, the upper bound on the FUR discriminates different physical theories with the help of Bell-like inequalities [3]. Furthermore, FURs can be applied to study the reduction of uncertainty in the presence of quantum correlation of the observed system with the other system called quantum memory [19,20].

We consider the following game. Alice prepares a large number of copies of a bipartite state ρ_{AB} between systems labeled by A and B. She then sends all the systems labeled by B to Bob. After getting them all, Bob asks Alice to steer each system in the eigenstates of a randomly chosen observable from the set $\{\mathcal{P},\mathcal{Q}\}$. Whenever Bob asks to be steered in an eigenstate of $\mathcal{P}$, Alice applies observable $\mathcal{S}$ to her system. Similarly, she applies observable $\mathcal{T}$ to steer Bob's system to an eigenstate of $\mathcal{Q}$. Alice's task is to convince Bob that they share steerable states by communicating her choices of observables and the outcomes. On other hand, Bob does not trust Alice. He only believes that Alice sent quantum systems and measured them. Bob is not convinced by Alice if the correlation of measurement outcomes can be described by a LHS model [4], i.e.,

$$P(a_{\mathcal{A}},b_{\mathcal{B}}) = \sum_{\lambda} P(\lambda)P(a_{\mathcal{A}}|\lambda)P_Q(b_{\mathcal{B}}|\lambda). \tag{6}$$

Here $(\mathcal{A},\mathcal{B}) \in \{(\mathcal{S},\mathcal{P}),(\mathcal{T},\mathcal{Q})\}$ are the observables, $a_{\mathcal{A}}$ and $b_{\mathcal{B}}$ are Alice's and Bob's measurement outcomes, respectively, and $P_Q(b_{\mathcal{B}}|\lambda)$ is the probability of obtaining outcome $b_{\mathcal{B}}$ after measuring a quantum system specified by the hidden variable λ.

Using $\sum_i x_i y_i \leqslant \max_i\{x_i\}\sum_i y_i$ for x_i, y_i positive, Eq. (6) becomes

$$P(b_{\mathcal{B}}|a_{\mathcal{A}}) \leqslant \max_{\lambda}[P_Q(b_{\mathcal{B}}|\lambda)] = P_Q(b_{\mathcal{B}}|\lambda_{\max}). \tag{7}$$

Since Bob chooses a random observable from $\{\mathcal{P},\mathcal{Q}\}$, inequality (7) becomes

$$\tfrac{1}{2}P(b_{\mathcal{P}}|a_{\mathcal{S}}) + \tfrac{1}{2}P(b_{\mathcal{Q}}|a_{\mathcal{T}}) \leqslant \max_{\mathcal{P}^*,\mathcal{Q}^*}\big[\tfrac{1}{2}P_Q(b_{\mathcal{P}^*}|\lambda_{\max}) + \tfrac{1}{2}P_Q(b_{\mathcal{Q}^*}|\lambda_{\max})\big], \tag{8}$$

where $\mathcal{P}^*, \mathcal{Q}^*$ range over all possible maximally incompatible measurements.

The above inequality is a fine-grained steering criterion satisfied by bipartite states that admit LHS models for the system B. Its violation for any combination of outcomes $\{a,b\}$ demonstrates steerability. In inequality (1) the constraints on states admitting LHS models are expressed in terms of average uncertainty where the average is taken over all measurement outcomes. In our case, we consider the uncertainty for each particular outcome in a fine-grained way. Calculating the right-hand side of inequality (8) for LHS models gives a steering inequality. This term measures the uncertainty arising from incompatible measurements $\mathcal{P}$ and $\mathcal{Q}$ and is bounded by the FUR.

Now we discuss Alice's cheating strategy when ρ_B is a qubit. Alice tries to maximize the left-hand side of inequality (8) using a LHS. We consider two different scenarios. In scenario I, Alice gets the description of $\{\mathcal{P},\mathcal{Q}\}$ before sending

the states to Bob. Therefore, her whole strategy, including the choice of the state ρ_B, depends on the choices of observables.

In scenario II, Alice prepares the states before getting the description of Bob's observables. She gets this information when the game starts. However, her communication can still depend on Bob's choice of observables.

Scenario I. Before sending system B, Alice knows that Bob is going to randomly chose either observable σ_z or observable σ_x. The optimal LHS strategy is the one that maximizes the fine-grained uncertainty relation. More precisely, depending upon the knowledge of Bob's winning condition and his set of observables, Alice prepares maximally certain states [12] that maximize the corresponding winning probability (given by the FUR) and send them to Bob. For a spin-up (resp. spin-down) winning condition, Alice prepares all systems in one of the eigenstates of $\frac{1}{\sqrt{2}}(\sigma_x+\sigma_z)$ [resp. $\frac{1}{\sqrt{2}}(\sigma_x-\sigma_z)$] and sends them to Bob. Then Bob wins with probability $\frac{1}{2}+\frac{1}{2\sqrt{2}}$ [12]. This is still true if the state of the system B is labeled by a variable λ that remains hidden to Bob. Using inequality (8), Bob is convinced that ρ_{AB} is steerable only when

$$P(b_{\mathcal{P}}|a_{\mathcal{S}})+P(b_{\mathcal{Q}}|a_{\mathcal{T}})>1+\frac{1}{\sqrt{2}}. \tag{9}$$

Scenario II. Here Alice prepares all systems without any knowledge of Bob's set of observables. In this case, we calculate the average winning probability of getting a spin-up outcome where the average is taken over set of possible observables and then maximize it with respect to all possible local hidden states. Bob can check that the state violates this maximum and thus conclude that it is steerable.

To calculate the maximum, assume that the hidden state is prepared along $\hat{n}$ of polar coordinates $\{\theta,\phi\}$, i.e., $\rho_B=\frac{1}{2}(I+\hat{n}.\vec{\sigma}^B)$, and that the choices of observables are $\mathcal{P}=\hat{p}\cdot\vec{\sigma}$ and $\mathcal{Q}=\hat{q}\cdot\vec{\sigma}$, where "$\hat{p}$" (resp. $\hat{q}$) is the unit vector of polar coordinates $\{\theta_{\hat{p}},\phi_{\hat{p}}\}$ (resp. $\{\theta_{\hat{q}},\phi_{\hat{q}}\}$).

To calculate the average winning probability over all possible set of observables for Bob, without loss of generality, we fix observable $\mathcal{P}$ and take the average over the observable $\mathcal{Q}$. The average value of the above winning probability is therefore

$$\begin{aligned}&\mathbb{E}\big[\tfrac{1}{2}P_Q(0_{\mathcal{P}})+\tfrac{1}{2}P_Q(0_{\mathcal{Q}})\big]\\&=\frac{1}{8\pi}\int_0^{2\pi}\int_0^{\pi}[P_Q(0_{\mathcal{P}})+P_Q(0_{\mathcal{Q}})]\sin(\theta_{\hat{q}})d\theta_{\hat{q}}d\phi_{\hat{q}}\\&=\tfrac{1}{4}[2+\sin(\theta)\sin(\theta_{\hat{q}})\cos(\phi-\phi_{\hat{q}})+\cos(\theta)\cos(\theta_{\hat{q}})].\end{aligned} \tag{10}$$

The maximum of this quantity is $\frac{3}{4}$. This is also true if a spin-down outcome is chosen as the winning condition. In this scenario, inequality (8) becomes

$$P(b_{\mathcal{P}}|a_{\mathcal{S}})+P(b_{\mathcal{Q}}|a_{\mathcal{T}})\leqslant\tfrac{3}{2}. \tag{11}$$

When inequality (11) is violated, the state ρ_{AB} is steerable.

Pure entangled state. Consider that Alice prepares the two-qubit state

$$|\psi\rangle_{AB}=\sqrt{\alpha}|00\rangle_{AB}+\sqrt{1-\alpha}|11\rangle_{AB}. \tag{12}$$

When Bob decides to measure σ_z^B, Alice makes a spin measurement along the direction $\{\theta_{\hat{s}},\phi_{\hat{s}}\}$, corresponding to the observable $\mathcal{S}$. Similarly, if Bob measures σ_x^B, Alice measures along $\{\theta_{\hat{t}},\phi_{\hat{t}}\}$, corresponding to the observable $\mathcal{T}$. When $a=b=0$, the left-hand side of inequality (8) becomes

$$\begin{aligned}&P\big(0_{\sigma_z^B}|0_{\mathcal{S}_A}\big)+P\big(0_{\sigma_x^B}|0_{\mathcal{T}_A}\big)\\&=\frac{(4\alpha-1)\cos(\theta_{\hat{s}})+2\alpha+1}{(4\alpha-2)\cos(\theta_{\hat{s}})+2}+\frac{\sqrt{(1-\alpha)\alpha}\sin(\theta_{\hat{t}})\cos(\phi_{\hat{t}})}{(2\alpha-1)\cos(\theta_{\hat{t}})+1}.\end{aligned}$$

When $\alpha\neq 0$ or 1, the maximum value of $P(0_{\sigma_z^B}|0_{\mathcal{S}_A})+P(0_{\sigma_x^B}|0_{\mathcal{T}_A})$ is 2. This is achieved for the choices $\theta_{\hat{s}}=\phi_{\hat{s}}=\phi_{\hat{t}}=0$ and $\theta_{\hat{t}}=\arccos(1-2\alpha)$. According to our steering test, all pure entangled state are thus maximally steerable: the value of $P(b_{\mathcal{P}}|a_{\mathcal{S}})+P(b_{\mathcal{Q}}|a_{\mathcal{T}})$ is equal to its algebraic maximum.

When Alice and Bob both measure either σ_z or σ_x, the left-hand side of inequality (8) becomes

$$P\big(0_{\sigma_z^B}|0_{\sigma_z^A}\big)+P\big(0_{\sigma_x^B}|0_{\sigma_x^B}\big)=\tfrac{3}{2}+\sqrt{\alpha(1-\alpha)}. \tag{13}$$

According to scenario II, the state $|\psi\rangle_{AB}$ is steerable for any $\alpha\neq 0$ or 1. In this case, the violation of our steering inequality is a function of $\sqrt{\alpha(1-\alpha)}$. Similarly, the violation of the CHSH inequality for the state $|\psi\rangle_{AB}$ is given by $2\sqrt{1+4\alpha(1-\alpha)}$ [21]. Therefore, this specific choice of measurement allows us connect the CHSH violation with the violation of our steering inequality.

Werner states. Here we consider that Alice and Bob share ρ_{AB}^W [given by Eq. (4)]. To steer Bob's system in a specific basis, Alice measures the observable corresponding to this basis on her particle, i.e., $\mathcal{P}=\mathcal{S}$ and $\mathcal{Q}=\mathcal{T}$. When Bob chooses his observable from the set $\{\sigma_z^B,\sigma_x^B\}$, for $a=b=0$, the left-hand side of inequality (8) becomes $P(0_{\sigma_z^B}|0_{\sigma_z^A})+P(0_{\sigma_x^B}0_{\sigma_x^A})=1+p$, where $P(0_{\sigma_z^B},0_{\sigma_z^A})=P(0_{\sigma_x^B},0_{\sigma_x^A})=\frac{1+p}{4}$ and $P(0_{\sigma_z^A})=P(0_{\sigma_x^A})=\frac{1}{2}$, and the observables σ_z^A and σ_x^A are applied to the state $\rho_A^W=\mathrm{Tr}_B[\rho_{AB}^W]$. The maximum Bell violation of a Werner state is $2\sqrt{2}p$. In scenario I, Werner states are shown to be steerable for $p>\frac{1}{\sqrt{2}}$. This matches state-of-the-art experiments with two measurement settings [11,16]. In [4] it was shown how to prove that Werner states are steerable for $p>\frac{1}{2}$ in the limit of an infinite number of measurement settings. Using our inequality in scenario II, Werner states are shown to be steerable for $p>\frac{1}{2}$. Formally, the set of possible measurements is infinite, but only two are chosen by each party. Notice that $p>1/2$ is tight since for $1/3<p\leqslant 1/2$, Werner states are entangled but not steerable.

We now connect our steering inequality with the secret key rate in 1SDIQKD, according to scenario I. First, we show that Eq. (9) satisfies a monogamy relation. Consider that Alice, Bob, and Charlie share the state ρ_{ABC}. Bob's measurement settings are still supposed to be σ_z and σ_x. We show that, considered separately, Alice and Bob and Bob and Charlie cannot both satisfy inequality (9) at the same time. Defining $\mathcal{T}_{A,B}=P(b_{\mathcal{P}}|a_{\mathcal{S}})+P(b_{\mathcal{Q}}|a_{\mathcal{T}})$ and $\mathcal{T}_{B,C}=P(b_{\mathcal{Q}}|c_{\mathcal{T}'})+P(b_{\mathcal{P}}|c_{\mathcal{S}'})$, our monogamy relation is

$$\frac{1}{2}(\mathcal{T}_{A,B}+\mathcal{T}_{B,C})\leqslant 1+\frac{1}{\sqrt{2}}. \tag{14}$$

The proof is by contradiction. Assume that $\frac{1}{2}(\mathcal{T}_{A,B}+\mathcal{T}_{B,C})>1+\frac{1}{\sqrt{2}}$. Now consider the mixed terms $P(b_{\mathcal{P}}|a_{\mathcal{S}})+P(b_{\mathcal{Q}}|c_{\mathcal{T}'})$ and $P(b_{\mathcal{Q}}|a_{\mathcal{T}})+P(b_{\mathcal{P}}|c_{\mathcal{S}'})$. Their average value

is equal to $\frac{1}{2}(\mathcal{T}_{A,B}+\mathcal{T}_{B,C})$. Moreover, one of the terms has to be larger than or equal to their average. Assume without loss of generality that the first one is and consider the state obtained by measuring Alice's and Charlie's shares of ρ_{ABC} and obtaining $a_{\mathcal{S}}$ and $c_{\mathcal{T}'}$, respectively. This state satisfies $\frac{1}{2}[P(b_{\mathcal{P}})+P(b_{\mathcal{Q}})]>\frac{1}{2}+\frac{1}{2\sqrt{2}}$, contradicting the bound on the fine-grained uncertainty relation discussed earlier.

This relation can be applied to derive a lower bound on the key rate of a 1SDIQKD protocol. We consider an entanglement-based protocol, in which Alice and Bob measure a state ρ and postselect on outcome bits for which they chose either measurements $\{\mathcal{P},\mathcal{S}\}$ or $\{\mathcal{Q},\mathcal{T}\}$. Bob's measurements $\mathcal{P}$ and $\mathcal{Q}$ are assumed to be maximally noncommuting. Alice and Bob estimate the violation of the steering inequality, that is, the value k such that $\frac{1}{2}[P(b_{\mathcal{P}}|a_{\mathcal{S}})+P(b_{\mathcal{Q}}|a_{\mathcal{T}})]=\frac{1}{2}+\frac{1}{2\sqrt{2}}+k$. Then, from Eq. (14), $\frac{1}{2}[P(b_{\mathcal{P}}|c_{\mathcal{S}'})+P(b_{\mathcal{Q}}|c_{\mathcal{T}'})]\leqslant\frac{1}{2}+\frac{1}{2\sqrt{2}}-k$.

These bounds immediately translate into bounds on the key rate of the protocol. Denote the random variable representing Alice's, Bob's, and Charlie's outcome bits by A, B, and C. Then the key rate $r=I(B:A)-I(B:C)$ [22] satisfies $r\geqslant\log_2[(\frac{1}{2}+\frac{1}{2\sqrt{2}}+k)/(\frac{1}{2}+\frac{1}{2\sqrt{2}}-k)]$. For maximum violation, the key rate is 0.5. In comparison, a similar approach by Pawłowski and Brunner led to a key rate of 0.0581 [23].

To summarize, we derived a steering inequality based on fine-grained uncertainty relations. In Ref. [11] the authors considered the maximum of the average correlation of joint measurements in a LHS model, over all possible combinations of outcomes. In Ref. [10] the authors considered the minimum of Bob's conditional entropy in a LHS model, where the condition is on Alice's communicated outcome. Here we considered the maximum conditional probability distribution in LHS models, where the condition is again on Alice's outcome. Our inequality generalizes both previous works. In the derived inequality, we considered only the sum of uncertainties of a particular measurement outcome for the measurement of two different observables. Hence, we did not require the probability distribution of all possible permutation of measurement outcomes, as described in [10].

According to our steering inequality, all pure entangled states are maximally steerable. Moreover, a suitable choice of the setting connects the violation of our steering inequality with its CHSH violation. Our steering inequality leads to a tight test for Werner states, which may in turn lead to more experimental-friendly settings for demonstrating steering. We improve over earlier results by reducing the number of measurements from infinity to two. In particular, with two measurements on each side, the steering inequality of Saunders *et al.* [inequality (3)] can only prove that Werner states are steerable for $p>\frac{1}{\sqrt{2}}$; this result is recovered by our steering inequality in scenario I [inequality (9)]. With three (ten) measurements on each side, the inequality of Saunders *et al.* can demonstrate steerability for $p>\frac{1}{\sqrt{3}}$ (0.5236) [11]. This approach only leads to a tight test for Werner states in the limit of infinitely many measurement settings [4,11]. Our steering inequality [inequality (11)] detects the steerability of any Werner state with $p>\frac{1}{2}$ with two measurement settings on each side. Any steerable Werner state can thus be detected with our inequality with the minimum possible number of measurement settings. Finally, based on a monogamy relation of our steering inequality, we have proved that the violation can be used to place a lower bound on the key rate of a 1SDIQKD protocol secure against individual attacks. We leave it as an open problem to extend it to collective attacks.

The authors thank Damian Markham, Eleni Diamanti, Anthony Leverrier, and Tom Lawson for suggestions to enrich this work. A.S.M. acknowledges support from DST Project No. SR/S2/LOP-08/2013 (India). T.P. and M.K. acknowledge financial support from ANR Retour des Post-Doctorants NLQCC (ANR-12-PDOC-0022-01).

[1] A. Einstein, D. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935); **32**, 446 (1936).
[3] J. S. Bell, Physics **1**, 195 (1964) ; J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969); G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).
[4] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007); S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).
[5] M. D. Reid, Phys. Rev. A **40**, 913 (1989).
[6] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
[7] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, *ibid.* **49**, 1804 (1982); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *ibid.* **81**, 3563 (1998); J. W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Nature (London) **403**, 515 (2000).
[8] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).
[9] P. Chowdhury, T. Pramanik, A. S. Majumdar, and G. S. Agarwal, Phys. Rev. A **89**, 012104 (2014).
[10] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011); J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, Phys. Rev. A **87**, 062103 (2013).
[11] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).
[12] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
[13] T. Pramanik and A. S. Majumdar, Phys. Rev. A **85**, 024103 (2012).
[14] A. Dey, T. Pramanik, and A. S. Majumdar, Phys. Rev. A **87**, 012120 (2013).
[15] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[16] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

[17] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[18] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
[19] T. Pramanik, S. Mal, and A. S. Majumdar, arXiv:1304.4506.
[20] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010); R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, *ibid.* **7**, 757 (2011); C. Li, J. Xu, X. Xu, K. Li, and G.-C. Guo, *ibid.* **7**, 752 (2011).
[21] N. Gisin, Phys. Lett. A **154**, 201 (1991).
[22] I. Csiszàr and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[23] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).