Facets of the Leggett–Garg inequality: some recent studies

Dipankar Home

Center for Astroparticle Physics and Space Science, Bose Institute, Kolkata 700 091, India

In this article, we begin by briefly reviewing the basics of the Leggett–Garg inequality which is a temporal analogue of Bell's inequality, based on the notions of realism and noninvasive measurability. This is followed by outlining the core ideas and key results of two different types of recent studies related to the Leggett–Garg inequality, bringing out its ramifications concerning unsharp measurements and quantum key distribution respectively.

Keywords: Leggett–Garg inequality, noninvasive measurability, quantum cryptography, realism, unsharp measurements.

Introduction

CENTRAL to the classical world view is the basic notion of realism, defined by assuming that at *any* instant, a system is in a definite state for which all its observable properties have definite values, irrespective of any measurement. A remarkable line of study that enables to show that models of quantum mechanical (QM) phenomena based on the notion of realism can be experimentally constrained was ushered in by the discovery of Bell's inequality (BI)[1]. This led to an extensive study of the experimentally verifiable incompatibility between BI and QM, BI being an algebraic consequence of the notion of realism used in conjunction with the locality condition. Enriching this line of study, a stimulating ingredient is provided by the Leggett–Garg inequality (LGI)[2] that can be regarded as a temporal analogue of BI in terms of the time-separated correlation functions corresponding to successive measurement outcomes for a system whose state may evolve in time.

The notion of *realism* is invoked in deriving LGI by assuming that a system is at any given instant in a definite one of the available states having definite values for all its observable attributes, regardless of any measurement being actually performed. A further ingredient for obtaining LGI, replacing the locality condition underlying BI, is the notion of *noninvasive measurability* (NIM) which means assuming that it is possible, in principle, to determine which of the states the system is in, without affecting the state itself or the subsequent evolution of the system. Of course, as in the derivation of BI, the principle of *induction* is also used in deriving LGI by assuming that if one measures a quantity on a subset chosen at random from a given set, the result one gets should be typical of the set as a whole.

The experimentally verified incompatibility between LGI and the QM predictions in appropriate examples would thus signify repudiation of the notion of realism that includes the assumption of NIM. (Note that the conjunction of realism and NIM is often referred to as the notion of *macro-realism*). Therefore, while furnishing a signature of distinctly quantum behaviour, the QM violation of LGI can be regarded as complementing that of BI in providing valuable insight into the nature of physical reality as entailed by the nonclassicality of quantum systems[3,4]. Hence, it has been of considerable interest to investigate the extent to which LGI is violated by QM for various types of systems. The original motivation that led to LGI was to use it for probing the possible limits of QM in the macroscopic regime, e.g. in the context of suitable experiments involving the rf-SQUID device[5]. In recent years, a variety of theoretical and experimental studies (reviewed, for example, by Emary *et al.*[6]) have sought to bring out various fundamental implications of LGI, and have probed the QM violation of LGI pertaining to different types of micro-systems, ranging from, say, solid-state qubits[7], nuclear spins[8], electrons[9] to oscillating neutral kaons and neutrinos[10].

Against the above backdrop, the present article concentrates on providing a concise overview of the essential results of two different types of studies along earlier unexplored directions concerning LGI that we have recently carried out involving different collaborators. One of these[11] formulates what has been called *Wigner's form of LGI* (WLGI), with the robustness of the QM violation of WLGI being compared with that of the usual LGI with respect to *unsharp measurements*[11]. The other work probes the possibility of an application of LGI in the context of *Quantum Cryptography*[12]. We begin by first discussing the standard form of LGI and the robustness of its QM violation for unsharp measurements.

The Leggett–Garg inequality and unsharp measurements

Let us focus on a two-state system whose temporal evolution consists of oscillations between the states, say, 1 and

e-mail: dhome@jcbose.ac.in

2. Let $Q(t)$ be an observable quantity such that, whenever measured, it is found to take a value $+1(-1)$ depending on whether the system is in the state 1(2). Next, consider a collection of experimental runs starting from the identical initial state at $t = 0$ (say, the instant from which the temporal evolution is induced by switching on an external field), such that in the first series of runs Q is measured at times t_1 and t_2; in the second, at t_2 and t_3; in the third, at t_3 and t_4; and in the fourth, at t_1 and t_4 (here $t_1 < t_2 < t_3 < t_4$). From such measurements, it is straightforward to determine the temporal correlations $C_{ij} \equiv \langle Q(t_i)Q(t_j)\rangle$. Then it is possible to adapt in this context, the argument leading to a Bell-type inequality, with the times t_i of measurements playing the role of apparatus settings that can be chosen at will, and using the following consequence of the assumptions of *realism* and NIM that were mentioned earlier. For any collection of runs corresponding to the same initial state at $t = 0$, an individual $Q(t_i)$ has the same definite value, irrespective of the pair $Q(t_i)Q(t_j)$ in which it occurs; e.g. the value of $Q(t_i)$ in any pair does *not* depend on whether any prior or subsequent measurement has been made on the system. Consequently, the combination $[Q(t_1)Q(t_2) + Q(t_2)Q(t_3) + Q(t_3)Q(t_4) - Q(t_1)Q(t_4)]$ is always +2 or −2. Taking the averages of the individual product terms in this expression over the respective series of runs, and using the assumption of *induction* mentioned earlier, the following form of LGI can then be readily obtained pertaining to the entire ensemble of runs

$$K \equiv C_{12} + C_{23} + C_{34} - C_{14} \le 2, \tag{1}$$

which, thus, provides realist constraint on the empirically measurable quantities such as the time-separated correlation functions for any two-state oscillation. Now, to explain how the notion of NIM can be satisfied by invoking the idea of *negative result measurement* (NRM), let us consider, say, the case in which Q is measured at t_1, followed by at t_2, corresponding to the determination of a typical correlation function, say

$$C_{12} = P_{++}(t_1, t_2) - P_{+-}(t_1, t_2) + P_{--}(t_1, t_2) - P_{-+}(t_1, t_2), \tag{2}$$

where $P_{++}(t_1, t_2)$ is the joint probability of finding the particle in the state 1 at both the instants t_1 and t_2; similarly, for $P_{+-}(t_1, t_2)$, $P_{--}(t_1, t_2)$, $P_{-+}(t_1, t_2)$ Note that the derivation of LGI requires essentially the *first measurement* of each such pair to satisfy NIM. This can be ensured through the NRM procedure as follows.

Let the measuring set-up be arranged so that if, say, the probe is triggered, $Q(t_1) = +1$, while if it is *not*, $Q(t_1) = -1$, thereby ensuring in the latter case that while the untriggered probe provides information about the value of Q, there is no interaction occurring between the probe and the measured particle; in other words, the condition of NIM is then satisfied. Now, if the results of those runs are only used for which $Q(t_1) = -1$, followed by the measurement of Q at t_2, discarding the results of the rest runs, these results can be used for determining the joint probabilities $P_{-+}(t_1, t_2)$ and $P_{--}(t_1, t_2)$. Similarly, for determining the other two joint probabilities $P_{+-}(t_1, t_2)$ and $P_{++}(t_1, t_2)$ occurring in C_{12}, the measuring set-up can be inverted so that a value of $Q(t_1) = -1$ triggers the probe, while for $Q(t_1) = +1$, it does *not*. In this way, one can determine C_{12} and, similarly, all the two-time correlation functions occurring in LGI by ensuring NIM through the use of the NRM procedure for the first measurement of any pair.

Any violation of LGI thus obtained can then be taken to repudiate the notion of realism because, as Leggett and his coworkers[2–4] have argued, the 'realist' statement that the particle 'is' in a definite state corresponding to a definite value of Q at any instant loses any meaning if the state can be affected by the NRM procedure, thereby implying that NIM is a logical corollary of realism in the context of NRM. It is, therefore, necessary to invoke the NRM procedure in order to ensure NIM which can help achieve loophole-free empirical scrutiny of LGI in a way that can be regarded as a clear test of realism defined in the sense stated earlier. Here it may be noted that recently, it has also been argued that NIM necessarily implies the notion of realism[13].

Now, having clarified the relevant basics, let us write the general form of LGI involving n pairs expressed in the following way[6]

$$-n \le K_n \le n - 2, \qquad \text{for odd } n \ge 3,$$

$$-(n-2) \le K_n \le n - 2, \qquad \text{for even } n \ge 4, \tag{3}$$

where $K_n = C_{21} + C_{32} + C_{43} + \ldots + C_{n(n-1)}$, and the correlation function $C_{ij} = \langle Q_i Q_j\rangle$. Considering a typical two-state oscillation, we are focussing here on a system oscillating between the two states $|A\rangle$ and $|B\rangle$ which are degenerate orthogonal eigenstates of the Hamiltonian H_0 corresponding to energy E_0, with a perturbing Hamiltonian H' inducing oscillatory transition between these two states, with $\langle A|H'|B\rangle = \langle B|H'|A\rangle = \Delta E$, and $\langle A|H'|A\rangle = \langle B|H'|B\rangle = E'$. The key point here is that at any instant, such a system is found to be either in the state $|A\rangle$ or in the state $|B\rangle$ corresponding to the measurement of the dichotomic observable $Q = |A\rangle\langle A| - |B\rangle\langle B| = P_+ - P_-$, where $P_+ = |A\rangle\langle A|$, $P_- = |B\rangle\langle B|$. Let the initial state at t_1 be of the general form $\rho_0(t_1) = |\psi_0\rangle\langle\psi_0|$, where

$$|\psi_0\rangle = \cos\theta|A\rangle + \exp(i\phi)\sin\theta|B\rangle, \tag{4}$$

and $\theta, \phi \in [0, \pi/2]$. For the above state, the probability of obtaining the measurement outcome, say, +1 at the instant t_1 is given by $\mathrm{tr}(\rho_0(t_1)P_+)$, and after this measurement, the pre-measurement state $\rho_0(t_1)$ changes to the state given by $\rho_+(t_1) = P_+\rho_0(t_1)P_+^\dagger/\mathrm{tr}(\rho_0(t_1)P_+)$ where $P_+ = |A\rangle\langle A| = P_+^\dagger$. Subsequently, the post-measurement

state evolves under the Hamiltonian $H = H_0 + H'$ to the state $\rho'_+(t_2) = U_{\Delta t\rho} + (t_1)U^{\dagger}_{\Delta t}$ at a later instant t_2 where $U_{\Delta t} = \exp(-iH\Delta t)$, taking $\hbar = 1$ and $\Delta t = t_2 - t_1$. Then, considering the subsequent measurement of Q at the instant t_2, the QM value of, say, the joint probability of obtaining both the outcomes +1 at the instants t_1 and t_2 is given by

$$P(Q_1+,\ Q_2+) = \mathrm{tr}(\rho_0(t_1)P_+)\mathrm{tr}(\rho'_+(t_2)P_+)$$

$$= \mathrm{tr}(U_{\Delta t}(P_+\rho_0(t_1)P_+)U^{\dagger}_{\Delta t}\ P_+) = \cos^2\theta\cos^2\tau, \quad (5)$$

where $\tau = \Delta E\Delta t$ (in the units of $\hbar = 1$), and the expression for the unitary matrix $U_{\Delta t} = \exp(-iH\Delta t)$ is as follows

$$U_{\Delta t} = \mathrm{e}^{-i(E_0+E')\Delta t}[\cos\tau\mathbb{I} - i\sin\tau(|A\rangle\langle B| + |B\rangle\langle A|)]. \quad (6)$$

Using similar expressions for other joint probabilities, one can therefore compute the QM values of relevant correlations functions for any initial state and study the QM incompatibility with LGI for the two-state oscillation under consideration. For any given n, pertaining to the general form of LGI given by eq. (3), the maximum QM value of K_n is then found to be $n\cos(\pi/n)$ (ref. 6). Hence, if the QM predictions are to *violate* eq. (3), the following inequality needs to hold good for any n

$$n\cos(\pi/n) > n - 2. \quad (7)$$

Note that the above treatment is valid essentially assuming ideal measurements. Next, we turn to examining the robustness of the QM violation of LGI in the context of *unsharp measurements*; i.e. if the relevant measurements are 'non-ideal'. In order to address this question, we take recourse to the formalism of what is known as *unsharp measurement*[14–18] which can be regarded as a particular case of commutating POVM. Note that for an *ideal* measurement of the dichotomic observable under consideration given by $Q = |A\rangle\langle A| - |B\rangle\langle B| = P_+ - P_-$, the respective probabilities of the outcomes ± 1 and the way a measurement affects the observed state are determined by the projection operators that can be written as $P_\pm = (1/2)(\mathbb{I} \pm Q)$ where $\mathbb{I} = |A\rangle\langle A| + |B\rangle\langle B|$.

Now, in order to capture the effect of imprecision involved in a *non-ideal* measurement, using the formalism of unsharp measurement[14–18], a parameter (λ) known as the sharpness parameter is introduced to characterize the precision of a measurement by defining what are referred to as the effect operators given by

$$F_\pm = (1/2)(\mathbb{I} \pm \lambda Q) = \lambda P_\pm + (1 - \lambda)\mathbb{I}/2, \quad (8)$$

where $(1 - \lambda)$ denotes the amount of white noise present in any unsharp measurment ($0 < \lambda \le 1$), and $F_\pm$ are mutually commuting operators with non-negative eigenvalues; $F_+ + F_- = \mathbb{I}$, while for $\lambda = 1$ corresponding to sharp measurements, $F_\pm$ reduce to projection operators $P_\pm$. Here an important point is that, instead of the projection operators used in the case of an ideal measurement, in an unsharp measurement, the operators $F_\pm$ determine the respective probabilities of the outcomes and the way a premeasurement state changes due to measurement.

Considering the generalized *Lüders* operations, for a specific type of unsharp measurement pertaining to a given state ρ, the probability of an outcome, say, +1 is given by $\mathrm{tr}(\rho F_+)$ for which the post-measurement state is given by $(\sqrt{F_+}\rho\sqrt{F_+^{\dagger}})/\mathrm{tr}(\rho F_+)$. Thus, in a given experiment, by estimating the difference between the actually observed probability of an outcome and the corresponding predicted value for an ideal experiment, the sharpness parameter λ pertaining to the experiment in question can be determined. This gives an operational significance to the parameter λ.

Now, using eq. (8) and by following the prescription outlined above, it is found that for unsharp measurements, if the QM predictions are to *satisfy* the general form of LGI given by eq. (3), the following inequality needs to hold good

$$\lambda^2 n\cos(\pi/n) \le n - 2, \quad (9)$$

for any n, which implies

$$\lambda \le \sqrt{\frac{n-2}{n\cos(\pi/2)}}. \quad (10)$$

By evaluating the derivative of the RHS of eq. (10) with respect to n, it is found that as n increases ($n \ge 3$), the RHS of eq. (10) also increases, thereby implying an increase in the critical value of λ (denoted by, say, λ_c) above which, as measurements become more precise, the QM results can *violate* the general form of LGI given by eq. (3). The *minimum value* of $\lambda_c (= \sqrt{2/3} \approx 0.816)$ occurs for $n = 3$. For $n = 4$, λ_c is given by $(1/2)^{1/4} \approx 0.84$, which is the same as the corresponding λ_c obtained for the Bell–CHSH inequality.

Wigner's form of the Leggett–Garg inequality and unsharp measurements

It is interesting that closely following the discovery of Bell's inequality, Wigner[19] had derived a different form of the local realist inequality applicable to the EPR-Bohm bipartite entangled state, that has only recently been generalized for any multipartite state[20]. Here we discuss the temporal version of Wigner's inequality[11] pertaining to an ensemble of systems undergoing temporal oscillation between the two states 1 and 2, as considered while deriving LGI. Wigner's argument requires assuming, as a

consequence of *realism*, the existence of overall joint probabilities, say, $\rho(Q_1, Q_2, Q_3)$ where Q_i is the outcome (± 1) of measuring Q at $t_i (i = 1, 2, 3)$ involving different combinations of outcomes of the relevant measurements. Here the assumption of *noninvasive measurability* implies that such overall joint probabilities would remain unaffected by measurements, and hence, by appropriate marginalization, the pairwise observable joint probabilities can be obtained. For example, the observable joint probability $P(Q_{1+}, Q_{2+})$ of obtaining the outcomes +1 and +1 for the sequential measurements of Q at the instants t_1 and t_2 respectively, can be written as

$$P(Q_{1+}, Q_{2+}) = \sum_{Q_3 = \pm} \rho(+,+,Q_3)$$

$$= \rho(+,+,+) + \rho(+,+,-). \qquad (11)$$

Writing similar expressions for the other measurable marginal joint probabilities, say, $P(Q_{1-}, Q_{3-})$ and $P(Q_{2+}, Q_{3-})$, one obtains

$$P(Q_{1+}, Q_{2+}) + P(Q_{1-}, Q_{3-}) - P(Q_{2+}, Q_{3-})$$

$$= \rho(+,+,+) + \rho(-,-,-). \qquad (12)$$

Then, invoking non-negativity of the joint probabilities occurring on the RHS of eq. (12), the following form of what may be called *Wigner's form of LGI* (WLGI) can be obtained in terms of three pairs of two-time joint probabilities

$$P(Q_{2+}, Q_{3-}) - P(Q_{1+}, Q_{2+}) - P(Q_{1-}, Q_{3-}) \le 0. \qquad (13)$$

Similarly, other forms of WLGI involving three pairs of two-time joint probabilities can be derived using various combinations of the observable joint probabilities. The complete set of such three-term WLGIs has been given in Saha *et al.*[11] which also provides the general form of WLGI in terms of n pairs of two-time joint probabilities. However, for illustrating the basic relevant features concerning the efficacy of WLGI, it suffices to confine attention to essentially three-term WLGIs.

Pertaining to the specific two-state oscillation considered earlier section in the text, a comprehensive study using three-term WLGIs as discussed in Saha *et al.*[11], reveals that while the QM violation of all the three-term WLGIs depends on the initial state, among all these inqualities, the maximum QM violation is obtained for the inequality in eq. (13), for the initial state given by eq. (4) when $\theta = 1.0666$ rad and $\phi = \pi/2$, whence the QM value of the left-hand side is ≈ 0.5043 taking the time interval $t_2 - t_1 = t_3 - t_2 = \Delta t$, such that $\tau = \Delta E \Delta t = 1.0083$ (in the units of $\hbar = 1$).

Now, in order to probe the effect of 'non-ideal' or unsharp measurements on the QM violation of WLGI, taking the parameters characterizing the initial state and the time evolution to be the same (as mentioned above) for which the QM violation of WLGI in eq. (13) is maximum for ideal measurements, the QM value of the LHS of WLGI in eq. (13) is a function of the sharpness parameter λ, given by the following form

$$P(Q_{2+}, Q_{3-}) - P(Q_{1+}, Q_{2+}) - P(Q_{1-}, Q_{3-})$$

$$= 0.3816\lambda(1 - \sqrt{1 - x^2} + 0.3726\lambda^2 - 0.25). \qquad (14)$$

Since the expression on the RHS of eq. (14) is a monotocially increasing function of $\lambda \in (0, 1]$, the solution of the equation involving this expression put to zero provides the critical value of λ above which, as measurements become more precise, WLGI in eq. (13) can be violated by the QM results. It is then checked that the only solution of such an equation within the allowed range of values of λ is approximately 0.69. Thus, the critical value of λ in this case is $\lambda_c \approx 0.69$, i.e. within this bound of λ for unsharp measurements, the QM results always satisfy WLGI in eq. (13). Now, comparing this value with the value of λ_c for the three-term LGI (which is also the minimum value of λ_c for any n-term LGI, as discussed earlier), it is seen that for the range of values of $\lambda \in (0.69, 0.816]$, the QM violation of WLGI can occur for unsharp or imprecise measurements, whereas in such situations no violation of LGI can be shown. This, therefore, shows the *nonequivalence* between WLGI and LGI.

It should be stressed that the above results pertain to the choice of a two-level system subjected to a suitable interaction causing temporal oscillation between the two states, and the study is based on a restricted class of generalized measurements characterized by the model of unsharp measurements that involves commuting POVMs. Here it is pertinent to note that recently the QM violation of LGI for multilevel systems has been studied[21]. Hence, a similar study is required using WLGI, apart from extending the comparative study between WLGI and LGI by considering different types of generalized measurements.

Application of the Leggett–Garg inequality for quantum key distribution

While in recent years there has been considerable upsurge of interest in studying various aspects of LGI, curiously, the question as to whether LGI can have any relevance in the context of quantum cryptography has yet remained unexplored. In this section we indicate a possible line of application of LGI for ensuring security against eavesdropping in a quantum key distribution (QKD) scheme that has recently been suggested[12]. We begin by briefly recapitulating the relevant basics.

The Bennett–Brassard 1984 (BB84) scheme was the first suggested QKD protocol that allows two remote

agents Alice and Bob to privately share a random bit string[22]. Based on quantum features like no-cloning and imperfect distinguishability of non-orthogonal states, it has been argued that such a QKD protocol can have unconditional security in the sense of being not dependent on any computational power[23]. On the other hand, the E91 QKD protocol was proposed by Ekert[24] that uses entangled pairs to generate secret bits with the security arising from detecting the violation of a Bell-type inequality. The underlying intuition is that if an eavesdropper Eve intervenes, the amount of violation of a Bell-type inequality would be affected and this would reveal her presence. Subsequently, another entanglement-based QKD scheme was proposed that was argued to be equivalent with the BB84 scheme[25]. Thereafter, a number of security proofs pertaining to a variety of attacks on the transmission channel have endowed quantum cryptography with considerable richness.

However, it has recently been realized that the unconditional security proofs of the QKD schemes have limited practical value because they depend on assuming that all the devices used for state preparation and measurements are *trusted* and *well characterized*. Certain sophisticated attack, known as the *device attack* (as opposed to the usually considered *channel attack* where Eve intercepts the transmitted states) can occur where, for example, in the BB84 scheme, the eavesdropper Eve may herself be the vendor who supplies states and devices to Alice and Bob. The cryptographic scenario in which one seeks to ensure security against device attacks is known as the *device-independent* (DI) scenario[26,27]. While BB84 is unconditionally secure against channel attacks, it is not secure in the DI scenario. On the other hand, the E91 scheme is secure in the DI scenario and the use of entanglement, involving the violation of Bell's inequality, is believed to be a necessary condition for DI security[27].

Given the above background, we will now outline the basic ideas of the recent attempt[12] made to ensure security of the BB84 scheme in a DI scenario using a particular version of LGI proposed by Brukner *et al.*[28] that is explained as follows. Let x_{t_1}, x'_{t_1} denote the measurement outcomes (± 1) at the instant t_1 for the observables x, x' respectively, while y_{t_2}, y'_{t_2} are the measurement results (± 1) at the instant t_2 for the observables y, y' respectively. Then, as a consequence of the assumptions of *realism* and *NIM*, similar to the argument used in deriving LGI given by the inequality in eq. (1), the following algebraic identity can be argued to be holding good for the predetermined measurement outcomes: $x_{t_1}(y_{t_2}, y'_{t_2}) + x'_{t_1}(y_{t_2} - y'_{t_2}) = \pm 2$. After averaging over many runs of a series of measurements, the form of LGI relevant to our discussion is then given by

$$\Lambda \equiv |\langle x_{t_1} y_{t_2} + x_{t_1} y'_{t_2} + x'_{t_1} y_{t_2} - x'_{t_1} y'_{t_2} \rangle| \leq 2, \qquad (15)$$

where Alice (Bob) has the choice of measuring the observables $x(y)$ or $x'(y')$ at the instants t_1 and t_2 respectively, where $t_2 > t_1$. Note that, unlike the other usual forms of LGI, this particular form does not involve time evolution of the system in any external field, and may be regarded as the temporal version of the Bell-CHSH inequality. Now, let us proceed to discuss how the above form of LGI can be invoked in the context of the BB84 protocol for ensuring security against a specific device attack known as the AGM attack[27].

We recall that the BB84 protocol involves Alice's transmission of states randomly prepared in the Pauli spin bases, X or Z. Bob makes random measurements in one of these two bases. Over a classical channel, Alice and Bob determine the cases where their bases match, discarding the rest. If Eve intercepts Alice's transmission to acquire information, because of the information-vs-disturbance trade-off, she inevitably disrupts the BB84 statistics, which is then detected by Alice and Bob. This constitutes the essential security of BB84. Here it is implicitly assumed that the devices used by Alice and Bob are *trustworthy* and that they are measuring the properties of the *same* particle. In a DI scenario, Eve can cheat by having them measure different particles by providing them the separable state[27] given by

$$\rho_{AB} = \frac{1}{4}(\Pi_{00}^{(12)} + \Pi_{11}^{(12)}) \otimes (\Pi_{++}^{(34)} + \Pi_{--}^{(34)}), \qquad (16)$$

where Π_{xy} indicates projector to the state $|x, y\rangle$. The bracketed superscripts in the definition of ρ_{AB} are particle labels. Eve has so arranged the devices such that particles 1 and 3 (2 and 4) are with Alice (Bob). When Alice and Bob measure $Z(X)$, they measure particles 1 and 2 (3 and 4). Notice that this reproduces the BB84 statistics, but after the public announcement of basis by Alice and Bob, Eve has the 'hidden variable' pertaining to the specific pair of particles Alice and Bob measure, whence she can find out their secret bit (0 or 1) with certainty without introducing any disturbance.

Here Eve's cheating hinges on the fact that Alice and Bob believe their system to be a single system of dimension two (a qubit), while in fact they are accessing a system of higher (= 16) dimensionality. Thus, it becomes crucial to rule out the so-called hidden dimensions of the Hilbert space describing the quantum systems used for QKD. For this purpose, a *modified BB84 protocol* has been proposed[12] that involves a type of DI security test using the form of LGI given by the inequality in eq. (15). The key steps of this scheme (called the *LG-BB84 protocol*) are as follows:

(i) An additional basis $M_{\pm} \equiv 1/\sqrt{2}(X \pm Y)$ is introduced at Bob's end, while Alice prepares the transmitted states randomly in X or Y basis.

(ii) Bob measures the incoming states randomly in X, Y or $M_{\pm}$ basis. Subsequently, Alice and Bob announce their preparation and measurement bases respectively.

(iii) If Alice and Bob's bases of preparation and measurement *match*, this results in a secret key.

(iv) For the *mismatch* of the bases corresponding to Bob's measurement in the X or Y basis, the measurement results are discarded, while for the measurement of Bob in the $M_{\pm}$ basis, the outcomes are used to test the violation of the form of LGI obtained from eq. (15) by replacing $x(x')$ and $y(y')$ with $X(Y)$ and $M_{+}(M_{-})$ respectively. Here Alice has a choice of preparing the state of her particle to be X or Y at the instant t_1, while Bob measures at $t_2(t_2 > t_1)$ in either M_{+} or M_{-} basis.

Eve's intervention in terms of cheat states can be detected in such a LG-BB84 scheme essentially because the LGI violating temporal correlation cannot be established by making measurements on two different particles. The LGI test thus serves to check whether Bob has received the *same* particle that Alice had transmitted. The relevant technical details have been discussed in Shenoy *et al.*[12] pertaining to an eavesdropping model, which is a combination of channel attack and device attack for which Eve mixes with the legitimate BB84 states a fraction of cheat states given by eq. (16), thereby demonstrating that the condition for security in the LG-BB84 protocol (i.e. when the error rate is less than a given tolerable limit) is equivalent to the requirement that Alice–Bob correlation data violate LGI. The computed error rate as well as the LGI violation observed by Alice and Bob critically depend on the fraction of cheat states present in the device attack.

To put it in a nutshell, the proposed LG-BB84 scheme goes beyond the usual BB84 protocol in ensuring security in a typical DI scenario. Importantly, this is achieved *without* the need to make use of entanglement; this is in *contrast* to all the proposed QKD protocols to-date that have been considered in the DI scenario.

It needs to be mentioned that in the treatment given here, it has been assumed that the cheat states are not transmitted and that devices used are 'memory-less'. The cryptographic scenario in which the former assumption does not hold good is known as the semi-device-independent scenario[29]. If the latter assumption is not made, 'memory attacks'[30] are allowed in which devices procured from adversial suppliers may reveal information about inputs and outcomes of earlier runs through the public communication channel used in the subsequent runs. It should be worthwhile to investigate what form of LGI can be used to suitably extend the LG-BB84 scheme to those DI scenarios which involve general attacks such as the ones mentioned above.

Concluding remarks

One-type of study discussed in this article formulates and compares Wigner's form of LGI with the usual LGI in terms of the robustness of their respective QM violations in the context of unsharp or non-ideal measurements which are treated by invoking a particular model of such measurements that has been widely discussed. Interestingly, this study indicates the possibility of using the QM violation of LGI in order to empirically probe the applicability of such a model of unsharp measurements with respect to any given non-ideal measurement set-up.

On the other hand, the other study discussed here seeks to bring out that LGI can be an important ingredient of quantum cryptography. Thus, this opens up a hitherto unexplored line of investigation concerning practical uses of LGI in the area of quantum information.

To summarize, the diversity of the studies reported in this article serves to underscore the potentiality of LGI as a powerful tool having varied ramifications, ranging from quantum foundations to quantum information.

1. Bell, J. S., On the Einstein Podolsky Rosen paradox. *Physics*, 1964, **1**(3), 195–200.
2. Leggett, A. J., and Garg, A., Quantum mechanics versus macroscopic realism: is the flux there when nobody looks? *Phys. Rev. Lett.*, 1985, **54**(9), 857–860; Leggett, A. J., Experimental approaches to the quantum measurement paradox. *Found. Phys.*, 1988, **18**(9), 939–952.
3. Leggett, A. J., Testing the limits of quantum mechanics: motivation, state of play, prospects. *J. Phys.: Condens. Matter*, 2002, **14**(15), R415–R451.
4. Leggett, A. J., Realism and the physical world. *Rep. Prog. Phys.*, 2008, **71**(2), 022001-1 to 022001-6.
5. van der Wal, C. H. *et al.*, Quantum superposition of macroscopic persistent-current states. *Science*, 2000, **290**(5492), 773–777; Friedman, J. R. *et al.*, Quantum superposition of distinct macroscopic states. *Nature*, 2000, **406**(6791), 43–46.
6. Emary, C, Lambert, N. and Nori, F., Leggett–Garg inequalities. *Rep. Prog. Phys.*, 2014, **77**(1), 016001-1 to 016001-25; Corrigendum, *Rep. Prog. Phys.*, 2014, **77**(3), 039501.
7. Waldherr, G., Neumann, P., Huelga, S. F., Jelezko, F. and Wrachtrup, J., Violation of a temporal Bell inequality for single spins in a diamond defect center. *Phys. Rev. Lett.*, 2011, **107**(9), 090401-1 to 090401-4.
8. Athalye, V., Roy, S. S. and Mahesh, T. S., Investigation of the Leggett–Garg inequality for precessing nuclear spins. *Phys. Rev. Lett.*, 2011, **107**(13), 130402-1 to 130402-5; Katiyar, H., Shukla, A., Rao, K. R. K. and Mahesh, T. S., Leggett–Garg inequalities. *Phys. Rev. A*, 2013, **87**(5), 052102-1 to 052102-5.
9. Emary, C., Lambert, N. and Nori, F., Leggett–Garg inequality in electron interferometers. *Phys. Rev. B*, 2012, **86**(23), 235447-1 to 235447-10.
10. Gangopadhyay, D., Home, D. and Roy, A. S., Probing the Leggett–Garg inequality for oscillating neutral kaons and neutrinos. *Phys. Rev. A*, 2013, **88**(2), 022115-1 to 022115-5.
11. Saha, D., Mal, S., Panigrahi, P. K. and Home, D., Wigner's form of the Leggett–Garg inequality, the no-signaling-in-time condition, and unsharp measurements. *Phys. Rev. A*, 2015, **91**(3), 032117-1 to 032117-7.
12. Shenoy, A. H., Aravinda, S., Srikanth, R. and Home, D., Exploring the role of Leggett–Garg inequality for quantum cryptography; arXiv:1310.0438[quant-ph].
13. Clemente, L. and Kofler, J., Necessary and sufficient conditions for macroscopic realism from quantum mechanics. *Phys. Rev. A*, 2015, **91**(6), 062103-1 to 062103-9.
14. Busch, P., Unsharp reality and joint measurements for spin observables. *Phys. Rev. D*, 1986, **33**(8), 2253–2261.
15. Busch, P., Grabowski, M. and Lahti, P. J., *Operational Quantum Physics, Lecture Notes in Physics Monographs*, Springer, New York, 1995, vol. 31.

16. Busch, P., Quantum states and generalized observables: a simple proof of Gleasons theorem. *Phys. Rev. Lett.*, 2003, **91**(12), 120403-1 to 120403-4.
17. Spekkens, R. W., Contextuality for preparations, transformations, and unsharp measurements. *Phys. Rev. A*, 2005, **71**(5), 052108-1 to 052108-17.
18. Busch, P. and Jaeger, G., Unsharp quantum reality. *Found. Phys.*, 2010, **40**(9–10), 1341–1367.
19. Wigner, E. P., On hidden variables and quantum mechanical probabilities. *Am. J. Phys.*, 1970, **38**(8), 1005–1009.
20. Home, D., Saha, D. and Das, S., Multipartite Bell-type inequality by generalizing Wigner's argument. *Phys. Rev. A*, 2015, **91**(1), 012102-1 to 012102-6.
21. Budroni, C. and Emary, C., Temporal quantum correlations and Leggett–Garg inequalities in multilevel systems. *Phys. Rev. Lett.*, 2014, **113**(5), 050401-1 to 050401-5.
22. Bennett, C. H. and Brassard, G., Quantum cryptography: public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984, pp. 175–179.
23. Shor, P. W. and Preskill, J., Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 2000, **85**(2), 441–444.
24. Ekert, A. K., Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 1991, **67**(6), 661–663.
25. Bennett, C. H., Brassard, G. and Mermin, N. D., Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 1992, **68**(5), 557–559.
26. Barrett, J., Hardy, L. and Kent, A., No signaling and quantum key distribution. *Phys. Rev. Lett.*, 2005, **95**(1), 010503-1 to 010503-4.
27. Acín, A., Gisin, N. and Masanes, L., From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 2006, **97**(12), 120405-1 to 120405-4.
28. Brukner, C., Taylor, S., Cheung, S. and Vedral, V., Quantum entanglement in time; arXiv:quant-ph/0402127.
29. Pawlowski, M. and Brunner, N., Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A*, 2011, **84**(1), 010302(R)-1 to 010302(R)-4.
30. Barrett, J., Colbeck, R. and Kent, A., Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 2013, **110**(1), 010503-1 to 010503-5.

ACKNOWLEDGEMENT. I thank the Department of Science and Technology, New Delhi for support (SR/S2/LOP-08/2013).

doi: 10.18520/v109/i11/1980-1986