Pramana – J. Phys. (2019) 93:67
https://doi.org/10.1007/s12043-019-1830-3

Violation of space–time Bell-CHSH inequality beyond the Tsirelson bound and quantum cryptography

C S SUDHEER KUMAR

NMR Research Centre and Department of Physics, Indian Institute of Science Education and Research, Pune 411 008, India
E-mail: sudheer.kumar@students.iiserpune.ac.in

MS received 25 June 2018; revised 26 April 2019; accepted 22 May 2019

Abstract. Here we show that if we insert context-dependent local unitary evolutions into the spatial (i.e. normal) Bell–Clauser–Horne–Shimony–Holt (Bell-CHSH) test, then it is possible to violate the space–time Bell-CHSH inequality maximally (i.e. up to 4). The correct context dependency can be achieved via post-selection. However, this does not contradict the Tsirelson quantum bound ($2\sqrt{2}$), because the latter has been derived without taking into consideration the context-dependent unitary evolutions and/or post-selection. As an important application, this leads to a more efficient (in terms of resource (singlets) and classical communication) and more sensitive (to eavesdropping) quantum key distribution (QKD) protocol, compared to Ekert's and Wigner's QKD protocols.

Keywords. Space–time Bell–Clauser–Horne–Shimony–Holt test; quantum key distribution; unitary evolution; post-selection.

PACS Nos 03.67.Dd; 03.65.Ta; 03.65.Ud

1. Introduction

'Correlations cry out for explanation' – Bell [1]. Assuming superquantum correlations (Popescu–Rohrlich (PR) box) and no signalling (i.e. superluminal communication is not possible), Popescu and Rohrlich [2] have shown that one can violate Bell's inequality [3–5] up to its algebraic bound (i.e. 4). Cabello [6] has also proposed a post-selection (on GHZ state)-based Bell test to achieve an algebraic bound. Here we propose yet another scheme to achieve the same. In the spatial (i.e. normal) Bell–Clauser–Horne–Shimony–Holt (Bell-CHSH) test, there is no unitary evolution. Alice and Bob randomly choose their observables and directly measure them locally on their respective entangled qubit states. As entangled particles are correlated over space in spite of measurement events being space-like separated (non-local correlation), the correlation between Alice's and Bob's measurement outcomes can go up to $2\sqrt{2}$, thereby violating the local realistic bound 2 [5].

Here we show that it is possible to boost the correlation over space (which led to $2\sqrt{2}$) further via context-dependent local unitary evolutions. But this requires for Bob to know what Alice has measured (i.e. Alice's choice of her observable only, but not her outcome of measuring the corresponding observable), which is not possible unless Alice can signal Bob (because they are space-like separated) [7]. Hence, to avoid the need for signalling, we provide an alternative scheme wherein Bob applies local unitary operations randomly, and then measures his observables. After all the measurements are performed, Alice and Bob post-select correct context-dependent local unitarily evolved states via classical communication (CC). By this procedure, Alice and Bob can achieve maximum possible correlation (i.e. 4) between their observables. However, this does not contradict the Tsirelson quantum bound ($2\sqrt{2}$), as the latter has been derived without taking into consideration the context-dependent local unitary evolutions and/or post-selection [5,8].

As an important application, our new scheme leads to a more efficient and more sensitive (to eavesdropping) quantum key distribution (QKD) protocol. QKD or quantum cryptography is a provably secure protocol using which private key bits can be generated between two parties over a public channel [5]. Security of QKD protocols is based on the fact that an eavesdropper

Published online: 07 August 2019

cannot steal the information without disturbing the quantum state [9–23]. Suppose Alice wants to send Bob a secret message 'Hi'. They somehow have shared a secret key 'qw' (e.g. they met personally in the past and shared (but this is not always feasible) or via QKD). Alice mixes her secret message with the secret key (encryption) and obtains 'Hi + qw = rd'. Alice sends 'rd' to Bob over a public channel. Then Bob decrypts the message to retrieve the original secret message: 'rd − qw = Hi'.

There are many types of QKD protocols, chief among them are as follows: BB84 [24] and its variants (not based on Bell's theorem for security) [5,25–27], Ekert's [28] QKD protocol and its variants [29,30], and device-independent QKD protocols which use entanglement and/or violation of Bell's inequality for their security [9,23,31–34], QKD via orthogonal states [35,36], (semi)counterfactual QKD protocols [9,37–39], continuous variable QKD protocols [9,40–44] and doing QKD considering noise in the channel [45,46].

Our space–time (ST) QKD protocol exploits violation of Bell's inequality for security. In our ST QKD protocol, half of the total resource (singlets) corresponds to the correct context-dependent unitarily evolved states. A small randomly chosen subset of this is utilised to test for eavesdropping, and the remaining large portion is utilised for secret key bits generation. We are going to show that our ST QKD protocol is more efficient (in terms of resource (singlets) and CC required to generate a given amount of secret key bits), and more sensitive (to eavesdropping) than Ekert's and Wigner's QKD protocols. QKD has become important, because the security of public key distribution protocols, like RSA, is under threat with the advent of quantum computers, which can find the prime factors of large numbers in polynomial time (Shor's algorithm) [5,47].

In §2 we describe the ST Bell-CHSH test using post-selection. In §3 we propose our ST QKD protocol and compare it with the other existing QKD protocols, and finally we summarise and conclude in §4.

2. ST Bell-CHSH test

Let Alice and Bob share N number of singlets:

$$|S_0\rangle = (|01\rangle - |10\rangle)/\sqrt{2} = -(|+-\rangle - |-+\rangle)/\sqrt{2},$$

where $|0\rangle, |1\rangle$ are eigenkets of Pauli-z matrix σ_z with eigenvalues $+1, -1$, respectively, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice's and Bob's clocks are synchronised and their measurement events are space-like separated. At time $t = t_j^A$, Alice measures locally the observable

$$A = \sigma_z \otimes I \quad \text{or} \quad C = \sigma_x \otimes I$$

on her jth qubit state (i.e. she measures σ_z or σ_x on her qubit state), according to the outcome of an unbiased coin toss, $j = 1, 2, \ldots, N$, I is the 2×2 identity matrix. Immediately after Alice's measurement, Bob applies the unitary operator

$$U_{\pm y} = \exp\left(\mp \mathrm{i}\frac{\pi}{4}\frac{\sigma_y}{2}\right) \tag{1}$$

to his jth qubit state where U_k is chosen randomly from the set $\{U_{+y}, U_{-y}\}$ with probability $\{1/2, 1/2\}$, respectively, $j = 1, 2, \ldots, N$. Then at time $t = t_j^B$ $(> t_j^A)$, Bob measures locally the observable

$$B = -I \otimes (\sigma_z + \sigma_x)/\sqrt{2}$$
$$\text{or } D = I \otimes (\sigma_z - \sigma_x)/\sqrt{2}$$

on his jth qubit state, according to the outcome of an unbiased coin toss, $j = 1, 2, \ldots, N$ [5].

Bob knows each of the N number of t_j^A's. As collapse is instantaneous (which is evident from the violation of spatial Bell-CHSH inequality [48,49]), Bob can carry out his operations immediately after Alice measures. We have the following eigenvalue equations:

$$\sigma_z|0\rangle = |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle, \quad \sigma_x|\pm\rangle = \pm|\pm\rangle,$$
$$\frac{-(\sigma_z + \sigma_x)}{\sqrt{2}}|\pm\rangle_B = \pm|\pm\rangle_B,$$
$$\frac{\sigma_z - \sigma_x}{\sqrt{2}}|\pm\rangle_D = \pm|\pm\rangle_D, \tag{2}$$

where

$$|+\rangle_B = \cos(\theta_1/2)|0\rangle + \mathrm{e}^{\mathrm{i}\pi}\sin(\theta_1/2)|1\rangle,$$
$$|-\rangle_B = \cos(\theta_2/2)|0\rangle + \sin(\theta_2/2)|1\rangle,$$
$$|+\rangle_D = \cos(\theta_2/2)|0\rangle + \mathrm{e}^{\mathrm{i}\pi}\sin(\theta_2/2)|1\rangle,$$
$$|-\rangle_D = \cos(\theta_1/2)|0\rangle + \sin(\theta_1/2)|1\rangle. \tag{3}$$

$\theta_1 = \pi - \pi/4, \theta_2 = \pi/4$. Quantum mechanically, the values of measurement outcomes a, c, b, d $(= \pm 1$, the eigenvalues) of observables A, C, B, D, respectively, are not preassigned before the measurement process. b, d depends on Alice's choice of observable, even though their measurement events are space-like separated. Measurement creates reality [50–55].

When Alice measures A locally, if her qubit collapses to $|0\rangle$ or $|1\rangle$, then Bob's qubit always collapses instantaneously to $|1\rangle$ or $|0\rangle$, respectively (spatial correlation due to entanglement). Similarly, when Alice measures C locally, if her qubit collapses to $|\pm\rangle$, then Bob's qubit collapses to $|\mp\rangle$.

2.1 *Post-selected perfectly (anti)correlated subensembles*

After N measurements, they select (via CC) the following four (out of eight) subensembles ($\mathscr{E}_i, i = 1, 2, 3, 4$) which correspond to applying correct context-dependent local unitary evolutions ($U_{\pm y}$):

($\mathscr{E}_1$) Alice had measured A, then Bob had evolved his qubit state under the unitary U_{+y} (i.e. counter-clockwise rotation about the y-axis by 45° on the Bloch sphere) to get $U_{+y}|1\rangle = |+\rangle_B$ or $U_{+y}|0\rangle = |-\rangle_B$, and then Bob had measured B. Then the product of measurement outcomes becomes $ab = +1 \times +1 = 1$ or $ab = -1 \times -1 = 1$. Hence knowing b, Bob can know a, i.e. $a = b$ (perfectly correlated). Hence $\langle A(t^A)B_1(t^B)\rangle = 1 = ab_1$, where B_i, D_i represent the association of B, D, respectively, with unitary evolution $U_{\mu_i}, i = 1, 2, \mu_1 = +y, \mu_2 = -y$, and b_i, d_i are measurement outcomes corresponding to B_i, D_i, respectively, $i = 1, 2$. More rigorously, the joint probability of Alice getting outcome a in a measurement of A and Bob, after applying U_{+y}, getting outcome b in a measurement of B is given by

$$p(a, b|U_{+y}) = \mathrm{Tr}(\mathscr{B}_b^{(2)} U_{+y}^{(2)} \mathscr{A}_a^{(1)} \rho_0 \mathscr{A}_a^{(1)} (U_{+y}^{(2)})^\dagger) \quad (4)$$

[56,57], where $a, b = +1, -1$, $\rho_0 = |S_0\rangle\langle S_0|$,

$$\mathscr{A}_{+1}^{(1)} = |0\rangle\langle 0| \otimes I, \quad \mathscr{A}_{-1}^{(1)} = |1\rangle\langle 1| \otimes I,$$

$$\mathscr{B}_{\pm 1}^{(2)} = I \otimes |\pm\rangle_B\langle\pm|_B, \quad U_{\pm y}^{(2)} = I \otimes U_{\pm y},$$

$$\Rightarrow \langle A(t^A)B_1(t^B)\rangle = \sum_{a,b} p(a, b|U_{+y})\, ab = 1 = ab_1, \quad (5)$$

where

$$p(a = +1, b = +1|U_{+y}) = p(a = -1, b = -1|U_{+y}) = 1/2,$$

$$p(a = +1, b = -1|U_{+y}) = p(a = -1, b = +1|U_{+y}) = 0.$$

($\mathscr{E}_2$) Alice had measured A, then Bob had evolved his qubit state under the unitary U_{-y} (i.e. clockwise rotation about the y-axis by 45° on the Bloch sphere) to get $U_{-y}|1\rangle = |-\rangle_D$ or $U_{-y}|0\rangle = |+\rangle_D$, and then he had measured D. Then the product of measurement outcomes becomes $ad = +1 \times -1 = -1$ or $ad = -1 \times +1 = -1$. $\Rightarrow a = -d$ (perfectly anticorrelated). Hence $\langle A(t^A)D_2(t^B)\rangle = -1 = ad_2$. More rigorously, the joint probability of Alice getting outcome a in a measurement of A and Bob, after applying U_{-y}, getting outcome d in a measurement of D is given by

$$p(a, d|U_{-y}) = \mathrm{Tr}(\mathscr{D}_d^{(2)} U_{-y}^{(2)} \mathscr{A}_a^{(1)} \rho_0 \mathscr{A}_a^{(1)} (U_{-y}^{(2)})^\dagger), \quad (6)$$

where $a, d = +1, -1$, and

$$\mathscr{D}_{\pm 1}^{(2)} = I \otimes |\pm\rangle_D\langle\pm|_D \Rightarrow \langle A(t^A)D_2(t^B)\rangle = \sum_{a,d} p(a, d|U_{-y})\, ad = -1 = ad_2, \quad (7)$$

where

$$p(a = +1, d = +1|U_{-y}) = p(a = -1, d = -1|U_{-y}) = 0,$$

$$p(a = +1, d = -1|U_{-y}) = p(a = -1, d = +1|U_{-y}) = 1/2.$$

($\mathscr{E}_3$) Alice had measured C, then Bob had evolved his qubit state under the unitary U_{-y} to get $U_{-y}|-\rangle = |+\rangle_B$ or $U_{-y}|+\rangle = |-\rangle_B$, and then he had measured B. Then the product of measurement outcomes becomes $cb = +1 \times +1 = 1$ or $cb = -1 \times -1 = 1$. $\Rightarrow c = b$ (perfectly correlated). Hence $\langle C(t^A)B_2(t^B)\rangle = 1 = cb_2$. More rigorously, the joint probability of Alice getting outcome c in a measurement of C and Bob, after applying U_{-y}, getting outcome b in a measurement of B is given by

$$p(c, b|U_{-y}) = \mathrm{Tr}(\mathscr{B}_b^{(2)} U_{-y}^{(2)} \mathscr{C}_c^{(1)} \rho_0 \mathscr{C}_c^{(1)} (U_{-y}^{(2)})^\dagger), \quad (8)$$

where $c, b = +1, -1$, and

$$\mathscr{C}_{\pm 1}^{(1)} = |\pm\rangle\langle\pm| \otimes I \Rightarrow \langle C(t^A)B_2(t^B)\rangle = \sum_{c,b} p(c, b|U_{-y})cb = 1 = cb_2, \quad (9)$$

where

$$p(c = +1, b = +1|U_{-y}) = p(c = -1, b = -1|U_{-y}) = 1/2,$$

$$p(c = +1, b = -1|U_{-y}) = p(c = -1, b = +1|U_{-y}) = 0.$$

($\mathscr{E}_4$) Alice had measured C, Bob had evolved his qubit state under the unitary U_{+y} to get $U_{+y}|-\rangle = |+\rangle_D$ or $U_{+y}|+\rangle = |-\rangle_D$, and then he had measured D. Then the product of measurement

outcomes becomes $cd = +1 \times +1 = 1$ or $cd = -1 \times -1 = 1$. $\Rightarrow c = d$ (perfectly correlated). Hence $\langle C(t^A)D_1(t^B)\rangle = 1 = cd_1$. More rigorously, the joint probability of Alice getting outcome c in a measurement of C and Bob, after applying U_{+y}, getting outcome d in a measurement of D is given by

$$p(c,d|U_{+y}) = \mathrm{Tr}(\mathscr{D}_d^{(2)} U_{+y}^{(2)} \mathscr{C}_c^{(1)} \rho_0 \mathscr{C}_c^{(1)} (U_{+y}^{(2)})^\dagger), \quad (10)$$

where

$$c,d = +1,-1 \Rightarrow \langle C(t^A)D_1(t^B)\rangle = \sum_{c,d} p(c,d|U_{+y})cd = 1 = cd_1, \quad (11)$$

and

$$p(c=+1,d=+1|U_{+y}) = p(c=-1,d=-1|U_{+y}) = 1/2,$$
$$p(c=+1,d=-1|U_{+y}) = p(c=-1,d=+1|U_{+y}) = 0.$$

Now substituting the above expectation values into the ST Bell-CHSH term, we obtain

$$\langle I_Q\rangle = \langle A(t^A)B_1(t^B)\rangle + \langle C(t^A)B_2(t^B)\rangle + \langle C(t^A)D_1(t^B)\rangle - \langle A(t^A)D_2(t^B)\rangle = 4$$
$$= ab_1 + cb_2 + cd_1 - ad_2 = I_Q, \quad (12)$$

which is the maximum possible violation of classical (local) upper bound 2. I_Q takes only one value, i.e. 4. Hence $\langle I_Q\rangle = I_Q = 4$ (i.e. there is no variance/error in experimentally evaluating the expectation value). $\langle I_Q\rangle = 4$ does not contradict the Tsirelson bound ($2\sqrt{2}$) [5,8], because local unitary evolutions are involved, and Alice and Bob are post-selecting the correct context-dependent local unitarily evolved subensembles. Both of these are not considered in deriving the Tsirelson bound.

There are two context dependencies here: (1) Whether Bob measures B in the context of A or in the context of C (A and C do not commute). This context dependency manifests as non-local correlation over space, as measurement events are space-like separated [50,51,54,55]. Similar is the context dependency for D. This results in $2 < \langle I_Q\rangle \leq 2\sqrt{2}$. (2) The context-dependent local unitary operations that Bob applies to his qubit states, as described above. This boosts the non-local correlation over space that is already present, to the maximum extent possible. If there was no non-local correlation over space (like in classical scenario), then unitary evolution cannot boost the correlation any further. Hence, even though there is no entanglement during unitary evolution, we are able to boost the correlation as there was entanglement (correlation) prior to unitary evolution. The state of Bob's qubit gets maximally (anti)correlated (with respect to measurement outcomes) with that of Alice's, as Bob applies $U_{\pm y}$. This results in $2\sqrt{2} < \langle I_Q\rangle \leq 4$. In other words, during unitary evolution, Bob's qubit evolves into such a state that measurement outcomes of Alice and Bob gets perfectly (anti)correlated.

As the singlet state $|S_0\rangle$ is Bell non-local, it is also Einstein–Podolsky–Rosen (EPR) steerable. This is because the Bell non-locality implies EPR steerability [58–60]. Further in our protocol, Alice and Bob use CC for post-selecting the correct context-dependent local unitarily evolved subensembles, and Bob uses local unitary operations only. Hence, the operations used by Alice and Bob (i.e. local operation with classical communication (LOCC)) are the natural free operations of the resource theory of entanglement [61].

Further, note that if we calculate the expectation values without post-selecting the strongly correlated subensembles,, then we obtain $\langle I_Q\rangle = 2$. This is because the strong correlation built up due to correct context-dependent $U_{\pm y}$ is destroyed by the wrong context-dependent $U_{\pm y}$. If we do not apply $U_{\pm y}$ at all, then we get $\langle I_Q\rangle = 2\sqrt{2}$ [5].

3. A more efficient and more sensitive ST QKD protocol

In the aforementioned ST Bell-CHSH test, Alice and Bob use a small portion of subensembles $\mathscr{E}_1$–$\mathscr{E}_4$ to test for eavesdropping/noise in the quantum channel. The remaining large portion of the subensembles $\mathscr{E}_1$–$\mathscr{E}_4$ is used for secret key bits generation. Note that to separate the subensembles $\mathscr{E}_1$–$\mathscr{E}_4$ from $\mathscr{E}_5$–$\mathscr{E}_8$ (which correspond to states evolved under wrong context-dependent $U_{\pm y}$), they need to publicly announce only their sequence of random choice of observables, and Bob's sequence of random choice of U_{+y}, U_{-y}, but not their measurement outcomes.

3.1 *Test for eavesdropping*

Alice and Bob test for eavesdropping as follows: They publicly announce a few sets of measurement outcomes chosen randomly from the subensembles $\mathscr{E}_1$–$\mathscr{E}_4$, and look for their perfect correlation ($a = b_1, c = b_2$, $c = d_1$) and perfect anticorrelation ($a = -d_2$). Perfect correlation/anticorrelation in each set of measurement outcomes is possible if and only if particles were maximally entangled in each set (which implies

no eavesdropping). They can also look for $\langle I_Q \rangle = 4$, as it does not require an ensemble ($\because \langle I_Q \rangle = I_Q$ (eq. (12)), and hence a minimum of four sets of measurement outcomes are sufficient to calculate $\langle I_Q \rangle$), unlike in Ekert's and Wigner's protocols which require an ensemble of large number of sets of measurement outcomes (table 1). If they obtain a perfect correlation/anticorrelation in more than, say, n (threshold value considering noise in the channel) sets of measurement outcomes, then they can safely conclude that there was no eavesdropping, and hence they can generate secret key bits. Else they have to discard the keys and start afresh.

3.2 *Secret key bits generation*

If there was no eavesdropping, then they can generate secret key bits using the remaining large portion of subensembles $\mathscr{E}_1$–$\mathscr{E}_4$ (whose outcomes are not publicly announced) as follows: Bob knows whether B has been measured in the context of A or C. Similarly D. Further $a = b_1, c = b_2, c = d_1$ (perfectly correlated). Hence, both Alice's and Bob's measurement outcomes will be either $+1$ or -1. Hence, they directly obtain the keys, whereas $a = -d_2$ (perfectly anticorrelated). Hence, if Alice's outcome is ± 1, then Bob's outcome will be ∓ 1. Hence, one of them has to invert to obtain the keys.

3.3 *Amount of CC required*

Ekert QKD protocol: Alice and Bob use three observables each [25]. They assign $0, 1, 00$ to their observables. Hence, each requires approximately $N/3+N/3+2N/3 = 4N/3$ bits of CC to publicly announce their sequence of random choice of observables. To test for eavesdropping, one of them has to announce their measurement outcomes of four subensembles out of nine, which requires $4N/9$ bits of CC. Hence, the total CC required is $28N/9 = 14M$ bits (because $N = M/K$ where K and M are defined in table 1).

Wigner QKD protocol: Alice and Bob use two observables each [25]. They assign $0, 1$ to their observables. Hence, each requires approximately $N/2 + N/2 = N$ bits of CC to publicly announce their sequence of random choice of observables. To test for eavesdropping, one of them has to announce their measurement outcomes of three subensembles out of four, which requires $3N/4$ bits of CC. Hence, total CC required is $11N/4 = 11M$ bits.

ST QKD protocol: Alice and Bob use two observables each. Hence, each requires approximately $N/2+N/2 = N$ bits of CC to publicly announce their sequence of random choice of observables. Further, Bob requires $N/2 + N/2 = N$ bits of CC to publicly announce his sequence of random choice of U_{+y}, U_{-y}. They choose, say, first, last or middle ϵN out of $N/2$ measurements which correspond to correct context-dependent unitarily evolved states to test for eavesdropping (no need to choose it randomly, because the $N/2$ measurements which correspond to correct context-dependent unitarily evolved states are themselves random). In fact, they can choose any consecutive ϵN out of $N/2$ measurements which correspond to correct context-dependent unitarily evolved states to test for eavesdropping. Hence, one of them requires ϵN bits of CC to announce the corresponding measurement outcomes to test for eavesdropping. Hence total CC required is $N(3 + \epsilon) = 2M(3 + \epsilon)/(1 - 2\epsilon)$ bits.

BB84′ QKD protocol (*a variant of BB84 with entangled photons* (*see ref.* [25])): Alice and Bob use two observables each [25]. Hence, each requires approximately $N/2+N/2 = N$ bits of CC to publicly announce their sequence of random choice of observables. To test for eavesdropping they require ϵN bits of CC as in ST QKD protocol. Hence, the total CC required is $N(2 + \epsilon) = 2M(2 + \epsilon)/(1 - 2\epsilon)$ bits. These are tabulated in table 1.

3.4 *Sensitivity to eavesdropping*

We define sensitivity $\mathscr{S}$ of a protocol (which uses violation of Bell type of inequalities for its security) to

Table 1. Ek, Wi, ST, and B′ stand for Ekert, Wigner, ST and BB84′ QKD protocols, respectively. Fraction of the total resource distributed for various purposes (columns 2–5): key (K):= for secret key bits generation, test (T):= to test for eavesdropping, discard (D):= not used for anything, wastage ($W = T + D$):= total amount of wastage [25]. N is the number of singlets ($|S_0\rangle$'s) required to generate M bits of secret key ($M = NK$). CC:= total amount of CC (in bits) required to generate M bits of secret key (see §3.3). $\mathscr{S}$ is the sensitivity to eavesdropping (eq. (13)). First three QKD protocols are based on Bell's theorem. E:= requires an ensemble of large number of $|S_0\rangle$s to test for eavesdropping (see §3.1 and 3.4 for explanation). $0 < \epsilon \ll 1/2$.

	K	T	D	W	N	CC	$\mathscr{S}$
Ek	2/9	$\frac{4}{9}$(E)	$\frac{3}{9}$	7/9	$\frac{9M}{2}$	14M	0.41
Wi	1/4	$\frac{3}{4}$(E)	0	3/4	4M	11M	0.04
ST	$\frac{1}{2} - \epsilon$	ϵ	$\frac{1}{2}$	$\frac{1}{2} + \epsilon$	$\frac{2M}{1-2\epsilon}$	$\frac{2M(3+\epsilon)}{1-2\epsilon}$	1
B′	$\frac{1}{2} - \epsilon$	ϵ	$\frac{1}{2}$	$\frac{1}{2} + \epsilon$	$\frac{2M}{1-2\epsilon}$	$\frac{2M(2+\epsilon)}{1-2\epsilon}$	–

eavesdropping as follows:

$$\mathscr{S} = \frac{\max\{|\langle I_Q\rangle|\} - |\text{Classical bound}|}{|\text{Algebraic bound}| - |\text{Classical bound}|}. \quad (13)$$

If $\max\{|\langle I_Q\rangle|\} = |\text{Classical bound}|$, then $\mathscr{S} = 0$, i.e. not at all sensitive to eavesdropping as required. Greater the difference between quantum upper bound and classical upper bound, stronger is the non-classical/quantum correlation in the state. As quantum correlation is very sensitive to eavesdropping, grater violation of Bell type of inequalities implies more sensitivity for eavesdropping.

In Ekert's QKD protocol

$\max\{|\langle I_Q\rangle|\} = 2\sqrt{2}$, $|\text{Classical bound}| = 2$,

$|\text{Algebraic bound}| = 4$

and hence

$\mathscr{S} = 0.414$ [25].

In Wigner's QKD protocol

$\max\{|\langle I_Q\rangle|\} = |-1/8|$,

$|\text{Classical bound}| = 0$,

$|\text{Algebraic bound}| = |-3|$

and hence

$\mathscr{S} = 0.0417$ [25].

In our ST QKD protocol

$\max\{|\langle I_Q\rangle|\} = 4$ (see eq.(12)),

$|\text{Classical bound}| = 2$, $|\text{Algebraic bound}| = 4$,

and hence $\mathscr{S} = 1$ (maximum sensitivity). These are tabulated in table 1.

A comparison of our ST QKD protocol with other QKD protocols is given in table 1. It is evident from the table that ST QKD protocol is more efficient (in terms of resource N and CC required to generate a given amount of secret key bits), and more sensitive (to eavesdropping) than Ekert's and Wigner's QKD protocols. This is achieved at the cost of introducing a simple local unitary evolution. ST is as efficient as BB84′ in all aspects except in the CC required (but BB84′ belongs to a different group, i.e. it is not based on Bell's theorem).

In Ekert's and Wigner's QKD protocols, the constraint $T \times N \gg 1$ (T, N are defined in table 1) must be satisfied to kill the error/variance in calculating expectation values corresponding to Bell's inequality (hence large ensemble measurement is necessary). But it is not required in ST QKD protocol as the products $ab_1 = +1, cb_2 = +1, cd_1 = +1, ad_2 = -1$ (eq. (12)) always (i.e. no variance in these products), unlike in Ekert's and Wigner's QKD protocols. Hence, when M is small (i.e. only a small amount of secret key bits are required), only ST and BB84′ are economical.

Further, we note that if Bob can store his qubit states in quantum memory till Alice publicly announces her sequence of random choice of measurement observables, then all entries in discard (D) column (table 1) can be made zero. Consequently, more key bits can be generated in Ekert, ST and BB84′. But storing quantum states against decoherence is a great challenge.

Finally, it is important to note that one can also observe the violation of Bell inequality greater than 2, and even up to its algebraic bound 4, due to loop holes (such as locality loop hole, detection or fair-sampling loop hole, using faked-state technique, etc.) in performing the Bell test as well [62–64]. However, in this paper, all our theoretical calculations are based on the assumption that there will not be any such loop holes in performing the Bell test. Hence, the algebraic bound 4, which we were able to achieve, was not due to any kind of such loop holes. Further, note that in our protocol, Alice and Bob are post-selecting with respect to their choice of measurement observables only, but not with respect to their measurement outcomes. In the ST-QKD protocol, Alice and Bob publicly announce their choice of measurement observables only, but not their measurement outcomes, and then post-select accordingly. Hence, the violation of Bell inequality, which Alice and Bob achieve (which is up to 4), is not due to fair-sampling loop hole (this corresponds to post-selecting with respect to measurement outcomes [64,65]). If it were so, then our protocol could not have been used for QKD.

4. Summary and conclusion

We showed that if we insert context-dependent local unitary evolutions into the normal Bell test, then it is possible to violate ST Bell-CHSH inequality maximally (i.e. up to 4). The correct context dependency can be achieved via post-selection. We presented a scheme to boost the correlation over space to the maximum extent possible (i.e. 4) via local unitary evolutions and subsequent CC (i.e. post-selection). This does not contradict Tsirelson bound ($2\sqrt{2}$), as the latter does not take into consideration unitary evolutions and/or post-selection. Further, we showed that this leads to a more efficient and more sensitive (to eavesdropping) ST QKD protocol. ST QKD protocol is far efficient and economical in terms of resource (singlets, CC) required to generate a given amount of secret key bits, than Ekert's and Wigner's QKD protocols. This can be achieved at the cost of introducing a simple local unitary evolution (i.e. $\pm 45°$ rotation about the y-axis on the Bloch sphere).

However, compared to BB84′ (i.e. modified BB84), the ST QKD protocol is less efficient only in one aspect, i.e. CC required, and in other aspects it is the same as BB84′. We also showed that when the amount of secret key bits to be generated is small, only ST and BB84′ QKD protocols are economical.

Acknowledgements

The author acknowledges the useful discussions with Prof. T S Mahesh, Prof. R Srikanth, S Aravinda, Deepak Khurana, V S Anjusha and Soham Pal. Finally, he would like to thank anonymous referees for suggesting to quantify the amount of CC involved in various QKD protocols and for pointing out the fact that violation beyond Tsirelson bound is not due to any kind of possible loop holes in performing the Bell test.

References

[1] J S Bell, *Speakable and unspeakable in quantum mechanics* (Cambridge University Press, Cambridge, 1989)
[2] S Popescu and D Rohrlich, *Found. Phys*. **24(3)**, 379 (1994)
[3] J S Bell, *Physics* **1**, 195 (1964)
[4] J F Clauser, M A Horne, A Shimony and R A Holt, *Phys. Rev. Lett*. **23**, 880 (1969)
[5] M A Nielsen and I L Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2010), Cambridge Books Online
[6] A Cabello, *Phys. Rev. Lett*. **88**, 060403 (2002)
[7] C S Sudheer Kumar, A Biswas, A Sen(De) and U Sen, arXiv:1903.12096v1 [quant-ph] (March 2019)
[8] B S Cirel'son, *Lett. Math. Phys.* **4(2)**, 93 (1980)
[9] A S Hejamadi, A Pathak and R Srikanth, *Quanta* **6(1)**, 1 (2017)
[10] M Pawłowski, *Phys. Rev. A* **82**, 032313 (2010)
[11] E Biham, M Boyer, P O Boykin, T Mor and V Roychowdhury, *J. Crypt*. **19(4)**, 381 (2006)
[12] K Boström and T Felbinger, *Phys. Rev. Lett*. **89**, 187902 (2002)
[13] M Lucamarini and S Mancini, *Phys. Rev. Lett*. **94**, 140501 (2005)
[14] D Mayers, *J. ACM* **48(3)**, 351 (2001)
[15] P W Shor and J Preskill, *Phys. Rev. Lett*. **85**, 441 (2000)
[16] H K Lo and H F Chau, *Science* **283(5410)**, 2050 (1999)
[17] K Inoue and T Honjo, *Phys. Rev. A* **71**, 042305 (2005)
[18] E Waks, H Takesue and Y Yamamoto, *Phys. Rev. A* **73**, 012344 (2006)
[19] W O Krawec, *Quant. Inf. Proc*. **15(5)**, 2067 (2016)
[20] V Scarani and R Renner, *Phys. Rev. Lett*. **100**, 200501 (2008)
[21] T C Ralph, *Phys. Rev. A* **62**, 062306 (2000)
[22] Z Q Yin, H W Li, W Chen, Z F Han and G C Guo, *Phys. Rev. A* **82**, 042335 (2010)
[23] A Boaron, B Korzh, R Houlmann, G Boso, C C W Lim, A Martin and H Zbinden, *J. Appl. Phys*. **120(6)**, 063101 (2016)
[24] C H Bennett and G Brassard, *International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984) Vol. 1, pp. 175–179
[25] T Jennewein, C Simon, G Weihs, H Weinfurter and A Zeilinger, *Phys. Rev. Lett*. **84**, 4729 (2000)
[26] C H Bennett, *Phys. Rev. Lett*. **68**, 3121 (1992)
[27] S Kak, *Pramana – J. Phys*. **54**, 709 (2000)
[28] A K Ekert, *Phys. Rev. Lett*. **67**, 661 (1991)
[29] C H Bennett, G Brassard and N D Mermin, *Phys. Rev. Lett*. **68**, 557 (1992)
[30] N Gisin, G Ribordy, W Tittel and H Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002)
[31] L Masanes, S Pironio and A Acin, *Nat. Commun.* **2**, 238 (2011)
[32] J Barrett, R Colbeck and A Kent, *Phys. Rev. A* **86**, 062326 (2012)
[33] U Vazirani and T Vidick, *Phys. Rev. Lett*. **113**, 140501 (2014)
[34] H L Yin, T Y Chen, Z W Yu, H Liu, L X You, Y B Zhou, S J Chen, Y Mao, M Q Huang, W J Zhang, H Chen, M J Li, D Nolan, F Zhou, X Jiang, Z Wang, Q Zhang, X B Wang and J W Pan, *Phys. Rev. Lett*. **117**, 190501 (2016)
[35] L Goldenberg and L Vaidman, *Phys. Rev. Lett*. **75**, 1239 (1995)
[36] A Avella, G Brida, I P Degiovanni, M Genovese, M Gramegna and P Traina, *Phys. Rev. A* **82**, 062309 (2010)
[37] H A Shenoy, R Srikanth and T Srinivas, *Eur. Phys. Lett.* **103(6)**, 60008 (2013)
[38] T G Noh, *Phys. Rev. Lett.* **103**, 230501 (2009)
[39] Y Sun and Q Y Wen, *Phys. Rev. A* **82**, 052318 (2010)
[40] T C Ralph, *Phys. Rev. A* **61**, 010303 (1999)
[41] M Hillery, *Phys. Rev. A* **61**, 022309 (2000)
[42] F Grosshans and P Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002)
[43] M D Reid, *Phys. Rev. A* **62**, 062308 (2000)
[44] I Derkach, V C Usenko and R Filip, *Phys. Rev. A* **93**, 032309 (2016)
[45] R D Sharma, K Thapliyal, A Pathak, A K Pan and A De, *Quantum Inf. Proc.* **15(4)**, 1703 (2016)
[46] K Thapliyal, A Pathak and S Banerjee, *Quantum Inf. Proc.* **16(5)**, 115 (2017)
[47] S Pal, S Moitra, V S Anjusha, A Kumar and T S Mahesh, *Pramana – J. Phys*. **92**: 1 (2019)
[48] M Genovese, G Brida, C Novero and E Predazziy, *Pramana – J. Phys*. **56**, 153 (2001)
[49] B Hensen, H Bernien, A E Dréau, A Reiserer, N Kalb, M S Blok, J Ruitenberg, R F L Vermeulen, R N Schouten, C Abellán, W Amaya, V Pruneri, M W Mitchell, M Markham, D J Twitchen, D Elkouss, S Wehner, T H Taminiau and R Hanson, *Nature* **526(7575)**, 682 (2015)
[50] A Peres, *J. Phys. A* **24(4)**, L175 (1991)

[51] S Kochen and E P Specker, *J. Math. Mech.* **17**, 59 (1967)
[52] N D Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990)
[53] A Einstein, B Podolsky and N Rosen, *Phys. Rev.* **47**, 777 (1935)
[54] A Grudka, K Horodecki, M Horodecki, P Horodecki, R Horodecki, P Joshi, W Kłobus and A Wójcik, *Phys. Rev. Lett.* **112**, 120401 (2014)
[55] E G Cavalcanti, *Phys. Rev. X* **8**, 021018 (2018)
[56] G Lüders, *Ann. Phys.* **15(9)**, 663 (2006)
[57] C Budroni and C Emary, *Phys. Rev. Lett.* **113**, 050401 (2014)
[58] M T Quintino, T Vértesi, D Cavalcanti, R Augusiak, M Demianowicz, A Acín and N Brunner, *Phys. Rev. A* **92**, 032107 (2015)
[59] M M Taddei, R V Nery and L Aolita, *Phys. Rev. A* **94**, 032106 (2016)
[60] H M Wiseman, S J Jones and A C Doherty, *Phys. Rev. Lett.* **98**, 140402 (2007)
[61] R Gallego and L Aolita, *Phys. Rev. X* **5**, 041008 (2015)
[62] I Gerhardt, Q Liu, A Lamas-Linares, J Skaar, V Scarani, V Makarov and C Kurtsiefer, *Phys. Rev. Lett*. **107**, 170404 (2011)
[63] E Pomarico, B Sanguinetti, P Sekatski, H Zbinden and N Gisin, *New J. Phys.* **13(6)**, 063031 (2011)
[64] W J Chu, X L Zong, M Yang, G Z Pan and Z L Cao, *Sci. Rep.* **6**, 28351 (2016)
[65] C Branciard, *Phys. Rev. A* **83**, 032123 (2011)