Role of Steering Inequality in Quantum Key Distribution Protocol

Kaushiki Mukherjee [1,*], *Tapaswini Patro* [2,†] & *Nirman Ganguly* [2,‡]

[1] *Department of Mathematics, Government Girls' General Degree College, Ekbalpore, Kolkata, India*
[2] *Department of Mathematics, Birla Institute of Technology and Science Pilani, Hyderabad Campus, Telangana, India*
E-mails: kaushiki.wbes@gmail.com, p20190037@hyderabad.bits-pilani.ac.in†, nirmanganguly@hyderabad.bits-pilani.ac.in‡*

Editors: *Vinayak Jagadish & Srikanth Radhakrishna*

Article history: Submitted on December 6, 2022; Accepted on April 11, 2023; Published on April 18, 2023.

Violation of Bell's inequality has been the mainspring for secure key generation in an entanglement assisted Quantum Key Distribution (QKD) protocol. Various contributions have relied on the violation of Bell inequalities to build an appropriate QKD protocol. Residing between Bell nonlocality and entanglement, there exists a hybrid trait of correlations, namely correlations exhibited through the violation of steering inequalities. However, such correlations have not been put to use in QKD protocols as much as their stronger counterpart, the Bell violations. In the present work, we show that the violations of the Cavalcanti–Jones–Wiseman–Reid (CJWR) steering inequalities can act as key ingredients in an entanglement assisted QKD protocol. We work with arbitrary two-qubit entangled states, and characterize them by their utility in such protocols. The characterization is based on the quantum bit error rate and violation of the CJWR inequality. Furthermore, we show that subsequent applications of local filtering operations on initially entangled states exhibiting no violation, lead to violations necessary for the successful implementation of the protocol. An additional vindication of our protocol is provided by the use of absolutely Bell–Clauser–Horne–Shimony–Holt (Bell–CHSH) local states, states which remain Bell–CHSH local even under global unitary operations.

Quanta 2023; 12: 1–21.

1 Introduction

Quantum cryptography promises to bring a paradigmatic change in the domain of secure information processing [1]. The state-of-the-art techniques, recently conceptualized, have led to profound implications in how we deal with secure messages [2]. The archetypal manifestation of quantum mechanics, namely quantum entanglement lies at the root of quantum cryptography. Quantum entanglement [3] makes it possible to realize protocols unimaginable in classical information theory.

An inherent constitution of quantum cryptography is key distribution, which in the simplest scenario can be interpreted as the task of generating a private key between two honest users who can communicate with each other over public channels. If one includes quantum resources for secure key generation, it can outperform protocols availing only classical resources. Such a difference stems from the fact that quantum protocols rely on the inherent random nature of quantum particles contrary to dependence on pseudo-randomness and computational complexity by classical protocols [4].

The seminal work by Bennett and Brassard [5] single-handedly pioneered the study of quantum key distribution protocols. In the protocol described in [5], commonly known as the BB84 protocol, the authors designed a bipartite key distribution protocol based on the idea of conjugate bases [6], with the involvement of the protagonists Alice (sender) and Bob (receiver). Measurement-induced disturbance in quantum systems [7] plays a key role in the protocol, which depends on *preparation and measurement scheme*. Several key generation protocols [8–14] based on this scheme have been designed since the BB84 protocol.

A departure from the *preparation and measurement scheme* is provided by the *entanglement assisted key distribution* protocols. The two parties now share an entangled state [3] and the presence of the eavesdropper is detected through the violation of a suitable Bell's inequality [15], like the Bell–Clauser–Horne–Shimony–Holt (Bell–CHSH) [16]. Such a scheme was envisaged by Ekert through his novel contribution [17]. Since its inception, strategies based on violation of Bell's inequalities have been used to design many QKD protocols [18–24].

In entanglement-assisted protocols, comparison of Alice and Bob's information content with that of an eavesdropper is the most obvious way to verify security [25]. However, violation of a suitable Bell's inequality provides a pragmatic alternative [26–29]. Although Bell violation is necessary for security, it has been shown that it is not sufficient [30, 31]. Consequent to a Bell violation, it becomes imperative to check the utility of the entangled state in successful key generation. In [32], the authors have characterized two-qubit states in this perspective, where the relation between Bell–CHSH violation and quantum bit error rate (QBER) [25] has been exploited.

Nonlocal correlations being the mainstay of QKD protocols necessitate exploitation of other manifestations of it. Quantum steering provides one such significant alternative, which remains sandwiched between entanglement and Bell nonlocal correlations. Schrödinger, pioneered the concept of steering [33, 34], whose operational significance came much later through the contributions in [35–37]. A series of works followed, detecting the steerability of correlations [38–47].

In order to detect whether any bipartite state ρ is steerable, we need a steering criterion. In [39], the authors derived a linear inequality, based on linear functions of expectation values of observables, commonly referred to as Cavalcanti–Jones–Wiseman–Reid (CJWR) inequality (for more details see Section 3.3). A closed form (based on the correlation tensor of the density matrix) to establish the violation of the said inequality, was derived in [47]. We have considered three measurement settings as in the two measurement scenarios it is equivalent to Bell–CHSH inequality. States which violate the CJWR inequality under three measurement settings are also commonly termed as F_3 steerable. In the present work, we address the following problem: *Given that a quantum state violates the CJWR inequality, can it be used in a QKD protocol?*

Our work, which considers an entanglement-assisted key distribution protocol, makes two very significant assumptions: (i) violation of CJWR inequality for three settings is necessary for security, (ii) minimum secure key rate [48] is dependent on quantum bit error rate only. Precisely speaking, we characterize the two-qubit state space based on the utility of a F_3 steerable state in a QKD protocol.

The above probe raises another imperative query, namely *can the useless states be made useful for QKD with an enhancement in the protocol?* We provide an affirmative answer, through the application of local filtering operations [49–51]. Analogous to the procedure which was obtained in [32] concerning the Bell–CHSH inequality, we modify our protocol to include local filtering operations to enhance the suitability of the otherwise useless states. Strikingly, it is also observed that some F_3 unsteerable two-qubit states can also be used for secure key generation in this modified protocol.

Usually, in any entanglement-assisted QKD protocol, the state shared between Alice and Bob is generated from some unknown source that can be under the control of an eavesdropper. If the source distributes an absolutely Bell–CHSH local entangled state [52, 53], then secure key generation becomes impossible if Bell–CHSH violation is considered. In conjunction with this, we propose a scenario where such states can also be made useful as steerability is a weaker form of nonlocality than Bell nonlocality.

New Contributions of this work: In the study of entanglement-assisted QKDs, the role of Bell nonlocality has seen multiple probes. In this perspective, the role of other nonclassical correlations beyond Bell–CHSH inequality warrants attention. In this context, it becomes imperative to analyze the role of steering nonlocality in entanglement assisted QKDs. We have characterized the entire two-qubit state space in perspective of using the violation of a steering inequality as a tool of security analysis in such QKD protocols. For our purpose, we have used the three settings CJWR steering inequality [39]. We have also explored the utility of applying suitable local filters to turn some useless states (in the context of their usefulness in the entanglement-assisted QKD protocol) into useful ones. Apart from that, the usefulness (if any) of absolutely Bell–CHSH local entangled states in such QKD protocols (relying on violation of CJWR inequality) has been analyzed.

The rest of our work is organized as follows: The motivation underlying the present study is provided in Section 2, followed by discussions on some mathematical prerequisites in Section 3. The entire characterization of two-qubit states is made in Section 4. In Section 5, the effect of local filtering operations in our QKD protocol is discussed. In Section 6, we discuss the case where absolute Bell–CHSH local states are used in the protocol. We end our discussion with some concluding remarks in Section 7.

2 Motivation

Over the years, violation of Bell–CHSH inequality has been used in analyzing security in entanglement-assisted QKD protocols. Recently, in [32], considering QBER as a metric of security analysis, the authors have completely characterized arbitrary two-qubit states based on their utility in such protocols. In this context, it may be noted that violation of a suitable steering inequality may be more helpful in exploiting the potential of two-qubit states in the protocol. To be more precise, there may exist entangled states which cannot be used in QKD protocols relying on Bell–CHSH violation but turn out to be useful in QKD protocols involving the violation of steering inequality. Such an intuition stems from the existing hierarchy of nonclassical correlations. From this perspective, it will be interesting to analyze the two-qubit state space based on the violation of an appropriate steering inequality. This motivates the present work. Using QBER as the metric of security analysis, we have provided a complete characterization of an arbitrary two qubit state based on its utility in an entanglement-assisted protocol involving the violation of a steering inequality. We have used the CJWR inequality [39] and the closed form for its violation [47]. Based on our analysis, it can now be checked whether a given two-qubit state is useful in such a protocol or not. Also, our findings will help to point out the existence of states useful in our protocol which are however useless if QKD protocol involves the violation of CHSH inequality.

At this point, it may be noted that before the present work, the concept of steering has been studied in the light of QKD protocols [54,55]. In [54], the authors established a link between the security of bipartite entanglement-assisted one-sided device-independent QKD scenario (only one of the two parties has trusted measurement devices) and the demonstration of quantum steering. The establishment of a steering inequality from the upper bound of the secret key rate is the main result of their paper. In [55], the concept of temporal steering is used for the same in preparation and measurement-based QKD schemes. However, to the best of the authors' knowledge, violation of a steering inequality about a state's efficacy in QKD protocols has not been probed earlier.

In the present work, we exploit the violation of the CJWR inequality to identify useful states in the QKD protocol. Precisely, we use the closed form derived in [47] to detect a such violation. Local filtering has been used to turn some useless states (in the context of the protocol) into useful ones. Besides, some entangled states (absolutely Bell–CHSH local states [52, 53]) turn out to be useful while considering the notion of F_3 steerability instead of Bell–CHSH violation.

3 Preliminaries and Notations

In this section, we put forward the notations to be used in our analysis with a revisit of some preliminary notions crucial to our analysis.

3.1 Bloch Matrix Representation

The density matrix ρ denotes an arbitrary two-qubit state shared between two parties and is given by

$$\rho = \frac{1}{4}(\mathbb{I}_2 \times \mathbb{I}_2 + \vec{\mathfrak{a}}.\vec{\sigma} \otimes \mathbb{I}_2 + \mathbb{I}_2 \otimes \vec{\mathfrak{b}}.\vec{\sigma} + \sum_{j_1,j_2=1}^{3} w_{j_1 j_2}\sigma_{j_1} \otimes \sigma_{j_2}) \tag{1}$$

with $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, σ_{j_k} denoting Pauli operators along three mutually perpendicular directions ($j_k = 1, 2, 3$). $\vec{\mathfrak{a}} = (x_1, x_2, x_3)$ and $\vec{\mathfrak{b}} = (y_1, y_2, y_3)$ denote local Bloch vectors ($\vec{\mathfrak{a}}, \vec{\mathfrak{b}} \in \mathbb{R}^3$) corresponding to party $\mathcal{A}$ and $\mathcal{B}$ respectively with $|\vec{\mathfrak{a}}|, |\vec{\mathfrak{b}}| \leq 1$, and $(w_{i,j})_{3\times3}$ stands for the correlation tensor matrix $\mathcal{W}$ (real matrix). Components $w_{j_1 j_2}$ of $\mathcal{W}$ are given by $w_{j_1 j_2} = \mathrm{Tr}[\rho\,\sigma_{j_1} \otimes \sigma_{j_2}]$.

$\mathcal{W}$ can be diagonalized by applying suitable local unitary operations [56, 57],where the simplified expression is then given by

$$\rho^{'} = \frac{1}{4}(\mathbb{I}_2 \times \mathbb{I}_2 + \vec{\mathfrak{m}}.\vec{\sigma} \otimes \mathbb{I}_2 + \mathbb{I}_2 \otimes \vec{\mathfrak{n}}.\vec{\sigma} + \sum_{j=1}^{3} \mathfrak{t}_{jj}\sigma_j \otimes \sigma_j). \tag{2}$$

The correlation tensor in Eq. (2) is given by $T = \mathrm{diag}(t_{11}, t_{22}, t_{33})$ where t_{11}, t_{22}, t_{33} are the eigenvalues of $\sqrt{\mathcal{W}^T\mathcal{W}}$, i.e., singular values of $\mathcal{W}$.

3.2 Entanglement Assisted Bipartite QKD Protocol

Consider any entanglement-assisted quantum key distribution (QKD) protocol [17, 32] involving two parties Alice (A) and Bob (B), who try to establish a secure key at the end of the protocol. Let a source Λ (unknown to Alice and Bob) distribute copies of a bipartite entangled state ρ between the two parties. Now Alice and Bob both perform local measurements on their respective subsystems and record their outcomes. For local measurements, each of them chooses randomly from a collection of N number of d-dimensional basis. Let $\mathfrak{C}_{A(B)} = \{\mathfrak{B}^{(\beta)}_{A(B)}\}_{\beta=1}^{N}$ denote the collection of N bases of Alice (Bob) where $\forall\beta$, $\mathfrak{B}^{(\beta)}_{A(B)}$ are given by

$$\mathfrak{B}^{(\beta)}_{A} = \{|\psi^{\beta}_{i}\rangle\}_{i=1}^{d} \text{ and} \mathfrak{B}^{(\beta)}_{B} = \{|\phi^{\beta}_{i}\rangle\}_{i=1}^{d}. \quad (3)$$

If $O^{(\beta)}_{A(B)}$ denote operators corresponding to the basis $\mathfrak{B}^{(\beta)}_{A(B)}$, then those are given by

$$O^{(\beta)}_{A(B)} = \{|\psi(\phi)^{\beta}_{i}\rangle\langle\psi(\phi)^{\beta}_{i}|\}_{i=1}^{d},\ \forall\beta = 1, ..., N. \quad (4)$$

Now the bases of Alice and Bob $\mathfrak{C}_{A}$ and $\mathfrak{C}_{B}$ are correlated in the following sense. Let for any fixed value of β (from $1, 2, ..., N$), Alice and Bob perform measurement in $\mathfrak{B}^{(\beta)}_{A}$ and $\mathfrak{B}^{(\beta)}_{B}$ respectively. In case ρ (shared between them) is a pure entangled state, then perfect correlations (between Alice and Bob's outputs) will imply that if Alice gets outcome $|\psi^{\beta}_{j}\rangle$ then Bob's outcome must be $|\phi^{\beta}_{j}\rangle$ ($\forall\, j$).

After performing measurements on N copies of ρ, a fraction of the measurement outcomes is used to analyze the joint statistics for verifying whether corresponding correlations are nonlocal. Such a verification is made by testing the violation of a Bell inequality. For the remaining part of the measurement outcomes, the parties publicly compare their measurement bases and keep outcomes only corresponding to the correlated bases (discarding the remaining outcomes). These outcomes (obtained from correlated bases) form the raw key [54]. The parties can then extract a secure key from the remaining part of the raw key by performing information reconciliation [48, 58] and privacy amplification [48].

3.2.1 Quantum Bit Error Rate

For any given state ρ, QBER (Q) is defined as the average mismatch between Alice and Bob's outcomes obtained when they measure in correlated bases. With $\mathfrak{C}_{A}$ and $\mathfrak{C}_{B}$ denoting collection of correlated bases (3) of the two parties (as considered above), QBER can be expressed as

$$Q = \frac{1}{N}\sum_{\beta=1}^{N}\sum_{i\neq j=1}^{d}\langle\psi^{\beta}_{i}\phi^{\beta}_{j}|\rho|\psi^{\beta}_{i}\phi^{\beta}_{j}\rangle. \quad (5)$$

The above expression of Q holds for any $N \leq d+1$ number of bases. For instance, when source Λ generates a two-qubit state ($d = 2$) and each party chooses from a collection of two bases, i.e., $|\mathfrak{C}_{A}| = |\mathfrak{C}_{B}| = 2$, QBER is given by [32]

$$Q = \frac{1}{4}(2 - \vec{u_1}.\mathcal{W}\vec{v_1} - \vec{u_2}.\mathcal{W}\vec{v_2}) \quad (6)$$

where $\vec{u}_i, \vec{v}_j$ $(i, j = 1, 2)$ denote Bloch vectors of the measurement bases of Alice and Bob respectively and $\mathcal{W}$ denotes the correlation tensor (1). Minimization over all possible measurement directions $\vec{u}_1, \vec{u}_2, \vec{v}_1, \vec{v}_2$ gives

$$Q \geq \frac{1}{4}(2 - \max_{i,j}(|t_{ii}| + |t_{jj}|)),\ i \neq j \quad (7)$$

where t_{11}, t_{22}, t_{33} denote the singular values of correlation tensor T of ρ' (2) and hence singular values of correlation tensor $\mathcal{W}$ of ρ (1).

3.3 Steering Inequality

Linear steering inequalities, based on linear functions of expectation values of observables, provide a useful way to detect the steerability of a state. In general, if a given state in finite dimensions is steerable, then there exists a linear criterion to exhibit steering [39]. In [39], a linear steering inequality was formulated, under the assumption that both the parties (Alice and Bob) sharing a bipartite state ρ perform n dichotomic quantum measurements (on their respective particles). Cavalcanti, Jones, Wiseman, and Reid (CJWR) derived a series of correlators based inequalities [39] for verifying the steerability of ρ:

$$\mathcal{F}_n(\rho, \nu) = \frac{1}{\sqrt{n}}|\sum_{l=1}^{n}\langle A_l \otimes B_l\rangle| \leq 1 \quad (8)$$

where $A_l = \hat{a}_l \cdot \vec{\sigma}$, $B_l = \hat{b}_l \cdot \vec{\sigma}$ with $\hat{a}_l \in \mathbb{R}^3$ being unit vectors, whereas $\hat{b}_l \in \mathbb{R}^3$ denote orthonormal vectors. $\nu = \{\hat{a}_1, \hat{a}_2, ...\hat{a}_n, \hat{b}_1, \hat{b}_2, ..., \hat{b}_n\}$ stands for the collection of measurement directions, $\langle A_l \otimes B_l\rangle = \mathrm{Tr}(\rho(A_l \otimes B_l))$ and $\rho \in \mathbb{H}_{\mathbb{A}} \otimes \mathbb{H}_{\mathbb{B}}$ is any bipartite quantum state. Violation of Eq. (8) ensures both-way steerability of ρ in the sense that it is steerable from A to B and vice versa. In particular, for $n = 3$, CJWR inequality (8) for three settings takes the form

$$\mathcal{F}_3(\rho, \nu) = \frac{1}{\sqrt{3}}|\sum_{l=1}^{3}\langle A_l \otimes B_l\rangle| \leq 1. \quad (9)$$

In [47], analytical expressions for the upper bound of CJWR steering inequality was formulated in terms of correlation tensor parameters of ρ. Analytical expression of the upper bound of corresponding inequality (9) is given by

$$\mathrm{Max}_{\nu}\mathcal{F}_3(\rho, \nu) = \sqrt{\mathrm{Tr}[\mathcal{W}^T\mathcal{W}]} \quad (10)$$

where $\mathcal{W}$ denote the correlation tensor corresponding to Bloch matrix representation of ρ (1). So, by the linear inequality (9), any two-qubit state ρ (1), shared between A and B is both-way F_3 steerable if

$$\sqrt{Tr[\mathcal{W}^T\mathcal{W}]} > 1. \quad (11)$$

3.4 Local Filtering Operations

Local filtering operations form a special class of sequential quantum operations [49–51]. By applying suitable local filtering operations, the entanglement concentration and nonlocal content of any state ρ can be increased. Let $M^{(1)}_{A(B)}$, $M^{(2)}_{A(B)}$ denote the local filtering operations applied by Alice (Bob) on their respective subsystems. Under the application of these filtering operation, state ρ gets transformed to a new state $\rho^{'}$ [50, 51]:

$$\rho^{'} = \frac{M^{(1)}_A \otimes M^{(1)}_B \rho (M^{(1)}_A \otimes M^{(1)}_B)^{\dagger}}{\mathrm{Tr}[M^{(1)}_A \otimes M^{(1)}_B \rho (M^{(1)}_A \otimes M^{(1)}_B)^{\dagger}]}. \quad (12)$$

For simplicity, we consider $M^{(2)}_{A(B)} = \sqrt{\mathbb{I}_2 - M^{(1)}_{A(B)}}$ with the following specific forms of $M^{(1)}_{A(B)}$:

$$\begin{aligned} M^{(1)}_A &= \epsilon_1|0\rangle\langle 0| + |1\rangle\langle 1| \quad (13)\\ M^{(1)}_B &= \epsilon_2|0\rangle\langle 0| + |1\rangle\langle 1|, \text{ with } \epsilon_1, \epsilon_2 \in [0, 1]. \quad (14)\end{aligned}$$

It may be noted here that local filtering operations for two-qubit states may be considered as single copy entanglement distillation operations [50, 51].

3.5 Absolutely Bell–CHSH local states

An intriguing status is presented by some quantum states which remain Bell–CHSH local even under the application of global unitary operations [52, 53]. Such states are termed as absolutely Bell–CHSH local [53].

If a_1, a_2, a_3, a_4 are eigenvalues of a two-qubit density matrix in descending order $a_1 \geq a_2 \geq a_3 \geq a_4$, then the state is absolutely Bell–CHSH local iff,

$$(2a_1 + 2a_2 - 1)^2 + (2a_1 + 2a_3 - 1)^2 \leq 1. \quad (15)$$

4 Characterizing arbitrary two-qubit states based on Q

In this section, we characterize any given quantum state concerning its utility in a QKD protocol. Before starting our analysis, we first discuss the scenario in detail.

4.1 Measurement Specifications

For our purpose, we consider the usual bipartite entanglement-assisted QKD protocol (Section 3.2) such that ρ shared between Alice and Bob is a two-qubit state ($d = 2$). At this junction, one may note that excepting the dimensionality (2 in this case), neither Alice nor Bob has any other information about ρ. In this protocol, each of the parties performs local measurements on their respective subsystems. Alice chooses randomly from a collection of three projective measurements in arbitrary directions $\mathfrak{C}_A = \{\mathfrak{B}^{(\beta)}_A\}^3_{\beta=1}$. Bob chooses randomly from a collection of three mutually unbiased bases (MUBs [59]): $\mathfrak{C}_B = \{\mathfrak{B}^{(\beta)}_B\}^3_{\beta=1}$. $\mathfrak{B}^{(\beta)}_{A(B)}$ are given by Eq. (3) for $d = 2$. Bases of Bob being mutually unbiased [59], $\langle\phi^{\beta}_i|\phi^{\beta^{'}}_{i^{'}}\rangle = \frac{1}{\sqrt{2}}$ where $i, i^{'} \in \{0, 1\}$ and $\beta \neq \beta^{'}$. Alice cannot use MUBs as this will make her measurements characterized. After making measurements, the parties reconcile their measurement bases publicly. Now with x, y denoting measurements and a, b denoting outcomes of Alice and Bob respectively, the correlation statistics $P(a, b|x, y)$, corresponding to a fraction of raw data (measurement outcomes) is used for checking the F_3 steerability of ρ via the violation of CJWR inequality for three settings (9). Both Alice and Bob perform projective measurements in arbitrary directions: $\vec{u}_i.\vec{\sigma}$ and $\vec{v}_i.\vec{\sigma}$ $(i = 1, 2, 3)$ respectively. $\forall i$, $\vec{u}_i$ and $\vec{v}_i$ represent Bloch vectors of measurement basis with Alice and Bob respectively. Each party choosing from a collection of three bases implies that each of them can choose to perform a projective measurement in any one of three arbitrary directions: $\vec{u}_1, \vec{u}_2, \vec{u}_3$ for Alice and $\vec{v}_1, \vec{v}_2, \vec{v}_3$ for Bob. While $\vec{u}_1, \vec{u}_2, \vec{u}_3$ is only unit vectors, $\vec{v}_1, \vec{v}_2, \vec{v}_3$ are orthonormal vectors so that Bob's measurements are mutually unbiased qubit measurements. Having specified the measurement scenario, we next approach to optimize the QBER (Q) for our scenario.

4.2 Optimization of Q

In a QKD protocol involving three measurement settings per party, Q (5) turns out to be

$$Q = \frac{1}{6}(3 - \sum_{i=1}^{3} \vec{u}_i.\mathcal{W}\vec{v}_i) \quad (16)$$

where $\mathcal{W}$ is the correlation tensor appearing in Bloch matrix representation of ρ (1). Minimization over all possible measurement directions $\vec{u}_1, \vec{u}_2, \vec{u}_3, \vec{v}_1, \vec{v}_2, \vec{v}_3$ gives (see Appendix I)

$$\begin{aligned} Q &\geq Q_{min}, \text{ where,}\\ Q_{min} &= \frac{1}{6}(3 - \sum_{i=1}^{3} t_{ii}). \quad (17)\end{aligned}$$

where $T = \mathrm{diag}(t_{11}, t_{22}, t_{33})$ denote correlation tensor of $\rho^{'}$ (2). As discussed in Section 3, t_{11}, t_{22}, t_{33} are the singular values of correlation tensor $\mathcal{W}$ of ρ (1). Now let ρ be an F_3 unsteerable state. For simplicity, let singular values of its correlation tensor ($\mathcal{W}$) satisfy

$$t^2_{11} + t^2_{22} + t^2_{33} = 1. \quad (18)$$

Now we minimize Q concerning all such possible F_3 unsteerable quantum states. Imposition of such a restriction is required as we are considering the violation of CJWR inequality (9) by ρ necessary for successful key generation in the protocol (using ρ). If Q_0 denote the least possible value of Q under such restriction (see Appendix II), then

$$Q_0 = 0.211. \tag{19}$$

Consequently, when any F_3 unsteerable state is used for key distribution, QBER generated in the protocol cannot be less than 0.211. The minimum error rate (Q_0) may also be referred to as the *critical error rate* of our QKD protocol. However, when any F_3 steerable state is used, QBER can be less than Q_0 (to be discussed in Section 4.4). Critical error rate (Q_0) is obtained for $t_{11} = t_{22} = t_{33} = \frac{1}{\sqrt{3}}$ (see Appendix II).

Having obtained the critical value of QBER (Q_0), we precisely list down the steps used to check the security of our protocol.

4.3 Steps of the QKD Protocol

Consider that N copies of a two-qubit state ρ are generated from a source and distributed between Alice and Bob. Each of them thus receives N qubits (one from each copy of ρ).

Step 1: Some of N copies, for instance, say $k_1 < N$ are used to test CJWR inequality. For that, the parties perform local projective measurements on their respective qubits (as discussed in Section 4.1). If corresponding statistics do not violate the inequality then the protocol is aborted. If the violation is observed then the users perform the next step.

Step 2: They measure remaining $N - k_1$ copies in local bases. Using classical communication, they compare their bases and keep the outputs corresponding to correlated bases only. A portion of those measurement statistics is then used to calculate QBER. If QBER exceeds Q_0, protocol is aborted. Else the remaining outputs corresponding to the correlated bases are used for secure key generation.

We next characterize two-qubit state spaces in the context of secure key generation.

4.4 Characterization of Two Qubit State Space

As already discussed before, here we intend to characterize an arbitrary two-qubit state ρ about its utility in the QKD scenario discussed in Section 3.2. As is evident from our discussion so far in Section 4, analyzing the singular value space of correlation tensor $\mathcal{W}$ (1) suffices for our purpose.

In general, since ρ is a quantum state, each of $t_{11}, t_{22}, t_{33} \in [0, 1]$. Let C denote a unit cuboid:

$$C = \{(t_{11}, t_{22}, t_{33}) : 0 \leq t_{11}, t_{22}, t_{33} \leq 1\}. \tag{20}$$

So density matrix corresponding to any point lying outside the cuboid C (20) does not represent any valid quantum state (see Fig. 1). For the rest of our analysis, we denote the quantum state corresponding to any point R inside C as ρ_R. Now, consider the unit sphere (S, say) with center at the origin given by Eq. (18). Only first octant (S_+, say) of S lies inside C. F_3 unsteerable states reside on and inside S_+. So any point lying inside C but outside S_+ corresponds to an F_3 steerable quantum state (see Fig. 1). Now, as discussed in Section 4.2, when an F_3 unsteerable state ρ is used then $Q \geq Q_0$. This in turn restricts the singular values of $\mathcal{W}$ (corresponding to ρ):

$$t_{11} + t_{22} + t_{33} \leq \sqrt{3}. \tag{21}$$

Eq. (21) represents region lying below a tangent plane to S_+ at the point $P(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})$. Clearly when ρ corresponding to any point lying below or on the tangent plane (21) is used in the protocol, estimated QBER is greater than or at most equal to the critical error rate (Q_0). On the contrary, when ρ used in the protocol corresponds to any point (R, say) lying above the same plane, QBER is less than Q_0. Clearly, in such a case, the point R lies outside S_+ (see Fig. 1). Consequently, ρ_R is F_3 steerable. Under our assumption of CJWR inequality's violation necessary for ensuring secure key generation in the protocol, ρ_R thus turns out to be useful. In this context, we consider *any state ρ as useful in our QKD protocol if QBER obtained in the protocol (using ρ) is less than Q_0*. Hence two-qubit state ρ corresponding to any point lying in C is useful if and only if

$$t_{11} + t_{22} + t_{33} > \sqrt{3}. \tag{22}$$

Now, let us focus on the region lying outside S_+ and inside C. Let L be any point lying in that region. So ρ_L is F_3 steerable. L may lie below or above the tangent plane (21). Utility of ρ_L thus depends on the position of L. To be precise, if L lies above the tangent plane then ρ_L is useful in our protocol whereas ρ_L turns out to be useless in the other case (L lying below the plane). This in turn points out the insufficiency of the F_3 steerability criterion to ensure secure key generation. Three settings CJWR inequality (9) being a Bell-type inequality, our observation simply points out the following:

Violation of a Bell-type inequality by any two-qubit state ρ is necessary but not sufficient to guarantee secure key generation in an entanglement assisted protocol involving ρ.

In practical situations owing to the unavailability of a pure entangled state for key distribution, observation of

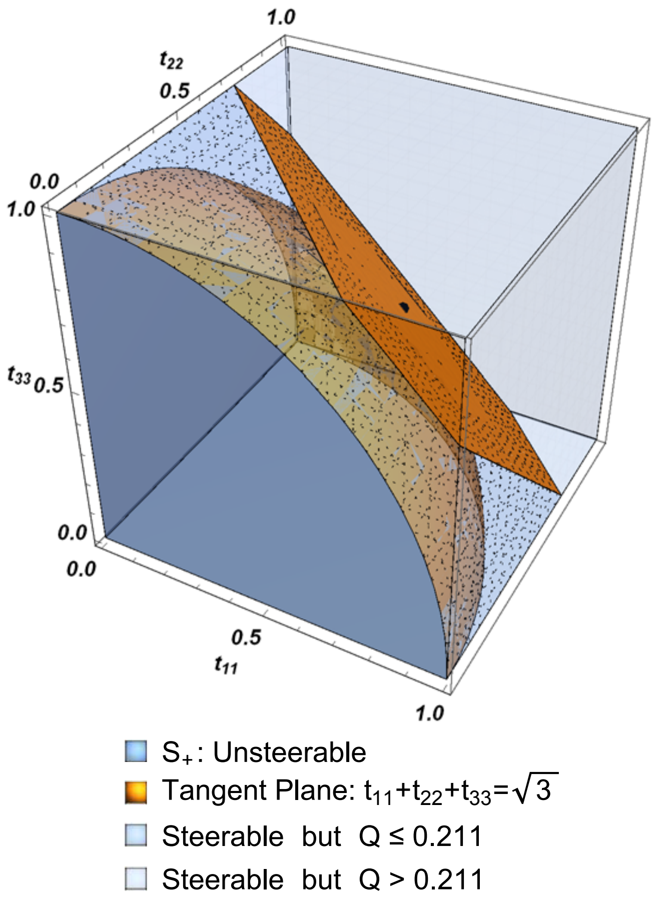

Figure 1: *Singular value space of correlation tensor of an arbitrary two-qubit state considered here. Cuboid indicates all possible two-qubit states whereas any point from the first octant S_+ of sphere S (18) gives F_3 unsteerable state. The region lying outside S_+ and below the tangent plane at $P(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})$ indicates steerable but useless states whereas that lying above the tangent plane gives useful states.*

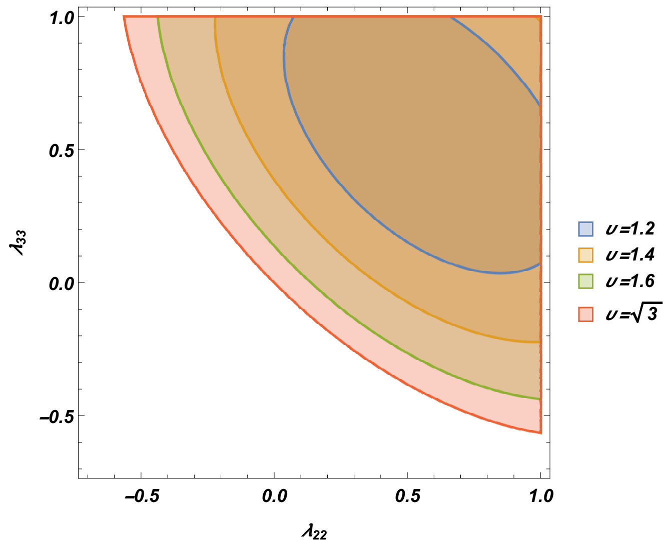

Figure 2: *Shaded regions give two-qubit states useful for QKD for some specific violation amounts of CJWR inequality observed in the protocol.*

maximal violation of CJWR inequality becomes impossible. Hence, based on the amount of violation, identifying two-qubit entangled states useful in entanglement-assisted QKD protocol is important from a practical view point.

Identifying Useful States: Let in a QKD protocol, CJWR inequality (9) be violated by some fixed amount $\mathcal{V}$ (say). Let ϱ be some unknown two-qubit state used in the corresponding protocol. Let $\lambda_{11}, \lambda_{22}, \lambda_{33}$ denote the singular values of the correlation tensor of ϱ. Violation being observed, restriction is imposed on these three unknown (as ϱ is unknown) quantities, namely

$$\begin{aligned}\lambda_{11}^2+\lambda_{22}^2+\lambda_{33}^2 &= \mathcal{V}^2\\ \text{Alternatively, } \lambda_{11} &= \sqrt{\mathcal{V}^2-\lambda_{22}^2-\lambda_{33}^2}. \end{aligned} \quad (23)$$

Now ϱ is useful for secure key generation in the protocol if it satisfies Eq. (22). Hence, ϱ is useful if

$$\sqrt{3}-\lambda_{33}-\lambda_{22} < \sqrt{\mathcal{V}^2-\lambda_{22}^2-\lambda_{33}^2} \leq 1. \quad (24)$$

Eq. (24) thus specifies the criterion required to be satisfied by an unknown state provided $\mathcal{V}$ amount of violation of CJWR inequality is observed in the protocol (see Fig. 2).

4.5 Illustrations

Let us now analyze the above characterization for a few well-known classes of two qubit states.

Bell Diagonal states: The class of Bell diagonal states [7] is represented as follows

$$\varrho_{Bell} = w_1|\psi^-\rangle\langle\psi^-|+w_2|\phi^+\rangle\langle\phi^+|+w_3|\phi^-\rangle\langle\phi^-|+w_4|\psi^+\rangle\langle\psi^+|, \quad (25)$$

with $w_i \in [0,1]$ $\forall i = 1,2,3,4$, $\sum_{i=1}^4 w_i = 1$ and $|\phi^\pm\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$, $|\psi^\pm\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$ denote the Bell states. Eq. (25) is often referred to as the class of states having maximally mixed marginals.

The correlation matrix is given by diag$(1-2(w_1+w_3), 1-2(w_2+w_3), 1-2(w_1+w_2))$. Bell diagonal states are F_3 steerable provided the following relation holds

$$\sqrt{8\left(\sum_{i,j=1}^{3} w_i * w_j + w_4\right) - 5} > 1. \quad (26)$$

On the other hand, Bell diagonal states useful for QKD protocol(satisfying Eq. (22)) are characterized by

$$\sum_{i,j=1}^{3} |1-2(w_i+w_j)| > \sqrt{3}, \text{ where } i \neq j. \quad (27)$$

Combination of Eqs. (26,27) points out that not all F_3 steerable states from this family are useful for our QKD protocol (see Fig. 3).

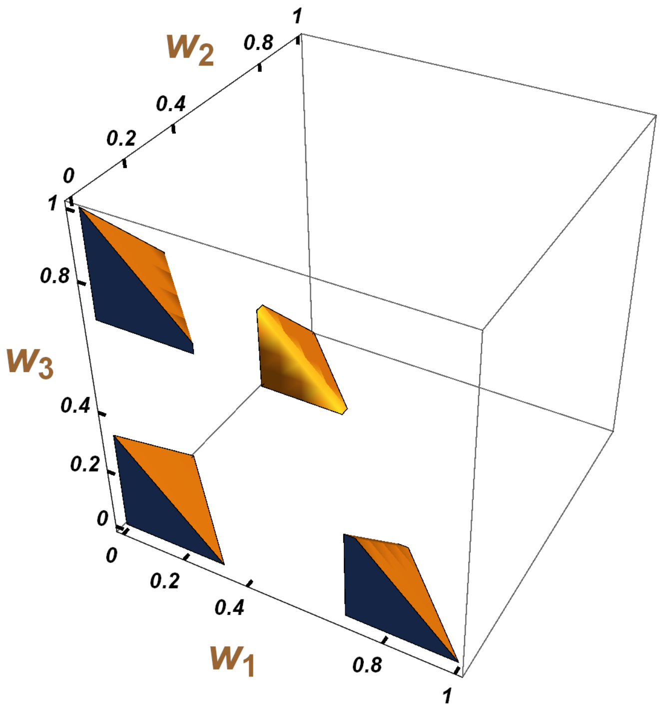

Figure 3: *Shaded region forms a part of parameter space of the Bell diagonal family (25). Bell diagonal state corresponding to any point in the shaded region is useful in QKD protocol.*

Now let us consider the Werner class of states from the family of Bell diagonal states

$$\varrho_W = \omega|\psi^-\rangle\langle\psi^-| + \frac{(1-\omega)}{4}\mathbb{I}_2 \times \mathbb{I}_2,\ \omega \in [0,1]. \quad (28)$$

For $\omega \in (0.5772, 1]$ corresponding member from Werner class (28) is F_3 steerable. Again Eq. (22) is satisfied for the same range of values of ω. Consequently for this subclass of Bell diagonal states (25), any F_3 steerable state is always useful in QKD protocol.

Family of States Not Diagonal in Bell Basis: Consider the following class [60, 61]

$$\gamma = q|\varphi\rangle\langle\varphi| + (1-q)|00\rangle\langle 00| \quad (29)$$

where $|\varphi\rangle = \cos\alpha|10\rangle + \sin\alpha|01\rangle$, with $\alpha \in [0, \frac{\pi}{4}]$ and $0 \leq q \leq 1$. This class of states was used in [60] for increasing maximally entangled fractions in an entanglement swapping network. Correlation tensor is given by diag$(q\sin 2\alpha, q\sin 2\alpha, 1-2q)$. A member from this family is F_3 steerable if

$$2q^2\sin^2 2\alpha + (1-2q)^2 > 1. \quad (30)$$

Again any state from this class is useful in QKD protocol in case it satisfies the following relation

$$2q\sin 2\alpha + |1-2q| > \sqrt{3}. \quad (31)$$

The QKD protocol will run successfully if states satisfying both the above relations (Eqs. (30,31)) are used in the protocol (see Fig. 4).

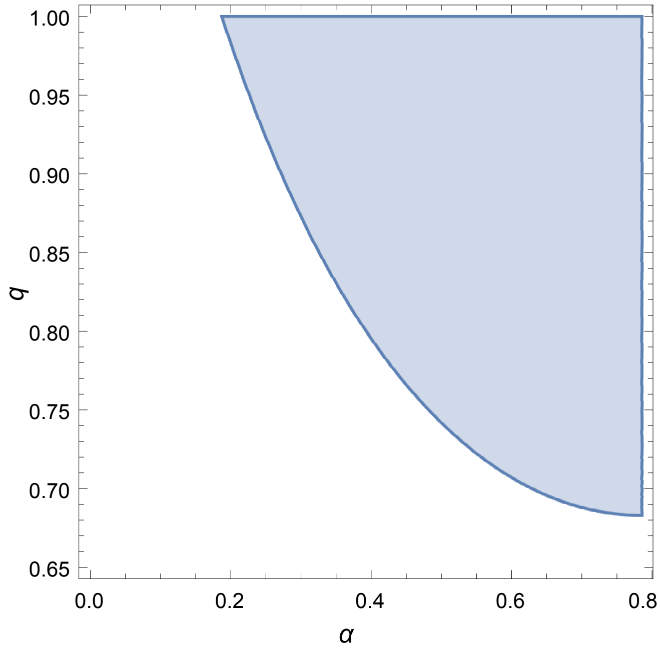

Figure 4: *Shaded region gives the states (29) which can be used for secure key generation.*

4.6 Higher Tolerance to QBER

Owing to the communication of quantum states over noisy channels, non-zero QBER is generated in any entanglement-assisted QKD protocol even in absence of any eavesdropper. For analyzing QBER tolerance in CHSH-based protocol with that in CJWR-based one, we assume that the QKD protocol involves only the legitimate users (Alice and Bob), i.e., the absence of any third party (eavesdropper). In [32], it was shown that an arbitrary two-qubit state is useful in standard entanglement-assisted QKD protocol (involving Bell–CHSH violation) if

$$\text{Max}\{t_{11} + t_{22}, t_{33} + t_{22}, t_{11} + t_{33}\} > \sqrt{2}. \quad (32)$$

However, the same state is useful in our protocol if it satisfies Eq. (22). Comparison of Eqs. (22,32) points out existence of two qubit states (see Fig. 5) satisfying Eqs. (22) but violating Eq. (32). Let us now explore with few specific instances in this regard.

Consider the family of Bell diagonal states (25). Any state from this family is not useful in the protocol relying on Bell–CHSH violation if

$$\text{Max}_{i,j=1}^{3}|1 - 2(w_i + w_j)| \leq \sqrt{2}, \text{ where } i \neq j. \quad (33)$$

However, the same state is useful in our protocol if Eq. (27) is satisfied. There exist states from this family (see Fig. 6) which satisfy both Eqs. (27,33).

For a more specific instance from this family (25), let us consider the Werner class of states (28). Any member from this subclass of Bell diagonal states, characterized

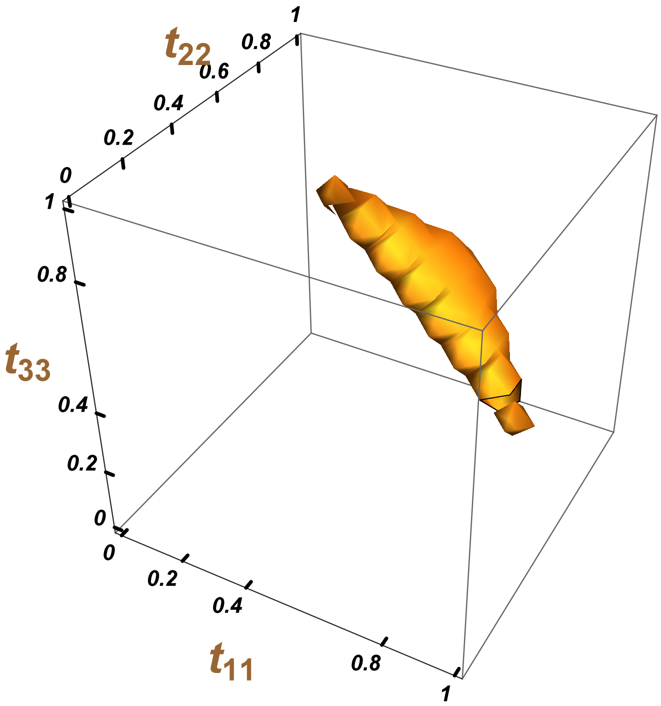

Figure 5: Shaded region forms a part of singular value space of correlation tensor of an arbitrary two-qubit state. State corresponding to any point from this region is useless in CHSH-based QKD protocol whereas the same is useful in our protocol.

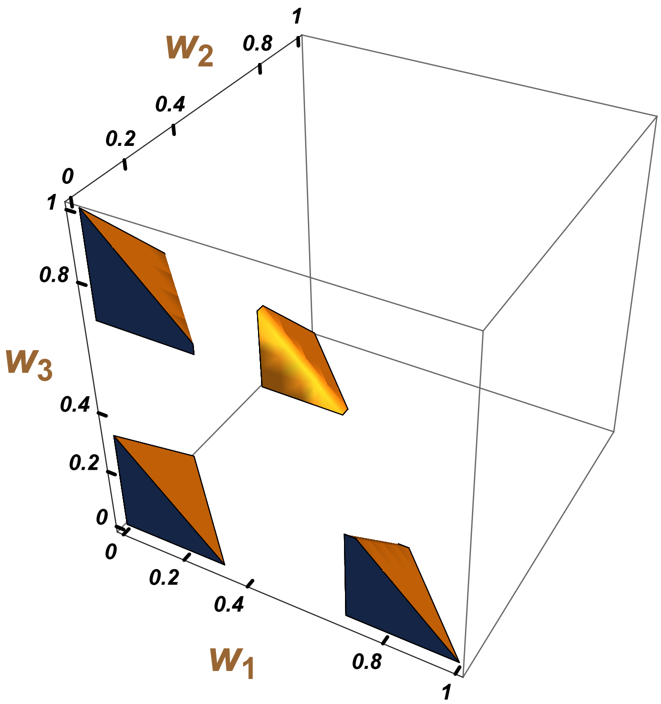

Figure 6: Shaded part of parameter space of Bell diagonal family (25) gives states useful in CJWR-based QKD protocol but useless in CHSH-based protocol.

by $\omega \in (0.5, 0.707]$, is useful in QKD protocol only if the protocol relies on violation of CJWR inequality.

For the family of states given by Eq. (29), a state is not

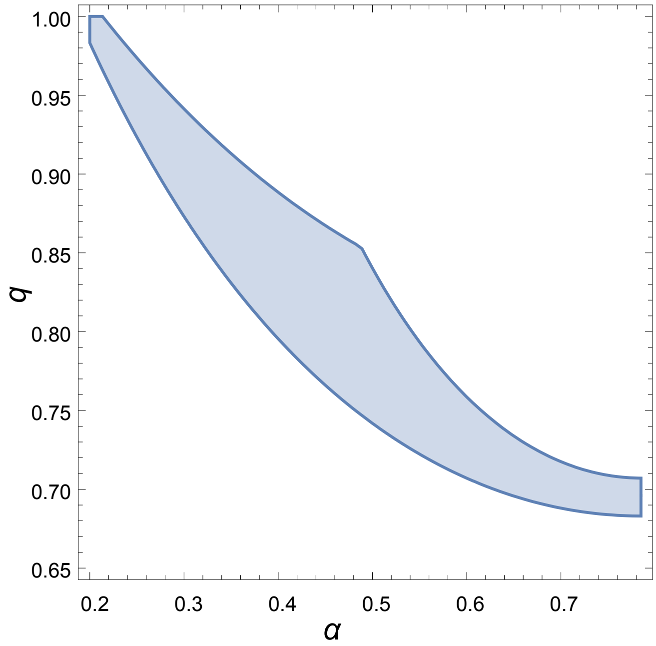

Figure 7: Shaded part of parameter space of family of states given by Eq. (29)) gives states useful in CJWR-based QKD protocol but useless in CHSH-based protocol.

useful in CHSH-based QKD protocol if

$$\mathrm{Max}\{2q\sin 2\alpha, q\sin 2\alpha + |1-2q|\} > \sqrt{2}. \tag{34}$$

Comparing Eq. (34) with Eq. (31), we get states that can be used in our protocol but are useless in CHSH-based ones (Fig. 7).

As discussed in Section 4.2, whenever an unsteerable state is used in our protocol QBER can never be less than $Q_0 = 0.211$. Critical value of QBER for our protocol (based on CJWR inequality) is greater than that obtained in the protocol when it relies upon Bell–CHSH inequality where $Q_0 = 0.14$ [32]. Hence, for any state ρ, if QBER in QKD protocol (assuming the absence of any eavesdropper) lies in the range $(0.14, 0.211]$, then the protocol can be used if it relies upon CJWR inequality's violation but cannot be used if it is based on Bell–CHSH violation. Consequently, the protocol turns out to be more QBER tolerant when based upon the notion of steerability compared to that obtained in Bell–CHSH-based QKD protocol.

5 Incorporating Local Filtering Operations in QKD

As noted before, local filtering operations are crucial to enhance utility in information processing tasks [62–64]. Let us now consider an entanglement-assisted protocol where both parties can perform local filtering operations before measuring their subsystems in correlated bases. We next discuss the protocol in detail.

5.1 Modified QKD Protocol

The steps of the protocol are specified below:

- Source Λ distributes many copies of a two qubit state (ρ) between the two parties Alice and Bob.
- On receiving the qubits, the parties perform full-state tomography.
- Being ensured that the shared state is an entangled state they perform local filtering operations: Alice using operators $\{M_A^{(1)}, M_A^{(2)}\}$ and Bob performing $\{M_B^{(1)}, M_B^{(2)}\}$ where the operators are specified in Section 3.4.
  It is known that in QKD protocols the optical system adopts a prescription wherein the photons are destroyed due to measurements. Hence the intermediate step given below is crucial.
- *Postselection of outcomes*: After completion of measurements, they announce the outcome of measurements in $\{M_A^{(i)}\}$ and $\{M_B^{(j)}\}$. They postselect those qubit pairs for which $M_A^{(1)}$ and $M_B^{(1)}$ clicked. Only these qubit pairs are considered further in the protocol discarding the remaining ones. Each pair of two-qubit states selected is denoted by $\rho^{'}$.
- Rest of the protocol runs as usual (Section 4.1).

5.2 Expression of $Q^{'}_{min}$

Let us now formulate the expression of $Q^{'}_{min}$, i.e., Q_{min} obtained from postselected state (obtained corresponding to clicking of measurement $M_A^{(1)}$ and $M_B^{(1)}$). Firstly, P_{succ} (possibility of measurement $M_A^{(1)}$ and $M_B^{(1)}$ clicking) takes the form

$$P_{succ} = \mathrm{Tr}[M_A^{(1)} \otimes M_B^{(1)} \rho (M_A^{(1)} \otimes M_B^{(1)})^{\dagger}], \qquad (35)$$

where $M_A^{(1)}, M_B^{(1)}$ are given by Eq. (13). Correlation tensor ($T_{filtered}$, say) of corresponding postselected state ($\rho_{filtered}$, say) obtained from the initial state $\rho^{'}$ (2) is given by

$$T_{filtered} = \begin{pmatrix} \epsilon_1\epsilon_2 t_{11} & 0 & \frac{1}{2}\mathfrak{m}_1\epsilon_1(\epsilon_2^2-1) \\ 0 & \epsilon_1\epsilon_2 t_{22} & \frac{1}{2}\mathfrak{m}_2\epsilon_1(\epsilon_2^2-1) \\ \frac{1}{2}\mathfrak{n}_1\epsilon_2(\epsilon_1^2-1) & \frac{1}{2}\mathfrak{n}_2\epsilon_2(\epsilon_1^2-1) & \frac{1}{4}(h_- - r_- - \epsilon_2^2(h_- + r_-) - \epsilon_1^2(h_+ - r_+) + \epsilon_2^2(h_+ + r_+)) \end{pmatrix} \qquad (36)$$

where $h_{\pm} = 1 \pm \mathfrak{m}_3$, $r_{\pm} = \mathfrak{n}_3 \pm t_{33}$. Sum of the singular values of $T_{filtered}$ (36) being given by trace of the matrix $\sqrt{(T_{filtered})^{*}T_{filtered}}$, QBER ($Q$) in the modified protocol is given by

$$Q^{'}_{min} = P_{succ} * \frac{1}{6}(3 - 2\sqrt{\sum_{i=1}^{2}(\epsilon_2^2(1-\epsilon_1^2)^2\mathfrak{n}_i^2 + 4\epsilon_1^2 t_{ii}^2) - \sqrt{\mathbf{B}}}) \qquad (37)$$

where $\mathbf{B}$ is a function of ϵ_1, ϵ_2:

$$\mathbf{B} = \epsilon_1^2\left(1-\epsilon_2^2\right)^2\left(\mathfrak{m}_1^2+\mathfrak{m}_2^2\right) + \left(h_- - r_- - \epsilon_2^2\left(h_- + r_-\right) + \epsilon_1^2\left(-h_+ + r_+ + \epsilon_2^2\left(h_+ + r_+\right)\right)\right)^2. \qquad (38)$$

Explicit form of success probability P_{succ} is given by

$$P_{succ} = \frac{1}{h_- - r_- + \epsilon_2^2(h_- + r_-) + \epsilon_1^2(h_+ - r_+ + \epsilon_2^2(h_+ + r_+))}. \qquad (39)$$

$Q^{'}_{min} < Q_0$ can thus be written as:

$$2\sqrt{\sum_{i=1}^{2}(\epsilon_2^2(1-\epsilon_1^2)^2\mathfrak{n}_i^2 + 4\epsilon_1^2 t_{ii}^2) - \sqrt{\mathbf{B}}} > 3 - Q_0 * \frac{6}{P_{succ}}. \qquad (40)$$

The above relation (40) in turn characterizes the states useful in the QKD after applying suitable local filtering operations of the form given by Eq. (13). For further discussion in this section, we will refer to this QKD protocol (with filtering operations) as *Modified QKD protocol* while that without any filtering operations as QKD protocol only. There exist two qubit states violating Eq. (22) but satisfying Eq. (40) for some values of ϵ_1, ϵ_2. Next, we provide some specific examples in support of our claim.

5.3 Illustrations

Consider the family of states given by Eq. (29). F_3 steerable members from this class which are useless in the QKD violate Eq. (31). Let any such F_3 steerable state be used in the modified protocol. For some suitable local filtering operations (specific values of ϵ_1, ϵ_2 in Eq. (13)), the protocol runs successfully (see Fig. 8, with the specific values mentioned therein). For a particular instance, consider $\alpha = 0.25$, $q = 0.9$ in Eq. (29). Before filtering $Q_{min} = 0.22839 > Q_0$. On using this state in the modified QKD protocol with $\epsilon_1 = 0.16119$ and $\epsilon_2 = 0.12563$, $P_{succ} \approx 0.015$, and by Eq. (37), $Q^{'}_{min} = 0.13756$. As $Q^{'}_{min} < Q_0$, so successful key generation takes place in the protocol. For some fixed values of α, range of noise level parameter q for useful states (30) are given in Table 1. Now, for obvious reasons, not all local filtering operations (13) turn out to be useful in the modified protocol. Depending on the state to be used, (ϵ_1, ϵ_2), parameterizing these operations (13) are to be selected. For the above class of states (29) considered, a suitable range of (ϵ_1, ϵ_2) is shown in Fig. 9.

Next, let F_3 unsteerable states [violating Eq. (30)] from this family be used in the modified protocol. Again for some suitable filtering operations made by the users, secure key generation becomes possible for some of these F_3 unsteerable states (see Fig. 9). Some specific instances are given in Table 1.

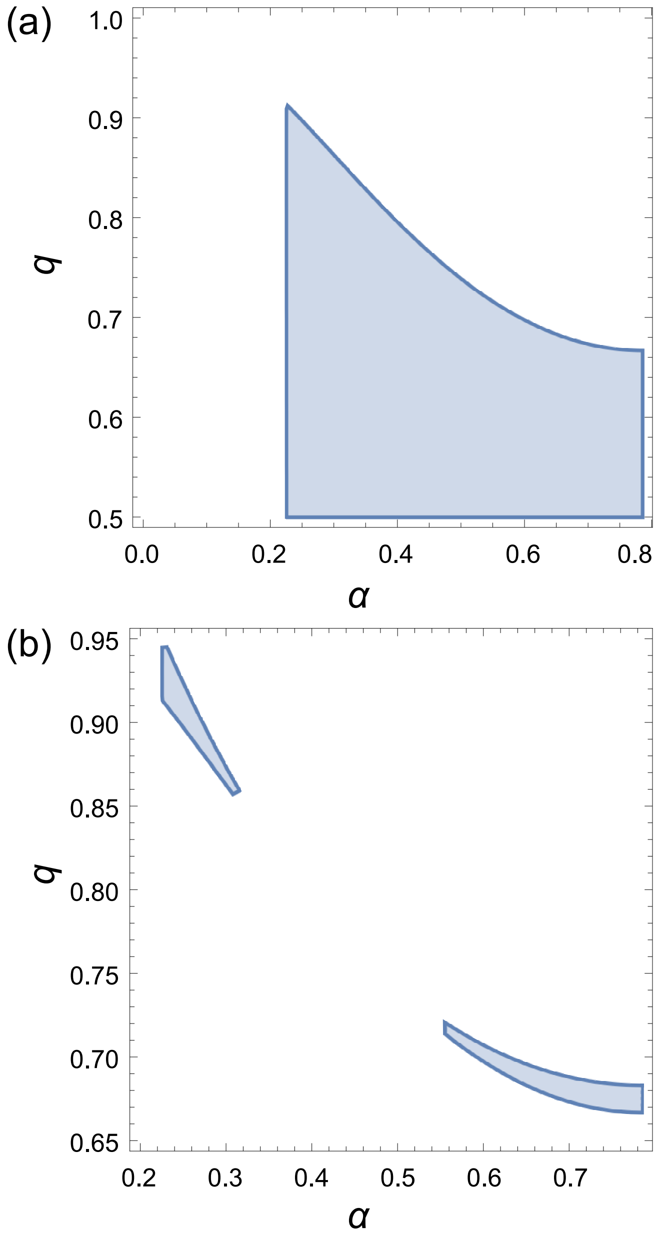

Figure 8: *Shaded region in subfigure (a) gives the unsteerable states (29) useful in the modified QKD protocol for* $\epsilon_1 = 0.02119$ *and* $\epsilon_2 = 0.02563$. *Similarly, the shaded region in subfigure (b) gives steerable states that are useful in the same modified protocol (i.e., for* $\epsilon_1 = 0.02119$ *and* $\epsilon_2 = 0.02563$*). None of these states (in both subfigures) is useful in the QKD protocol (without filtering operations).*

5.4 Other Local Filters

Now, as already stated before in Section 3, the form of filters (13) is not general. Depending on the state provided, another form of filters may also turn out to be suitable in the modified protocol. For instance, consider the well-known family of Gisin states [50]:

$$\gamma = s|\varphi\rangle\langle\varphi| + \frac{1-s}{2}(|11\rangle\langle 11| + |00\rangle\langle 00|) \qquad (41)$$

where $|\varphi\rangle = \cos\beta|01\rangle + \sin\beta|1\rangle$, with $\beta \in [0, \frac{\pi}{4}]$ and $0 \leq s \leq 1$. Correlation tensor of this class of states is $\text{diag}(s\sin 2\beta, s\sin 2\beta, 1-2s)$. Suitable local filters for this state are of the form [65]:

$$F_A^{(1)} = \sqrt{\tan(\beta)}|0\rangle\langle 0| + |1\rangle\langle 1| \qquad (42)$$

$$F_B^{(1)} = |0\rangle\langle 0| + \sqrt{\tan(\beta)}|1\rangle\langle 1| \qquad (43)$$

Correlation tensor of the postselected state [output corresponding to above filters (42)] is given by $\frac{1}{1-s+s\sin 2\beta}\text{diag}(s\sin 2\beta, s\sin 2\beta, -1+s+s\sin 2\beta)$. There exist members from this class of states (41), which turn out to be useful in our modified QKD protocol (see Fig. 10). For a particular example, consider the

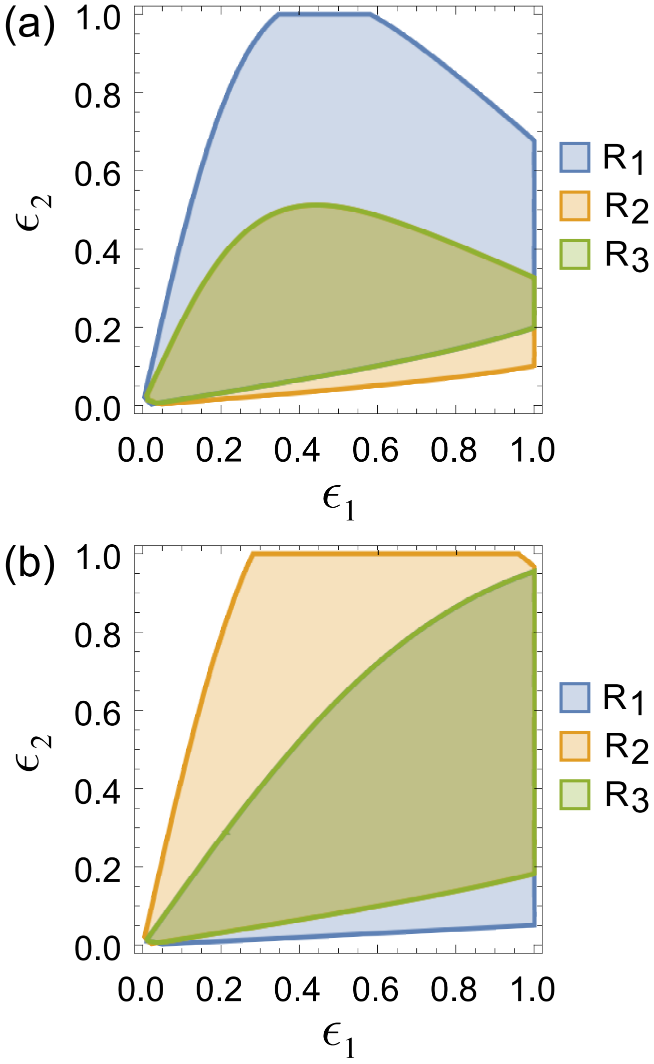

Figure 9: *The parameter space (ϵ_1, ϵ_2) characterizing local filtering operations is considered in both subfigures. Shaded regions characterize suitable local filtering operations (used in the modified QKD protocol) for some specific states from the class given by Eq. (29). Consider two F_3 unsteerable states specified by $(q, \alpha) = (0.6, 0.7)$ and $(q, \alpha) = (0.5, 0.4)$. In subfigure (a), any point in the region $R_1 \cup R_2$ gives suitable local filters for the first state, whereas that for the second state is given by any point from the region $R_2 \cup R_3$. Next consider two steerable states: $(q, \alpha) = (0.9, 0.26)$ and $(q, \alpha) = (0.68, 0.7)$. In subfigure (b), suitable local filters for these two steerable states are given by any point from region $R_1 \cup R_2$ and $R_2 \cup R_3$, respectively.*

state specified by $s = 0.87$ and $\beta = 0.29$. For this state $Q_{min} = 0.21774$. Success probability (P_{succ}) that $F_A^{(1)} \otimes F_B^{(1)}$ will click is 0.18 and $Q'_{min} = 0.14283$. The state is thus useful in the modified QKD protocol but cannot be used for the secure key generation before filtering.

After discussing how our QKD protocol can be modified by allowing the users to apply local filtering operations, we next consider another significant aspect of our protocol.

Table 1: *Modified QKD protocol with $\epsilon_1 = 0.15$, $\epsilon_2 = 0.02563$ is considered. For some specific values of state parameter α, range of the other parameter q is specified for which corresponding state is useful for secure key generation in this modified QKD protocol. The second column in the table indicates whether the state used in the protocol violates CJWR inequality or not. The last two instances point out the fact that initially F_3 unsteerable states can also be used for the modified QKD protocol.*

State parameter	F_3 Steerability	Range of q
$\alpha = 0.24$	Steerable	[0.904, 1]
$\alpha = 0.7$	Steerable	[0.674, 1]
$\alpha = 0.2$	Unsteerable	[0.5, 1]
$\alpha = 0.6$	Unsteerable	[0.52, 1]

6 Absolute Bell–CHSH Local States In Secure Key Generation

Our QKD protocol is semi-device independent in the sense that the source distributing the particles (among the parties) is not trusted but both the parties perform quantum measurements (see Section 3.3). So entangled state is distributed from some unknown source Λ. Let an untrusted third party Eve has access to Λ. So if ρ be the state generated from Λ, then Eve has access to both the qubits of ρ. Let, Eve measure ρ in some suitable global basis such that ρ transforms into ρ', where ρ' remains entangled but becomes Bell–CHSH local in the new basis. Under the control of Eve, source Λ thus distributes an absolutely Bell–CHSH local state ρ' between Alice and Bob in the protocol. Unlike that any standard QKD protocol relying on Bell–CHSH violation, our protocol can securely generate keys for some of these states. Owing to the existence of absolutely Bell–CHSH local F_3 steerable two-qubit states, our QKD protocol gives an advantage over the standard ones. We provide an example below.

Consider the family of Bell diagonal states (25). Parameters of absolutely Bell–CHSH local states from this family satisfy [53]:

$$\mathrm{Max}_{(i,j,k)}[1 - 4(w_i - w_i^2 - w_i * w_j - w_i * w_k) \\ -2(w_j + w_k - w_j^2 - w_k^2)] \leq \frac{1}{2} \quad (44)$$

where (i, j, k) denote all possible cyclic permutations

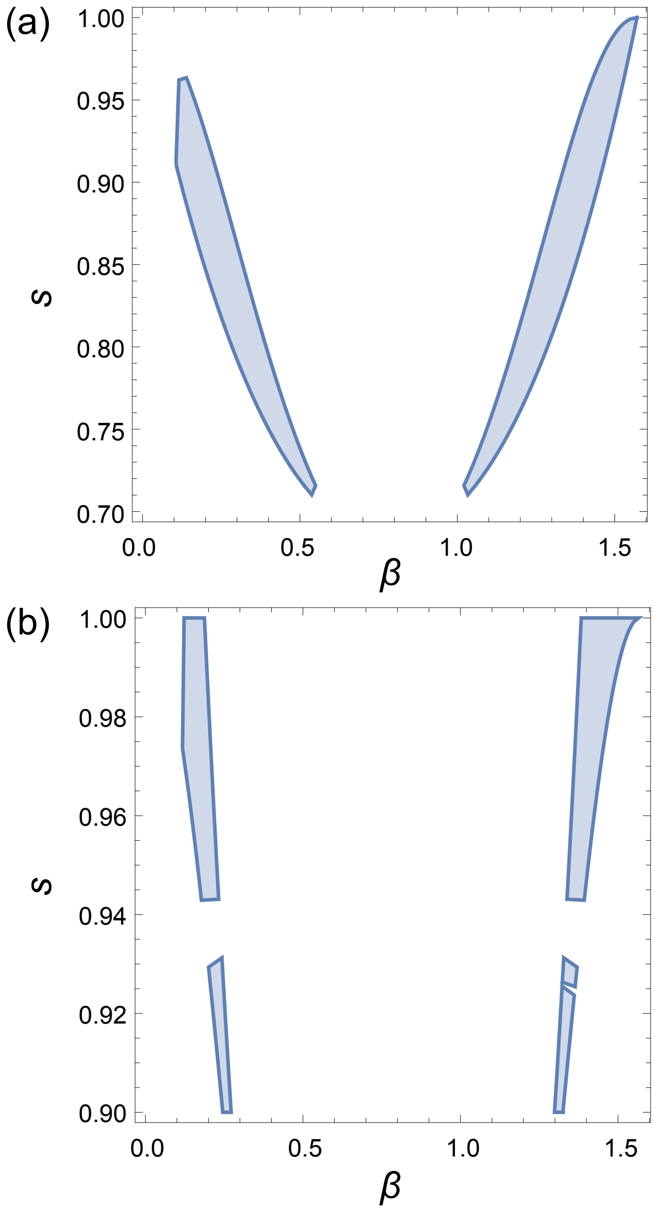

Figure 10: *Subfigure (a) gives F_3 unsteerable states (41) useful in the modified QKD protocol. Similarly, the shaded region in subfigure (b) gives steerable states that are useful in the modified protocol. None of these states (in both subfigures) is useful in the QKD protocol (without filtering operations).*

(of length three) over $1, 2, 3$: $(1, 2, 3)$, $(2, 3, 1)$ $(3, 1, 2)$. Let any such state gets distributed between the two users of the protocol. Some of these states satisfy Eq. (27). Consequently, the protocol runs successfully for them (see Fig. 11).

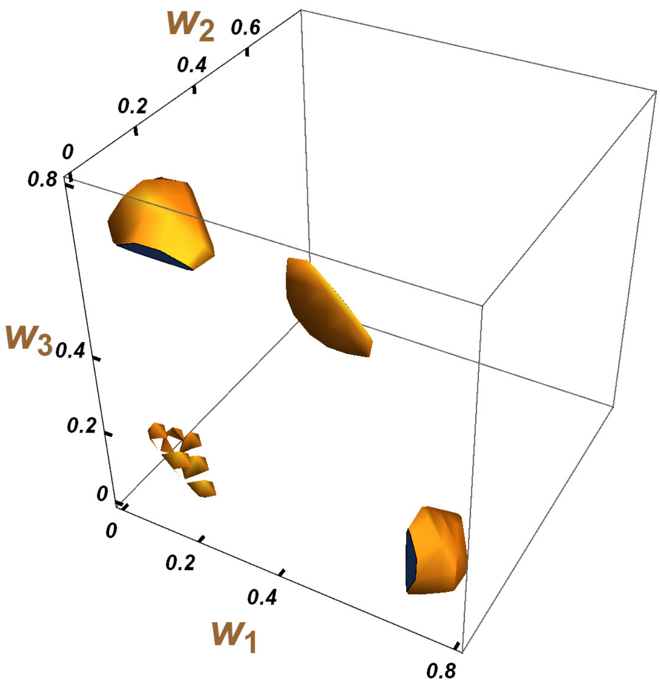

Figure 11: *Corresponding to any point from the shaded regions of the parameter space (w_1, w_2, w_3), absolutely local Bell diagonal state (25) is useful in our QKD protocol.*

7 Discussion

The notion of Bell nonlocality has been rigorously analyzed concerning the study of QKD in entanglement-assisted protocols. However, whether Bell's violation provides a sufficient criterion is a matter of great debate. The present discussion points out the insufficiency of a Bell-type inequality in this perspective. CJWR inequality (9), a Bell-type inequality for detecting the steerability is used here, to prescribe a QKD protocol. Using the notion of F_3 steerability, characterization of arbitrary two-qubit state is obtained in the context of its usefulness in QKD protocol. Interestingly, any F_3 steerable Werner state is useful in QKD protocol. For any amount of violation $\mathcal{V}$ of Eq. (9), one can identify whether the state (giving $\mathcal{V}$ amount of violation) is useful in the protocol or not. Such identification is completely based on the singular values of the correlation tensor of the corresponding state.

Furthermore, in case local filtering operations are allowed (before the users perform local base measurements) in the protocol, some F_3 unsteerable states become useful in the modified QKD protocol. The utility of absolutely local Bell–CHSH states in our modified protocol further buttresses our work.

Critical quantum bit error rate Q_0 (19) in our protocol is greater than that obtained for protocol depending on Bell–CHSH nonlocality ($Q_0 = 0.14$ [32]). Increased number of measurement settings per party (2 in [32] and 3 here) is one of the potent causes for such a contrast.

To perform entanglement based QKD protocols, one needs to transmit part of quantum systems through noisy channels, which can in turn affect the state of the quantum systems. In this non-ideal scenario identification of states offering utility in QKD assumes significance, which our work addresses.

In experimental situations, there exist loopholes in testing any correlator-based inequality. Owing to experimental imperfections, testing CJWR inequality (Bell-type inequality) may suffer from three major loopholes: locality loopholes (due to hidden communication between the parties [66, 67]), detection loopholes (due to unfair sampling of ensemble which is measured [68]) and freedom-of-choice loophole (owing to possible influences from or on the selection of measurement settings [69]). Our protocol, being based on CJWR violation, these loopholes will exist in any experimental demonstration of the same. Also, classical communication over a public channel (for key generation) forms a potent factor of experimental imperfections. Furthermore, in the modified QKD protocol, the parties need to perform full tomography (involving classical communication between the parties) on the quantum state received from the source. After state tomography, in case the state turns out to be an entangled one, local filtering operations are performed followed by the usual steps of QKD protocol. The parties need to communicate classically for performing state tomography which may again potentially open up loopholes for the protocol. In [70], an experimental demonstration of Einstein–Podolsky–Rosen steering has been provided where each of detection, locality, and freedom of choice loophole is closed simultaneously. It will be interesting to explore possible means of closing the loopholes arising in our protocol.

As already specified before, the entire analysis in our work is applicable for those QKD protocols where the secure key rate is a function of QBER (Q) only [25]. However owing to the complexity of practical situations, $\mathfrak{r}_{min}$ may depend on many other factors. So, characterizing arbitrary two-qubit states for more general QKDs is a potential source of future research. A generalization of the scheme to include other Bell-like inequalities also warrants attention. Also, it will be interesting to analyze the situation when the users of the protocol do not have any knowledge about the dimension of the quantum state distributed by the source.

Acknowledgement

Tapaswini Patro would like to acknowledge the support from DST-Inspire fellowship No. DST/INSPIRE Fellowship/2019/IF190357. We are grateful to Shashank Gupta for his useful insights.

Author contributions

K. Mukherjee developed the main idea of the work, performed the analysis, and wrote the paper. N. Ganguly and T. Patro cross-checked the findings and also assisted K. Mukherjee in writing the paper. All the authors have read and approved the final manuscript.

8 Appendix I

8.1 Proof regarding optimization of $\mathcal{Q}$ (16)

Let $\vec{\mathfrak{m}} = (m_1, m_2, m_3)$ denote an arbitrary direction. Eigenbasis operators corresponding to projective measurement along $\vec{\mathfrak{m}}$ are given by $\{\frac{\mathbb{I}_2+\vec{\mathfrak{m}}.\vec{\sigma}}{2}, \frac{\mathbb{I}_2-\vec{\mathfrak{m}}.\vec{\sigma}}{2}\}$. Now, as discussed in the main text, in our QKD protocol each of Alice and Bob perform projective measurements along any one of three arbitrary directions: $\vec{u}_1, \vec{u}_2, \vec{u}_3$ for Alice and $\vec{v}_1, \vec{v}_2, \vec{v}_3$ for Bob. So for Alice the collection of measurement basis operators (4) is given by

$$O_A^{(j)} = \{\frac{\mathbb{I}_2 + \vec{u}_j.\vec{\sigma}}{2}, \frac{\mathbb{I}_2 - \vec{u}_j.\vec{\sigma}}{2}\}, \; j = 1, 2, 3. \tag{45}$$

Similarly, collection of measurement basis operators of Bob is given by

$$O_B^{(j)} = \{\frac{\mathbb{I}_2 + \vec{v}_j.\vec{\sigma}}{2}, \frac{\mathbb{I}_2 - \vec{v}_j.\vec{\sigma}}{2}\}, \; j = 1, 2, 3. \tag{46}$$

As discussed in the main text, corresponding to correlated bases of Alice and Bob, the operator bases are given by $O_A^{(j)}, O_B^{(j)} (j = 1, 2, 3)$.

An arbitrary two qubit state ρ (1) is shared between Alice and Bob. In case Alice and Bob measure $\vec{u}_i.\vec{\sigma}, \vec{v}_i.\vec{\sigma}$, probability of them obtaining mismatching outputs while measuring in correlated bases is given by

$$P_j = \frac{1}{4} \sum_{i=0,1} \mathrm{Tr}[(\mathbb{I}_2 + (-1)^i \vec{u}_j.\vec{\sigma}) \otimes (\mathbb{I}_2 + (-1)^{i+1} \vec{v}_j.\vec{\sigma}).\rho], \tag{47}$$

$\forall\, j = 1, 2, 3$. Using Eq. (47) the expression for quantum bit error rate Q (5) becomes

$$\begin{aligned} Q &= \sum_{i=1}^{3} P_i = \frac{1}{6}(3 - \sum_{i=1}^{3} \sum_{j=1}^{3} u_{ij} \sum_{k=1}^{3} w_{jk} v_{ik}) \\ &= \frac{1}{6}(3 - \sum_{i=1}^{3} \vec{u}_i.W\vec{v}_i), \end{aligned} \tag{48}$$

where $\vec{u}_i = (u_{i1}, u_{i2}, u_{i3})^t$ and $\vec{v}_i = (v_{i1}, v_{i2}, v_{i3}), \forall i = 1, 2, 3$. Eq. (48) gives Eq. (16).

8.2 Proof of Eq. (17)

We perform minimization of Q over all possible bases of the two parties. Clearly Q is summation of the probability terms appearing in Eq. (47). Let us introduce a few notations $G_i^{z_1}$, $H_i^{z_2}, \forall i = 1, 2, 3$ for ease of use in further calculations

$$
\begin{aligned}
G_i^{z_1} &= \frac{1}{2}(\mathbb{I}_2 + (-1)^{z_1}\vec{u_i}.\vec{\sigma}),\ z_1 = 0, 1 && (49)\\
H_i^{z_2} &= \frac{1}{2}(\mathbb{I}_2 + (-1)^{z_2}\vec{v_i}.\vec{\sigma}),\ z_2 = 0, 1. && (50)
\end{aligned}
$$

Now, let L_a and L_b denote the local unitary operations such that

$$\rho = (L_a \otimes L_b)\rho^{'}(L_a \otimes L_b)^{\dagger}. \tag{51}$$

Let the unitary operations be specified as follows

$$L_{a(b)} = \begin{pmatrix} l_{a(b)}^{(11)} & l_{a(b)}^{(12)} \\ l_{a(b)}^{(21)} & l_{a(b)}^{(22)} \end{pmatrix}. \tag{52}$$

Using Eq. (51), $\forall j = 1, 2, 3$, from Eq. (47), we get

$$
\begin{aligned}
P_j &= \sum_{i=0,1} \mathrm{Tr}[G_j^i \otimes H_j^{i+1}((L_a \otimes L_b)\rho^{'}(L_a \otimes L_b)^{\dagger})] = \sum_{i=0,1} \mathrm{Tr}[(L_a \otimes L_b)^{\dagger} G_j^i \otimes H_j^{i+1}(L_a \otimes L_b)\rho^{'}]\\
&= \sum_{i=0,1} \mathrm{Tr}[(L_a^{\dagger} G_j^i L_a) \otimes (L_b^{\dagger} H_j^{i+1} L_b)\rho^{'}].
\end{aligned} \tag{53}
$$

From Eq. (53), consider the term $L_a^{\dagger} G_j^i L_a$ for $i = 0$ (say). Let us now further analyze this term. Using Eqs. (49,52), we get

$$L_a^{\dagger} G_j^0 L_a = L_a^{\dagger}\frac{1}{2}(\mathbb{I}_2 + \vec{u_j}.\vec{\sigma})L_a = \frac{1}{2}(\mathbb{I}_2 + L_a^{\dagger}\vec{u_j}.\vec{\sigma}L_a). \tag{54}$$

Now using Eq. (52), $L_a, L_a^{\dagger}$ can be expressed in terms of Pauli matrices$(\sigma_1, \sigma_2, \sigma_3)$ as follows

$$
\begin{aligned}
L_a &= \frac{1}{2}((l_a^{(11)} + l_a^{(22)})\mathbb{I}_2 + (l_a^{(11)} - l_a^{(22)}))\sigma_3 + (l_a^{(12)} + l_a^{(21)})\sigma_1 + \imath(l_a^{(12)} - l_a^{(21)})\sigma_2\\
L_a^{\dagger} &= \frac{1}{2}((\overline{l_a^{(11)}} + \overline{l_a^{(22)}})\mathbb{I}_2 + (\overline{l_a^{(11)}} - \overline{l_a^{(22)}}))\sigma_3 + (\overline{l_a^{(12)}} + \overline{l_a^{(21)}})\sigma_1 + \imath(\overline{l_a^{(21)}} - \overline{l_a^{(12)}})\sigma_2
\end{aligned} \tag{55}
$$

with $\overline{l_a^{(ij)}}$ denoting complex conjugate of $l_a^{(ij)}$. Using Eq. (55), from Eq. (54), we get

$$
\begin{aligned}
L_a^{\dagger}\vec{u_j}.\vec{\sigma}L_a &= \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \text{ where,}\\
A_{11} &= (l_{a(b)}^{(21)}(u_{j1} - \imath u_{j2}) + l_{a(b)}^{(11)}u_{j3})\overline{l_{a(b)}^{(11)}} + (l_{a(b)}^{(11)}(u_{j1} + \imath u_{j2}) - l_{a(b)}^{(21)}u_{j3})\overline{l_{a(b)}^{(21)}}\\
A_{12} &= (l_{a(b)}^{(21)}(u_{j1} - \imath u_{j2}) + l_{a(b)}^{(11)}u_{j3})\overline{l_{a(b)}^{(12)}} + (l_{a(b)}^{(11)}(u_{j1} + \imath u_{j2}) - l_{a(b)}^{(21)}u_{j3})\overline{l_{a(b)}^{(22)}}\\
A_{21} &= (l_{a(b)}^{(22)}(u_{j1} - \imath u_{j2}) + l_{a(b)}^{(12)}u_{j3})\overline{l_{a(b)}^{(11)}} + (l_{a(b)}^{(12)}(u_{j1} + \imath u_{j2}) - l_{a(b)}^{(22)}u_{j3})\overline{l_{a(b)}^{(21)}}\\
A_{22} &= (l_{a(b)}^{(22)}(u_{j1} - \imath u_{j2}) + l_{a(b)}^{(12)}u_{j3})\overline{l_{a(b)}^{(12)}} + (l_{a(b)}^{(12)}(u_{j1} + \imath u_{j2}) - l_{a(b)}^{(22)}u_{j3})\overline{l_{a(b)}^{(22)}}.
\end{aligned} \tag{56}
$$

L_a being an unitary matrix, $L_a.L_a^{\dagger} = L_a^{\dagger}.L_a = \mathbb{I}_2$. Using that we get

$$
\begin{aligned}
|l_a^{(11)}|^2 + |l_a^{(12)}|^2 &= 1\\
|l_a^{(21)}|^2 + |l_a^{(22)}|^2 &= 1\\
l_a^{(22)}\overline{l_a^{(12)}} &= -l_a^{(21)}\overline{l_a^{(11)}}\\
l_a^{(11)}\overline{l_a^{(21)}} &= -l_a^{(12)}\overline{l_a^{(22)}}.
\end{aligned} \tag{57}
$$

Using above set of relations (57), $L_a^\dagger \vec{u_j}.\vec{\sigma} L_a$ (56) can be expressed in terms of Pauli matrices as follows

$$L_a^\dagger \vec{u_j}.\vec{\sigma} L_a = \vec{u_j}^{'}.\vec{\sigma} \tag{58}$$

where $\vec{u_j}^{'} = (u_{j1}^{'}, u_{j2}^{'}, u_{j3}^{'})$. Its components are specified as follows

$$\begin{aligned}
u_{j1}^{'} &= \frac{1}{2}(\iota u_{j2}(-l_a^{(22)}\overline{l_a^{(11)}} - l_a^{(21)}\overline{l_a^{(12)}} + l_a^{(12)}\overline{l_a^{(21)}} + l_a^{(11)}\overline{l_a^{(22)}}) + u_{j1}(l_a^{(22)}\overline{l_a^{(11)}} + l_a^{(21)}\overline{l_a^{(12)}} + l_a^{(12)}\overline{l_a^{(21)}} + l_a^{(11)}\overline{l_a^{(22)}}) \\
&\quad + u_{j3}(-l_a^{(22)}\overline{l_a^{(21)}} - l_a^{(21)}\overline{l_a^{(22)}})) \\
u_{j2}^{'} &= \frac{\iota}{2}(u_{j1}(l_a^{(22)}\overline{l_a^{(11)}} - l_a^{(21)}\overline{l_a^{(12)}} + l_a^{(12)}\overline{l_a^{(21)}} - l_a^{(11)}\overline{l_a^{(22)}}) + u_{j2}(l_a^{(22)}\overline{l_a^{(11)}} - l_a^{(21)}\overline{l_a^{(12)}} - l_a^{(12)}\overline{l_a^{(21)}} + l_a^{(11)}\overline{l_a^{(22)}}) \\
&\quad + \iota u_{j3}(-l_a^{(22)}\overline{l_a^{(21)}} + l_a^{(21)}\overline{l_a^{(22)}})) \\
u_{j3}^{'} &= u_{j1}(-l_a^{(22)}\overline{l_a^{(12)}} - l_a^{(12)}\overline{l_a^{(22)}}) + \iota u_{j2}(l_a^{(22)}\overline{l_a^{(12)}} - l_a^{(12)}\overline{l_a^{(22)}}) + u_{j3}(-1 + 2l_a^{(22)}\overline{l_a^{(22)}}).
\end{aligned} \tag{59}$$

On simplification of the above equations, each component of $\vec{u_j}^{'}$ turns out to be real quantity

$$\begin{aligned}
u_{j1}^{'} &= u_{j2}(\mathrm{Im}[l_a^{(22)}\overline{l_a^{(11)}}] + \mathrm{Im}[l_a^{(21)}\overline{l_a^{(12)}}]) + u_{j1}(\mathrm{Re}[l_a^{(22)}\overline{l_a^{(11)}}] + \mathrm{Re}[l_a^{(21)}\overline{l_a^{(12)}}]) - 2u_{j3}\mathrm{Re}[l_a^{(22)}\overline{l_a^{(21)}}] \\
u_{j2}^{'} &= u_{j1}(-\mathrm{Im}[l_a^{(22)}\overline{l_a^{(11)}}] + \mathrm{Im}[l_a^{(21)}\overline{l_a^{(12)}}]) + 2u_{j3}\mathrm{Im}[l_a^{(22)}\overline{l_a^{(21)}}] + u_{j2}(\mathrm{Re}[l_a^{(22)}\overline{l_a^{(11)}}] - \mathrm{Re}[l_a^{(21)}\overline{l_a^{(12)}}]) \\
u_{j3}^{'} &= -1 + 2|l_a^{(22)}|^2 - 2u_{j2}\mathrm{Im}[l_a^{(22)}\overline{l_a^{(12)}}] - 2u_{j1}\mathrm{Re}[l_a^{(22)}\overline{l_a^{(12)}}].
\end{aligned} \tag{60}$$

Using above relations, length of $\vec{u_j}^{'}$ turns out to be 1.

So, in totality, Eq. (54) can be expressed as

$$L_a^\dagger G_j^0 L_a = \frac{1}{2}(\mathbb{I}_2 + \vec{u_j}^{'}.\vec{\sigma}) \tag{61}$$

where $\vec{u_j}^{'}$ is a unit length real vector for each of $j = 1, 2, 3$.

Analogous argument can be put for each of $L_a^\dagger G_j^1 L_a$, $L_a^\dagger H_j^0 L_a$ and $L_a^\dagger H_j^1 L_a$. So P_j (53) now becomes

$$P_j = \frac{1}{4}\sum_{i=0,1} \mathrm{Tr}[(\mathbb{I}_2 + (-1)^i \vec{u_j}^{'}.\vec{\sigma}) \otimes (\mathbb{I}_2 + (-1)^{i+1}\vec{v_j}^{'}.\vec{\sigma}).\rho^{'}], \tag{62}$$

where $\vec{v_j}^{'}.\vec{\sigma} = L_b^\dagger \vec{v_j}.\vec{\sigma} L_b$. Using Eq. (62), Q now becomes

$$\begin{aligned}
Q &= \frac{1}{6}(3 - \sum_{i=1}^{3}\sum_{j=1}^{3} u_{ij}^{'} \sum_{k=1}^{3} T_{jk} v_{ik}^{'}) \\
&= \frac{1}{6}(3 - \sum_{i=1}^{3} \vec{u_i}^{'}.T\vec{v_i}^{'}) \\
&= \frac{1}{6}(3 - \sum_{i=1}^{3} \langle \vec{u_i}^{'}, T\vec{v_i}^{'} \rangle)
\end{aligned} \tag{63}$$

where $T = \mathrm{diag}(t_{11}, t_{22}, t_{33})$ is the correlation tensor of $\rho^{'}$ (2). To prove Eq. (17), we now need to minimize Q (63) over all possible measurement directions $\vec{u_j}^{'}, \vec{v_j}^{'} (j = 1, 2, 3)$.

$$\begin{aligned}
|\langle \vec{u_i}^{'}, T\vec{v_i}^{'} \rangle| &\leq ||\vec{u_i}^{'}|| ||T\vec{v_i}^{'}|| \; \forall i = 1, 2, 3 \\
&= ||T\vec{v_i}^{'}|| \text{ as } ||\vec{u_i}^{'}|| = 1 \\
-||T\vec{v_i}^{'}|| &\leq \langle \vec{u_i}^{'}, T\vec{v_i}^{'} \rangle \leq ||T\vec{v_i}^{'}|| \\
\text{So, } \sum_{i=1}^{3} \langle \vec{u_i}^{'}, T\vec{v_i}^{'} \rangle &\leq \sum_{i=1}^{3} ||T\vec{v_i}^{'}||
\end{aligned} \tag{64}$$

Hence, by Eqs. (63,64), we get

$$Q \geq \frac{1}{6}(3 - \sum_{i=1}^{3} ||T\vec{v_i}^{'}||). \tag{65}$$

As said in the main text, Alice is not allowed to perform measurements in mutually unbiased basis whereas Bob performs measurement in mutually unbiased bases (MUBs). Now for local dimension $d = 2$, up to global phase factor, there exist three possible MUBs [59]: $\{|0\rangle, |1\rangle\}$, $\{\frac{|0\rangle \pm |1\rangle}{2}\}$ and $\{\frac{|0\rangle \pm \iota|1\rangle}{2}\}$. Collection of possible operator bases for each of Alice and Bob are enlisted in Table 2. Minimization of Q is now performed over all these measurement operators.

Now, all $t_{ii} \geq 0$. So minimum value of R.H.S. of Eq. (65) is obtained for $\vec{v_1}^{'} = \vec{m}_3$, $\vec{v_2}^{'} = \vec{m}_5$ and $\vec{v_3}^{'} = \vec{m}_1$ (see Table 2):

$$Q = \frac{1}{6}(3 - t_{11} - t_{22} - t_{33}). \tag{66}$$

Expression for Q_{min} (17) is thus obtained.

Table 2: *All possible mutually unbiased operator bases for local dimension 2 are specified here for Bob. Corresponding direction $\vec{m}$ of projective measurement $\vec{m}.\vec{\sigma}$ is given. Clearly, up to global phase, the three possible MUB operator bases are given corresponding to directions $\vec{m_1}, \vec{m_3}$ and $\vec{m_5}$. Each of three measurement directions of Bob is thus given by third column of the table, i.e., $\forall j = 1, 2, 3$, $\vec{v_j}' \in \{\vec{m_1}, \vec{m_2}, \vec{m_3}, \vec{m_4}, \vec{m_5}, \vec{m_6}\}$. As Bob performs three measurement in MUBs, so if $\vec{v_1}'$ is one of $\vec{m_1}$ or $\vec{m_2}$ (say), then $\vec{v_2}' \neq \vec{m_1}, \vec{m_2}$. It can be any one of from ($\vec{m_3}$,$\vec{m_4}$) or from ($\vec{m_5}$,$\vec{m_6}$). If say $\vec{v_2}' = \vec{m_3}$, then $\vec{v_3}'$ is any one of $\vec{m_5}$ or $\vec{m_6}$.*

i	O_i	$\vec{m_i}$
1	$\{\vert 0\rangle\langle 0\vert, \vert 1\rangle\langle 1\vert\}$	$\vec{m_1} = (0, 0, 1)$
2	$\{-\vert 0\rangle\langle 0\vert, -\vert 1\rangle\langle 1\vert\}$	$\vec{m_2} = (0, 0, -1)$
3	$\{\frac{1}{2}(\vert 0\rangle\langle 0\vert + \vert 0\rangle\langle 1\vert + \vert 1\rangle\langle 0\vert + \vert 1\rangle\langle 1\vert), \frac{1}{2}(\vert 0\rangle\langle 0\vert - \vert 0\rangle\langle 1\vert - \vert 1\rangle\langle 0\vert + \vert 1\rangle\langle 1\vert)\}$	$\vec{m_3} = (1, 0, 0)$
4	$\{-\frac{1}{2}(\vert 0\rangle\langle 0\vert + \vert 0\rangle\langle 1\vert + \vert 1\rangle\langle 0\vert + \vert 1\rangle\langle 1\vert), -\frac{1}{2}(\vert 0\rangle\langle 0\vert - \vert 0\rangle\langle 1\vert - \vert 1\rangle\langle 0\vert + \vert 1\rangle\langle 1\vert)\}$	$\vec{m_4} = (-1, 0, 0)$
5	$\{\frac{1}{2}(\vert 0\rangle\langle 0\vert + \imath\vert 0\rangle\langle 1\vert + \imath\vert 1\rangle\langle 0\vert - \vert 1\rangle\langle 1\vert), \frac{1}{2}(\vert 0\rangle\langle 0\vert - \imath\vert 0\rangle\langle 1\vert - \imath\vert 1\rangle\langle 0\vert - \vert 1\rangle\langle 1\vert)\}$	$\vec{m_5} = (0, 1, 0)$
6	$\{-\frac{1}{2}(\vert 0\rangle\langle 0\vert + \imath\vert 0\rangle\langle 1\vert + \imath\vert 1\rangle\langle 0\vert - \vert 1\rangle\langle 1\vert), -\frac{1}{2}(\vert 0\rangle\langle 0\vert - \imath\vert 0\rangle\langle 1\vert - \imath\vert 1\rangle\langle 0\vert - \vert 1\rangle\langle 1\vert)\}$	$\vec{m_6} = (0, -1, 0)$

9 Appendix II

9.1 Proof regarding critical error rate (19)

It may be noted that minimizing Q_{min} (17), is equivalent to maximizing the following expression

$$f(t_{11}, t_{22}, t_{33}) = t_{11} + t_{22} + t_{33} \tag{67}$$

where $f(t_{11}, t_{22}, t_{33})$ is a symmetric function of eigenvalues of the correlation tensor of ρ (1). Here we use Lagrange multiplier's method to maximize $f(t_{11}, t_{22}, t_{33})$ subjected to the constraint provided by Eq. (18).

Let γ_1 be the Lagrange multiplier. Consider the following function

$$F_1(t_{11}, t_{22}, t_{33}, \gamma_1) = t_{11} + t_{22} + t_{33} + \gamma_1(t_{11}^2 + t_{22}^2 + t_{33}^2 - 1). \tag{68}$$

Partial differentiation of $F_1(t_{11}, t_{22}, t_{33}, \gamma_1)$ with respect to each of the variables t_{11}, t_{22}, t_{33} gives

$$\frac{\partial F_1}{\partial t_{ii}} = 1 + 2\gamma_1 t_{ii},\ i = 1, 2, 3. \tag{69}$$

Critical point is then given by $\frac{\partial F_1}{\partial t_{ii}} = 0$ which in turn gives

$$t_{ii} = -\frac{1}{2\gamma_1},\ i = 1, 2, 3. \tag{70}$$

Using Eq. (70), in Eq. (18), we get

$$\gamma_1 = \pm\frac{\sqrt{3}}{2}. \tag{71}$$

Now, for this case, as all $t_{ii} \geq 0$, so by Eqs. (69,70), $\gamma_1 = -\frac{\sqrt{3}}{2}$. Critical point ($K_1$, say) is thus given by

$$K_1 = (\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}). \tag{72}$$

Now calculating second order differential of $F_1(t_{11}, t_{22}, t_{33}, \gamma_1)$, we get

$$\begin{aligned} d^2F_1(t_{11}, t_{22}, t_{33}, \gamma_1) &= \sum_{i,j=1}^{3} \frac{\partial^2 F_1}{\partial t_{ii}\partial t_{jj}}(dt_{ii}dt_{jj}) \\ &= 2\gamma_1(dt_{ii})^2 \\ &= -\frac{1}{\sqrt{3}} \\ &< 0. \end{aligned} \tag{73}$$

Eq. (72) points out that d^2F turns out to be negative at all points. Hence, K_1 is the maxima of the objective function f (67), maximum value being given by

$$f(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}) = \sqrt{3}. \tag{74}$$

Eqs. (17,74) in turn give Eq. (19).

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum cryptography. *Reviews of Modern Physics* 2002; **74**(1):145–195. doi:10.1103/RevModPhys.74.145.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics* 2020; **12**(4):1012–1236. arXiv:1906.01645. doi:10.1364/AOP.361502.

[3] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki. Quantum entanglement. *Reviews of Modern Physics* 2009; **81**(2):865–942. arXiv:quant-ph/0702225. doi:10.1103/RevModPhys.81.865.

[4] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal* 1949; **28**(4):656–715. doi:10.1002/j.1538-7305.1949.tb00928.x.

[5] C. H. Bennett, G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Theoretical Computer Science* 2014; **560**(1):7–11. arXiv:2003.06557. doi:10.1016/j.tcs.2014.05.025.

[6] S. Wiesner. Conjugate coding. *SIGACT News* 1983; **15**(1):78–88. doi:10.1145/1008908.1008920.

[7] M. A. Nielsen, I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 2010. doi:10.1017/cbo9780511976667.

[8] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters* 1992; **68**(21):3121–3124. doi:10.1103/PhysRevLett.68.3121.

[9] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters* 1998; **81**(14):3018–3021. doi:10.1103/PhysRevLett.81.3018.

[10] H. Bechmann-Pasquinucci, N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A* 1999; **59**(6):4238–4248. doi:10.1103/PhysRevA.59.4238.

[11] L. Goldenberg, L. Vaidman. Quantum cryptography based on orthogonal states. *Physical Review Letters* 1995; **75**(7):1239–1243. arXiv:quant-ph/9502021. doi:10.1103/PhysRevLett.75.1239.

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics* 2009; **81**(3):1301–1350. doi:10.1103/RevModPhys.81.1301.

[13] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, J.-W. Pan. Measurement-device-independent quantum key distribution over 200 km. *Physical Review Letters* 2014; **113**(19):190501. arXiv:1407.8012. doi:10.1103/PhysRevLett.113.190501.

[14] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. 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, J.-W. Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters* 2016; **117**(19):190501. arXiv:1606.06821. doi:10.1103/PhysRevLett.117.190501.

[15] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics* 1964; **1**(3):195–200. doi:10.1103/PhysicsPhysiqueFizika.1.195.

[16] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters* 1969; **23**(15):880–884. doi:10.1103/PhysRevLett.23.880.

[17] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters* 1991; **67**(6):661–663. doi:10.1103/PhysRevLett.67.661.

[18] F. Xu, B. Qi, Z. Liao, H.-K. Lo. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Applied Physics Letters* 2013; **103**(6):061101. doi:10.1063/1.4817672.

[19] X. Yang, K. Wei, H. Ma, S. Sun, H. Liu, Z. Yin, Z. Li, S. Lian, Y. Du, L. Wu. Measurement-device-independent entanglement-based quantum key distribution. *Physical Review A* 2016; **93**(5):052303. doi:10.1103/PhysRevA.93.052303.

[20] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters* 2007; **98**(23):230501. doi:10.1103/PhysRevLett.98.230501.

[21] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics* 2009; **11**(4):045021. doi:10.1088/1367-2630/11/4/045021.

[22] E. Woodhead, A. Acín, S. Pironio. Device-independent quantum key distribution with asymmetric CHSH inequalities. *Quantum* 2021; **5**:443. doi:10.22331/q-2021-04-26-443.

[23] U. Vazirani, T. Vidick. Fully device-independent quantum key distribution. *Physical Review Letters* 2014; **113**(14):140501. arXiv:1210.1810. doi:10.1103/PhysRevLett.113.140501.

[24] P. Sekatski, J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, N. Sangouard. Device-independent quantum key distribution from generalized CHSH inequalities. *Quantum* 2021; **5**:444. doi:10.22331/q-2021-04-26-444.

[25] A. Ferenczi, N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Physical Review A* 2012; **85**(5):052310. doi:10.1103/PhysRevA.85.052310.

[26] M. Froissart. Constructive generalization of Bell's inequalities. *Il Nuovo Cimento B* 1981; **64**(2):241–251. doi:10.1007/BF02903286.

[27] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner. Bell nonlocality. *Reviews of Modern Physics* 2014; **86**(2):419–478. doi:10.1103/RevModPhys.86.419.

[28] D. Collins, N. Gisin. A relevant two qubit Bell inequality inequivalent to the CHSH inequality. *Journal of Physics A: Mathematical and General* 2004; **37**(5):1775. arXiv:quant-ph/0306129. doi:10.1088/0305-4470/37/5/021.

[29] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Physical Review Letters* 2002; **88**(4):040404. doi:10.1103/PhysRevLett.88.040404.

[30] A. Acín, N. Gisin, L. Masanes. From Bell's theorem to secure quantum key distribution. *Physical Review Letters* 2006; **97**(12):120405. arXiv:quant-ph/0510094. doi:10.1103/PhysRevLett.97.120405.

[31] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, A. Acín. Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. *Physical Review Letters* 2021; **127**(5):050503. doi:10.1103/PhysRevLett.127.050503.

[32] J. Singh, S. Ghosh, Arvind, S. K. Goyal. Role of Bell–CHSH violation and local filtering in quantum key distribution. *Physics Letters A* 2021; **392**:127158. doi:10.1016/j.physleta.2021.127158.

[33] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society* 1935; **31**(4):555–563. doi:10.1017/S0305004100013554.

[34] E. Schrödinger. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society* 1936; **32**(3):446–452. doi:10.1017/S0305004100019137.

[35] H. M. Wiseman, S. J. Jones, A. C. Doherty. Steering, entanglement, nonlocality, and the Einstein–Podolsky–Rosen paradox. *Physical Review Letters* 2007; **98**(14):140402. arXiv:quant-ph/0612147. doi:10.1103/PhysRevLett.98.140402.

[36] S. J. Jones, H. M. Wiseman, A. C. Doherty. Entanglement, Einstein–Podolsky–Rosen correlations, Bell nonlocality, and steering. *Physical Review A* 2007; **76**(5):052116. doi:10.1103/PhysRevA.76.052116.

[37] M. D. Reid. Demonstration of the Einstein–Podolsky–Rosen paradox using nondegenerate parametric amplification. *Physical Review A* 1989; **40**(2):913–923. doi:10.1103/PhysRevA.40.913.

[38] Z. Y. Ou, S. F. Pereira, H. J. Kimble, K. C. Peng. Realization of the Einstein–Podolsky–Rosen paradox for continuous variables. *Physical Review Letters* 1992; **68**(25):3663–3666. doi:10.1103/PhysRevLett.68.3663.

[39] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, M. D. Reid. Experimental criteria for steering and the Einstein–Podolsky–Rosen paradox. *Physical Review A* 2009; **80**(3):032112. doi:10.1103/PhysRevA.80.032112.

[40] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, P. H. Souto Ribeiro. Revealing hidden Einstein–Podolsky–Rosen nonlocality. *Physical Review Letters* 2011; **106**(13):130402. doi:10.1103/PhysRevLett.106.130402.

[41] M. Żukowski, A. Dutta, Z. Yin. Geometric Bell-like inequalities for steering. *Physical Review A* 2015; **91**(3):032107. doi:10.1103/PhysRevA.91.032107.

[42] J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, J. C. Howell. Einstein–Podolsky–Rosen steering inequalities from entropic uncertainty relations. *Physical Review A* 2013; **87**(6):062103. doi:10.1103/PhysRevA.87.062103.

[43] S. Jevtic, M. J. W. Hall, M. R. Anderson, M. Zwierz, H. M. Wiseman. Einstein–Podolsky–Rosen steering and the steering ellipsoid. *Journal of the Optical Society of America B* 2015; **32**(4):A40–A49. doi:10.1364/josab.32.000a40.

[44] F. Verstraete. A study of entanglement in quantum information theory. Ph.D. thesis. Leuven, Belgium (2002). https://biblio.ugent.be/publication/8603813.

[45] S. Jevtic, M. Pusey, D. Jennings, T. Rudolph. Quantum steering ellipsoids. *Physical Review Letters* 2014; **113**(2):020402. doi:10.1103/PhysRevLett.113.020402.

[46] S. J. Jones, H. M. Wiseman. Nonlocality of a single photon: paths to an Einstein–Podolsky–Rosen-steering experiment. *Physical Review A* 2011; **84**(1):012110. doi:10.1103/PhysRevA.84.012110.

[47] A. C. S. Costa, R. M. Angelo. Quantification of Einstein–Podolsky–Rosen steering for two-qubit states. *Physical Review A* 2016; **93**(2):020103. doi:10.1103/PhysRevA.93.020103.

[48] R. Renner. Security of quantum key distribution. *International Journal of Quantum Information* 2008; **6**(1):1–127. doi:10.1142/S0219749908003256.

[49] S. Popescu. Bell's inequalities and density matrices: revealing "hidden" nonlocality. *Physical Review Letters* 1995; **74**(14):2619–2622. doi:10.1103/PhysRevLett.74.2619.

[50] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Physics Letters A* 1996; **210**(3):151–156. doi:10.1016/S0375-9601(96)80001-6.

[51] F. Verstraete, J. Dehaene, B. DeMoor. Local filtering operations on two qubits. *Physical Review A* 2001; **64**(1):010101. doi:10.1103/PhysRevA.64.010101.

[52] F. Verstraete, M. M. Wolf. Entanglement versus Bell violations and their behavior under local filtering operations. *Physical Review Letters* 2002; **89**(17):170401. doi:10.1103/PhysRevLett.89.170401.

[53] N. Ganguly, A. Mukherjee, A. Roy, S. S. Bhattacharya, B. Paul, K. Mukherjee. Bell–CHSH violation under global unitary operations: Necessary and sufficient conditions. *International Journal of Quantum Information* 2018; **16**(4):1850040. doi:10.1142/s0219749918500405.

[54] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, H. M. Wiseman. One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering. *Physical Review A* 2012; **85**(1):010301. arXiv:1109.1435. doi:10.1103/PhysRevA.85.010301.

[55] K. Bartkiewicz, A. Černoch, K. Lemr, A. Miranowicz, F. Nori. Temporal steering and security of quantum key distribution with mutually unbiased bases against individual attacks. *Physical Review A* 2016; **93**(6):062345. doi:10.1103/PhysRevA.93.062345.

[56] O. Gamel. Entangled Bloch spheres: Bloch matrix and two-qubit state space. *Physical Review A* 2016; **93**(6):062320. doi:10.1103/PhysRevA.93.062320.

[57] S. Luo. Quantum discord for two-qubit systems. *Physical Review A* 2008; **77**(4):042303. doi:10.1103/PhysRevA.77.042303.

[58] G. Brassard, L. Salvail. Secret-key reconciliation by public discussion. in: T. Helleseth (Ed.), Advances in Cryptology – EUROCRYPT '93. Vol. 765 of *Lecture Notes in Computer Science*. Springer, Berlin, 1994. pp. 410–423. doi:10.1007/3-540-48285-7_35.

[59] S. Brierley. Mutually unbiased bases in low dimensions. Ph.D. thesis. York, England (2009). https://etheses.whiterose.ac.uk/587/.

[60] J. Modławska, A. Grudka. Increasing singlet fraction with entanglement swapping. *Physical Review A* 2008; **78**(3):032321. doi:10.1103/PhysRevA.78.032321.

[61] A. Wójcik, J. Modławska, A. Grudka, M. Czechlewski. Violation of Clauser–Horne–Shimony–Holt inequality for states resulting from entanglement swapping. *Physics Letters A* 2010; **374**(48):4831–4833. arXiv:1007.4775. doi:10.1016/j.physleta.2010.09.069.

[62] S. Goswami, S. Ghosh, A. S. Majumdar. Protecting quantum correlations in presence of generalised amplitude damping channel: the two-qubit case. *Journal of Physics A: Mathematical and Theoretical* 2021; **54**(4):045302. arXiv:1903.03550. doi:10.1088/1751-8121/abd59f.

[63] S. Datta, S. Goswami, T. Pramanik, A. S. Majumdar. Preservation of a lower bound of quantum secret key rate in the presence of decoherence. *Physics Letters A* 2017; **381**(10):897–902. doi:10.1016/j.physleta.2017.01.019.

[64] S. Gupta, D. Das, A. S. Majumdar. Distillation of genuine tripartite Einstein–Podolsky–Rosen steering. *Physical Review A* 2021; **104**(2):022409. doi:10.1103/PhysRevA.104.022409.

[65] F. Hirsch. Hidden nonlocality. Master's thesis. Geneva, Switzerland (2013). https://www.unige.ch/sciences/physique/files/9914/8906/3550/Travail-de-Master.pdf.

[66] A. Aspect, J. Dalibard, G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters* 1982; **49**(25):1804–1807. doi:10.1103/PhysRevLett.49.1804.

[67] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters* 1998; **81**(23):5039–5043. doi:10.1103/PhysRevLett.81.5039.

[68] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature* 2001; **409**(6822):791–794. doi:10.1038/35057215.

[69] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, A. Zeilinger. Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences* 2010; **107**(46):19708–19713. doi:10.1073/pnas.1002780107.

[70] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, A. Zeilinger. Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering. *New Journal of Physics* 2012; **14**(5):053030. doi:10.1088/1367-2630/14/5/053030.