Eavesdropping a Quantum Key Distribution network using sequential quantum unsharp measurement attacks

Yash Wath
Indian Institute of Science Education and Research, Tirupati 517507, India

Hariprasad M
Pondicherry University, Chinna Kalapet, Kalapet, Puducherry 605014, India

Freya Shah
Udgam School for Children, Ahmedabad 380051, India

Shashank Gupta
S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700 106, India

(Dated: February 6, 2022)

We investigate the possibility of eavesdropping a quantum key distribution network by local sequential quantum unsharp measurement attacks by the eavesdropper. In particular, we consider a pure two-qubit state shared between two parties Alice and Bob, sharing quantum steerable correlations that form the one-sided device-independent quantum key distribution network. One qubit of the shared state is with Alice and the other one going to the Bob’s place is intercepted by multiple sequential eavesdropper who perform quantum unsharp measurement attacks thus gaining some positive key rate while preserving the quantum steerable correlations for the Bob. In this way, Bob will also have positive secret key rate although reduced. However, this reduction is not that sharp and can be perceived due to decoherence and imperfection of the measurement devices. At the end, we show that unbounded number of eavesdropper can also get secret information in some specific scenario.

PACS numbers:

I. INTRODUCTION

Quantum network is a network of observers that are connected by quantum channels. The main idea is to use quantum channels to transfer secret information from one observer to another. This forms the quantum key distribution (QKD) network [1]. There are two distinct classes of QKD protocols in the literature: 1. Prepare and measure [2, 3], and 2. Entanglement-assisted [4]. One distinct advantage that entanglement-assisted QKD protocols offers is the ability to check its security based on monogamy relations via the violation of steering or Bell inequalities.

Quantum key distribution protocols have been proven to be secure against eavesdropping and noise [5]. The rigorous security proof was by Mayers [6, 7]. The other development in this direction were based on entanglement distillation [8, 9]. The work by Shor and Preskill [10] used the Mayer’s result and the ideas of quantum error correction to prove the security of the BB84 protocol.

With the discovery of photon-number-splitting (PNS) attacks [11], security proofs came to deal with the loophole of theoretical single-photon source [12]. With increasing quantum technological advancement, the possibility of newer kind of attacks by the adversary raises the question on the security of such QKD protocols time and again. Here, we investigate the security of one-sided device-independent quantum key distribution (1S-DIQKD) networks [13] under the possibility of quantum unsharp measurement attacks by the Eavesdropper.

Quantum steering [14–21] is an intermediate correlation between entanglement and Bell nonlocality, was discovered by E. Schrödinger as an interpretation of the famous work by Einstein-Podolsky-Rosen [22]. It is the key resource behind 1S-DIQKD networks [13] under the possibility of quantum unsharp measurement attacks by the Eavesdropper.

Quantum steering [14–21] is an intermediate correlation between entanglement and Bell nonlocality, was discovered by E. Schrödinger as an interpretation of the famous work by Einstein-Podolsky-Rosen [22]. It is the key resource behind 1S-DIQKD networks [13] under the possibility of quantum unsharp measurement attacks by the Eavesdropper.

In the present work, we address the question raised above by finding the upper bound on the number of Eves that can share the secret key rate by finding the violation of fine-grained steering inequality [23] such that the Bob has secret key rate value more than any Eve in the network. Since, the Bob is getting a positive key rate, he will not terminate the protocol and perceive the reduction in the key rate value as an effect of the noise or the imperfection of the measurement devices. We also present...
a strategy by which an unbounded number of Eves can have access to secret information in some specific scenario [26], thus raising the magnitude of the criticality of such QKD protocols.

The plan of the paper is as follows: in Section II we recapitulate and present the basic tools that are required for further investigation. The measurement framework involving multiple sequential Eves used in this paper is also described in this Section. In Section III, we present the main analysis of this paper, and discuss the results obtained in the context of sequential eavesdropping of the 1S-DIQKD network when the initially shared two-qubit state is maximally entangled. We then discuss a strategy that gives rise to unbounded number of eavesdroppers. Finally, we conclude in Section IV.

II. PRELIMINARIES

In this section, we discuss in brief the concept of EPR steering and its connection with the one-sided device-independent quantum key distribution (1S-DIQKD). We then briefly discuss the quantum sequential measurement attacks in the context of eavesdropping.

A. Steering and 1S-DIQKD

Consider that a bipartite state $\rho$ is shared among two observers, say, Alice and Bob. In the steering scenario, Alice tries to steer Bob’s particles via her input and output measurement choices. Alice’s measurement operators are denoted by $A_{a|x}$, where $x$ is the choice of her input and $a$ is the outcome. After Alice’s measurement, each element of the set $\{\sigma^B_{a|x}\}$ of unnormalized conditional states on Bob end is given by,

$$\sigma^B_{a|x} = \text{Tr}_A [ (A_{a|x} \otimes I_B) \rho ].$$

This set of conditional states is called an assemblage. The entangled or the separable nature of the state imposes constraint on the observed assemblage. When the initial state $\rho$ is not entangled, then each element (1) of the assemblage $\{\sigma^B_{a|x}\}_{a,x}$ is of the following form,

$$\sigma^B_{a|x} = \sum_\lambda p_\lambda p_A(a|x) \rho^B_\lambda \quad \forall a,x.$$

Here, $p_A(a|x)$ denotes the probability of getting the outcome $a$ when Alice performs the measurement denoted by $x$ on the local state $\rho^A_x$. If any element of the assemblage $\{\sigma^B_{a|x}\}_{a,x}$ cannot be written in the form (2), then the assemblage indicates that the state $\rho$ possesses entanglement. In other words, when an element of the assemblage $\{\sigma^B_{a|x}\}_{a,x}$ cannot be written in the form (2), then the assemblage demonstrate EPR steering from Alice to Bob.

In literature, steering has been detected using logical contradiction, uncertainty relations and inequalities.

Here, we use the optimal fine-grained steering criteria to demonstrate steering and use the monogamy relation to study the 1S-DIQKD of steerable states [23]. Alice performs a dichotomic measurements $\{A_{a|x}\}$ s.t. $a, x \in \{0,1\}$ and communicates her input choice and outcome to Bob. In order to check whether the state is steerable, Bob performs measurements in two mutually unbiased basis, say, $\{\sigma_x, \sigma_z\}$ with outcome $b \in \{0,1\}$. The shared state $\rho$ is steerable, if the conditional probability distribution violates the following relation:

$$\frac{1}{2} [ P(B_{b|0}|A_{a|0}) + P(B_{b|1}|A_{a|1}) ] \leq \frac{3}{4}$$

(3)

Now, if the shared state $\rho$ between Alice and Bob is maximally steerable, then none of these systems can be steerable with any other system [23]. This nature is called monogamy of steerable states. This behaviour of steerable states put a lower bound on the secret key rate in 1S-DIQKD (one-sided device independent because one of the systems is not trusted, here Alice). The lower bound on the secret key rate ($r$), corresponding to the shared state $\rho$ which violates the above inequality (3) is given by [23].

$$r \geq \log_2 \left[ \frac{1}{2} \frac{3 + \delta}{4 - \delta} \right]$$

(4)

Here, $\delta \in (0, \frac{1}{2})$ is the degree of violation of the inequality (3).

B. Sequential quantum unsharp measurement attacks

We now describe the idea of quantum unsharp measurement attacks performed by the eavesdropper for sequential eavesdropping the 1S-DIQKD network.

Consider a bipartite system of state $\rho$ consisting of spatially separated two spin-$\frac{1}{2}$ particles. In this case, we consider multiple Eves ($\varepsilon^1, \varepsilon^2, \cdots, \varepsilon^n$) perform measurements on the second particle sequentially. On the other hand, a single Alice perform projective measurements on the first particle. Here we ask the following question:

- How many Eves can gain positive secret key rate while preserving the quantum steerable correlations (positive key rate greater than any of the Eves) for the Bob?

Since our aim is to explore how many Eves can gain positive secret key rate through the violation of Fine-grained steering inequality (3), multiple Eves cannot perform projective measurements. If any Eve performs a projective measurement, then the EPR steerability of the state will be completely lost and Bob will know that there is an eavesdropping in the network. Hence, each $n$ Eves in the sequence should perform weak measurements.

The aforementioned scenarios are depicted in Figure 1. Next, let us briefly discuss the quantum unsharp measurement attacks used by the eavesdroppers (For details,
In a sharp projective measurement attack, one obtains the maximum amount of information at the cost of maximum disturbance to the state which is detected by the Alice and Bob. On the other hand, in our scenario, Eve\textsuperscript{m} passes on the respective particle to Eve\textsuperscript{m+1} after getting some positive key rate. Hence, in this case, Eve\textsuperscript{m} needs to access the positive secret key rate by disturbing the state minimally so that Eve\textsuperscript{m+1} (or, Bob at the end) can also get positive secret key rate. This can be achieved by unsharp measurements \cite{27} which may be characterized by two real parameters: the quality factor \( G \) and the precision \( F \) of the measurement. \( F \) quantifies the extend to which the initial state of the system remains undisturbed during the measurement process and \( G \) quantifies the information gain due to the measurement. In case of projective measurement, \( F = 0, G = 1 \). For dichotomic measurements on a qubit system, the optimal trade-off relation is given by, \( F^2 + G^2 = 1 \) \cite{27}.

The above optimal trade-off relation between information gain and quality factor is achieved under unsharp measurement formalism \cite{24,28}. Unsharp measurement \cite{29,30} is one particular class of positive operator valued measurements (POVM) \cite{29,30}. Consider a dichotomic observable \( O = \Pi_0 - \Pi_1 \) with outcomes 0 and 1, where \( \Pi_0 \) and \( \Pi_1 \) denote the projectors associated with the outcomes 0 and 1 respectively, with \( \Pi_0 + \Pi_1 = \mathbb{I} \) and \( \Pi^2_{0/1} = \Pi_{0/1} \). Given the observable \( O \), a dichotomic unsharp observable \( O^\lambda = E^\lambda_0 - E^\lambda_1 \) \cite{31,32} can be defined which is associated with the sharpness parameter \( \lambda \in (0,1] \). Here, the effect operators \( E^\lambda_{0/1} \) are given by,

\[
E^\lambda_{0/1} = \lambda \Pi_{0/1} + (1 - \lambda) \frac{I_2}{2}.
\]

This is obtained by mixing projective measurements with white noise. The probability of getting the outcomes 0 and 1, when the above unsharp measurement is performed on the state \( \rho \), are given by \( \text{Tr}[\rho E^\lambda_0] \) and \( \text{Tr}[\rho E^\lambda_1] \) respectively. Using the generalized von Neumann-Lüders transformation rule \cite{29}, the states after the measurements, when the outcomes 0 and 1 occurs, are given by,

\[
\frac{\sqrt{E^\lambda_0} \rho \sqrt{E^\lambda_0}}{\text{Tr}[\rho E^\lambda_0]} \quad \text{and} \quad \frac{\sqrt{E^\lambda_1} \rho \sqrt{E^\lambda_1}}{\text{Tr}[\rho E^\lambda_1]}\text{, respectively.}
\]

Unsharp measurements has already been demonstrated using trapped-ion \cite{33} and photonic systems \cite{34–38}. Here, using an appropriate interferometer one can realize the unsharp measurement formalism. Further, the sharpness parameter can be controlled by fine-tuning the arrangement of various components in the interferometer. This raises a critical question related to the security of QKD networks where multiple Eves in the sequence perform unsharp measurement attacks where as Alice and Bob perform sharp measurements.

### III. EAVESDROPPING BY MULTIPLE SEQUENTIAL EVES

Using the formalism discussed in the previous section, we are now in a position to explore the maximum number of Eves that can gain the positive secret key rate such that Bob also gets the positive key rate greater than any of the Eves. Before proceeding, let us recapitulate some previous relevant results on sequential detection of steering.

It has been shown \cite{24} that at most two Bob can sequentially be steered with a single Alice when the singlet state is initially shared and each party is performing dichotomic measurements. Now, in order to demonstrate steering, entanglement is necessary and hence, it can be concluded that two Bob can sequentially detect entanglement of the singlet state in a one-sided DI scenario with a single Alice. These results are probed through the quantum violation of the analogous CHSH inequality \cite{39}.

Here, we ask a similar question, but in the one-sided device-independent quantum key distribution scenario. Let Alice perform dichotomic projective measurement of the spin component observable in the direction \( \hat{x}_0 \), or \( \hat{x}_1 \). Bob performs dichotomic projective measurement of the spin component observable in the direction \( \hat{y}_0 \), or \( \hat{y}_1 \). Eve\textsuperscript{m} (where \( m \in \{1, 2, \ldots, n\} \)) performs dichotomic unsharp measurement of the spin component observable in the direction \( \hat{x}_0^m \), or \( \hat{x}_1^m \). The outcomes of each measurement is 0 or 1.

The projectors associated with Alice’s sharp spin component measurement in the direction \( \hat{x}_i \) (with \( i \in \{0, 1\} \)) are given by, \( A_{a|i} = \frac{I_2 + (-1)^a \hat{x}_i \cdot \vec{\sigma}}{2} \) (with \( a \in \{0, 1\} \) being the outcome of Alice’s sharp measurement). Similarly, the projectors associated with Bob’s sharp spin component measurement in the direction \( \hat{y}_j \) (with \( j \in \{0, 1\} \)) can be written as \( B_{b|j} = \frac{I_2 + (-1)^b \hat{y}_j \cdot \vec{\sigma}}{2} \) (with \( b \in \{0, 1\} \) being the outcome of Bob’s sharp measurement).

Here, \( \vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) \) is a vector composed of three Pauli matrices. The directions \( \hat{x}_i \) and \( \hat{y}_j \) can be
expressed as,
\[ \hat{x}_i = \sin \theta_i^x \cos \phi_i^x \hat{X} + \sin \theta_i^x \sin \phi_i^x \hat{Y} + \cos \theta_i^x \hat{Z}, \]
and
\[ \hat{y}_j = \sin \theta_j^y \cos \phi_j^y \hat{X} + \sin \theta_j^y \sin \phi_j^y \hat{Y} + \cos \theta_j^y \hat{Z}, \]
where \( i, j \in \{0, 1\} \); \( 0 \leq \theta_i^x \leq \pi; \ 0 \leq \phi_i^x \leq 2\pi; \) \( 0 \leq \phi_j^y \leq 2\pi. \) \( \hat{X}, \hat{Y}, \hat{Z} \) are three orthogonal unit vectors in Cartesian coordinates.

The effect operators associated with Eve’s unsharp measurement of spin component observable along the direction \( \hat{z}_k^m \) (with \( k \in \{0, 1\} \)) are given by,
\[ E_{\hat{z}_k^m}^{\lambda_m} = \lambda_m \frac{\mathbb{I}_2 + (-1)^m \hat{z}_k^m \cdot \vec{\sigma}}{2} + (1 - \lambda_m) \frac{\mathbb{I}_2}{2}, \]
with \( m \in \{0, 1\} \) being the outcome of Eve’s unsharp measurement and \( \lambda_m \) \((0 < \lambda_m \leq 1)\) is the sharpness parameter corresponding to Eve’s unsharp measurement. The direction \( \hat{z}_k^m \) is given by,
\[ \hat{z}_k^m = \sin \theta_k^m \cos \phi_k^m \hat{X} + \sin \theta_k^m \sin \phi_k^m \hat{Y} + \cos \theta_k^m \hat{Z}, \]
where \( k \in \{0, 1\}; \ 0 \leq \theta_k^m \leq \pi; \ 0 \leq \phi_k^m \leq 2\pi. \)

There are conditional probabilities appearing in the inequality (3). In the following, we compute these conditional probabilities between Eve’s and Alice.

The conditional probability of occurrence of the outcome \( c^1 \) when Eve performs unsharp measurement of spin component observable along the direction \( \hat{z}_k^1 \) given that Alice performs projective measurements of spin component observables along the directions \( \hat{x}_i \) and got the outcome \( a \) on the shared bipartite state \( \rho \), is given by,
\[ P(E_{c^1|z_k^1}^{a|\hat{x}_i}|A_{a|x_i}) = \frac{\text{Tr} \left[ A_{a|x_i} \otimes E_{c^1|z_k^1}^{a|\hat{x}_i} \right] \cdot \rho}{\text{Tr} \left[ A_{a|x_i} \otimes \mathbb{I}_2 \right] \cdot \rho}. \]

After performing unsharp measurement, Eve passes her particle to Eve². The unnormalized post-measurement reduced state at Eve²’s end, after Eve performs the outcome \( c^1 \) by performing unsharp measurement of spin component observable along the direction \( \hat{z}_k^1 \) and Alice get the outcomes \( a \) by performing sharp measurements of spin component observables along the directions \( \hat{x}_1 \) is given by,
\[ \rho_{un}^2 = \text{Tr}_{A^2} \left[ A_{a|\hat{x}_1} \otimes \frac{\mathbb{I}_2 + (-1)^{a} \hat{x}_1 \cdot \vec{\sigma}}{2} \otimes \sqrt{E_{c^1|z_k^1}^{a|\hat{x}_1}} \right] \cdot \rho \cdot \text{Tr} \left[ A_{a|\hat{x}_1} \otimes \mathbb{I}_2 \right] \cdot \rho. \]

where,
\[ \sqrt{E_{c^1|z_k^1}^{a|\hat{x}_1}} = \sqrt{\frac{1 + \lambda_i}{2} \left( \mathbb{I}_2 + (-1)^{a} \hat{x}_1 \cdot \vec{\sigma} \right)} \]
\[ + \sqrt{\frac{1 - \lambda_i}{2} \left( \mathbb{I}_2 - (-1)^{a} \hat{x}_1 \cdot \vec{\sigma} \right)}. \]

In order to get the reduced state, the partial trace has been taken over the Alice’s subsystem.

Now, Eve² also performs unsharp measurement attack (associated with sharpness parameter \( \lambda_2 \)) of spin component observable along the direction \( \hat{z}_k^2 \) on the reduced state \( \rho_{un}^2 \), and gets the outcome \( c^2 \). The joint probability of occurrence of the outcomes \( a, c^1, c^2 \), when Eve¹, Eve² perform unsharp measurements of spin component observables along the directions \( \hat{z}_k^1, \hat{z}_k^2 \) respectively and Alice perform projective measurements of spin component observables along the directions \( \hat{x}_i \), is given by,
\[ P(A_{a|x_i}, E_{c^1|z_k^1}, E_{c^2|z_k^2}) = \text{Tr} \left[ E_{c^2|z_k^2}^{a|\hat{x}_i} \cdot \rho_{un}^2 \right]. \]

This from the joint probability of obtaining the outcomes \( c^2, a \), by Eve², Alice, respectively, can be calculated as,
\[ P(A_{a|x_i}, E_{c^2|z_k^2}) = \sum_{c^1=0}^{1} \left[ P(A_{a|x_i}, E_{c^1|z_k^1}, E_{c^2|z_k^2}) P(z_k^1) \right] + P(A_{a|x_i}, E_{c^1|z_k^1}, E_{c^2|z_k^2}) P(z_k^2). \]

Here, \( P(z_k^1) \) is the probability of Eve¹’s unsharp measurement of spin component observable in the direction \( \hat{z}_k^1 \) \((k \in \{0, 1\})\). Since, we restrict ourselves to unbiased input scenario, the two measurement settings for Eve¹ are equally probable, i.e., \( P(z_k^1) = P(z_k^2) = \frac{1}{2} \). Now, the conditional probability of occurrence of the outcomes \( c^2 \) when Eve² perform unsharp measurements of spin component observable along the direction \( \hat{z}_k^2 \) given that Alice perform projective measurements of spin component observables along the directions \( \hat{x}_i \) and got the outcome \( a \), is given by,
\[ P(E_{c^2|z_k^2}^{a|\hat{x}_1}|A_{a|x_i}) = \frac{P(A_{a|x_i}, E_{c^2|z_k^2})}{\text{Tr} \left[ A_{a|x_i} \otimes \mathbb{I}_2 \right] \cdot \rho}. \]

Using the expression (15) for the conditional probability, the two terms appearing in inequality (3) can be easily calculated for detection of EPR steering by Eve². Using the violation of the inequality one can easily determine the positive secret key rate value for Eve² in terms of the sharpness parameter \( \lambda_2 \). Following the above-mentioned approach, the two terms appearing on the left
hand side of the inequality (3) in the context of Eve\textsuperscript{m}, Alice and Bob can be calculated. In the following, we consider that the initial state is a two-qubit maximally entangled state.

1. When the two-qubit maximally entangled state is initially shared

Let us consider that the two-qubit maximally entangled state given by \( |\psi_s\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \) is shared between Alice and Bob, where

\[
|\psi_s\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle).
\]  

(16)

Here, \(|0\rangle\) and \(|1\rangle\) denotes two mutually orthonormal states in \(\mathbb{C}^2\). Here, multiple Eves perform sequential unsharp measurement attacks on the second qubit.

At first, we will find out the maximum number of Eves, who can access positive secret key rate such that the Bob will also have positive secret key rate greater than any of the Eves. This will be probed through the quantum violation of the inequality (3) and the relation (4).

We start by finding out whether Eve\textsuperscript{1} and Eve\textsuperscript{2} can sequentially access positive secret key rate. In other words, we will find out whether Eve\textsuperscript{1} and Eve\textsuperscript{2} can sequentially have the secret key rate (4) value say ‘r’ such that Bob has the secret key rate ≥ r. In this case, the measurements of the Eves’ are unsharp where as that of Alice and Bob are sharp. We observe that, for example, when Eve\textsuperscript{1} and Eve\textsuperscript{2} get \( r = 0.1 \), then Bob gets \( r = 0.634 \). This happens for the following choices of measurement settings by Alice: \((\theta_1^s, \phi_1^s, \theta_2^s, \phi_2^s) = (0, 0, \frac{\pi}{2}, 0)\), with \( \lambda_1 = 0.552 \) and \( \lambda_2 = 0.602 \). Note that, here the choices of measurement settings by Eves and Bob are in two mutually unbiased basis \((\sigma_x, \sigma_z)\). Hence, we can conclude that Eve\textsuperscript{1} and Eve\textsuperscript{2} can access secret key rate value of 0.1 such that Bob also have positive value of secret key rate. Note that the secret key rate at Bob’s end would be higher if there were no Eve’s. However, this reduction in the value of secret key rate is not sharp and Bob may perceive it due to decoherence or imperfection of the measurement devices.

Next, we ask whether Eve\textsuperscript{1}, Eve\textsuperscript{2} and Eve\textsuperscript{3} can sequentially access positive secret key rate such that Bob also have positive secret key rate. We observe that, when Eve\textsuperscript{1}, Eve\textsuperscript{2} and Eve\textsuperscript{3} get \( r = 0.2 \), then Bob gets \( r = 0.269 \). This happens for the same choices of measurement settings by Alice as mentioned above, with \( \lambda_1 = 0.604 \), \( \lambda_2 = 0.672 \) and \( \lambda_3 = 0.772 \). Hence, Eve\textsuperscript{1}, Eve\textsuperscript{2} and Eve\textsuperscript{3} can access secret key rate when the maximally entangled two-qubit state is initially shared.

Proceeding this way, we find the upper bound on the number of Eves’ that can access secret key rate of value 0.1, 0.2 and 0.3 respectively such that the Bob has secret key rate of value more than that each sequential Eve can access. These results are summarized in Table I, II and III. The permissible range of each \( \lambda_m \) depends on the values \( \lambda_1, \lambda_2, \ldots, \lambda_{m-1} \). In the table, we have presented the permissible range of each \( \lambda_m \) for the minimum permissible value of each \( \lambda_1, \lambda_2, \ldots, \lambda_{m-1} \). The permissible range of \( \lambda_m \) will be smaller than this if we take other value \( \lambda_i > \lambda_{i+1} \forall i < m \), and the maximum number of Eves may get reduced. Note that as the value of the secret key rate associated with Eves increases the number of Eves that can perform these quantum unsharp measurement attacks decreases as even higher value of the key rate is demanded at the Bob’s end. Hence, Bob can assure the security of the QKD network by having higher secret key rate and terminating the protocol in adverse scenario.

Next, we devise a strategy where unbounded number of Eves can access the positive secret key rate when the initial shared state is a non-maximally entangled two-qubit pure state.
| Eve[^m] | Secret key rate for each Eve is 0.3 | Permissible λ[^m] range |
|---|---|---|
| Eve[^1] | 1 ≥ λ[^1] > λ[^1̂] = 0.655 | |
| Eve[^2] | 1 ≥ λ[^2] > λ[^2̂] = 0.747 | when λ[^i] = λ[^2̂] \lor i < 2 |
| Eve[^3] | No valid range for λ[^i] for any λ[^i] with i < 3 |

TABLE III: The permissible ranges of the sharpness parameters λ[^m] (where 0 < λ[^m] ≤ 1) of Eve[^m] in order to access secret key rate r = 0.3 when the two-qubit maximally entangled state is initially shared such that the Bob has a positive secret key rate r = 0.447 (> 0.3) at the end.

2. Eavesdropping by unbounded number of Eves

Here, let us consider that the two-qubit non-maximally entangled state \( \rho_0 = |\psi\rangle \langle \psi| \) is initially shared between Alice and Bob, where

\[
|\psi\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle.
\]

The fine-grained inequality (3) has following properties: 1. Any non-maximally entangled pure state of the form (17) maximally violates the inequality for the following measurements by the two parties:

\[
\begin{align*}
A_1 &= \sigma_z, \\
B_1 &= \sigma_x \\
A_2 &= \cos(2\theta)\sigma_z + \sin(2\theta)\sigma_x, \\
B_2 &= \sigma_x
\end{align*}
\]

(18)

2. When maximally violated, the value of the secret key rate is also maximum i.e. 1. However, in general we may not get maximal violation. In that case, one can show that the secret key rate is a continuous function of the value of the inequality close to the maximum violation.

Strategy for unbounded eavesdropping: Each Eve chooses between measurements of \( \sigma_z \) and \( \sigma^\lambda_m \) with outcomes \( c^i \in \{0, 1\} \) (\( \sigma^\lambda_m \) with 0 outcome is \( M_0^A M_0 \), where \( M_0 = \cos(\lambda_m)|0\rangle \langle 0| + \sin(\lambda_m)|1\rangle \langle 1| \), and 1 are the eigenbasis of the \( \sigma_z \) operator). The parameters λ[^m] are fixed before the beginning of the QKD protocol. The initial entangled state shared between Alice and Eve[^1] is \( |\psi^1_A\rangle \) [see Eq. (17) with \( \theta = \theta_1 \)]. If the first unsharp measurement of the operator \( \sigma^\lambda_m \) is made by Eve[^1] on the initial state \( |\psi^1_{\theta_1}\rangle \), the post-measured state is of the form:

\[
|\psi^2_A(\theta_1, \lambda_1)\rangle = U^A_{\lambda_1}(\theta_1, \lambda_1) \otimes V^E_{\lambda_1}(\theta_1, \lambda_1) |c(00)\rangle + s|11\rangle
\]

(19)

where, \( c = \cos(\theta_1(\theta_1, \lambda_1)), s = \sin(\theta_1(\theta_1, \lambda_1)), \) the two unitaries \( U^A_{\lambda_1} \) and \( V^E_{\lambda_1} \) and the angle \( \theta_1(\theta_1, \lambda_1) \in (0, \pi/4] \) depend on the outcome \( c^i \) and the angles \( \theta_1 \) and \( \lambda_1 \).

After his measurement, Eve[^1] applies the unitary \( (V^E_{\lambda_1})^\dagger \) conditioned on his outcome \( c^i \), on the post-measured state going to Eve[^2]. This allows Eve[^2] to use the same two measurements \( \sigma^\lambda_{2^2} \) and \( \sigma_z \) independent of the outcome \( c^i \) since the unitary \( V^E_{\lambda_1} \) is cancelled. The procedure will be applied by each Eve[^m] after his measurement before sending the post-measured state to the next Eve[^m+1]. If the system passed through only the unsharp measurements, the state received by the Bob at the end can be one of the \( 2^{n-1} \) potential states considering there are ‘n’ Eves. This depend on all the Eves (\( E^n \)) outcomes (one for each combination \( c^1, c^2, \ldots, c^{n-1} \)) of outcomes obtained by the Eves, these can be computed before the beginning of the QKD protocol. Any of these states can be written as:

\[
|\psi^\lambda_{\theta, n-1}^A\rangle = U^A_{\lambda}(\theta_{\theta+1}, \lambda) \otimes I_2 \left[ \cos(\theta_{\theta+1})(00) + \sin(\theta_{\theta+1})(11) \right]
\]

(20)

where the angles \( \theta_{\theta+1} \) and the matrix \( U^A_{\lambda}(\theta_{\theta+1}) \) both depend on the outcomes \( c^\theta_{\theta+1} \), on the initial angle \( \theta_1 \) and the sharpness parameters \( \lambda_m \) of the Eves. Bob as usual performs the sharp projective measurements along \( \sigma_z \) and \( \sigma_x \) direction where as Alice performs measurements along \( \sigma_z \) and her second measurement is

\[
A_2^{\lambda_{\theta+1}} = U^A_{\lambda}(\theta_{\theta+1}, \lambda) \otimes (\cos(\mu_{\theta+1})\sigma_z + \sin(\mu_{\theta+1})\sigma_x) (U^A_{\lambda}(\theta_{\theta+1}, \lambda))^\dagger
\]

(21)

where \( \tan(\mu_{\theta+1}) = \sin(2\theta_{\theta+1}) \). These measurements maximally violate the fine-grained inequality and give maximal value of the secret key rate irrespective of the number of Eves. Note that the Alice’s measurements depend on the outcome choices and unsharpness measurement parameters of the Eves and hence the probability of Alice performing measurement in the right direction decreases as the number of Eves increases. However, Alice will try to perform measurement in this direction because she along with Bob wants to maximally violate the inequality and achieve maximal secret key rate. This way unbounded number of Eves can also access the secret keys in this 1S-DIQKD network.

IV. CONCLUSIONS

Quantum steerable correlations are the key resource for one-sided device-independent quantum key distribution task. The monogamy relations restrict the sharing of steerable resource, thus guaranteeing the security of the key distribution task. However, these monogamy restrictions are violated if the parties perform unsharp measurements [24]. It is fair to assume that adversary also has resources to do unsharp measurements and then it is legitimate to rethink about the security of such QKD networks.

In the present study, we address the security of 1S-DIQKD networks by considering the quantum unsharp measurement attacks by the eavesdroppers. We have considered a QKD network constituting two spatially separated spin-\( \frac{1}{2} \) particles, one with Alice and the other one while going to Bob is intercepted by multiple eavesdroppers who gain some positive key rate by performing local quantum unsharp measurement attacks while preserving...
the quantum steerable correlations for the Bob. We find an upper bound on the number of such Eves.

We find that at most 4, 3, and 2 number of Eves can access the secret keys when the secret key rate for each Eve is 0.1, 0.2 and 0.3 respectively. In each case, Bob has secret key rate at least more than that Eve has access to. This is the unbiased case when both the measurements of Eves are unsharp. In ref. [24] at most two observers can share quantum steering when each observer is performing dichotomic measurements. However, we have obtained a maximum of 4 Eves when each party is performing dichotomic measurements showing an increment from the previous work. On the other hand in biased case when only the measurement corresponding to Eves’ measurement is unsharp and each Eve perform some unitary operation before sending the post-measured state to next Eve followed by the particular Alice’s measurement (21), we get an unbounded number of Eves. Bob can assure the security of QKD protocol by having higher secret key rate and terminating the protocol in adverse scenario of the security of QKD protocol by having higher secret key rate below a threshold value. Determining this threshold as a function of Eve’s key rate or environmental noise is worth looking in the future.

Before concluding, it may be noted that sequential sharing of bipartite steering [36] have already been experimentally demonstrated. Our study raises a valid question towards the security of IS-DIQKD networks that can be easily compromised using the available experimental techniques. Finally, the analysis presented here could be used to address the secrecy aspects of other important tasks like quantum secret sharing [40] under quantum unsharp measurement attacks in near future.

V. ACKNOWLEDGEMENTS

SG acknowledges S. N. Bose National Centre for Basic Sciences, Kolkata for the financial support. Authors acknowledge QWorld for organising QIntern 2021. SG thanks Shiladitya Mal for fruitful discussion.

[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).
[2] C. H. Bennett and G. Brassard, Quantum cryptography, public key distribution and coin tossing, IEEE Press, New York, (1984).
[3] Charles H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68, 3121 (1992).
[4] Artur K. Ekert, Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67, 661 (1991).
[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dužek, N. LÃ¶rkkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).
[6] Dominic Mayers, Unconditionally Secure Quantum Bit Commitment is Impossible, Phys. Rev. Lett. 78, 3414 (1997).
[7] Dominic Mayers, Unconditional security in quantum cryptography, JACM 48, 351 (2001).
[8] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera, Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels, Phys. Rev. Lett. 77, 2818 (1996).
[9] Hoi-Kwong Lo and H. F. Chau, Is Quantum Bit Commitment Really Possible?, Phys. Rev. Lett. 78, 3410 (1997).
[10] Peter W. Shor and John Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. 85, 441 (2000).
[11] Gilles Brassard, Norbert LÃ¶rkkenhaus, Tal Mor, and Barry C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. 85, 1330 (2000).
[12] Norbert LÃ¶rkkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A. 61, 052304 (2000).
[13] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, Phys. Rev. A. 85, 010301(R) (2012).
[14] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, Rev. Mod. Phys. 92, 015001 (2020).
[15] E. Schrödinger, Discussion of Probability Relations between Separated Systems, Proc. Cambridge Philos. Soc. 31, 553 (1935).
[16] E. Schrödinger, Probability relations between separated systems, Proc. Cambridge Philos. Soc. 32, 446 (1936).
[17] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox, Phys. Rev. Lett. 98, 140402 (2007).
[18] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Entanglement, Einstein-Podolsky-Rosen correlations, Bell nonlocality, and steering, Phys. Rev. A. 76, 052116 (2007).
[19] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman and M. D. Reid, Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox, Phys. Rev. A 80, 032112 (2009).
[20] J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, Einstein-Podolsky-Rosen steering inequalities from entropic uncertainty relations, Phys. Rev. A 87, 062103 (2013).
[21] Shashank Gupta, Debarshi Das, and A. S. Majumdar, Distillation of genuine tripartite Einstein-Podolsky-Rosen steering, Phys. Rev. A 104, 022409 (2021).
[22] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Phys. Rev. 47, 777 (1935).
[23] T. Pramanik, M. Kaplan and A. S. Majumdar, Fine-grained Einstein-Podolsky-Rosen steering inequalities, Phys. Rev. A 90, 050305(R) (2014).
[24] Souradeep Sasmal, Debarshi Das, Shiladitya Mal, and A. S. Majumdar, Steering a single system sequentially by
multiple observers, Phys. Rev. A 98, 012305 (2018).

[25] Shashank Gupta, Ananda G. Maity, Debarshi Das, Arup Roy, and A. S. Majumdar, Genuine Einstein-Podolsky-Rosen steering of three-qubit states by multiple sequential observers, Phys. Rev. A 103, 022421 (2021).

[26] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. AcAÁn, Unbounded randomness certification using sequences of measurements, Phys. Rev. A 95, 020102(R) (2017).

[27] R. Silva, N. Gisin, Y. Guryanova, and Sandu Popescu, Multiple Observers Can Share the Nonlocality of Half of an Entangled Pair by Using Optimal Weak Measurements, Phys. Rev. Lett. 114, 250401 (2015).

[28] S. Mal, A. S. Majumdar, D. Home, Sharing of Nonlocality of a Single Member of an Entangled Pair of Qubits Is Not Possible by More than Two Unbiased Observers on the Other Wing, Mathematics 4 48 (2016).

[29] P. Busch, Unsharp reality and joint measurements for spin observables, Phys. Rev. D 33, 2253 (1986).

[30] P. Busch, M. Grabowski, and P. J. Lahti, Operational Quantum Physics (Springer-Verlag, Berlin, 1997).

[31] M. Banik, Md. R. Gazi, S. Ghosh, and G. Kar, Degree of complementarity determines the nonlocality in quantum mechanics, Phys. Rev. A 87, 052125 (2013).

[32] P. Busch, T. Heinosaari, J. Schultz, and N. Stevens, Comparing the degrees of incompatibility inherent in probabilistic physical theories, Europhys. Lett. 103, 10002 (2013).

[33] S. K. Choudhary, T. Konrad, and H. Uys, Implementation schemes for unsharp measurements with trapped ions, Phys. Rev. A 87, 012131 (2013).

[34] M.-J. Hu, Z.-Y. Zhou, X.-M. Hu, C.-F. Li, G.-C. Guo, and Y.-S. Zhang, Observation of non-locality sharing among three observers with one entangled pair via optimal weak measurement, npj Quantum Information 4, 63 (2018).

[35] M. Schiavon, L. Calderaro, M. Pittaluga, G. Vallone, and P. Villoresi, Three-observer Bell inequality violation on a two-qubit entangled state, Quantum Sci. Technol. 2 015010 (2017).

[36] Y.-H. Choi, S. Hong, T. Pramanik, H.-T. Lim, Y.-S. Kim, H. Jung, S.-W. Han, S. Moon, and Y.-W. Cho, Demonstration of simultaneous quantum steering by multiple observers via sequential weak measurements, Optica 7, 675 (2020).

[37] G. Foletto, L. Calderaro, G. Vallone, and P. Villoresi, Experimental demonstration of sequential quantum random access codes, Phys. Rev. Research 2, 033205 (2020).

[38] H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental Characterization of Unsharp Qubit Observables and Sequential Measurement Incompatibility via Quantum Random Access Codes, Phys. Rev. Lett. 125, 080403 (2020).

[39] Eric G. Cavalcanti, Christopher J. Foster, Maria Fuwa, and Howard M. Wiseman, Analog of the Clauser-Horne-Shimony-Holt inequality for steering, J. Opt. Soc. Am. B 32, A74 (2015)

[40] M. Hillery, V. Buzeck, and A. Berthiaume, Quantum secret sharing, Phys. Rev. Lett. 68, 3121 (1992)