Device-independent quantum key distribution using random quantum states

Subhankar Bera1 · Shashank Gupta1,2 · A. S. Majumdar1

Received: 27 August 2022 / Accepted: 18 January 2023 / Published online: 11 February 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
We Haar uniformly generate random states of various ranks and study their performance in an entanglement-based quantum key distribution (QKD) task. In particular, we analyze the efficacy of random two-qubit states in realizing device-independent (DI) QKD. We first find the normalized distribution of entanglement and Bell-nonlocality which are the key resource for DI-QKD for random states ranging from rank-1 to rank-4. The number of entangled as well as Bell-nonlocal states decreases as rank increases. We observe that the decrease in the secure key rate is more pronounced in comparison with that of the quantum resource with the increase in rank. We find that the pure state and Werner state provide the upper and lower bound, respectively, on the minimum secure key rate of all mixed two-qubit states possessing the same magnitude of entanglement under general as well as optimal collective attack strategies.

Keywords Quantum cryptography · Quantum key distribution · Quantum security

1 Introduction

Quantum mechanics offers safe encryption solution based on fundamental laws (Quantum Cryptography) rather than on computation difficulty (Rivest–Shamir–Adleman algorithm) [1]. Quantum key distribution (QKD) is the most celebrated protocol in quantum cryptography [2]. There is another approach called post-quantum cryptogra-
which uses conventional cryptography to develop alternative public key encryption schemes that are hard even for a quantum computer to break [3]. However, these are secure against the known quantum attacks, whereas security of QKD protocols is, in principle, independent of all future advances in computational power or algorithm.

There are two distinct classes of QKD protocols in the literature: (a) prepare-and-measure schemes [4, 5] and (b) entanglement-based schemes [6]. In prepare-and-measure schemes, one party prepares the quantum state and encodes the key information which is then transmitted to the other party who decodes this by performing specific measurements. The security is based on the no-cloning principle [7]. On the other hand, the entanglement-based scheme uses the entanglement between the parties to share the key. The security is based on monogamy relations [8, 9].

Device imperfections and implementation loopholes in realistic QKD setups can compromise the security of any QKD protocol. However, device-independent QKD protocols based on entanglement remove such concern over imperfections by demonstrating QKD using uncharacterized devices [10, 11]. Security can be checked using classical constraints on correlations between the parties via Bell’s inequalities, though it has been shown recently that violation of Bell-CHSH inequality is not sufficient for secure QKD [12, 13]. Device independence allows QKD with uncharacterized devices [10, 14–17]. Its security has been proved effective against collective attacks [18, 19]. On a different front, device-independent quantum secure direct communication has been recently proposed [20–22]. Moreover, several interesting works have been proposed on QKD such as long-distance continuous-variable QKD using optical fiber [23], twin-field QKD [24, 25] and reference-frame-independent QKD using coherent states [26].

Most of the previous works on QKD have considered specific classes of pure states [27]. In experiments, generation and maintenance of perfect pure states are challenging because of environmental decoherence. This results in the natural creation of mixed states that need to be studied to get a complete picture. Two-qubit and qudit pure states have been thoroughly studied and their performance in entanglement-based QKD has been properly analyzed [1, 4–6, 28]. On the other hand, limited results are known for mixed states [1, 5] because of multiple state parameters giving rise to multivariate optimization problems. In this work, our aim is to investigate the performance of two-qubit mixed states of different ranks in entanglement-based QKD.

Random states appear naturally in any experimental system. They not only arise naturally in chaotic processes, but can be generated also in a systematic manner based on randomness in the outcome of quantum measurements [29]. Moreover, against the intuition of observing random behavior, it has been found that random states exhibit some universal features. Examples include the performance of random states for certain communication tasks wherein it has been shown that the dense coding capacity and the teleportation fidelity decrease with the increase in the rank of randomly generated states [30].

Randomly generated density matrices [31–34] provide a vital tool for studying the trends of typical states in state space. Random states were instrumental in disproving a long-standing conjecture in quantum information theory regarding additivity of minimal output entropy [35]. Random states have been also utilized for constructive feedback from a non-Markovian noisy environment [36]. Recently, advantage
of employing two random key basis instead of one in device-independent (DI)-QKD has been demonstrated [37]. Some recent interesting works have been proposed on DI-QKD such as rate–distance limit of DI-QKD [38] and photonic demonstration of DI-QKD [39]. The above studies motivate us to explore whether some universal understanding of DI-QKD tasks could be obtained using random states.

In the present work, we investigate the performance of Haar uniformly generated random states in entanglement-based QKD tasks. In particular, we estimate the average secure key rate of states having different ranks in DI-QKD. We first inspect the resourcefulness of the generated random state by quantifying its entanglement and Bell-nonlocality. Our results show that the efficacy of DI-QKD in terms of the secure key rate decreases with the increase in rank of the random state. We further demonstrate that for mixed two-qubit states of any rank possessing the same magnitude of entanglement, the secure key rate of DI-QKD lies between the secure key rate of a pure state and that of a Werner state under general as well as optimal collective attack strategies.

The paper is organized in the following way. In Sec.(2), we recapitulate the generation of random states of different ranks with the aim of utilizing them as resource for DI-QKD. In Sec.(3), we present the device-independent QKD scenario under consideration and provide our analysis for the resourcefulness of the randomly generated states in terms of Bell-nonlocality, as well as their secure key rates. Finally, we present a summary of our results in Sec.(4).

2 Preliminaries

Let us first briefly describe the procedure to generate random states. We randomly simulate complex numbers from a Gaussian distribution with mean 0 and standard deviation unity, denoted $G(0, 1)$. This ensures that the measure is Haar uniform.

**Pure states** Two-qubit pure states are then randomly generated using four such random complex numbers.

$$|\psi_1\rangle = \sum_{ij} c_{ij} |i\rangle \otimes |j\rangle$$  \hspace{1cm} (1)

here $|i\rangle, |j\rangle \in \{|0\rangle, |1\rangle\}$ form the computational basis of the first and second qubit, respectively.

**Mixed states** Random two-qubit mixed states of various ranks are generated from an appropriate pure state in a product Hilbert space by partial tracing of the suitable subsystem.

**Rank-2** Mixed two-qubit density matrices of rank-2 are generated from random tripartite pure states in $2 \otimes 2 \otimes 2$ by tracing out any one of the three qubits [30, 36].

$$|\psi_2\rangle = \text{Tr}_i \left[ \sum_{i,j,k=0,1} c_{ijk} |i\rangle \otimes |j\rangle \otimes |k\rangle \right]$$  \hspace{1cm} (2)
**Rank-3** Mixed two-qubit density matrices of rank-3 are generated from random tripartite pure states in $3 \otimes 2 \otimes 2$ by tracing out the qutrit [30, 36].

$$|\psi_3\rangle = \text{Tr}_i \left[ \sum_{i=0,1,2} \sum_{j,k=0,1} c_{ijk} |i\rangle \otimes |j\rangle \otimes |k\rangle \right]$$  \hspace{1cm} (3)

**Rank-4** Mixed two-qubit density matrices of rank-4 are generated from random quadripartite pure states in $2 \otimes 2 \otimes 2 \otimes 2$ by tracing out any two of the four qubits [30, 36].

$$|\psi_4\rangle = \text{Tr}_{ij} \left[ \sum_{i,j,k,l=0,1} c_{ijkl} |i\rangle \otimes |j\rangle \otimes |k\rangle \otimes |l\rangle \right]$$  \hspace{1cm} (4)

Next, let us recapitulate the quantum resources that are relevant for the present study. Quantum mechanics offers several nonclassical resources that give advantage in different communication tasks. Here, we are interested in the following resources:

**Entanglement** Entanglement of any two-qubit state can be quantified using negativity and logarithmic negativity. Using Eq. (1–4), we generate rank-1 to rank-4 random states, respectively, and we take partial transpose of those numerically generated states and determine the eigenvalues \{$\lambda_1, \lambda_2, \lambda_3, \lambda_4$\}. Logarithmic negativity is defined as $\text{LN} = \log_2(2N + 1)$ (where, $N(=|\sum_j \lambda_j|)$ is negativity and $\lambda_j$ are the negative eigenvalues of the partially transposed state).

**Bell-nonlocality** For a given random two-qubit state $\rho_{AB}$, the maximum value of Bell-nonlocality that can be achieved for optimal measurements is $2 \sqrt{\lambda_1^2 + \lambda_2^2}$. Here, $\lambda_1$ and $\lambda_2$ are the two largest singular values of the correlation matrix $T (t_{ij} = \text{Tr}[(\sigma_i \otimes \sigma_j).\rho_{AB}])$ and $\sigma_{i(j)}$ are the Pauli matrices.

We study the performance of randomly generated states in DI-QKD tasks. Our entire calculations and analysis are based on $10^6$ Haar uniformly generated states for each rank. The distribution of states is quantified in terms of the following parameters, as defined below.

For a given rank of random state, the normalized distribution of quantum resource is defined as the ratio between the number of states having an amount of QR, i.e., $a \leq Q_c \leq b$, with $Q_c$ being the measure of quantum correlation (entanglement or Bell-nonlocality) and the total number of generated random states. Mathematically,

$$P^n_D = \frac{\text{Number of states with } Q_c \in [a, b]}{N_0}$$  \hspace{1cm} (5)

with $N_0$ being the total number of simulated states. Here, ‘n’ stands for normalized and ‘D’ stands for distribution. $Q_c$ denotes logarithmic negativity and violation of Bell-CHSH inequality, in case of entanglement and Bell-nonlocality, respectively. We divide the range of $Q_c \in (0, 1]$ in 10 parts to determine the normalized distribution of quantum resource in simulated random states. The normalized distribution of
entanglement is given by

\[ E_{nD} = \frac{\text{Number of states with } LN \in [a, b]}{N_0} \quad (6) \]

Similarly, the normalized distribution of Bell-nonlocality is defined as

\[ N_{nD} = \frac{\text{Number of states with Bell violation } \in [a, b]}{N_0} \quad (7) \]

The mean distribution of quantum resource is the ratio between the total number of quantum resourceful state and the total number of generated random states for a fixed rank, given by

\[ F_m^D = \frac{\sum F_n^D}{N_0} \quad (8) \]

where we have summed over the entire range of \( a \) and \( b \). Here, ‘m’ stands for mean distribution. This quantity represents the fraction of resourceful states. We consider Bell-nonlocal correlations as quantum resource and analyze the mean distribution of the Bell-nonlocality for the randomly simulated random states as follows:

\[ N_{mD} = \frac{\text{Number of states violating Bell-inequality}}{N_0} \quad (9) \]

We investigate the performance of the random states based on the above-mentioned quantities. As observed from previous studies [30], the number of resourceful state decreases as the rank increases. For a particular rank, the fraction of Bell-nonlocal states is lower than that of entangled states, exemplifying the hierarchy of these correlations for a large number of random states [40].

In Fig. 1, we plot the normalized distribution of entangled random two-qubit states against logarithmic negativity. As shown in Fig. 1, a large fraction of simulated pure states 85% have higher value of logarithmic negativity (0.5 and above), whereas mixed state have percentage 43.8, 16.6, 5.5, respectively, for rank-2, 3, 4 states that have logarithmic negativity 0.5 and above. This implies that as the rank of the state increases, its tendency to have higher value of entanglement decreases. We observed that the quantum resourcefulness of the state decreases as the rank increases. The rest of the paper attempts to answer whether similar behavior is observed in the entanglement-based quantum key distribution task. Specifically, we address the effect of rank and QR of the random state on its performance in DI-QKD.

3 Bell-nonlocality and secure key rate of DI-QKD

Let us first briefly recapitulate the protocol of DI-QKD. Consider the two uncharacterized parties Alice and Bob sharing a bipartite entangled state \( \rho_{AB} \) in \( \mathbb{C}^2 \otimes \mathbb{C}^2 \) as shown in Fig. 2. The two parties want to establish a secure key. For this, each of them perform
Fig. 1 Normalized distribution of entangled ($E_{\text{nd}}$) random two-qubit states (vertical axis) against logarithmic negativity (LN) (horizontal axis). We mentioned only the upper value of the LN (b) in the horizontal axis for brevity of notation. Thus, 0.1 denotes the range (0,0.1] (Color figure online)

Fig. 2 Device-independent quantum key distribution task

dichotomic measurements in two mutually unbiased measurement bases (MUBs) and get two outcomes. Alice performs measurement of the observables randomly chosen from the input $x \in \{0, 1\}$ and gets the outcome $a \in \{0, 1\}$. Similarly, Bob randomly chooses the input measurement $y \in \{0, 1\}$ and gets the outcome $b \in \{0, 1\}$. In the post-processing stage, both the parties publicly compare their input measurements and keep only those outcomes for which their inputs are correlated.

Our protocol is similar to E91 protocol [6]. In a DI-QKD protocol, the devices are untrusted. The security is guaranteed by checking Bell-inequality violation from the measurement statistics. The basic steps of our DI-QKD protocol are as follows:

Quantum state preparation Alice generates a pair of entangled photons at her lab (random two-qubit state). She keeps one of the entangled photons and sends the other to Bob’s lab through a quantum channel.

Springer
Quantum measurement Alice performs measurement of the observable randomly chosen from the input $x \in \{0, 1\}$ and gets the outcome $a \in \{0, 1\}$. Similarly, Bob randomly chooses the input measurement $y \in \{0, 1\}$ and gets the outcome $b \in \{0, 1\}$. During post-processing stage, Alice and Bob keep the cases when their inputs are correlated and discard all other cases.

Bell-inequality violation Alice and Bob use a fraction of inputs and outputs to ensure the Bell-inequality violation. Those cases are also discarded as the output values are disclosed.

Secure symmetric key generation Alice and Bob perform bidirectional error correction on their output values and perform privacy amplification on the corrected keys depending upon the information disclosed (function of the quantum bit error rate (QBER)) and Eve’s attacking strategy. The final keys are the secured symmetric keys. The equality can be verified using a family of universal hash functions.

Let us determine the secret key rate under different Eve’s attack strategies. In the ideal scenario with no attack, Alice and Bob are left with perfectly identical keys. However, imperfections in state preparation, transmission, measurement processes and eavesdropping can yield differences in their key strings. Alice and Bob can estimate the error rate after comparing a small portion of their secure key. Formally, QBER for a given state $\rho_{AB}$ is defined as the average mismatch between the outcomes of Alice and Bob. Let us denote Alice’s two MUBs as $\{ |x_\alpha^a \rangle \}_{a=0}^1$ (for $\alpha \in (0,1)$) which are correlated with Bob’s MUBs $\{ |y_\alpha^b \rangle \}_{b=0}^1$ (for $\alpha \in (0,1)$). The perfect correlation between Alice and Bob would imply that Alice and Bob perform measurements in the same basis and when Alice’s outcome is $|x_1^a \rangle$, Bob’s outcome must be $|y_1^b \rangle$. In the nonideal scenario, there can be nonzero probability of observing $|x_1^a \rangle$ in Alice’s subsystem and $|y_1^b \rangle$ in Bob’s subsystem where $a \neq b$. Hence, the QBER which is an average of all these mismatch probabilities can be expressed as

$$QBER = \frac{1}{2} \sum_{\alpha=0}^1 \sum_{a \neq b=0}^1 \langle x_\alpha^a y_\alpha^b | \rho_{AB} | x_\alpha^a y_\alpha^b \rangle$$

$$= \frac{1}{4} (2 - |\lambda_1| - |\lambda_2|) \quad (10)$$

where $\lambda_1$ and $\lambda_2$ are the two largest singular values of the correlation matrix $T$ ($t_{ij} = \text{Tr}[(\sigma_i \otimes \sigma_j) \cdot \rho_{AB}]$) each of which is bounded from above by 1.

The security of entanglement-based QKD necessarily requires the demonstration of nonlocal correlations. So, for example, violation of Bell-CHSH inequality is required for the security of a DI-QKD since none of the two parties are trusted in this scenario. Note that the violation of the Bell-CHSH inequality is the necessary criterion and not sufficient [12], and hence, there are states that violate the Bell-CHSH inequality but still are not useful for the task of key distribution.

Note that for a given two-qubit state $\rho_{AB}$ the maximum value of Bell-CHSH inequality that can be achieved for optimal measurements is $2\sqrt{\lambda_1^2 + \lambda_2^2}$ (say, $S$). Using Eq. (10), QBER can be written in terms of Bell-nonlocality ($S$) as
\[
QBER = \frac{1}{2} \left(1 - \sqrt{\frac{S^2}{16} + \frac{1}{2} ||\lambda_1|| ||\lambda_2||} \right)
\]  
(11)

From the above equation, we can see that with the increase in Bell-nonlocality (S), the QBER may decrease. The security proof provides a bound on the rate at which Alice and Bob can extract a secure key. The rate at which unconditionally secure key against Eve’s attacks can be extracted is given by

\[
r(\rho_{ABE}) = I(A : B) - I(A : E)
\]  
(12)

where \(\rho_{ABE}\) is the joint state between Alice, Bob and Eve and I is the Holevo quantity or the quantum mutual information. Usually, the joint state \(\rho_{ABE}\) is not known to Alice and Bob. So, the key rate is calculated from the QBER estimation after the error correction algorithm and the effective state after the post-selection (sifting etc.) is given by

\[
\xi(\rho_{AB}) = \sum_u p(u)\rho_{XYE}^u \otimes |u\rangle\langle u|
\]  
(13)

The effective key rate is then,

\[
\tilde{r}(\xi(\rho_{AB})) = \mathbb{I}(\xi(\rho_{AB})) - \mathbb{I}'(\xi(\rho_{AB}))
\]  
(14)

where \(\mathbb{I}(\xi(\rho_{AB})) = \sum_u p(u)I_u(X : Y)\) and \(\mathbb{I}'(\xi(\rho_{AB})) = \sum_u p(u)I_u(X : E)\). Eve has the freedom to choose any attack, if it creates a state \(\rho_{AB}\) contained in the set of all bipartite states \(\{\rho_{AB}\}\) that are compatible with the measurement outcomes \(p(a, b|x, y)\), and have a given reduced state \(\rho_A\). The minimum secure key rate under such assumption is

\[
r_{\text{min}} = \inf_{\rho_{AB}} \tilde{r}(\xi(\rho_{AB}))
\]  
(15)

Since the global state shared between Alice, Bob and Eve are not known, the secure key rate can be determined as a function of the QBER using Eq. (13, 14, 15).

Secret key rate under collective attacks (CA) In the case of collective attacks, the eavesdropper applies the same attack on each system of Alice and Bob. Here the minimum secure key rate is a function of QBER(Q) and S. The minimum secure key rate is given by [18]

\[
r_{\text{Cmin}} \geq 1 - h(Q) - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right)
\]  
(16)

where \(h\) is binary entropy and \(S = 2\sqrt{\lambda_1^2 + \lambda_2^2}\) is the Bell-CHSH violation.

Secret key rate under optimal symmetric collective attacks (OSCA) For the case of optimal symmetric collective attacks (attack optimized over the symmetries of the
Fig. 3 Normalized distribution of Bell-nonlocal ($N_{nd}$) random two-qubit states (vertical axis) against the violation of the Bell-CHSH inequality (BV) (horizontal axis). We mention only the upper value of the Bell’s inequality violation in the horizontal axis for brevity of notation. Thus, 2.082 denotes the range (2, 2.082] (Color figure online)

protocol, state and measurements of the communicating parties) by the eavesdropper in entanglement-assisted protocols for two-qubit states with two measurement settings per qubit, the minimum secure key rate is given by [19]

$$r_{S_{\text{min}}} = 1 + 2(1 - Q)\log_2(1 - Q) + 2Q\log_2 Q$$  \hspace{1cm} (17)

We have two separate conditions for the security of a DI-QKD protocol. One being $r_{C(S)_{\text{min}}} > 0$ for a secure key to be distilled while the second is the requirement that the underlying entangled state violates the Bell-CHSH inequality. While it can be seen that there exist no states with nonvanishing secure key and no Bell-CHSH violation, there do exist states which show Bell-CHSH violation but have vanishing secure key.

We now study the behavior of Bell-nonlocal correlations and minimum secure key rate of random states in DI-QKD. In particular, we first analyze the normalized distribution of Bell-nonlocal correlations (Eq. 5) as shown in Fig. 3. It is seen that the tendency of a random state to achieve large value of Bell-CHSH inequality (2.5 and above) decreases with increasing rank. We find 39.9, 1.9, 0.05 and 0.001 to be the respective percentage of the simulated rank-1, 2, 3 and 4 states that achieve Bell-inequality value of 2.5.

We next perform a comparative study of the mean distribution of $r_{C(S)_{\text{min}}}$ and Bell-nonlocality of all four ranks. The fraction of random states that have nonzero value of the secure key rate is given by
It is seen that the number of randomly simulated states that are Bell-nonlocal as well as the states which provide positive minimum secure key rate decreases with the increase in the rank of the states. The percentages of states that are Bell-nonlocal and give positive secure key rate are 56.8, 8.2, 0.70 and 0.05 for rank-1, 2, 3 and 4, respectively, under optimal symmetric collective attacks. Similarly, under collective attacks, the percentages are 36.8, 1.6, 0.04 and 0.001 for rank-1, 2, 3 and 4, respectively, under collective attacks. Hence, the number of states giving positive secret key rate under general collective attack is less than that under optimal symmetric collective attacks.

Note that the respective percentage of Bell-nonlocal states are higher in both cases. This again implies that all Bell-nonlocal states are not suitable for DI-QKD, reinforcing a similar claim in a recent work [12]. Moreover, the rate of the decrease in $r_{C(S)\text{min}}$ is more prominent than Bell-nonlocality implying that higher-rank Bell-nonlocal states are less useful for DI-QKD. The number of states that are Bell-nonlocal and have positive secure key rate under general collective attacks is less in comparison with that in the optimal symmetric collective attack for every rank. This behavior is expected because in the general collective attack strategy, Eve has the freedom to devise a...

\[ \hat{F}_D^r = \frac{N^r}{N_0} \]
strategy to maximize mutual information, whereas in the optimal symmetric attack, the quantum protocol, state and measurement symmetries put constraints over the strategy of Eve. This constrains Eve’s mutual information and relaxes the secure key rate requirements.

For a given rank of the random state, the average secure key rate is given by the ratio of the sum of the secure key rate of the simulated states to the number of states that have nonzero value of the secure key rate, as

$$\bar{r} = \frac{\sum_i r_i}{N'}$$  \hspace{1cm} (19)

where $r_i$ is the secure key rate of the $i$th state and $N'$ is the total number of states that have nonzero value of the secure key rate. The average key rate computed using Eq. (19) in DI-QKD under optimal symmetric collective attacks is 0.36, 0.15, 0.09 and 0.07 for rank-1, 2, 3 and 4 states, whereas, under collective attacks, the average key rate is 0.34, 0.14, 0.09 and 0.06 for rank-1, 2, 3 and 4 states, respectively, as shown in Table 1. The average key rate in both situations where Eve does a general or optimal collective attack decreases with increasing rank implying that the tendency to generate positive secure key rate decreases with increasing rank. The average key rates in both the attack strategies are nearly the same for a given rank. Our entire calculations are based on $10^6$ Haar uniformly generated states for each case. We find that a large fraction of pure states have positive value of minimum secure key rate and are Bell-nonlocal in comparison with the mixed two-qubit states. This is in accordance with a previous study [36] where it was observed that large fraction of randomly generated mixed states are Bell local states. However, this is in contrast to the observation for teleportation fidelity where it was found that with increasing rank, relative number of states that are local but gives nonclassical fidelity increases [30].

We observe that on average, the quantum resourcefulness of the randomly generated states decreases with an increase in rank and this could be the reason that the performance of the state also decreases in the DI-QKD task as its rank increases. In particular, pure states perform better than rank-2 states, and in turn, rank-2 states perform better than rank-3 and rank-4 states. Interestingly, there are states of different

| No. of random states that violate the Bell-CHSH inequality (among $10^6$ random states) | No. of random states that have positive secure key rate under OSCA | No. of random states that have positive secure key rate under CA | Average secure key rate (OSCA) | Average secure key rate (CA) |
|---------------------------------|------------------|------------------|-----------------|-----------------|
| R-1 1000000                    | 568522           | 368453           | 0.36            | 0.34            |
| R-2 297642                     | 82314            | 16662            | 0.15            | 0.14            |
| R-3 54464                      | 7060             | 423              | 0.09            | 0.09            |
| R-4 8258                       | 498              | 11               | 0.07            | 0.06            |
ranks which have the same value of the entanglement, but have different values of the minimum secure key rate. To illustrate this feature, we next perform a comparative study of pure states, general rank-2 states and Werner states. Werner states are the simplest and most studied two-qubit mixed states that help in understanding the effect of noise on maximally entangled Bell states. We determine the minimum secure key rate of these three states in terms of the negativity to show the distinction in performance for the same value of the entanglement.

An arbitrary two-qubit pure state in a Schmidt decomposition has the form

$$|\psi_p\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$$  \hspace{1cm} (20)

where $|0\rangle$ and $|1\rangle$ are the eigenstates of the reduced density matrices, and eigenvalues of the local density matrices are $\cos^2 \frac{\theta}{2}$ and $\sin^2 \frac{\theta}{2}$. The negativity of the pure state is given by the square root of the determinant of its reduced density matrix, i.e., $\sin \frac{\theta}{2}$.

Any two-qubit mixed state of rank-2 can be expressed as,

$$\rho_2^2 = p_1 |\psi_1\rangle \langle \psi_1| + (1 - p_1) |\psi_2\rangle \langle \psi_2|$$ \hspace{1cm} (21)

where $|\psi_1\rangle = \alpha |0\eta_1\rangle + \beta |1\eta_2\rangle$, $|\psi_2\rangle = \alpha |0\eta_1^+\rangle + \beta |1\eta_2^+\rangle$, $|\eta_1\rangle = a|0\rangle + b|1\rangle$ and $|\eta_2\rangle = a'|0\rangle + b'|1\rangle$ with $|\eta_1^+\rangle$ and $|\eta_2^+\rangle$ being orthogonal states to $|\eta_1\rangle$ and $|\eta_2\rangle$, respectively. The coefficients are taken to be real for simplicity and each of the states are normalized, i.e., $a^2 + b^2 = a'^2 + b'^2 = 1$ and $0 \leq p_1 \leq 1$ The entanglement of state $\rho_2^2$ in Eq. (21) is given by

$$N_2 = \frac{1}{2} \left[ \sqrt{p_1^2 - x - p_1} \right], \text{ if } p_1 < 0.5$$ \hspace{1cm} (22)

$$N_2 = \frac{1}{2} \left[ \sqrt{(1 - p_1)^2 + x - (1 - p_1)} \right], \text{ if } p_1 > 0.5$$ \hspace{1cm} (23)

where $x = 4\alpha^2\beta^2(a'b - ab')^2(2p_1 - 1)$. The state parameter $p_1$ of rank-2 state (21) can be expressed in terms of the negativity, as

$$p_1 = \frac{N^2 - \alpha^2\beta^2(a'b - ab')^2}{N - 2\alpha^2\beta^2(a'b - ab')^2}, \text{ if } p_1 < 0.5$$ \hspace{1cm} (24)

$$p_1 = \frac{N(N + 1) + \alpha^2\beta^2(a'b - ab')^2}{2\alpha^2\beta^2(a'b - ab')^2 + N}, \text{ if } p_1 > 0.5$$ \hspace{1cm} (25)

Next, the two-qubit Werner state is given by

$$\rho_W = p|\phi^+\rangle \langle \phi^+| + \frac{(1 - p)}{4} I_4$$ \hspace{1cm} (26)

where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with $0 \leq p \leq 1$ and $I_4$ being the identity matrix in Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. One can take any other maximally entangled Bell state instead.

 Springer
of $|\phi^+\rangle$ in the expression of the Werner state but the final expression of the minimum secure key rate is same. The negativity of the Werner state is $\frac{3p-1}{4}$.

We now calculate the secure key rate of the rank-2 state (21) in terms of negativity ($N$). Similarly, we calculate the secure key rate of the pure state and Werner state in terms of the negativity (see Appendix (1) for the respective expressions). In Fig. 5, we plot the minimum secure key rate of the pure state, the general rank-2 state and the Werner state in terms of negativity. The figure clearly shows that states with the same value of the negativity can have different performances ($r_{C(S)_{\text{min}}}$) in the DI-QKD task. It can also be seen that the secure key rate of the rank-2 two-qubit state lies in between the secure key rate of pure state and the Werner state at same value of negativity for both categories of collective attack, i.e.,

$$r_{C(S)_{\text{min}}}(\rho_p) \geq r_{C(S)_{\text{min}}}(\rho_2^2) \geq r_{C(S)_{\text{min}}}(\rho_W)$$

where $r_{C(S)_{\text{min}}}$ is the minimum secure key rate in our DI-QKD scenario (17).

We further find numerically, that rank-3 and rank-4 states also have the minimum secure key rate within the envelope formed by the pure state and the Werner state for the same value of negativity. Figure 5 shows that 78.6% of rank-2 states, 39.8% of rank-3 states and 22.7% of rank-4 states have $r_{S_{\text{min}}}$ 0.1 and above under OSCA. Further, Figure 6 shows that 74.6% of rank-2 states, 28.2% of rank-3 states and 16.4% of rank-4 states have $r_{C_{\text{min}}}$ equals 0.1 or above under CA. All of them are inside the envelope formed by the pure state and the Werner state. Our above analysis can be summarized as the following result:

![Image](https://example.com/image.png)
Fig. 6 Minimum secure key rate of randomly generated rank-2, rank-3, rank-4 states, pure state and the Werner state in DI-QKD are plotted versus the negativity for the case of collective attacks. It is clear that the pure state and the Werner state provides the upper and lower bound, respectively, on the minimum secure key rate of mixed two-qubit states in DI-QKD (Color figure online)

**Result** The secure key rate of any mixed two-qubit state in DI-QKD is lower bounded by the secure key rate of the two-qubit Werner state and upper bounded by the secure key rate of the pure state possessing the same value of the negativity under general as well as optimal collective attacks by Eve.

### 4 Conclusions

Quantum key distribution is set to become an integral part of modern cryptographic applications. In theory, unconditional security has been shown for the prepare-and-measure as well as the entanglement-based schemes. However, in practice, perfect quantum key distribution cannot be achieved due to the presence of different decohering factors, device imperfections and implementation loopholes. Therefore, it is of prime importance to study quantum key distribution protocols using randomly generated states rather than confining to specific set of states, with the aim of obtaining a universal perspective.

In this work, we have studied the secure key rate of randomly generated two-qubit states of all four ranks in entanglement-based QKD. Our analysis is based on numerical results obtained by considering $10^6$ states corresponding to each rank. We first estimate the fraction of states in each rank which are Bell-nonlocal and the fraction of states which yield positive secure key rate in DI-QKD under general as well as optimal collective attacks by eavesdropper. We show that both Bell-nonlocality and the minimum secure key rate decrease with the increase in rank in general as well as
optimal attack strategy, which is a fundamental feature of such randomly generated states.

From our analysis, we have observed that with increasing rank the decrease in secure key rate is more pronounced compared to Bell-CHSH violation. The ratio of the number of states that have quantum resource (entangled as well as Bell-nonlocal) as a function of rank decreases slowly in comparison with the ratio of the number of states that give positive secure key rate as a function of rank. For example, the ratio of the number of rank-3 states that are Bell-nonlocal to the number of rank-2 states that are Bell-nonlocal is 0.183, whereas the respective ratio for the number of states that give positive key rate is only 0.085 under optimal symmetric collective attacks and 0.025 under collective attack, respectively. It may be noted that quantum resourcefulness is a necessary condition to obtain secure key rate. However, the secure key rate generation is more demanding, and hence, the number of states that give secure key rate is lesser compared to the number of resourceful states.

Our results further show that states with the same magnitude of entanglement can lead to different values of the secure key rate. We demonstrate that the minimum secure key rate of all two-qubit mixed states is upper bounded by the key rate of the pure state and lower bounded by the key rate of the Werner state possessing the same value of entanglement quantified by their negativity in both optimal and general collective attack strategy. It would be worth studying whether the above bounds can be obtained using analytical methods. It might also be interesting to study in future the effect of statistical fluctuations in the number of randomly generated states on the above bounds. Moreover, our present analysis should motivate further studies on the resilience of random states against particular quantum attacks in QKD protocols, as well as under other sources of error such as channel loss and misalignment rate [41].

A detailed study using random state provides a source-independent analysis and establishes an efficiency and performance profile of the quantum task under consideration. For example, the random states can give a precise idea about the performance of higher-rank mixed states in tasks like quantum multiparty cryptography [42], secure quantum secret sharing [43], quantum conference key agreement [44], quantum private query [45] and quantum secure direct communication [20, 21]. This in turn should further be useful in understanding the efficiency of such tasks under decoherence. This is so because decoherence can be modeled as a black box whose input may be a random state and the output is some different random state, in order to analyze the efficacy of employing random states in various quantum information protocols.

Acknowledgements SB and ASM acknowledge support from the Project No. DST/ICPS/QuEST/2018/98 from the Department of Science and Technology, Government of India. SG acknowledges the support from QuNu Labs Pvt Ltd.

Data availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest All authors declare that they have no conflict of interest with any organization or entity in the subject matter or materials discussed in this manuscript.
Appendix A Minimum secure key rate in DI-QKD

- General rank-2 state:

The matrix form of general rank-2 state (21) is as follows:

\[
\rho_2 = \begin{pmatrix}
    a^2(p_1(a^2 - b^2) + b^2) & a^2b(2p_1 - 1) & a\beta(p_1a' - b(p_1 - 1)b') & a\beta(b(p_1 - 1)a' + ap_1b') \\
    a^2b(2p_1 - 1) & a^2(p_1(b^2 - a^2) + a^2) & a\beta(p_1(ba' + ab') - ab') & a\beta((a - ap_1)a' + bp_1b') \\
    a\beta((a - ap_1)a' + bp_1b') & a\beta(p_1(ba' + ab') - ab') & \beta^2(p_1(a')^2 - (b')^2) & \beta^2(2p_1 - 1)a'b' \\
    a\beta(b(p_1 - 1)a' + ap_1b') & a\beta(p_1(ba' + ab') - ab') & \beta^2(2p_1 - 1)a'b' & \beta^2(p_1(b')^2 - (p_1 - 1)(a')^2)
\end{pmatrix}
\]  

(A1)

Next, we compute the eigenvalues of the correlation matrix (T) of the general rank-2 state. The matrix elements of the correlation matrix are \( t_{ij} = \text{Tr}[(\sigma_i \otimes \sigma_j)\rho_2^2] \). The correlation matrix is:

\[
\begin{pmatrix}
    2a\beta(2p_1 - 1)(ba' + ab') & 0 & 2a\beta(2p_1 - 1)(aa' - bb') \\
    0 & 2a\beta(ba' - ab') & 0 \\
    2(2p_1 - 1)(aa^2b - \beta^2a'b') & 0 & (2p_1 - 1)(a^2(b^2 - a^2) - \beta^2(a')^2 + \beta^2(b')^2)
\end{pmatrix}
\]  

(A2)

The eigenvalues of the correlation matrix (A2) are:

\[
\begin{align*}
\lambda_1 &= y \\
\lambda_2 &= \frac{1}{2}(1 - 2p_1)\left[\alpha^2(b^2 - a^2) + \beta^2(a^2 - b^2) - y' + \sqrt{(2ab\alpha^2 - y + \beta^2(1 - 2a'b') - z)\beta^2(1 + 2a'b') - 2ab\alpha^2 - y + z}\right] \\
\lambda_3 &= \frac{1}{2}(1 - 2p_1)\left[\alpha^2(b^2 - a^2) + \beta^2(a^2 - b^2) - y' - \sqrt{(2ab\alpha^2 - y + \beta^2(1 - 2a'b') - z)\beta^2(1 + 2a'b') - 2ab\alpha^2 - y + z}\right]
\end{align*}
\]  

(A3)

where \( y = 2a\beta(ab' - a'b) \), \( y' = 2a\beta(a'b + ab') \) and \( z = 2a\beta(a'a - bb') \). We determine the quantum bit error rate (QBER) in DI-QKD using Eq. (10) for the case \( (ab' = a'b) \).

\[
\text{QBER} = \frac{1}{4}(2 - |\lambda_2| - |\lambda_3|) \\
= \frac{1}{4}\left[2 - |(1 - 2p_1)(\alpha^2(b^2 - a^2) + \beta^2(a^2 - b^2) - y')|\right]
\]  

(A4)
The $r_{\text{Smin}}(\rho_2^2)$ under optimal symmetric collective attacks (OSCA) is calculated using Eq. (17)

$$r_{\text{Smin}}(\rho_2^2(p_1, a, a', \alpha)) = \frac{1}{2 \log(2)} \left[ \log \left( \frac{1}{4} \left( (1 - 2p_1) \left( a^2 \left( b^2 - a^2 \right) + \beta^2 \left( (a')^2 - (b')^2 \right) - y' \right) + 2 \right) \right) \right]$$

Substituting $p_1$ in terms of $N$ using Eq. (24) for the case $(ab' = a'b)$, we get

$$r_{\text{Smin}}(\rho_2^2) = \frac{1}{2 \log 2} \left[ \log 4 + \log \left( \frac{1}{4} (2 - (1 - 2N)((b^2 - a^2)a^2 - 4ab\alpha a' + \beta^2(a^2 - b^2))) \right) \right]$$

$$+ \log \left( \frac{1}{4} (2 + (1 - 2N)((b^2 - a^2)a^2 - 4ab\alpha a' + \beta^2(a^2 - b^2))) \right)$$

$$+ \log(4) \right]$$

Similarly for the case of collective attacks (CA), using Eq. (10, 16) we obtain the $r_{\text{Cmin}}(\rho_p)$ in terms of negativity $N$,

$$r_{\text{Cmin}}(\rho_p^2) = \frac{1}{\log 16} \left[ -2 \log 16 + (2 - \Omega) \log(2 - \Omega) + (2 + \Omega) \log(2 + \Omega) \right]$$

$$+ 2(1 + \sqrt{\Delta - 1}) \log(1 + \sqrt{\Delta - 1}) + 2(1 - \sqrt{\Delta - 1}) \log(1 - \sqrt{\Delta - 1}) \right]$$

$$\Omega = (1 - 2N) \left( (b^2 - a^2)\alpha^2 - 4ab\alpha a' + \beta^2 (a^2 - b^2) \right),$$

$$\Delta = 2(1 - 2N)^2 \left( (2aba' + \beta^2 + 2\alpha bb'b' - 2a'(a\alpha b + \beta^2 b') - 2bb'\alpha b + 2a'(a\alpha b + b^2) \right) + \left( (b^2 - a^2)\alpha^2 + (a')^2 - (b')^2 \right)^2 \beta^2 \right).$$

We vary the state parameters in the step size of 0.01 to numerically determine the minimum secure key rate as a function of the negativity ($N$).
• General pure state

The matrix form of a general pure state (20) is as follows:

$$ \rho_p = \begin{pmatrix} \cos^2 \frac{\theta}{2} & 0 & 0 & \frac{\sin \theta}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{\sin \theta}{2} & 0 & 0 & \sin^2 \frac{\theta}{2} \end{pmatrix} $$  \hspace{1cm} (A8)

The correlation matrix $t_{ij} = \text{Tr}[\sigma_i \otimes \sigma_j, \rho_p]$ is:

$$ \begin{pmatrix} \sin \theta & 0 & 0 \\ 0 & -\sin \theta & 0 \\ 0 & 0 & 1 \end{pmatrix} $$  \hspace{1cm} (A9)

We obtain $r_{S_{\min}}(\rho_p)$ under optimal symmetric collective attacks (OSCA), for the pure state using Eq. (10) and Eq. (17) in terms of negativity $N$,

$$ r_{S_{\min}}(\rho_p) = -\log 64 + (1 - 2N) \log(1 - 2N) + (3 + 2N) \log(3 + 2N) \over \log 4 $$  \hspace{1cm} (A10)

For the case of collective attacks (CA), using Eq. (10) and Eq. (16) we obtain the $r_{C_{\min}}(\rho_p)$ in terms of negativity $N$,

$$ r_{C_{\min}}(\rho_p) = \frac{1}{\log 16} \left[ -8 \log 2 + (3 + 2N) \log(3 + 2N) + (3 - 6N) \log(1 - 2N) \\ + (2 + 4N) \log(1 + 2N) \right] $$  \hspace{1cm} (A11)

• Werner state

The matrix form of the Werner state (26) is as follows:

$$ \rho_w = \begin{pmatrix} \frac{1+p}{4} & 0 & 0 & \frac{p}{2} \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & \frac{1-p}{4} & 0 \\ \frac{p}{2} & 0 & 0 & \frac{1+p}{4} \end{pmatrix} $$  \hspace{1cm} (A12)

For the Werner state, the correlation matrix $t_{ij} = \text{Tr}[\sigma_i \otimes \sigma_j, \rho_w]$ is:

$$ \begin{pmatrix} p & 0 & 0 \\ 0 & -p & 0 \\ 0 & 0 & p \end{pmatrix} $$  \hspace{1cm} (A13)
We obtain $r_{S_{\text{min}}}(\rho_w)$ under optimal symmetric collective attacks (OSCA), for the Werner state using Eqs. (10, 17) in terms of negativity $N$,

$$
 r_{S_{\text{min}}}(\rho_w) = \log 8 + (2 - 4N) \log(\frac{1-2N}{3}) + 4(1 + N) \log(\frac{2(1+N)}{3}) \log 8
$$

(A14)

Using Eq. (10, 16), we obtain the $r_{C_{\text{min}}}(\rho_w)$ under collective attacks (CA), in terms of negativity $N$,

$$
 r_{C_{\text{min}}}(\rho_w) = \frac{1}{6} \log 2 \left[ -12 \log 3 + 2(1 - 2N) \log(1 - 2N) + (4 + 4N) \log(2 + 2N) \\
+ (3 - \delta) \log(3 - \delta) + (3 + \delta) \log(3 + \delta) \right]
$$

(A15)

where $\delta = \sqrt{-7 + 16N + 32N^2}$.

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74, 145 (2002)
2. Xu, F., Ma, X., Zhang, Q., Lo, H.K., Pan, J.W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. 92, 025002 (2020)
3. Bernstein, D.J., Lange, T.: Post-quantum cryptography. Nature 549, 23461 (2017)
4. Bennett, C.H., Brassard, G.: Quantum cryptography, public key distribution and coin tossing. Theor. Comput. Sci. 560 (Part 1), 7–11 (2014)
5. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121 (1992)
6. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67, 661 (1991)
7. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature 299, 802–803 (1982)
8. Pawłowski, M.: Security proof for cryptographic protocols based only on the monogamy of Bell’s inequality violations. Phys. Rev. A 82, 032313 (2010)
9. Pramanik, T., Kaplan, M., Majumdar, A.S.: Fine-grained Einstein–Podolsky–Rosen steering inequalities. Phys. Rev. A 90, 050305(R) (2014)
10. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. 98, 230501 (2007)
11. Vazirani, U., Vidick, T.: Fully device independent quantum key distribution. Phys. Rev. Lett. 113, 140501 (2014)
12. Farkas, M., Juandó, M.B., Łukanowski, K., Kolodyński, J., Acín, A.: Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. Phys. Rev. Lett. 127, 050503 (2021)
13. Singh, J., Ghosh, S., Arvind, Goyal, S.K.: Role of Bell-CHSH violation and local filtering in quantum key distribution. Phys. Rev. A 392, 127158 (2021)
14. Kolodyński, J., Mättar, A., Skrzypczyk, P., Woodhead, E., Cavalcanti, D., Banaszek, K., Acín, A.: Device-independent quantum key distribution with single-photon sources. Quantum 4, 260 (2020)
15. Metger, T., Dulek, Y., Coladangelo, A., Friedman, R.A.: Device-independent quantum key distribution from computational assumptions. New J. Phys. 23, 123021 (2021)
16. Nadlinger, D.P., Drmota, P., Nichol, B.C., Araneda, G., Main, D., Srinivas, R., Lucas, D.M., Ballance, C.J., Ivanov, K., Tan, E.Y.-Z., Sekatski, P., Urbanke, R.L., Renner, R., Sangouard, N., Bancal, J.-D.: Experimental quantum key distribution certified by Bell’s theorem. Nature 607, 682–686 (2022)
17. Xu, F., Zhang, Y.Z., Zhang, Q., Pan, J.: Device-independent quantum key distribution with random post selection. Phys. Rev. Lett. 128, 110506 (2022)
18. Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., Scarani, V.: Device-independent quantum key distribution secure against collective attacks. New J. Phys. 11, 045021 (2009)

19. Ferenczi, A., Lütkenhaus, N.: Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. Phys. Rev. A 85, 052310 (2012)

20. Zhou, L., Sheng, Y.B., Long, G.L.: Device-independent quantum secure direct communication against collective attacks. Sci. Bull. 65(1), 12–20 (2020)

21. Zhou, L., Sheng, Y.B.: One-step device-independent quantum secure direct communication. Sci. China Phys. Mech. Astron. 65, 250311 (2022)

22. Zhang, W., Ding, D.S., Sheng, Y.B., Zhou, L., Shi, B.S., Guo, G.C.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. 118, 220501 (2017)

23. Zhou, L., Sheng, Y.B.: Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys. Rev. Lett. 125, 010502 (2020)

24. Park, J., Lee, J., Heo, J.: Improved statistical fluctuation analysis for twin-field quantum key distribution. Quant. Inf. Process. 20, 127 (2021)

25. Lu, Y.F., Wang, Y., Jiang, M.S., Liu, F., Zhang, X.X., Bao, W.S.: Finite-key analysis of sending-or-not-sending twin-field quantum key distribution with intensity fluctuations. Quant. Inf. Process. 20, 135 (2021)

26. She, L.G., Zhang, C.M.: Reference-frame-independent quantum key distribution with modified coherent states. Quant. Inf. Process. 21, 161 (2022)

27. Horodecki, K., Horodecki, M., Horodecki, P., Leung, D., Oppenheim, J.: Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity. IEEE Trans. Inf. Theory 54(6), 2604–2620 (2008)

28. Kaszlikowski, D., Oi, D.K.L., Christandl, M., Chang, K., Ekert, A.K., Kwek, L.C., Oh, C.H.: Quantum cryptography based on qutrit Bell inequalities. Phys. Rev. A 67, 012310 (2003)

29. Banerjee, R., Pal, A.K., de Sen, A.: Universality in distribution of monogamy scores for random multiqubit pure states. Phys. Rev. A 101, 042339 (2020)

30. Gupta, R., Gupta, S., Mal, S., De Sen, A.: Performance of dense coding and teleportation for random states: augmentation via preprocessing. Phys. Rev. A 103, 032608 (2021)

31. Kendon, V.M., Zyczkowski, K., Munro, W.J.: Bounds on entanglement in Qudit subsystems. Phys. Rev. A 66, 062310 (2002)

32. Kłobus, W., Burchardt, A., Kołodziejski, A., Pandit, M., Vértesi, T., Życzkowski, K., Laskowski, W.: k-uniform mixed states. Phys. Rev. A 100, 032112 (2019)

33. Gross, D., Flammia, S.T., Eisert, J.: Most quantum states are too entangled to be useful as computational resources. Phys. Rev. Lett. 102, 190501 (2009)

34. Rethinasamy, S., Roy, S., Chanda, T., De Sen, A., Sen, U.: Universality in distribution of monogamy scores for random multiqubit pure states. Phys. Rev. A 99, 042302 (2019)

35. Schumacher, B., Nielsen, M.A.: Quantum data processing and error correction. Phys. Rev. A 54, 2629 (1996)

36. Gupta, R., Gupta, S., Mal, S., De Sen, A.: Constructive feedback of non-Markovianity on resources in random quantum states. Phys. Rev. A 105, 012424 (2022)

37. Schwonnek, R., Goh, K.T., Primaatmaja, I.W., Tan, E.Y.Z., Wolf, R., Scarani, V., Lim, C.C.W.: Device-independent quantum key distribution with random key basis. Nat. Commun. 12, 2880 (2021)

38. Xie, Y.M., Li, B.H., Cao, X.Y., Liu, W.B., Yin, H.L., Chen, Z.B.: Overcoming the rate-distance limit of device-independent quantum key distribution. Opt. Lett. 46, 1632 (2021)

39. Liu, W.Z., Zhang, Y.Z., Chen, Y.Z., Li, M.H., Liu, Y., Fan, J., Xu, F., Zhang, Q., Pan, J.W.: Toward a photonic demonstration of device-independent quantum key distribution. Phys. Rev. Lett. 129, 050502 (2022)

40. Wiseman, H.M., Jones, S.J., Doherty, A.C.: Steering, entanglement, nonlocality, and the Einstein–Podolsky–Rosen paradox. Phys. Rev. Lett. 98, 140402 (2007)

41. Li, B.H., Xie, Y.M., Li, Z., Weng, C.X., Li, C.L., Yin, H.L., Chen, Z.B.: Long-distance twin-field quantum key distribution with entangled sources. Opt. Lett. 46, 5529 (2021)

42. Fu, Y., Yin, H.L., Chen, T.Y., Chen, Z.B.: Long-distance measurement-device-independent multiparty quantum communication. Phys. Rev. Lett. 114, 090501 (2015)

43. Gu, J., Xie, Y.M., Liu, W.B., Fu, Y., Yin, H.L., Chen, Z.B.: Secure quantum secret sharing without signal disturbance monitoring. Opt. Express 29, 32244 (2021)
44. Li, Z., Cao, X.Y., Li, C.L., Weng, C.X., Gu, J., Yin, H.L., Chen, Z.B.: Finite-key analysis for quantum conference key agreement with asymmetric channels. Quant. Sci. Technol. 6, 045019 (2021)
45. Maitra, A., Paul, G., Roy, S.: Device-independent quantum private query. Phys. Rev. A 95, 042344 (2017)

Publisher’s Note  Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.