Secure One-Sided Device-Independent Quantum Key Distribution Under Collective Attacks with Enhanced Robustness

Pritam Roy,[1, *] Subhankar Bera,[1, †] and A. S. Majumdar[1, ‡]

[1] *S. N. Bose National Centre for Basic Sciences,*
Block JD, Sector III, Salt Lake, Kolkata 700 106, India

We study the security of a quantum key distribution (QKD) protocol under the one-sided device-independent (1sDI) setting, which assumes trust in only one party's measurement device. This approach effectively provides a balance between the experimental viability of device-dependent (DD-QKD) and the minimal trust assumptions of device-independent (DI-QKD). An analytical lower bound on the asymptotic key rate is derived to provide security against collective attacks, in which the eavesdropper's information is limited only by the function of observed violation of a linear quantum steering inequality, specifically the three-setting Cavalcanti–Jones–Wiseman–Reid (CJWR) inequality. We provide a closed-form key rate formula by reducing the security analysis to mixtures of Bell-diagonal states by utilizing symmetries of the steering functional. We show that the protocol tolerates higher quantum bit error rates (QBER) than present DI-QKD protocols by benchmarking its performance under depolarizing noise. Furthermore, we explore the impact of detection inefficiencies and show that, in contrast to DI-QKD which requires near-perfect detection, secure key generation can be achieved even with lower detection efficiency on the untrusted side. These findings demonstrate the viability of using 1sDI-QKD with current technology and highlight its advantages as a steering-based substitute for secure quantum communication.

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties to share a secret key, with security provided by the principles of quantum physics rather than computational assumptions [1, 2]. The seminal BB84 protocol [3] demonstrated that quantum states cannot be measured without disturbing them, enabling the detection of any eavesdropping attempt. Thereafter, the E91 protocol [4] introduced an entanglement-based approach where security is certified via Bell inequality violation[5, 6], and the BBM92 protocol [7] proposed a related scheme that employs entanglement[8] without relying on nonlocal correlations. Although these protocols are theoretically secure under idealized assumptions, real-world implementations involve imperfect and potentially untrusted devices, opening up vulnerabilities through various adversarial attacks [9, 10].

Attack strategies in QKD are typically classified into individual, collective, and coherent attacks, in increasing order of generality. In individual attacks, the adversary measures each signal independently [11–15], whereas in collective attacks, Eve interacts identically with each signal but defers measurement for joint processing [10, 16]. Coherent attacks are the most powerful, allowing arbitrary joint operations on all signals [17, 18]. Security proofs against these strategies often rely on entanglement [8] or Bell nonlocality [5, 6, 19], and were initially device-dependent [17, 20]. To address trust issues in devices, the device-independent QKD (DI-QKD) paradigm has gained prominence, particularly after foundational security results [16, 21]. DI-QKD has since advanced through protocols using asymmetric Bell inequalities [22], random states [23], or random measurement bases [24], and experimental demonstrations [25, 26]. Security is guaranteed solely by the violation of Bell inequalities [5, 6], making DI-QKD the most robust cryptographic framework. However, its implementation remains challenging due to strict requirements such as high detection efficiency [27] and loophole-free Bell tests [28–32].

To mitigate the practical limitations of DI-QKD, particularly the need for high detection efficiencies and entanglement, several intermediate frameworks have been introduced. Semi-device-independent QKD (SDI-QKD)[33] ensures security by assuming trusted state preparation while leaving measurement devices uncharacterized. Notably, variants based on quantum contextuality[34] have demonstrated security without relying on nonlocality. In comparison, measurement-device-independent QKD (MDI-QKD) [35, 36] achieves security under the assumption of trusted entangled state preparation, even with untrusted measurement devices.

Under ideal collective attacks, control over just one measurement device and the source is sufficient to compromise security, as demonstrated by the security analyses in Refs. [16, 27]. The 1sDI-QKD framework, which fits in between DI-QKD and SDI/MDI/DD-QKD in the hierarchy of trust models, is based on this observation and assumes trust in only one party's device, usually Bob. The structure of 1sDI-QKD is consistent with the concept of quantum steering, which was first proposed by Schrödinger [37], and formalized later by Wiseman *et al.* [38]. Various criteria, such as Reid's uncertainty-based test [39], the CJWR inequality [40, 41], entropic [42], fine-grained [43], and sum-uncertainty-

[*] roy.pritamphy@gmail.com
[†] berasanu007@gmail.com
[‡] archan@bose.res.in

relation-based formulations [44], can be used to identify steering, which captures the ability of a trusted party to nonlocally affect the state of an untrusted party. Its distinction from entanglement and Bell nonlocality has been established both theoretically [45, 46] and experimentally [40, 47], and further quantified using dedicated measures [48–51]. Steering has also been shown to play an important role in certification of quantum states and measurements in the one-sided device-independent scenario [52–54].

Several protocols have explored the 1sDI-QKD regime under various assumptions and models [43, 55–58]. The works of Branciard et al. [55] and Tomamichel et al. [56] have focused on entropy-based security proofs for BBM92-like or prepare-and-measure schemes, and although they align with the steering scenario, their security bounds depend solely on QBER and are not explicitly connected to steering inequality violations. Pramanik et al. [43] considered individual attacks and demonstrated steering-based security only in that limited regime. Mukherjee et al. [57] focused on the usefulness of steerable states in QKD but did not analyze explicit attack models. More recently, Masini and Sarkar [58] have employed a semidefinite-programming-based approach for proving security against coherent attacks, but without deriving closed-form expressions.

To the best of our knowledge, no existing 1sDI-QKD protocol derives a closed-form asymptotic key rate that quantitatively depends on the violation of a steering inequality, in direct analogy with how DI-QKD protocols relate Bell violations to Eve's information [16, 27]. This gap motivates the need for analytical key rate expressions based on observable steering violations, which would simplify certification and enhance practical relevance.

The DI-QKD security proof by Acín et al.[16] is notable for analytically linking Bell inequality violations to asymptotic key rates, enabling device-independent certification based on observable quantities. Motivated by this, in the current work we establish a closed-form bound for 1sDI-QKD where the key rate is directly expressed in terms of steering inequality violation, thus operationalizing the role of steering in secure key generation. Among various criteria [39, 40, 42, 43, 46], the Cavalcanti–Jones–Wiseman–Reid (CJWR) inequality [40, 41] is especially suited for this task due to its linearity, geometric clarity, and analytical applicability to a broad class of two-qubit states.

In this work, we evaluate a 1sDI-QKD protocol that employs the CJWR steering inequality as a security witness. The protocol uses three binary Pauli measurements per party, with key bits extracted from rounds where both parties measure along σ_z, ensuring low data leakage. The other rounds are used to estimate the CJWR parameter $\mathcal{F}_3$, enabling security verification without basis reconciliation. The security of our protocol is analyzed under collective attacks, where the adversary applies identical and independent operations across rounds. A composable lower bound on the asymptotic key rate is derived using the Devetak–Winter formula, with the CJWR violation acting as the key security witness. Leveraging dimensionality reduction and symmetry arguments, we focus on Bell-diagonal states, for which both the Holevo quantity and the CJWR parameter admit closed-form expressions. This enables an explicit key rate formula in terms of the observed QBER and steering inequality violation.

We evaluate the robustness of our CJWR-based 1sDI-QKD protocol under depolarizing noise, showing that it tolerates a QBER of up to 8.62%, higher than standard DI-QKD protocols, while relying on weaker trust assumptions than DD schemes. To address practical imperfections, we model detection inefficiency on the untrusted side via null outcomes and derive key rate expressions for both post-selected and non-post-selected scenarios. Our analysis reveals that secure key generation remains possible with detection efficiencies as low as 74.5% under ideal visibility, surpassing typical DI-QKD detection efficiency thresholds [18, 22, 27, 55] and emphasizing the protocol's practical advantage in lossy settings.

The manuscript is organized as follows. Section II motivates the use of the CJWR inequality in the context of one-sided device-independent quantum key distribution along with outlining the general framework of 1sDI-QKD. In Section III, we present the security proof under optimal collective attacks. Section IV discusses the robustness of the CJWR-based 1sDI-QKD protocol, while Section V examines the effects of detection inefficiency. Finally, Section VI highlights the salient features of our approach and outlines future research directions.

II. CJWR-BASED 1SDI-QKD PROTOCOL

Entanglement-based QKD provides inherent security based on quantum mechanics. The BBM92 scheme [7] depends on strong measurement correlations without utilizing nonlocality, whereas the Ekert91 protocol [4] certifies key security through violations of Bell inequality. Due to its sensitivity to loss and detection inefficiencies, DI-QKD [10, 16, 25, 27] undermines trust in all devices but is experimentally demanding. The 1sDI-QKD [55, 56], where only one party's device is trusted (typically Bob's), provides a practical alternative. Here, quantum steering [37, 38], an intermediate form of nonclassicality, enables security certification against an untrusted device, making 1sDI-QKD more tolerant to experimental imperfections.

Quantum Steering [37, 38] is a form of quantum correlation that lies between entanglement and Bell nonlocality. It captures the ability of one party to influence the conditional state of another through local measurements nonlocally. A bipartite state is said to be steerable when it cannot be described by a local hidden state (LHS) model, where the trusted party's outcomes arise from a pre-existing quantum ensemble independent of the untrusted party's measurement choice. Violations of steering inequalities [40–43, 47] thus serve as one-sided device-independent witnesses of quantumness. Among these, the CJWR inequality [40] offers a symmetric and experimentally [47, 59] friendly criterion for detecting steering in two-qubit systems, making it particularly suited for 1sDI-QKD protocols.

For n measurement settings per party, the CJWR steering function is defined as

$$\mathcal{F}_n(\rho, \mu) = \frac{1}{\sqrt{n}} \left| \sum_{i=1}^{n} \langle A_i \otimes B_i \rangle \right| \leq 1, \tag{1}$$

where $A_i = \hat{u}_i \cdot \vec{\sigma}$, $B_i = \hat{v}_i \cdot \vec{\sigma}$, and $\mu = \{\hat{u}_i; \hat{v}_i\}_{i=1}^{n}$ specifies the measurement directions, with $\hat{v}_i$ orthonormal and $\hat{u}_i$ unit vectors in $\mathbb{R}^3$.

In two-qubit systems, the two-setting CJWR inequality $\mathcal{F}_2$ fails to identify certain steerable states that remain Bell local [47, 48]. To detect such states and highlight the distinction between steering and Bell nonlocality, we consider the three-setting measure $\mathcal{F}_3$. This steering function can alternatively be expressed in terms of the singular values $\lambda_1, \lambda_2, \lambda_3$ of the correlation matrix T associated with ρ_{AB}, where the matrix elements are defined as $t_{ij} = \mathrm{Tr}[(\sigma_i \otimes \sigma_j)\rho_{AB}]$. These singular values characterize the strength of quantum correlations between the two subsystems along orthogonal measurement directions. In this form, the steering function becomes

$$\mathcal{F}_3 = \sqrt{\lambda_1^2 + \lambda_2^2 + \lambda_3^2}. \tag{2}$$

A violation of the bound, i.e., $\mathcal{F}_3 > 1$, confirms that the state ρ_{AB} is steerable from Alice to Bob. Such violations serve as a practical witness for steering-based quantum correlations and form the foundation for establishing security in 1sDI-QKD protocols.

The three-setting CJWR inequality shares a symmetry structure similar to the CHSH inequality but captures a different class of nonclassical correlations, particularly relevant in one-sided device-independent scenarios. Its experimental applicability and robustness motivate the adoption of the CJWR function as the steering witness in our 1sDI-QKD protocol, as detailed below.

Protocol Overview: Alice and Bob share the maximally entangled Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, i.e., $\rho_{AB} = |\phi^+\rangle\langle\phi^+| \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Bob's measurement device is trusted and fully characterized, while Alice's is treated as a black box. Both parties randomly choose inputs $x, y \in \{1, 2, 3\}$, corresponding to Pauli observables: $A_1 = \sigma_x$, $A_2 = -\sigma_y$, $A_3 = \sigma_z$ for Alice; and $B_1 = \sigma_x$, $B_2 = \sigma_y$, $B_3 = \sigma_z$ for Bob (See Fig.1).

Security is certified through the violation of the CJWR steering inequality for 3-setting ($n = 3$) Eq. (1) :

$$\mathcal{F}_3 = \frac{1}{\sqrt{3}} \left| \sum_{i=1}^{3} \langle A_i \otimes B_i \rangle \right| \leq 1, \tag{3}$$

with $\mathcal{F}_3 > 1$ indicating steerability from Alice to Bob despite Alice's untrusted device.

Only the rounds in which both parties measure in the σ_z basis (i.e., $x = y = 3$) are used for raw key generation, and the corresponding outcomes are kept secret. In contrast, the outcomes from rounds where the measurement settings span all three Pauli bases ($x, y \in \{1, 2, 3\}$) are publicly disclosed and used solely for evaluating the steering parameter $\mathcal{F}_3$. This separation between security estimation and key extraction prevents basis mismatch and simplifies the key rate analysis. Moreover, by disclosing outcomes only in the non-key-generating rounds, the protocol limits information leakage and aligns structurally with Bell-based DI-QKD protocols, such as that of Acín *et al.* [16], enabling a direct comparison of steering- and Bell-based security frameworks. The quantum bit error rate (QBER) quantifies the probability that Alice and Bob obtain different outcomes when measuring in the same basis. Specifically, the QBER is defined as,

$$Q = p(a_3 \neq b_3 \mid A_3, B_3), \tag{4}$$

representing the probability that their outcomes disagree when both measure observables A_3 and B_3, which ideally should yield identical results in the absence of noise or eavesdropping.

After parameter estimation, Alice and Bob proceed to the classical post-processing stage. They first perform *error correction* over an authenticated classical channel to reconcile discrepancies in their raw keys. This is followed by *privacy amplification*, typically using universal hashing [60], to compress the reconciled key and remove any partial information available to an eavesdropper. The amount of extractable secret key is directly determined by the measured QBER and the observed steering violation F_3, ensuring composable security even in the presence of device imperfections on Alice's side.

III. SECURITY ANALYSIS AGAINST COLLECTIVE ATTACKS

In our protocol, only Bob's measurement device is assumed to be trusted and well characterized, while Alice's device is treated as completely untrusted. This setting defines the 1sDI scenario, where the security of the key must be established without relying on any knowledge about Alice's internal operations. Instead, all security claims are based entirely on the observed correlations between Alice and Bob's measurement outcomes.

Although this model is less restrictive than DI-QKD, it still provides strong security guarantees. In particular, it avoids certain experimental challenges such as the detection loophole, which limits the practicality of device-independent approaches [27]. In what follows, we show how the violation of the CJWR steering inequality, along with the measured QBER, can be used to certify the presence of secure correlations and to derive a bound on the secret key rate. The CJWR inequality violation serves as evidence of nonclassical steering correlations,

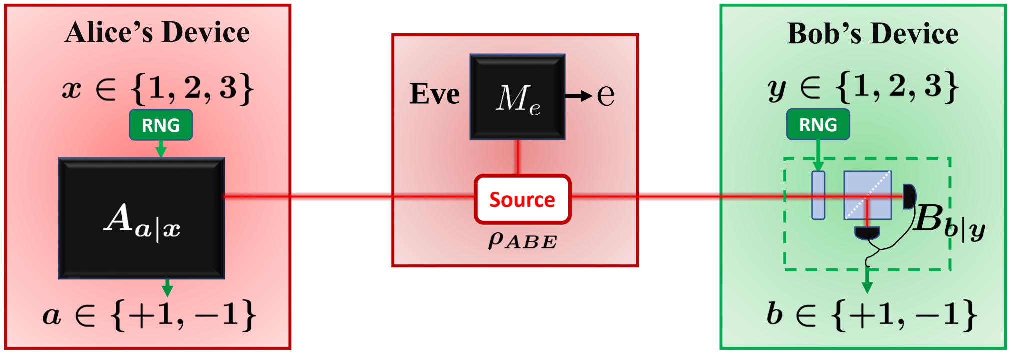

FIG. 1: Schematic of a one-sided device-independent QKD protocol. A source distributes entangled two-qubit states to Alice and Bob. Alice's device is untrusted (black box), while Bob's is fully trusted. Inputs $x, y \in \{1,2,3\}$ are chosen using trusted random number generators, yielding binary outcomes $a, b \in \{+1,-1\}$. Security is certified via quantum steering, e.g., violation of the CJWR inequality.

assuming trust only in Bob's measurement device. Together, these quantities allow Alice and Bob to estimate Eve's accessible information.

We assume that Alice, Bob, and Eve share a tripartite pure state $|\Phi_{\mathrm{ABE}}\rangle \in \mathcal{H}_{\mathrm{A}}^{\otimes N} \otimes \mathcal{H}_{\mathrm{B}}^{\otimes N} \otimes \mathcal{H}_{\mathrm{E}},$, where N is the number of rounds used for key generation. Without loss of generality, we take the local Hilbert spaces to be of equal finite dimension, i.e., $\mathcal{H}_{\mathrm{A}} \simeq \mathcal{H}_{\mathrm{B}} \simeq \mathbb{C}^d$.

For the security analysis, we assume that Eve performs a collective, or i.i.d., attack [10, 16, 18, 19, 21, 27, 61–67]. In this setting, the state and measurement procedure used by Eve are the same in every round, and independent across rounds. As a result, the total shared state between Alice, Bob, and Eve takes the form $|\Phi_{\mathrm{ABE}}\rangle = |\phi_{\mathrm{ABE}}\rangle^{\otimes N}$, where $|\phi_{\mathrm{ABE}}\rangle$ the state is shared in a single round of the protocol. In addition, we assume that the devices are memoryless, meaning the measurement in each round depends only on the current input and not on previous rounds.

We adopt a one-way classical post-processing strategy from Bob to Alice, following the approach of Refs. [16, 19, 27, 62]. Under this setting, the asymptotic key rate can be bounded using the Devetak–Winter formula[61]:

$$r^{\mathrm{1sDI}} \geq I(A_3 : B_3) - \chi(B_3 : E), \tag{5}$$

where $I(A_3 : B_3)$ is the mutual information between Alice and Bob, and $\chi(B_3 : E)$ is the Holevo quantity, representing an upper bound on the information accessible to Eve about Bob's outcomes.

The choice of Bob-to-Alice communication is particularly advantageous in our protocol, as also discussed in Ref. [62]. Since Bob's device is trusted, this direction of classical post-processing allows for a tighter bound on Eve's accessible information. Consequently, the relevant leakage term in the key rate expression is $\chi(B_3 : E)$, rather than $\chi(A_3 : E)$, which would apply if Alice's data were revealed in the classical post-processing step.

Our main objective is to derive an upper bound on Eve's accessible information, quantified by the Holevo quantity $\chi(B_3 : E)$. To achieve this, we follow a sequence of steps outlined below:

Step 1: To compute a tight upper bound on Eve's accessible information, we simplify the analysis using techniques similar in spirit to those introduced in Ref. [27]. In the one-sided device-independent scenario, Bob's measurement device is fully trusted and assumed to perform Pauli measurements. Therefore, even if Eve prepares a general state in $\mathbb{C}^d \otimes \mathbb{C}^d$, Bob effectively accesses only a two-dimensional Hilbert space. As a result, without loss of generality, we can assume that the shared state distributed by Eve is a qudit–qubit state. Certain symmetries inherent in the CJWR inequality can be used to simplify the analysis by reducing the effective dimension of the shared state. This is formalized in the following lemma.

Lemma 1 (Reduction to a two-qubit subspace)**.** *Let $\rho \in \mathbb{C}^d \otimes \mathbb{C}^2$ be a bipartite quantum state, where Bob performs projective measurements along the Pauli directions $\sigma_1, \sigma_2, \sigma_3$, and Alice performs Hermitian dichotomic observables A_1, A_2, A_3 satisfying $A_l^2 = \mathbb{I}$. Then, the quantum steering expression*

$$\mathcal{F}_3(\rho) := \frac{1}{\sqrt{3}} \left| \sum_{l=1}^{3} \langle A_l \otimes \sigma_l \rangle_\rho \right| \tag{6}$$

is bounded by $\mathcal{F}_3(\rho) \leq \sqrt{3}$. The bound is tight if and only if the observables A_l mutually anticommute. In such cases, the optimal value is achieved in a two-qubit system.

Proof. Define the CJWR operator:

$$\mathcal{B}_{\mathrm{CJWR}} := \sum_{l=1}^{3} A_l \otimes \sigma_l.$$

Expanding the square of the CJWR operator,

$$\begin{aligned}\mathcal{B}^2_{\text{CJWR}} &= \left(\sum_l A_l \otimes \sigma_l\right)^2 \\ &= 3\,\mathbb{I}\otimes\mathbb{I} + \sum_{l<m}[A_l, A_m]\otimes\sigma_l\sigma_m,\end{aligned}$$

where we used $A_l^2 = \mathbb{I}, \sigma_l^2 = \mathbb{I}$, and the anticommutation relations $\{\sigma_l, \sigma_m\} = 0$ for $l \neq m$, which implies $\sigma_m\sigma_l = -\sigma_l\sigma_m$.

If the observables mutually anticommute, i.e., $\{A_l, A_m\} = 0$ for $l \neq m$, then $[A_l, A_m] = 2A_lA_m$. Hence,

$$\mathcal{B}^2_{\text{CJWR}} = 3\,\mathbb{I}\otimes\mathbb{I} + 2\sum_{l<m} A_lA_m \otimes \sigma_l\sigma_m.$$

Each term $A_lA_m \otimes \sigma_l\sigma_m$ has operator norm at most 1, since all factors are unitary.

We use the operator norm (or spectral norm) to bound the CJWR steering operator. For a Hermitian operator O, the operator norm is defined as

$$\|O\|_\infty = \sup_{\|\psi\|=1} |\langle\psi|O|\psi\rangle|,$$

which corresponds to the largest eigenvalue in magnitude of O. Using this, we obtain the following bound on the CJWR operator:

$$\|\mathcal{B}^2_{\text{CJWR}}\|_\infty \leq 3 + 6 = 9, \quad \Rightarrow \quad \|\mathcal{B}_{\text{CJWR}}\|_\infty \leq 3.$$

An explicit example achieving the maximum is given by choosing $A_l = \sigma_l$ and taking ρ as the maximally entangled singlet state, for which $\mathcal{F}_3(\rho) = \sqrt{3}$ [40, 48].

Our proof strategy mirrors the dimensionality reduction argument employed in the CHSH scenario [68], where any two dichotomic observables with eigenvalues ±1 are shown to generate a two-dimensional invariant subspace. In our case, the set of three mutually anticommuting observables A_1, A_2, A_3 similarly generate a representation of the real Clifford algebra $\text{Cl}_3(\mathbb{R})$, whose minimal irreducible representation is two-dimensional [69]. This justifies the restriction to a two-qubit system without loss of generality. Hence, there exists a subspace $\mathcal{H}_2 \subseteq \mathcal{H}_A$ such that A_l act as σ_l on $\mathcal{H}_2 \cong \mathbb{C}^2$.

Define the projected state $\rho_{\text{eff}} := (P\otimes\mathbb{I})\rho(P\otimes\mathbb{I}) \in \mathbb{C}^2\otimes\mathbb{C}^2$, where $P : \mathcal{H}_A \to \mathcal{H}_2$ is the projection. Since the CJWR operator acts trivially outside this subspace,

$$\mathcal{F}_3(\rho) = \mathcal{F}_3(\rho_{\text{eff}}).$$

This completes the proof that the optimal value of the CJWR expression is achieved within a two-qubit subspace, and any higher-dimensional scenario does not offer an advantage.

Step 2: In the previous step, we argued that, without loss of generality, Eve can restrict herself to preparing a bipartite state in $\mathbb{C}^2\otimes\mathbb{C}^2$, where Alice's measurements are fixed to be qubit Pauli observables. We now investigate which class of $\mathbb{C}^2\otimes\mathbb{C}^2$ states enables Eve to extract the maximum possible information, while maintaining an optimal value of the CJWR expression between Alice and Bob. In the following lemma, we show that any such two-qubit state $\rho \in \mathbb{C}^2\otimes\mathbb{C}^2$ can be reduced to a Bell-diagonal form without affecting the CJWR value.

Lemma 2 (Reduction to Bell-diagonal form)**.** *Let $\rho \in \mathbb{C}^2\otimes\mathbb{C}^2$ be a two-qubit state shared between Alice and Bob, and suppose Bob performs fixed Pauli measurements $\sigma_x, \sigma_y, \sigma_z$. Then there exists a Bell-diagonal state ρ_Λ such that the CJWR steering expression*

$$\mathcal{F}_3(\rho) = \frac{1}{\sqrt{3}}\left|\sum_{i=1}^3 \langle A_i\otimes\sigma_i\rangle_\rho\right|$$

remains unchanged:

$$\mathcal{F}_3(\rho) = \mathcal{F}_3(\rho_\Lambda).$$

Moreover, ρ_Λ can be obtained from ρ by applying a symmetrization under conjugation by $\sigma_y\otimes\sigma_y$ followed by taking the real part.

Proof. The CJWR functional depends only on the two-point correlators $\langle A_i\otimes\sigma_i\rangle$, and not on local marginals or off-diagonal coherences in other Bell-state bases. Consider the symmetrized state:

$$\bar{\rho} = \frac{1}{2}\left[\rho + (\sigma_y\otimes\sigma_y)\rho(\sigma_y\otimes\sigma_y)\right].$$

This operation preserves all correlators of the form $\langle A_i\otimes\sigma_i\rangle$, since the Pauli matrices σ_i are either invariant or change sign under conjugation by σ_y, and A_i can be redefined accordingly. As a result,

$$\mathcal{F}_3(\rho) = \mathcal{F}_3(\bar{\rho}).$$

Moreover, this conjugation eliminates off-diagonal elements connecting Bell states with opposite $\sigma_y\otimes\sigma_y$ eigenvalues.

To remove the remaining imaginary parts of the off-diagonal terms, we take the real part:

$$\begin{aligned}\rho_\Lambda &= \frac{1}{2}(\bar{\rho} + \bar{\rho}^*) \\ &= \begin{pmatrix}\Lambda_{\Phi^+} & & & \\ & \Lambda_{\Psi^-} & & \\ & & \Lambda_{\Phi^-} & \\ & & & \Lambda_{\Psi^+}\end{pmatrix}\end{aligned} \tag{7}$$

yielding a real, symmetric state diagonal in the Bell basis (i.e. $\{|\Phi^+\rangle, |\Psi^-\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$). Since both steps preserve the relevant correlators, we have:

$$\mathcal{F}_3(\rho) = \mathcal{F}_3(\rho_\Lambda),$$

and thus it suffices to restrict the security analysis to Bell-diagonal states.

Following the symmetrization, the state ρ can be locally rotated within the (x,z) plane to arrange the Bell-state eigenvalues in a fixed order [27], such as $\Lambda_{\Phi^+} \geq \Lambda_{\Psi^-}$ and $\Lambda_{\Phi^-} \geq \Lambda_{\Psi^+}$, without affecting the CJWR functional. These rotations are unitary operations that preserve two-qubit correlators $\langle A_i \otimes \sigma_i \rangle$, and thus leave $\mathcal{F}_3(\rho)$ invariant.

Step 3: Without loss of generality, Eve can send any mixture of Bell-diagonal state like $\rho_{AB} = \sum_\Lambda p_\Lambda \rho_\Lambda$, where Λ is a classical ancilla known to her. Now, we need to calculate the Holevo bound $\chi_\Lambda(B_3 : E)$ for that Bell-diagonal state. For the Bell diagonal state the Holevo bound $\chi_\Lambda(B_3 : E)$ can be calculated as,

$$\begin{aligned}\chi_\Lambda(B_3:E) &= S(\rho_E) - \sum_{b_3=\pm 1} p(b_3)\, S(\rho_{E|b_3}) \\ &= -\sum_{i=1}^{4} \Lambda_i \log_2 \Lambda_i - \frac{1}{2}\left(S(\rho_{E|+1}) + S(\rho_{E|-1})\right),\end{aligned} \tag{8}$$

here $\Lambda_1 = \Lambda_{\Phi^+}, \Lambda_2 = \Lambda_{\Psi^-}, \Lambda_3 = \Lambda_{\Phi^-}, \Lambda_4 = \Lambda_{\Psi^+}$.

To determine a secure key rate in a 1sDI-QKD, we use Bob's σ_z measurement to assess Eve's accessible information, $\chi_\Lambda(B_3 : E)$. This decision is motivated by the necessity for device-independent security proofs to provide a strong, worst-case bound on Eve's knowledge that is valid for all attacks compatible with the observed steering or CJWR violation. The upper bound on $\chi_\Lambda(B_3 : E)$ is given by,

$$\chi_\Lambda(B_3:E) \leq -\sum_{i=1}^{4} \Lambda_i \log_2 \Lambda_i - h(\Lambda_1 + \Lambda_3). \tag{9}$$

Here $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$, h(x) is the binary entropy. The upper bound in Eq. (9) is tight for Bell-diagonal states when Bob measures σ_z, which is the case where Eve gains maximal information (see Lemma 5 of Ref. [27]). Although Bob's trusted apparatus allows flexibility in choosing an optimal measurement basis for key generation (e.g., $\vec{\sigma}\cdot\hat{n}$), analyzing σ_z ensures a conservative, analytically tractable security proof that avoids reliance on numerical optimization and guarantees robustness across implementations. This approach, standard in DI and 1sDI-QKD, strengthens the security analysis by addressing the worst-case scenario, ensuring the key remains secure as long as the observed Bell violation exceeds the classical threshold.

We use the entropic inequality given in Lemma 6 of Ref. [27] to upper-bound Eve's accessible information. It states that for a Bell-diagonal state with eigenvalues $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$ (all ≥ 0 and summing to 1), $\mathcal{R}^2 = (\Lambda_1 - \Lambda_2)^2 + (\Lambda_3 - \Lambda_4)^2$, and taking into account $S(\Lambda) = -\sum_{i=1}^{4} \Lambda_i \log_2 \Lambda_i - h(\Lambda_1 + \Lambda_3)$, the following inequality holds:

$$\mathcal{S}(\Lambda) \leq h\left(\frac{1+\sqrt{2\mathcal{R}^2 - 1}}{2}\right) \quad \text{if } \mathcal{R}^2 > \frac{1}{2}, \tag{10}$$

$$\mathcal{S}(\Lambda) \leq 1 \quad \text{if } \mathcal{R}^2 \leq \frac{1}{2}, \tag{11}$$

with equality in the first bound if and only if either $\Lambda_{1,3} = 0$ or $\Lambda_{2,4} = 0$.

Step 4: We now relate Eve's accessible information to the CJWR function $\mathcal{F}_3(\rho)$. For a Bell-diagonal state ρ_Λ, the correlation matrix T^Λ is diagonal in the Pauli basis, with entries given by $T_{11}^\Lambda = \Lambda_1 - \Lambda_2 - \Lambda_3 + \Lambda_4$, $T_{22}^\Lambda = -\Lambda_1 - \Lambda_2 + \Lambda_3 + \Lambda_4$, $T_{33}^\Lambda = \Lambda_1 - \Lambda_2 + \Lambda_3 - \Lambda_4$. The optimal CJWR value for such a state is

$$\mathcal{F}_3^\Lambda = \sqrt{(T_{11}^\Lambda)^2 + (T_{22}^\Lambda)^2 + (T_{33}^\Lambda)^2}.$$

As shown in Step 3 under optimal attack, this can be compactly written as $\mathcal{F}_3^\Lambda = \sqrt{4\mathcal{R}^2 - 1}$, where $\mathcal{R}$ is defined in terms of the Bell-state probabilities and the threshold $\mathcal{R} = 1/\sqrt{2}$ corresponds to the classical limit for the CJWR inequality, analogous to the CHSH case in Ref. [27].

Since Eve's most general collective strategy can involve preparing a mixture of Bell-diagonal states, we consider $\rho_{AB} = \sum_\Lambda p_\Lambda \rho_\Lambda$. In this case, her accessible information is given by

$$\chi(B_3:E) = \sum_\Lambda p_\Lambda \chi_\Lambda(B_3:E). \tag{12}$$

Using the entropic bound from Step 3, $\chi_\Lambda(B_3 : E) \leq \mathcal{S}(\mathcal{F}_3^\Lambda)$, and the fact that $\mathcal{S}(\cdot)$ is concave, we obtain

$$\chi(B_3:E) \leq \sum_\Lambda p_\Lambda \mathcal{S}(\mathcal{F}_3^\Lambda) \leq \mathcal{S}\left(\sum_\Lambda p_\Lambda \mathcal{F}_3^\Lambda\right).$$

Moreover, by convexity of the CJWR expression (see Eq. (3)) and the triangle inequality ($|a+b| \leq |a| + |b|$), it holds that $\mathcal{F}_3(\rho_{AB}) \leq \sum_\Lambda p_\Lambda \mathcal{F}_3(\rho_\Lambda)$, which implies

$$\chi(B_3:E) \leq \mathcal{S}\left(\mathcal{F}_3(\rho_{AB})\right).$$

Assuming uniform marginals for Alice and Bob, the mutual information becomes $I(A_3 : B_3) = 1 - h(Q)$, where Q is QBER. Combining all steps, the key rate under optimal collective attacks in the 1sDI scenario (see Eq. (5)) is lower bounded by

$$r^{1s\mathrm{DI}} \geq 1 - h(Q) - h\left(\frac{1+\sqrt{(\mathcal{F}_3^2 - 1)/2}}{2}\right). \tag{13}$$

IV. NOISE TOLERANCE OF CJWR-BASED 1SDI-QKD

To quantitatively compare the noise tolerance of 1sDI-QKD against DI and DD protocols, we consider a widely used noise model in the QKD literature [10, 16, 27, 55, 70–72]. In this model, the maximally entangled Bell state

$|\phi^+\rangle$ is subjected to depolarizing noise, resulting in the mixed state

$$\rho_\nu = \nu \left|\phi^+\right\rangle \left\langle\phi^+\right| + (1-\nu)\frac{\mathbb{I}}{4}, \tag{14}$$

where $\nu \in [0,1]$ denotes the visibility, quantifying the strength of the noise. To evaluate the secret key rate achievable in the 1sDI-QKD scenario, we employ Eq. (13) and compute the relevant quantities from this state. The QBER is given by $Q = \frac{1-\nu}{2}$, as obtained from Eq. (4), while the CJWR correlator evaluates to $\mathcal{F}_3 = \nu\sqrt{3}$. We can rewrite this $(Q, \mathcal{F}_3)$ as a correlation,

$$\mathcal{F}_3 = \sqrt{3}(1-2Q). \tag{15}$$

This relation in Eq. (15) is independent of any assumptions on the source or Alice's measurement device, relying solely on the observed statistics $Q, \mathcal{F}_3$.

For the DI and DD scenarios, we use the corresponding key rate expressions derived in previous works. In the DI case, the key rate is bounded using the observed violation of a Bell inequality, typically the CHSH inequality, following the approach of Ref. [16]. The relevant key rate expression is a function of the CHSH parameter $\mathcal{B}$ and QBER Q, which, under depolarizing noise, takes the form $\mathcal{B} = 2\sqrt{2}\nu$ and $Q = \frac{1-\nu}{2}$. In the CHSH scenario, the correlation is given by $\mathcal{B} = 2\sqrt{2}(1-2Q)$[16]. In contrast, the key rate for the device-dependent (DD) scenario [16] is computed under the assumption of full trust in both the state preparation and measurement devices. In this setting, the Devetak–Winter formula [61] applies directly, with the secret key rate determined by the mutual information between Alice and Bob and the conditional entropy of Eve.

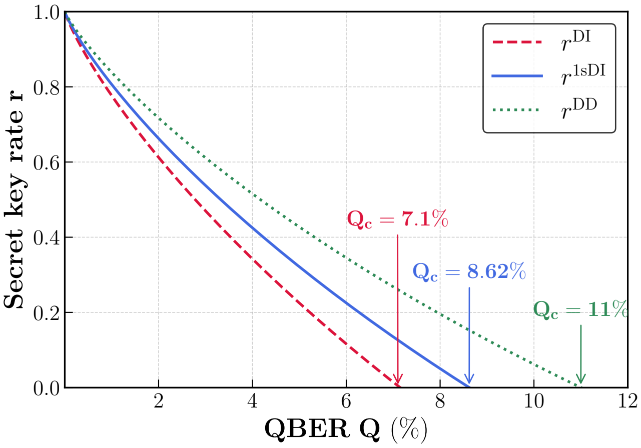

FIG. 2: Comparison of key rates (r) as a function of the QBER (Q). The red dashed line represents the key rate r^{DI} in the DI scenario based on Bell inequality violation. The blue solid line corresponds to the 1sDI key rate r^{1sDI} certified via CJWR steering inequality violation. The green dotted line shows the DD key rate r^{DD}, where both parties' devices are trusted.

To enable a consistent and transparent comparison across different security models, we evaluate the key rates for the DD, 1sDI, and DI scenarios using a common depolarizing noise model ρ_ν, parameterized by the visibility ν. The resulting key rates, plotted as functions of the QBER in Fig. 2, reveal distinct noise thresholds for each protocol. For the fully DI-QKD protocol, the critical QBER is $Q_c^{\mathrm{DI}} = 7.1\%$ [10, 16, 27], while in the DD scenario it increases to approximately 11% [16, 17, 27]. Our CJWR-based 1sDI-QKD protocol achieves a critical QBER of $Q_c^{\mathrm{1sDI}} = 8.62\%$, which lies between these two regimes:

$$Q_c^{\mathrm{DI}} < Q_c^{\mathrm{1sDI}} < Q_c^{\mathrm{DD}}. \tag{16}$$

This intermediate robustness highlights the advantage of the 1sDI setting, which tolerates more noise than fully device-independent protocols while considering fewer assumptions than fully device-dependent approaches. Furthermore, our protocol compares favorably with other steering- or nonlocality-based schemes: for instance, a DI-QKD protocol based on three-setting Bell inequalities yields a threshold of $Q_c = 7.5\%$ [18], while one employing an asymmetric Bell inequality reports $Q_c = 8.34\%$ [22].

V. DETECTION EFFICIENCY IN 1SDI-QKD

While our previous analysis assumes ideal detection conditions, realistic implementations of QKD must account for detection inefficiencies, particularly due to the well-known detection loophole [10, 27], which poses a major challenge for DI-QKD protocols. In such protocols, where both parties are untrusted, achieving secure key distribution requires very high detection efficiencies. Specifically, efficiencies on the order of 92.3% [27] or even 94.5% [18, 55] are necessary under assumptions of ideal visibility ($\nu = 1$).

The primary reason for such stringent requirements is that Eve may exploit undetected events in either party's device to simulate nonlocal correlations. However, in the 1sDI scenario, only one party (Alice) is untrusted, while the other (Bob) uses a trusted, fully characterized measurement device. This relaxation allows for more practical implementations with comparatively lower detection efficiency thresholds.

In the 1sDI scenario, detection inefficiency manifests through no-click events on Alice's side, which we denote by the null outcome $\varnothing$. This effectively increases Alice's output alphabet to three possible outcomes: $\{+1, -1, \varnothing\}$. Following the approach of Ref. [27], we address this by deterministically mapping the null outcome to -1, thereby reducing the measurement to a binary-output POVM. The resulting effective measurement operators on Alice's side take the form

$$\left\{\eta_A A_{+1|i},\ \eta_A A_{-1|i} + (1-\eta_A)\mathbb{I}\right\}, \tag{17}$$

where $\eta_A \in [0,1]$ denotes Alice's detection efficiency, and $A_{\pm1|i}$ are the ideal POVM elements for input i.

Since Bob's device is trusted, we do not explicitly model his inefficiency and consider only those rounds in which his detector clicks. As Eve cannot exploit losses on the trusted side, this selective treatment remains secure and operationally relevant.

There are two natural ways to incorporate the detection inefficiency into the key rate analysis. In the first, we adopt a non-post-selected strategy, retaining all rounds, including those where Alice registers a null outcome. In this case, the QBER becomes $Q_{\mathrm{PS}'} = \frac{1-\nu\eta_A}{2}$, explicitly dependent on the product of the state visibility ν and Alice's detection efficiency η_A.

In contrast, a postselection-based strategy, similar to that used in Ref. [55], discards all rounds in which Alice does not report a valid outcome. In this case, the QBER is independent of η_A and takes the form $Q_{\mathrm{PS}} = \frac{1-\nu}{2}$.

It is important to emphasize that although postselection may improve the observed QBER, it cannot be used when estimating Eve's information. Post-selection can introduce side information to Eve if she has any control or knowledge over the detection process, especially since Alice's device is untrusted. Consequently, the bound on Eve's Holevo information must be derived from the entire ensemble of rounds, without post-selection, to preserve composability.

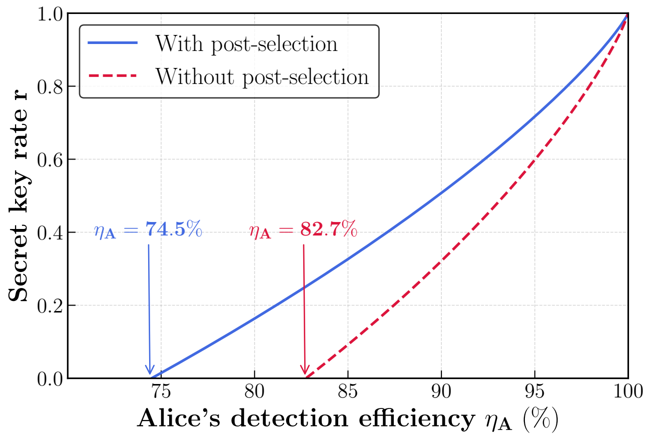

FIG. 3: Comparison of secret key rates r as a function of Alice's detection efficiency η_A under ideal visibility ($\nu = 1$) for a 1sDI-QKD protocol. The red dashed curve corresponds to the key rate without post-selecting QBER (Eq. 18), while the blue solid curve represents the post-selected case (Eq. 19), where QBER is constant. Post-selection allows secure key generation at lower detection efficiencies, down to 74.5%, highlighting a practical advantage over fully device-independent QKD.

To model the effect of loss on the steering parameter, we adopt the null-outcome mapping described above. Under this model, the observed CJWR steering parameter becomes $\mathcal{F}_3 = \eta_A \nu \sqrt{3}$, indicating that detection inefficiency scales linearly with the visibility and degrades the strength of the observed steering correlations.

Using this modified expression, we can now write the corresponding key rate expressions for the two cases. When no post-selection is applied, the secure key rate becomes

$$r^{1sDI}_{\mathrm{PS}'} = 1 - h(Q_{\mathrm{PS}'}) - h\left(\frac{1+\sqrt{(\mathcal{F}_3^2-1)/2}}{2}\right), \quad (18)$$

whereas under postselection, the key rate is given by

$$r^{1sDI}_{\mathrm{PS}} = \eta_A(1-h(Q_{\mathrm{PS}})) - h\left(\frac{1+\sqrt{(\mathcal{F}_3^2-1)/2}}{2}\right). \quad (19)$$

These expressions provide a complete and realistic framework for evaluating the performance of our 1sDI-QKD protocol under lossy conditions. The post-selection strategy benefits from improved QBER but at the cost of reduced key throughput, while the non-post-selected version ensures data integrity at the expense of tighter efficiency requirements.

In Fig. 3, we illustrate how the secret key rate varies with Alice's detection efficiency η_A, assuming perfect visibility ($\nu = 1$). The red dashed curve corresponds to the case without post-selection, where a key can be generated only if η_A exceeds 82.7%. The blue solid curve shows the postselected strategy, which lowers the threshold to 74.5%. These values are already significantly below the critical efficiencies typically required for DI-QKD, where values above 92% are common [27, 55].

To explore how visibility impacts the security threshold, we further examine the relationship between ν and the minimum detection efficiency needed for key generation. As shown in Fig. 4, the threshold η_A decreases with increasing visibility (ν). For all values of ν, the post-selected strategy performs better, consistently allowing secure key generation at lower detection efficiencies. At $\nu = 1$, we recover the earlier thresholds from Fig. 3, confirming consistency between the two analyses.

When compared with other known QKD protocols, our approach remains competitive. In entanglement-based protocols with a trusted Bob, critical detection efficiencies are around 89.6% without postselection and 83.3% with postselection [18, 55]. In the DI setting under collective attacks, the requirements are even stricter 92.3% without postselection and 88.9% with it [27]. The original one sided DI-QKD protocol proposed by Branciard *et al.* achieves lower thresholds of 78% (without postselection) and 65.9% (with postselection) using a two-setting BBM92 like scheme and an entropic uncertainty-based proof [55]. Under ideal detection conditions, the key rate obtained from this protocol matches that of the standard entanglement-based BB84 or BBM92 protocols analyzed under coherent attacks [10, 17, 27].

Our protocol is inspired by the Ekert91 framework and is based on the violation of the CJWR steering inequality [40]. The security is established not via Bell inequality violation, but through quantum steering, which provides a robust and realistic alternative when only one device is trusted. The key rate is analytically derived assuming collective attacks, and the bound on Eve's information is obtained following the approach in Ref. [16]. Notably,

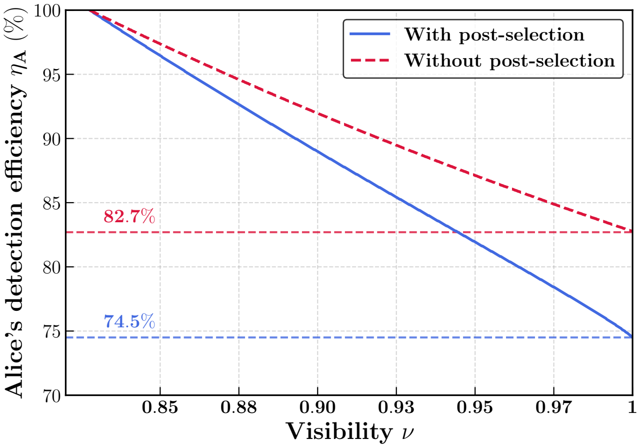

FIG. 4: Threshold detection efficiency of Alice's device η_A (in %) required for a positive secret key rate $r^{1sDI} > 0$ as a function of the source visibility ν. The non-postselected strategy is denoted by the red dashed line, while the postselection case is represented by the solid blue line.

the critical detection efficiency in steering based protocols depends on the chosen steering inequality. While we use a fixed bound, experimental studies suggest that the threshold can be adapted based on observed efficiencies [59], potentially pushing the security threshold even lower.

VI. SALIENT FEATURES AND OUTLOOK

We have presented a security framework for 1sDI-QKD based on the violation of the CJWR steering inequality, offering a practically motivated middle ground between DI and DD quantum cryptographic protocols. By assuming trust only in Bob's measurement device and treating Alice's device as completely untrusted, our approach aligns well with realistic scenarios, such as asymmetric user-server QKD architectures.

The main strength of our result is that the derived key rate under optimal collective attacks depends solely on two directly measurable quantities: the QBER and the CJWR steering violation $\mathcal{F}_3$. Similar to DI-QKD approaches based on Bell inequality violations [16], this avoids the need to reconstruct or assume an explicit quantum state model, allowing the key rate to be calculated from observed statistics. By reducing the analysis to an effective two-qubit Bell-diagonal scenario and relating $\mathcal{F}_3$ to Eve's Holevo information, we obtain a closed-form expression for the asymptotic key rate that is both analytical and operationally meaningful. Whereas previous 1sDI-QKD protocols, like those by Branciard et al. [55], Tomamichel et al. [56], and Masini and Sarkar [58], rely upon entropy-based uncertainty relations or numerical postprocessing, our approach explicitly incorporates steering violation into the key rate bound. This makes the protocol particularly attractive for experimental implementations with constrained resources.

Furthermore, our protocol remains robust against depolarizing noise, tolerating up to 8.62% QBER by relying solely on the observed correlations $(Q, \mathcal{F}_3)$. For comparison, DI-QKD protocols using three-setting Bell inequalities tolerate up to $Q_c = 7.5\%$ [18], while those based on asymmetric Bell inequalities reach $Q_c = 8.34\%$ [22]. The resulting performance approaches that of fully trusted DD schemes, yet preserves significant device-independence, reinforcing the value of 1sDI-QKD in practical implementations. Our protocol also shows favourable thresholds under detection inefficiency, remaining secure with efficiencies as low as 74.5% under post-selection. This compares favorably to DI-QKD thresholds, which often demand efficiencies greater than 87%, as demonstrated in recent photonic DI-QKD (with noisy preprocessing) implementation [25].

This work's analytical framework opens up a number of promising directions for the advancement of 1sDI-QKD in practice. Incorporating noisy preprocessing [31, 73] is a crucial extension that could lower the critical detection-efficiency threshold and increase robustness against experimental imperfections. In addition, experimental studies [59] show that linear steering inequalities can be modified to account for observed losses, as discussed in Section V. This suggests that our detection thresholds could be made more tolerant in practical implementations. Another significant step towards composable security is the establishment of finite-size security through the use of entropy accumulation techniques [66, 67]. Lastly, investigating alternative steering inequalities with improved loss and noise resilience [43, 44] may increase the applicability of our method across various quantum network architectures. Such directions collectively aim to strengthen the viability of 1sDI-QKD as a secure and scalable solution for near-term quantum communication.

[1] C. E. Shannon, Communication theory of secrecy systems, The Bell System Technical Journal **28**, 656 (1949).

[2] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM **21**, 120–126 (1978).

[3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[4] A. K. Ekert, Quantum cryptography based on bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[5] J. S. Bell, On the einstein podolsky rosen paradox, Physics Physique Fizika **1**, 195 (1964).

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23**, 880–884 (1969).

[7] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without bell's theorem, Phys. Rev. Lett. **68**, 557 (1992).

[8] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[10] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[11] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Eavesdropping on quantum-cryptographical systems, Phys. Rev. A **50**, 1047–1056 (1994).

[12] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, Security of quantum cryptography against individual attacks, Phys. Rev. A **57**, 2383–2398 (1998).

[13] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A **61**, 052304 (2000).

[14] M. Curty and N. Lütkenhaus, Intercept-resend attacks in the bennett-brassard 1984 quantum-key-distribution protocol with weak coherent pulses, Phys. Rev. A **71**, 062301 (2005).

[15] P. Roy, S. Sasmal, S. Bera, S. Gupta, A. Roy, and A. Majumdar, Sequential attack impairs security in device-independent quantum key distribution, arXiv preprint arXiv:2411.16822 (2024).

[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[17] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, Phys. Rev. Lett **85**, 441–444 (2000).

[18] L. Masanes, S. Pironio, and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nature Communications **2**, 238 (2011).

[19] A. Acín, N. Gisin, and L. Masanes, From bell's theorem to secure quantum key distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[20] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[21] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[22] E. Woodhead, A. Acín, and S. Pironio, Device-independent quantum key distribution with asymmetric chsh inequalities, Quantum **5**, 443 (2021).

[23] S. Bera, S. Gupta, and A. S. Majumdar, Device-independent quantum key distribution using random quantum states, Quantum Information Processing **22**, 109 (2023).

[24] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y.-Z. Tan, R. Wolf, V. Scarani, and C. C.-W. Lim, Device-independent quantum key distribution with random key basis, Nature communications **12**, 2880 (2021).

[25] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, Toward a photonic demonstration of device-independent quantum key distribution, Phys. Rev. Lett. **129**, 050502 (2022).

[26] W. Zhang, T. van Leent, K. Redeker, and et al., A device-independent quantum key distribution system for distant users, Nature **607**, 687 (2022).

[27] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New Journal of Physics **11**, 045021 (2009).

[28] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong loophole-free test of local realism, Phys. Rev. Lett. **115**, 250402 (2015).

[29] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-loophole-free test of bell's theorem with entangled photons, Phys. Rev. Lett. **115**, 250401 (2015).

[30] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang, L. You, W. J. Munro, J. Yin, J. Zhang, C.-Z. Peng, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan, Test of local realism into the past without detection and locality loopholes, Phys. Rev. Lett. **121**, 080404 (2018).

[31] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution, Phys. Rev. Lett. **124**, 230502 (2020).

[32] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, npj quantum information **9**, 10 (2023).

[33] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302 (2011).

[34] S. Gupta, D. Saha, Z.-P. Xu, A. Cabello, and A. S. Majumdar, Quantum contextuality provides communication complexity advantage, Phys. Rev. Lett. **130**, 080802 (2023).

[35] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[36] Y. Choi, O. Kwon, M. Woo, K. Oh, S.-W. Han, Y.-S. Kim, and S. Moon, Plug-and-play measurement-device-independent quantum key distribution, Phys. Rev. A **93**, 032319 (2016).

[37] E. Schrödinger, Discussion of probability relations between separated systems, Mathematical Proceedings of the Cambridge Philosophical Society **31**, 555–563 (1935).

[38] 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).

[39] M. D. Reid, Demonstration of the einstein-podolsky-rosen paradox using nondegenerate parametric amplification, Phys. Rev. A **40**, 913 (1989).

[40] 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).

[41] J.-L. Chen, C. Wu, L.-C. Kwek, C. H. Oh, and M.-L. Ge, A universal steering criterion, Scientific Reports **3**, 2143 (2013).

[42] 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).

[43] T. Pramanik, M. Kaplan, and A. S. Majumdar, Fine-grained einstein-podolsky-rosen–steering inequalities, Phys. Rev. A **90**, 050305 (2014).

[44] A. G. Maity, S. Datta, and A. S. Majumdar, Tighter einstein-podolsky-rosen steering inequality based on the sum steering relation, Phys. Rev. A **96**, 052326 (2017).

[45] 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).

[46] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Revealing hidden einstein-podolsky-rosen nonlocality, Phys. Rev. Lett. **106**, 130402 (2011).

[47] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Experimental EPR-steering using Bell-local states, Nature Physics **6**, 845 (2010).

[48] A. C. S. Costa and R. M. Angelo, Quantification of einstein-podolsky-rosen steering for two-qubit states, Phys. Rev. A **93**, 020103 (2016).

[49] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, Rev. Mod. Phys. **92**, 015001 (2020).

[50] D. Cavalcanti and P. Skrzypczyk, Quantum steering: a review with focus on semidefinite programming, Reports on Progress in Physics **80**, 024001 (2016).

[51] D. Das, S. Datta, C. Jebaratnam, and A. S. Majumdar, Phys. Rev. A **97**, 022110 (2018).

[52] I. Supic and M. J. Hoban, New J. Phys. **18**, 075006 (2016).

[53] S. Goswami, B. Bhattacharya, D. Das, S. Sasmal, C. Jebarathinam, and A. S. Majumdar, Phys. Rev. A **98**, 022311 (2018).

[54] Z. Bian, A. S. Majumdar, C. Jebarathinam, K. Wang, L. Xiao, X. Zhan, Y. Zhang, and P. Xue, Phys. Rev. A **101**, 020301(R) (2020).

[55] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, Phys. Rev. A **85**, 010301 (2012).

[56] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, One-sided device-independent qkd and position-based cryptography from monogamy games, in *Advances in Cryptology – EUROCRYPT 2013*, edited by T. Johansson and P. Q. Nguyen (Springer Berlin Heidelberg, Berlin, Heidelberg, 2013) pp. 609–625.

[57] K. Mukherjee, T. Patro, and N. Ganguly, Role of steering inequality in quantum key distribution protocol, Quanta **12** (2023), published: 2023-04-18.

[58] M. Masini and S. Sarkar, One-sided di-qkd secure against coherent attacks over long distances, arXiv preprint arXiv:2403.11850 (2024).

[59] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde, Arbitrarily loss-tolerant einstein-podolsky-rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole, Phys. Rev. X **2**, 031003 (2012).

[60] R. Renner, Security of quantum key distribution, International Journal of Quantum Information **6**, 1 (2008).

[61] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207–235 (2005).

[62] A. Acín, S. Massar, and S. Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers, New Journal of Physics **8**, 126–126 (2006).

[63] J. Barrett, L. Hardy, and A. Kent, No signaling and quantum key distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[64] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Transactions on Information Theory **55**, 4337 (2009).

[65] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nature Communications **3**, 634 (2012).

[66] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nature Communications **9**, 459 (2018).

[67] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, Communications in Mathematical Physics **379**, 867 (2020).

[68] L. Masanes, Asymptotic violation of bell inequalities and distillability, Phys. Rev. Lett. **97**, 050503 (2006).

[69] P. Lounesto, *Clifford Algebras and Spinors*, 2nd ed. (Cambridge University Press, 2001).

[70] 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, and P. Wallden, Advances in quantum cryptography, Advances in Optics and Photonics **12**, 1012 (2020).

[71] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[72] R. Renner and R. Wolf, Quantum advantage in cryptography, AIAA Journal **61**, 1895–1910 (2023).

[73] P. Sekatski, J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, and N. Sangouard, Device-independent quantum key distribution from generalized CHSH inequalities, Quantum **5**, 444 (2021).