

Partially device-independent quantum cryptography in asymmetric networks

Jun-Hao Wei^{1,2}, Shu-Ming Hu^{1,2}, Nuo-Ya Yang^{1,2}, Shuai Zhao^{3,*}, Li Li^{1,2,4,†}, Nai-Le Liu^{1,2,4,‡} and Kai Chen^{1,2,4,§}

¹*Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*

²*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

³*School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China*

⁴*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*



(Received 3 February 2026; accepted 18 June 2026; published 14 July 2026)

Quantum key distribution (QKD) enables secure key generation between distant users, yet its standard device-dependent implementations rely on fully characterized and accurately modeled devices. Device-independent (DI) QKD removes this assumption by certifying privacy solely from Bell inequality violations, but its stringent experimental demands severely hinder scalability. In realistic quantum networks, asymmetric levels of device trust can naturally arise from diverse implementation conditions across nodes. Motivated by this, we investigate partially DI scenarios in which only a subset of parties operate trusted devices. Built upon the Brown-Fawzi-Fawzi method [Quantum 8, 1445 (2024)], we employ a semidefinite programming hierarchy tailored to estimate the conditional von Neumann entropies in such settings. This approach provides efficiently computable lower bounds on asymptotic rates of cryptographic protocols with broad applicability. By reexamining representative bipartite and tripartite communication tasks under the partially DI framework, we demonstrate that enforcing trust on the devices of a subset of parties never degrades key or randomness expansion rates and, in certain cases, can substantially increase them owing to the network asymmetry. Our results highlight the impact of device trustworthiness on cryptographic security and facilitate scalable implementations in practical asymmetric network architectures.

DOI: [10.1103/53w8-6v5z](https://doi.org/10.1103/53w8-6v5z)

I. INTRODUCTION

Quantum key distribution (QKD) [1–5] enables two distant parties to establish a secret key that is identical between them and provably inaccessible to any eavesdropper. The security of standard QKD protocols, such as the BB84 scheme [6], typically relies on the assumption that all users' devices are accurately modeled and maintain well calibrated. Consequently, imperfections in realistic implementations may lead to potential vulnerabilities, as demonstrated by various hacking experiments [7–11].

Device-independent (DI) QKD [12–17] provides a means to overcome the stringent requirement of fully characterized quantum operations. Its security is certified solely by the violation of Bell inequalities. In the DI-QKD setup, each party measures a subsystem of an unknown entangled state without trusting the internal workings of the associated measurement

apparatus. Enormous efforts on both theoretical and experimental fronts have advanced the development of DI-QKD across diverse scenarios [18–23].

Despite its conceptual elegance, the implementation of DI-QKD remains challenging, which has stimulated the exploration of a broad range of semi-device-independent frameworks. These schemes introduce certain assumptions on the quantum operations to make them more experimentally feasible than fully DI protocols, while offering enhanced security compared with standard device-dependent (DD) QKD. For example, one can impose constraints on the dimension [24,25] or the overlaps [26,27] of the quantum states, or relax trust in the measurement devices [28]. Prior work has also considered a one-sided device-independent (1SDI) QKD setting [29], analogous to quantum steering scenario [30], where one party operates trusted devices and the other party's apparatus remains entirely untrusted. This represents a modest yet well-justified relaxation of the fully DI model and the simplest instance of asymmetric trust among the parties.

With the advent of large-scale quantum networks [31–35], variations in device performance and implementation conditions across network nodes can give rise to asymmetric trust structures in practice [36,37]. In a general multipartite network, the devices belonging to a nonempty strict subset of the communicating parties may be assumed to be fully trusted and well characterized, while the remaining nodes are treated as completely untrusted. This setting defines the asymmetric networks considered in this work and naturally

*Contact author: zhaoshuai@hdu.edu.cn

†Contact author: eidos@ustc.edu.cn

‡Contact author: nlliu@ustc.edu.cn

§Contact author: kaichen@ustc.edu.cn

captures configurations in which different nodes operate with varying levels of trust and calibration.

In parallel, the demand for cryptographic protocols naturally extends beyond bipartite scenarios toward secure multipartite communication [38–40]. Motivated by these physical considerations, in this work we investigate partially DI quantum cryptographic protocols that go beyond bipartite key distribution, encompassing multipartite quantum conference key agreement (QCKA) [41] and randomness expansion (RE) tasks [42,43]. We focus primarily on the tripartite configurations, as they exemplify heterogeneous trust among multiple parties, which constitutes the fundamental feature of partially DI networked cryptography. They thus provide a minimal yet representative setting within the considered framework, and the extension to more parties is straightforward.

To evaluate the performance of partially DI protocols, we exploit an adapted semidefinite programming (SDP) hierarchy and integrate it with the state-of-the-art Brown-Fawzi-Fawzi (BFF) method [44]. The hierarchy is versatile, as it adapts to a broad range of scenarios. Moreover, as observed in our numerical case studies, the approach attains tight results at relatively low relaxation levels, with notably reduced computational overhead compared to fully DI bounds. We implement the hierarchy by combining existing SDP toolboxes with a custom block-matrix reformulation. We apply the partially DI framework to several representative communication tasks using the same configurations as in fully DI or DD settings, thereby illustrating how relaxing the trust assumptions impacts their performance. Additionally, we derive numerical bounds on the achievable privacy for several well-known Bell inequalities, as well as for steering inequalities specifically formulated for the partially DI regime [37]. Our results also indicate that genuine multipartite entanglement (GME) is not necessary to certify privacy in partially DI protocols. This observation is consistent with similar findings in both fully DI and DD regimes [45,46], and highlights the practical feasibility of implementing such protocols with existing technologies.

II. SETUP

We first introduce the typical entanglement-based QKD setup with one-sided device independence, as illustrated in Fig. 1(a). We note that this setup is identical to that considered in Ref. [29], yet our analysis is not restricted to the qubit case. In this scenario, Alice is assumed to have precise knowledge of the measurements implemented in each round of the protocol, with no side information about these operations being accessible to any eavesdropper or untrusted participant. On the other hand, Bob's device is regarded as an untrusted black box that could, in principle, be controlled by an eavesdropper, Eve. We denote the inputs and outputs of Alice (Bob) by $X(Y)$ and $\hat{A}(\hat{B})$, respectively. Here, $\hat{A}$ and $\hat{B}$ represent the classical registers of Alice and Bob, whereas A and B refer to their corresponding quantum systems. The measurement operators performed by Alice's trusted device in response to her randomly selected input x are denoted as $\{M_{a|x}\}$, while those associated with Bob's untrusted device for his randomly selected input y are denoted as $\{N_{b|y}\}$.

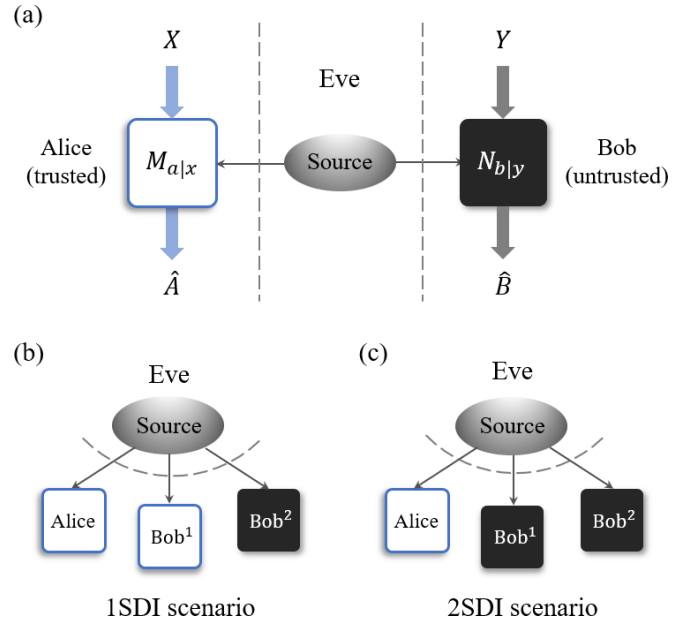


FIG. 1. Schematic illustration of partially device-independent quantum cryptography. (a) Bipartite scenario with one-sided device independence. In each round, Alice and Bob receive subsystems of a quantum state distributed by a source that may be controlled by Eve. Alice performs trusted measurements on her subsystem with input X and output $\hat{A}$. In contrast, Bob's device, with input Y and output $\hat{B}$, is completely untrusted and treated as a black box. (b) 1SDI scenario involving three communicating parties. Only Bob²'s device is untrusted, while those of Alice and Bob¹ are trusted. (c) Two-sided device-independent (2SDI) scenario involving three communicating parties. The devices of both Bob¹ and Bob² are untrusted, whereas only Alice's device is trusted.

Extending to the n -partite case with $n \geq 3$, one can define a family of partially DI settings ranging from one-sided to $(n-1)$ -sided device independence. Throughout this work, Alice is always assumed to be the trustworthy party and the sender of one-way error correction information. The remaining communicating parties are denoted as Bob¹, Bob², and so on, with their respective outputs denoted as $\hat{B}^1$, $\hat{B}^2$, etc. As the number of untrusted parties increases, fewer assumptions about device trustworthiness are required, and the protocol gradually reduces to the fully DI regime. Such a family of protocols is particularly relevant to quantum networks with asymmetric trust imposed on different nodes. For illustrative purposes and also due to computational limitations, we focus on the 1SDI and 2SDI cases involving three communicating parties [see Figs. 1(b) and 1(c), respectively]. Nevertheless, we emphasize that the analysis method is broadly applicable to more general multipartite scenarios.

We consider the collective attack model [3,14,47], in which all devices are assumed to behave in an independent and identically distributed (IID) manner across different rounds and are free of memory effects. This type of attack is known to be asymptotically optimal [48]. Moreover, we confine our analysis to the configuration of the so-called spot-checking protocol [49], where the secret key is extracted exclusively from the rounds with a particular input, e.g., (x^*, y^*) in QKD setups.

In bipartite QKD protocols, as Eve may control the source distributing the states, an unknown tripartite state ρ_{ABE} is shared among Alice, Bob, and Eve at the start of each round. The asymptotic secret key rate of a QKD protocol with one-way error correction is given by the Devetak-Winter formula [50]:

$$R_{\text{QKD}} \geq H(\hat{A}_{x^*}|E) - H(\hat{A}_{x^*}|\hat{B}_{y^*}). \quad (1)$$

Here, $H(\hat{A}_{x^*}|E)$ is the conditional von Neumann entropy quantifying Eve's uncertainty about Alice's raw key in a single IID round. It is evaluated on the classical-quantum state obtained after Alice performs her measurement corresponding to input x^* :

$$\rho_{\hat{A}_{x^*}E} = \sum_a |a\rangle\langle a| \otimes \text{Tr}_{AB}[\rho_{ABE}(M_{a|x^*} \otimes I_{BE})]. \quad (2)$$

The term $H(\hat{A}_{x^*}|\hat{B}_{y^*})$ denotes the conditional Shannon entropy measuring the amount of information Alice should reveal to Bob for error correction and can be directly observed from the two parties' data. Here, we assume an ideal error correction efficiency of 1.

Multipartite QCKA protocols, in the asymptotic regime and against collective attacks, are further considered. As an extension of bipartite QKD, the parties aim to establish a common string of secret bits from their measurement outputs, known as the conference key. The conference key rate with one-way error correction is given by the difference between Alice's conditional entropy and the maximal error reconciliation cost [51]:

$$R_{\text{QCKA}} \geq H(\hat{A}_{x^*}|E) - \max_s H(\hat{A}_{x^*}|\hat{B}_{y_s^*}), \quad (3)$$

where $\hat{B}_{y_s^*}^s$ denotes the register storing the output of Bob^s in response to his input y_s^* and $(x^*, \{y_s^*\}_s)$ are the inputs used for key generation. Since the error terms $H(\hat{A}_{x^*}|\hat{B}_{y_s^*}^s)$ are directly accessible from measurement statistics as well, we still only need to lower bound the conditional entropy $H(\hat{A}_{x^*}|E)$ for a similarly defined classical-quantum state.

Finally, in the context of RE protocols, the parties' outputs are used to extract randomness, which expands the initial randomness employed to choose measurement inputs. The goal is to extract random bits rather than shared secret keys from the parties' outputs; thus, only Eve's uncertainty about the outcomes is relevant. This can be quantified by $H(\hat{A}_{x^*}|E)$ for Alice's results and, analogously, by $H(\hat{A}_{x^*}\hat{B}_{y^*}|E)$ for the joint outcomes [52,53].

III. ASYMPTOTIC RATE CALCULATION

A. Bounding the conditional von Neumann entropy

In the asymptotic setting considered here, the conditional von Neumann entropy is the quantity that naturally enters the key rate formula, and hence constitutes the central goal in evaluating the protocol performance. However, it is highly nonlinear with respect to the underlying classical-quantum state. Fortunately, the recently established BFF method [44] allows for the direct evaluation of the conditional von Neumann entropy and has been applied in several related works [15,22,45,54,55]. Notably, the conditional von Neumann entropy of a bipartite quantum state can be expressed in terms of the quantum relative entropy as

$$H(A|B)_{\rho_{AB}} := -D(\rho_{AB} \| I_A \otimes \rho_B), \quad (4)$$

where I_A is the identity operator on system A. The following Lemma then bounds the quantum relative entropy by a converging sequence of expressions that can be handled within SDP, facilitating the key rate calculation.

Lemma 1 (Brown, Fawzi, Fawzi). Consider a finite-dimensional Hilbert space $\mathcal{H}$ and two positive semidefinite operators ρ and σ on $\mathcal{H}$. Suppose $\rho \leq \lambda\sigma$ for some $\lambda \in \mathbb{R}_+$. Then, for any $m \in \mathbb{N}$, there exists a choice of $t_1, \dots, t_m \in (0, 1]$ and $w_1, \dots, w_m < 0$, such that

$$D(\rho \| \sigma) \leq -c_m - \sum_{k=1}^{m-1} \frac{w_k}{t_k \ln 2} \times \inf_{Z \in \mathcal{B}(\mathcal{H}), \|Z\| \leq \alpha_k} \text{Tr}[\rho(Z + Z^\dagger + (1 - t_k)Z^\dagger Z) + t_k \text{Tr}[\sigma Z Z^\dagger]], \quad (5)$$

where $c_m = (\sum_{k=1}^m \frac{w_k}{t_k \ln 2} - \frac{\lambda}{m^2 \ln 2}) \text{Tr}(\rho)$, $\mathcal{B}(\mathcal{H})$ is the set of bounded operators on $\mathcal{H}$ to itself, and $\alpha_k = \frac{3}{2} \max\{\frac{1}{t_k}, \frac{\lambda}{1-t_k}\}$. Moreover, as $m \rightarrow \infty$, the right-hand side converges to the quantum relative entropy $D(\rho \| \sigma)$.

By adapting Lemma 1, one can obtain a sequence of optimization problems whose solutions give lower bounds on $H(\hat{A}_{x^*}|E)$ in the partially DI scenario. The following proposition specifies the corresponding objectives in the SDP formulation.

Proposition 1. Let $m \in \mathbb{N}$ and let $t_1, \dots, t_m$ and $w_1, \dots, w_m$ be the nodes and weights of an m -point Gauss-Radau quadrature on $[0, 1]$, chosen with an end point $t_m = 1$. Denote ρ_{ABE} as the initial quantum state shared among Alice, Bob, and Eve. Let $\{M_{a|x^*}\}$ denote the measurement operators performed by Alice's *trusted* device upon the input $X = x^*$. Furthermore, for each $k = 1, \dots, m-1$, let $\alpha_k = \frac{3}{2} \max\{\frac{1}{t_k}, \frac{1}{1-t_k}\}$. Then, $H(\hat{A}_{x^*}|E)$ is never smaller than

$$c_m + \sum_{k=1}^{m-1} \frac{w_k}{t_k \ln 2} \sum_a \inf_{Z_a \in \mathcal{B}(\mathcal{H}_E), \|Z_a\| \leq \alpha_k} \text{Tr}[\rho_{AE}(M_{a|x^*} \otimes (Z_a + Z_a^\dagger + (1 - t_k)Z_a^\dagger Z_a) + t_k(I_A \otimes Z_a Z_a^\dagger))], \quad (6)$$

where $c_m = \sum_{k=1}^{m-1} \frac{w_k}{t_k \ln 2}$. Moreover, these lower bounds converge to $H(\hat{A}_{x^*}|E)$ as $m \rightarrow \infty$.

The proof of the above proposition follows directly from Ref. [44] by simply treating Alice's measurements as known

operators, and is thus omitted here. Note that the Z_a operators on Eve's system E , whose dimension is unknown, are non-Hermitian.

To obtain valid lower bounds on the conditional entropy, the optimization must also be carried out over all possible states, uncharacterized measurements, and Hilbert spaces. Meanwhile, one can enforce any relevant constraints of the form $\sum_{abxy} c_{abxy}^{(l)} \text{Tr}[\rho_{ABE}(M_{a|x} \otimes N_{b|y} \otimes I_E)] \geq v^{(l)}$, which

may stand for the observed joint probability distribution of the devices or the violation of a steering inequality. In addition, note that the infimum over the Z_a operators can be moved outside the inner summation over a ; thus, one can run $m-1$ much smaller SDPs, each involving as many Z_a variables as the number of possible values of a (e.g., two variables when Alice's output is binary). Hence, we aim to solve the following optimization problem for each $k = 1, \dots, m-1$:

$$\begin{aligned} V_k = & \inf \sum_a \text{Tr}[\rho_{ABE}(M_{a|x^*} \otimes I_B \otimes (Z_a + Z_a^\dagger + (1-t_k)Z_a^\dagger Z_a) + t_k(I_A \otimes I_B \otimes Z_a Z_a^\dagger))], \\ \text{subject to } & \sum_{abxy} c_{abxy}^{(l)} \text{Tr}[\rho_{ABE}(M_{a|x} \otimes N_{b|y} \otimes I)] \geq v^{(l)} & \text{for all } l \\ & \sum_b N_{b|y} = I & \text{for all } y \\ & N_{b|y} \geq 0 & \text{for all } b, y \\ & \|Z_a\| \leq \alpha_k & \text{for all } a \\ & N_{b|y} \in \mathcal{B}(\mathcal{H}_B), Z_a \in \mathcal{B}(\mathcal{H}_E) & \text{for all } a, b, y, \\ & \rho_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE}) \end{aligned} \quad (7)$$

where the infimum is over all collections $(\rho_{ABE}, \{N_{b|y}\}, \{Z_a\})$ and $\mathcal{D}(\mathcal{H}_{ABE})$ is the set of quantum states on the joint Hilbert space $\mathcal{H}_{ABE}$. Consequently, the conditional entropy $H(\hat{A}_{x^*}|E)$ is bounded from below by $\sum_{k=1}^{m-1} \frac{w_k}{t_k \ln 2} (1 + V_k)$. We also observe that, consistent with Ref. [44], including the operator inequalities $\|Z_a\| \leq \alpha_k$ does not improve the lower bound in most relevant cases; thus, we omit them to accelerate the computations.

For the conditional entropy of two joint outcomes $H(\hat{A}_{x^*} \hat{B}_{y^*}|E)$, a lower bound can be likewise obtained as

$$c_m + \sum_{k=1}^{m-1} \frac{w_k}{t_k \ln 2} \sum_{ab} \inf_{Z_{ab} \in \mathcal{B}(\mathcal{H}_E), \|Z_{ab}\| \leq \alpha_k} \text{Tr}[\rho_{ABE}(M_{a|x^*} \otimes N_{b|y^*} \otimes (Z_{ab} + Z_{ab}^\dagger + (1-t_k)Z_{ab}^\dagger Z_{ab}) + t_k(I_A \otimes I_B \otimes Z_{ab} Z_{ab}^\dagger))], \quad (8)$$

and the optimization problems can be formulated similarly, with constraints appropriately adjusted for the considered partially DI scenario.

We remark that, to extend beyond the asymptotic regime, the entropy accumulation theorem and its generalized form [56–58] provide us a powerful approach for analyzing finite-size security across the DD, partially DI, and fully DI scenarios. Within this framework, the key rate against general coherent attacks can still be expressed in a form essentially analogous to Eq. (1), up to a correction term independent of the number of rounds. Alternatively, by exploiting the dual formulation of the SDP together with martingale-based analysis [54,59], one can also rigorously incorporate the finite-size and non-IID effects.

B. A steering hierarchy

We now introduce a steering hierarchy that relaxes the above optimization problem to a sequence of semidefinite programs, building on and extending the hierarchy of Ref. [60]. To begin with, let us define the set L of all relevant operators acting on the untrusted parties (including Eve), namely, $L = \{I_{BE}, \{N_{b|y}\}_{b,y}, \{Z_a\}_a, \{Z_a^\dagger\}_a\}$. For simplicity, we drop the explicit tensor product structure between systems B and E in what follows. Next, we construct an extended set $S \supseteq L$, whose elements are monomials generated from the operators in L . With the set S in hand, we define a block matrix Γ as

$$\begin{aligned} \Gamma &= \sum_{i,j} |i\rangle\langle j|_R \otimes \Gamma_{i,j}, \quad \text{with } \Gamma_{i,j} \\ &= \text{Tr}_{BE}[\rho_{ABE}(I_A \otimes E_j^\dagger E_i)], \end{aligned} \quad (9)$$

where $E_i \in S$ for $i = 1, \dots, |S|$ and R denotes an ancillary register. Each block $\Gamma_{i,j}$ has the same dimension as the trusted party's system.

By construction, the block matrix Γ is positive semidefinite and hence Hermitian, as we proved in Appendix A. Crucially, the objectives and relevant constraints in Eq. (7) can be expressed in terms of the blocks of Γ . For instance, the term $\text{Tr}[\rho_{ABE}(M_{a|x^*} \otimes Z_a)]$ appearing in Eq. (7) can be rewritten as $\text{Tr}[\text{Tr}_{BE}[\rho_{ABE}(I_A \otimes Z_a)]M_{a|x^*}]$ by invoking the independence of Alice's device together with the identity $\text{Tr}_A[X_{AB}(I \otimes Y_B)] = \text{Tr}_A[X_{AB}]Y_B$. Similarly, the observed joint probability distribution $p(a, b|x, y) = \text{Tr}[\rho_{ABE}(M_{a|x} \otimes N_{b|y})]$ gives rise to linear constraints on specific blocks of Γ , that is, $p(a, b|x, y) = \text{Tr}[\text{Tr}_{BE}[\rho_{ABE}(I_A \otimes N_{b|y})]M_{a|x}]$. It should be noted that certain blocks of Γ (e.g., those involving Z_a) remain undetermined, and some of them may not even be Hermitian [61]. Overall, we aim to minimize the objectives in Eq. (7) over Γ subject to the positive semidefinite condition $\Gamma \geq 0$ and all constraints implied by the observed data and the operator relations. This yields tractable SDPs that can be efficiently solved for many cases of practical interest.

The relaxation heavily depends on the choice of the operator set S . A starting choice is $S_1 = L$, consisting of all

S	I_{BE}	$N_{0 0}$	$N_{0 1}$	Z_0	Z_1	$Z_0^\dagger$	$Z_1^\dagger$
I_{BE}	ρ_A	$N_{0 0}$	$N_{0 1}$	$(Z_0)^\dagger$	$(Z_1)^\dagger$	Z_0	Z_1
$N_{0 0}$		$N_{0 0}$	$N_{0 1}N_{0 0}$	$(N_{0 0}Z_0)^\dagger$	$(N_{0 0}Z_1)^\dagger$	$N_{0 0}Z_0$	$N_{0 0}Z_1$
$N_{0 1}$			$N_{0 1}$	$(N_{0 1}Z_0)^\dagger$	$(N_{0 1}Z_1)^\dagger$	$N_{0 1}Z_0$	$N_{0 1}Z_1$
Z_0				$Z_0^\dagger Z_0$	$Z_1^\dagger Z_0$	Z_0^2	$Z_1 Z_0$
Z_1					$Z_1^\dagger Z_1$	$Z_0 Z_1$	Z_1^2
$Z_0^\dagger$						$Z_0 Z_0^\dagger$	$Z_1 Z_0^\dagger$
$Z_1^\dagger$							$Z_1 Z_1^\dagger$

FIG. 2. An illustration of the moment matrix constructed from the minimal monomial set $S = \{I_{BE}, N_{0|0}, N_{0|1}, Z_0, Z_1, Z_0^\dagger, Z_1^\dagger\}$. The reduced state is $\rho_A = \text{Tr}_{BE}(\rho_{ABE})$. All bold symbols denote block matrix variables of the form $\mathbf{X} = \text{Tr}_{BE}[\rho_{ABE}(I_A \otimes \mathbf{X})]$, with Hermitian conjugate denoted by $(\mathbf{X})^\dagger$. Black entries represent non-Hermitian block matrix variables, while blue entries correspond to Hermitian ones. The lower-triangular blocks are omitted, as they are determined by the Hermiticity of the moment matrix.

degree-one monomials. As an illustrative example, consider the minimal scenario in which Alice and Bob have binary inputs and outputs. To simplify the SDP, it suffices to restrict Bob's measurement operators to two linearly independent ones, $N_{0|0}$ and $N_{0|1}$, instead of all four projectors. The explicit moment matrix at the lowest level of the relaxation is shown in Fig. 2. Enlarging S to include higher-degree monomials produces increasingly tighter relaxations and correspondingly better bounds on $H(\hat{A}_{X^*}|E)$. A common choice is the hierarchy S_r for $r = 1, 2, \dots$, where S_r contains all monomials up to degree r , such that $S_1 \subset S_2 \subset \dots$. Each level of the hierarchy is never weaker than the previous one. In practice, however, it is often advantageous to consider intermediate levels, where a given S_r is augmented with a selected subset of monomials of degree $r + 1$, achieving a balance between computational cost and accuracy.

The hierarchy considered here offers two major advantages. First, it provides a high degree of flexibility, which underscores the versatility of the present approach and facilitates its adaptation to a wide range of partially DI quantum cryptographic protocols. Second, in many tasks even the first-level relaxation—supplemented in some instances by a few degree-two monomials—already appears sufficient to yield tight bounds. This can be understood from the structure of the partially DI scenario considered here: Since Alice is trusted, her operators enter the constraints and objective as known quantities, so that most terms in the SDPs can be represented by blocks associated with degree-one monomials. In the numerical examples considered below, the computation time is largely reduced compared to that required for a DI bound under the same configuration, typically by about a factor of 5. We also observe no improvement upon including additional monomials, suggesting that the obtained bounds are already optimal.

IV. NUMERICAL RESULTS

Using the numerical technique introduced in the previous section, we now proceed to compute lower bounds on the rates of several key distribution and random number generation protocols, and compare them with known analytical results. In the asymptotic regime, we always assume,

without loss of generality, that each party uses a single basis for key generation or randomness extraction, chosen with probability approaching 1. Meanwhile, the other testing bases are selected with negligible probability and serve only to bound Eve's information. For simplicity, here we focus on the idealized case in which the devices are assumed to operate with unit detection efficiency, as is often the case for experimental platforms based on atomic systems [16,17]. Photon losses, however, can be effectively modeled as local depolarization noise, as will be done below, by assigning random outcomes to no-detection events [62].

A. BB84-type protocols

As a starting point, we first examine the simplest entanglement-based QKD scheme within the 1SDI framework. Here, a source distributes maximally entangled two-qubit states, $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, to Alice and Bob. Both parties have two inputs and binary outputs. In accordance with the entanglement-based BB84 (also known as BBM92) protocol [1], the trusted Alice performs projective measurements $M_{0|0} = (I + \sigma_Z)/2$, $M_{1|0} = (I - \sigma_Z)/2$, $M_{0|1} = (I + \sigma_X)/2$, $M_{1|1} = (I - \sigma_X)/2$, while the untrusted Bob is supposed to perform the same measurement operators on his system. Here and throughout, σ_X , σ_Y , and σ_Z denote the Pauli matrices. It has been shown that this entanglement-based formulation is equivalent to the prepare-and-measure BB84 protocol [63]. The analytical key rate formula is

$$r_{\text{BB84}} = 1 - h(e_b) - h(e_p) = 1 - 2h\left(\frac{1-V}{2}\right), \quad (10)$$

where $e_{b(p)}$ is the bit (phase) error rate and $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function. The distributed state is assumed to undergo a global depolarizing channel with visibility V ; thus, the quantum bit error rate (QBER) is $(1-V)/2$. Moreover, one may extend this setup to a 1SDI variant of the six-state protocol by including two additional measurement operators, $M_{0|2} = (I + \sigma_Y)/2$, $M_{1|2} = (I - \sigma_Y)/2$, for both parties [64]. In this case, both Alice and Bob have three inputs, each with binary outputs.

We compute the asymptotic key rates [Eq. (1)] of the two configurations described above with Gauss-Radau quadratures of $m = 2, 4$, and 8 nodes, respectively, adopting relaxation level 1 for the 1SDI BB84 setup and level 1 + ZZ for the 1SDI six-state setup. Here, ZZ represents the degree-two monomials $\{Z_a^\dagger Z_a\}_a$ with $a = 0, 1$. The probability distribution of the testing basis serves as constraints of the SDPs. The semidefinite relaxations were generated via the Python package NCPOL2SDPA [65], with PICOS [66] used to explicitly construct block matrix variables, and the resulting SDP instances were optimized using the solver MOSEK [67]. We find that a Gauss-Radau quadrature of eight nodes suffices to yield tight results, and this also applies to other scenarios. The two setups yield identical numerical key rates—up to six decimal places—for all tested quadrature nodes; therefore, we plot only one of them in Fig. 3(a). Previous works based on alternative numerical techniques [25,68] have shown that, for both the 1SDI BB84 [69] and six-state protocols, the key rates coincide with the fully DD BB84 key rate r_{BB84} .

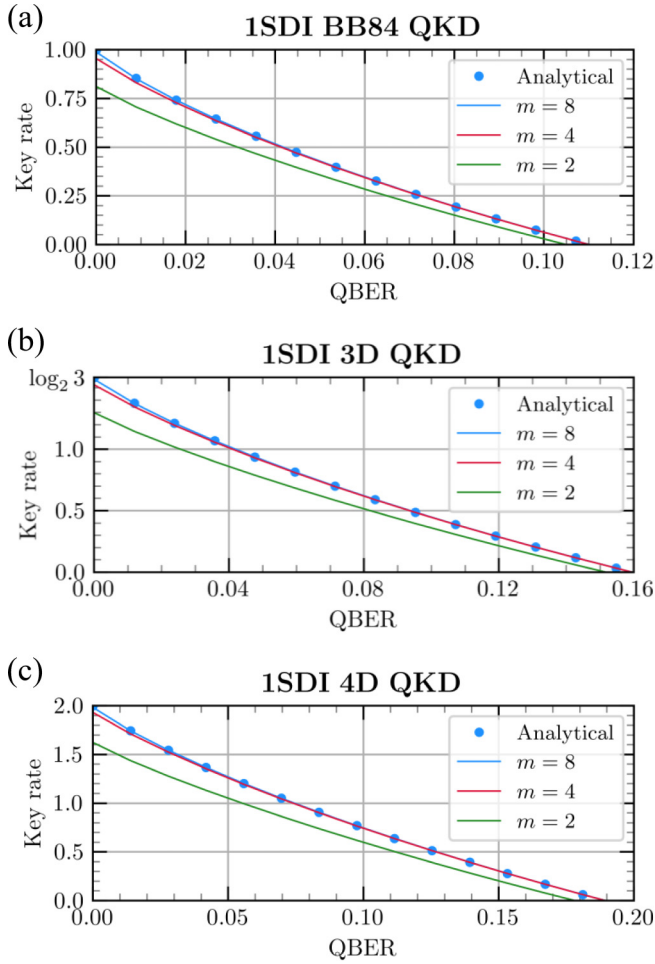


FIG. 3. Lower bounds on the key rates of 1SDI BB84-type protocols. (a) 1SDI BB84 protocol. For both configurations, in which each party has two or three measurement settings, the computed key rates coincide with the analytical expression in Eq. (10). Each SDP instance is solved in under 1 s. (b) 1SDI three-dimensional protocol. For configurations with two, three, or four measurement settings per party, the obtained key rates match the analytical two-basis formula in Eq. (11) for $d = 3$. Each SDP requires several seconds to solve. (c) 1SDI four-dimensional protocol. For configurations with two or three measurement settings per party, the computed key rates coincide with the analytical two-basis formula in Eq. (11) for $d = 4$. Each SDP takes several minutes to solve, and configurations with more settings take even longer. For the three- and four-dimensional cases, the key rates obtained for $m = 2, 4, 8$ are identical for all measurement configurations.

Therefore, our results also provide optimal bounds and further support the conjecture [25] that, in the 1SDI scenario where Bob's measurements are uncharacterized, introducing a third measurement setting does not enhance the achievable key rate compared to using only two. We note that, however, this conjecture remains to be proven.

Next, we move on to the high-dimensional and multipartite scenarios, which remain unexplored in the partially DI context. High-dimensional quantum encoding is known to offer both enhanced information capacity and improved robustness against noise [70–73]. In the high-dimensional protocols

addressed here, the source distributes a d -dimensional maximally entangled state $\sum_{i=0}^{d-1} |ii\rangle/\sqrt{d}$, and Alice and Bob perform measurements in d -dimensional mutually unbiased bases (MUBs) for $d \geq 3$. Two families of protocols can be considered [70], with both parties implementing either two MUBs or all $d + 1$ MUBs. For the former two-basis protocol [71], the asymptotic DD key rate under global depolarizing noise with visibility V is given by

$$r_{\text{HD}} = \log_2 d - 2 \left[-Q \log_2 \frac{Q}{d-1} - (1-Q) \log_2 (1-Q) \right], \quad (11)$$

where the QBER is given by $Q = \frac{d-1}{d} V$.

We numerically investigate the performance of high-dimensional 1SDI-QKD for $d = 3$ and $d = 4$. The asymptotic key rates of protocols employing different numbers of MUBs (ranging from two up to all available MUBs) are calculated using the hierarchy given in Eq. (9) at relaxation level 1 + ZZ. Intriguingly, as illustrated in Figs. 3(b) and 3(c), we find that for both dimensions, the 1SDI key rates coincide with the DD two-basis key rate in Eq. (11) to six decimal accuracy, irrespective of how many MUBs are employed. The results for $d = 3$ and 4 provide strong numerical evidence that, in 1SDI protocols, implementing more MUBs does not improve the achievable key rate beyond that obtained with two bases, and the same behavior is expected to persist in higher-dimensional protocols.

Furthermore, we extend the analysis to tripartite cryptographic tasks, namely, QCKA. In analogy with the construction in Sec. III B, the block matrix for the tripartite 2SDI setting, in which only Alice's device is trusted, takes the form

$$\Gamma^{2\text{SDI}} = \sum_{i,j} |i\rangle\langle j| \otimes \text{Tr}_{B^1 B^2 E} [\rho_{AB^1 B^2 E} (I_A \otimes E_j^\dagger E_i)], \quad (12)$$

with E_i drawn from a chosen set of operators acting on the untrusted subsystems $B^1 B^2 E$. Besides, for the tripartite 1SDI scenario, where both Alice and Bob¹ characterize their devices, the block matrix is defined as

$$\Gamma^{1\text{SDI}} = \sum_{i,j} |i\rangle\langle j| \otimes \text{Tr}_{B^2 E} [\rho_{AB^1 B^2 E} (I_{AB^1} \otimes E_j^\dagger E_i)], \quad (13)$$

where E_i now belongs to the selected set of operators on the untrusted parties $B^2 E$. Note that each block of $\Gamma^{1\text{SDI}}$ has a higher dimension given by the product of the two trusted systems, but as a trade-off in computational cost, the set L contains fewer operators.

In the tripartite QCKA protocol demonstrated here, a source distributes maximally entangled three-qubit GHZ states $(|000\rangle + |111\rangle)/\sqrt{2}$, subject to a global depolarizing channel with visibility V . Each communicating party is supposed to measure the respective subsystem in the σ_X and σ_Z bases. The asymptotic key rate of this protocol [Eq. (3)] can be expressed analytically as [38]

$$\begin{aligned} r_{\text{QCKA}}^{(3)} &= 1 - h(e_p) - \max \{h(e_b^{AB^1}), h(e_b^{AB^2})\} \\ &= 1 - 2h\left(\frac{1-V}{2}\right), \end{aligned} \quad (14)$$

where $e_b^{AB^s}$ denotes the pairwise quantum bit error rate of the raw keys shared between Alice and Bob^s, i.e., the probability that two parties obtain different outcomes in σ_Z -basis

measurements. We now consider both the 1SDI and 2SDI versions of this QCKA protocol. Akin to the entanglement-based BB84 case, two measurement configurations are examined: one where each party measures in $\{\sigma_X, \sigma_Z\}$, and another where $\{\sigma_X, \sigma_Y, \sigma_Z\}$ are employed. Remarkably, in both configurations the computed conference key rates reproduce the DD rate employing two bases [Eq. (14)] within numerical precision. The QCKA results obtained with different numbers of Gauss-Radau quadrature nodes likewise coincide with the corresponding QKD results shown in Fig. 3(a) up to 10^{-6} , and are therefore not plotted here. Our results are summarized in the following observation.

Observation 1. For BB84-type partially DI protocols, where measurement settings are identical across all parties, we numerically observe that in bipartite 1SDI settings with local dimensions $d = 2, 3, 4$, and in tripartite 1SDI and 2SDI settings with local dimensions $d = 2$, the asymptotic key rates obtained using two or more measurement bases are equal to the corresponding two-basis device-dependent key rates.

Based on the considered numerical examples, we expect that a similar equivalence may extend more generally to higher-dimensional and multipartite BB84-type partially DI protocols. In device-dependent scenarios, it is well known that employing more measurement bases can lead to higher key rates [39,64,71]. However, the present results suggest that once the trust in one party's measurement device is removed, the constraints provided by extra measurement bases no longer benefit the communicating parties and do not further restrict the power of Eve under collective attacks, resulting in identical entropy bounds. One possible intuition is that the measurements implemented by untrusted devices are no longer guaranteed to be complementary as in device-dependent cases, and BB84-type correlations are not sufficient to certify their complementarity. Previous work [69] has analytically shown that the two-dimensional bipartite 1SDI protocol with two bases achieves the asymptotic key rate r_{BB84} , indicating that the entanglement-based BB84 protocol is essentially 1SDI. A rigorous proof for protocols involving more measurement bases remains elusive. Our numerical results shed light on a notable feature of partially DI quantum cryptography, and we hope that this observation may stimulate further investigations leading to more definitive conclusions.

B. Protocols based on Bell-type correlations

Aside from BB84-type protocols, it is also fruitful to explore the scenarios where the parties are equipped with different measurement bases. Such protocols are in close resemblance to the original DI-QKD or DI-QCKA [62,74–76], with the essential difference that here we allow a subset of the parties to fully trust their own devices.

1. Bipartite key distribution

We begin with a variable 1SDI-QKD [29] setup to investigate the role of observed correlations. Suppose Alice and Bob share a depolarized Bell state $V|\Phi^+\rangle\langle\Phi^+| + (1-V)I/4$, potentially entangled with Eve. Alice is assumed to trust her measurement apparatus, which consists of two bases $A_0 = \sigma_Z$ and $A_1 = \sigma_X$, with A_0 used for key generation. Bob's device is untrusted and is modeled

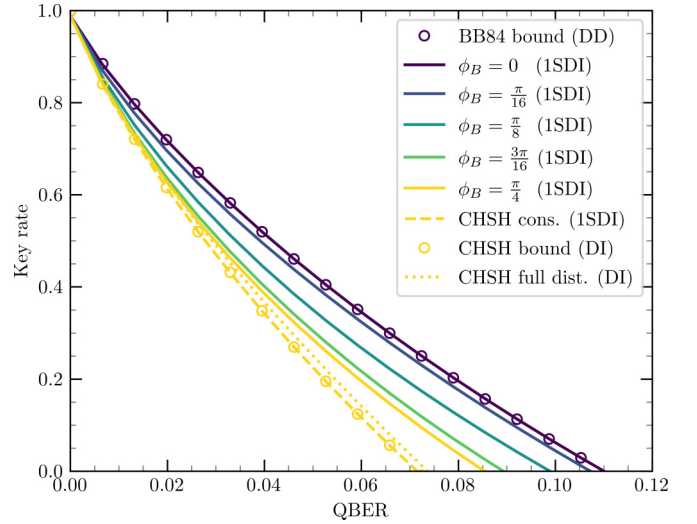


FIG. 4. Key rate as a function of the QBER under different measurement settings ϕ_B in the 1SDI scenario. The solid colored lines represent 1SDI key rates for $\phi_B = 0, \pi/16, \pi/8, 3\pi/16$, and $\pi/4$, respectively. The BB84 bound in the DD scenario [Eq. (10)] (purple circles), the DI bound derived from the CHSH violation [Eq. (15)] (yellow circles), and the numerical DI key rate obtained from the full probability distribution (yellow dotted line) are also plotted for comparison. We also evaluate the 1SDI key rate at $\phi_B = \pi/4$ using only the CHSH value as a constraint (yellow dashed line). The gradual decrease of the key rate with increasing ϕ_B illustrates the transition from the DD to the DI regime.

as performing orthogonal measurements in the x - z plane of the Bloch sphere, parametrized as $B_0 = \cos \phi_B \sigma_Z + \sin \phi_B \sigma_X$ and $B_1 = -\sin \phi_B \sigma_Z + \cos \phi_B \sigma_X$. When $\phi_B = 0$, the protocol reduces to the entanglement-based BB84 protocol [1]. To enable key generation when $\phi_B \neq 0$, we supplement Bob with an additional basis $B_2 = \sigma_Z$. In the special case $\phi_B = \pi/4$, the protocol shares the same implementation with the original DI-QKD protocol [13]. Alice and Bob may characterize the correlations either through the full probability distribution of all non-key-generation rounds or via the violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality $S_C = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$, where $\langle A_x B_y \rangle = \sum_{a,b} p(a=b|x,y) - p(a \neq b|x,y)$. The well-known DI lower bound on the conditional entropy in terms of the CHSH value is given by [13]

$$H(\hat{A}_{x^*}|E) \geq 1 - h\left(\frac{1 + \sqrt{S_C^2/4 - 1}}{2}\right). \quad (15)$$

We evaluate the performance of the 1SDI protocols for different values of ϕ_B by computing the conditional von Neumann entropy $H(\hat{A}_0|E)$, using the full probability distribution as constraints in Eq. (7). The numerical results are shown as solid curves in Fig. 4. For comparison, we also plot the analytical DI-QKD key rate based on Eq. (15), as well as the numerical DI key rate obtained via the Navascués-Pironio-Acín (NPA) hierarchy [77] exploiting the full probability distribution. For completeness, we also compute the 1SDI key rate at $\phi_B = \pi/4$ using the CHSH value

S_C as the only constraint and find exact agreement with the analytical DI key rate [Eq. (15)] up to six decimal accuracy. It is worth noting that in Ref. [78], a tight lower bound on the conditional min-entropy in terms of the CHSH violation was shown to remain valid in a prepare-and-measure scenario under only the qubit assumption. Despite the different entropy measures and assumptions involved, the present result and Ref. [78] exhibit the same qualitative feature: The entropy bound obtained under a more restricted set of assumptions coincides with that derived in a less constrained scenario.

In addition, it is well known that exploiting the full probability distribution can enhance key rates in DI-QKD [15,20,79], while our numerical results show that this advantage carries over to 1SDI-QKD. Notably, for $\phi_B = \pi/4$, the 1SDI key rates obtained from the full distribution are consistently higher than their DI counterparts, with the improvement becoming more pronounced at higher noise levels. To further illustrate this, we compute the numerical 1SDI key rate using data from a DI-QKD experiment [16]. The asymptotic key rate obtained from Eq. (15) is 0.5861, while the numerical DI key rate [81] derived from the full probability distribution is 0.6028. In comparison, the numerical 1SDI key rate [82] obtained using the steering hierarchy reaches 0.6370. These results showcase that partial device characterization can yield a clear improvement in the achievable key rate given Bell-type correlations, with the enhancement becoming more pronounced as noise increases.

2. Tripartite key agreement

Next, we dive into quantum cryptography protocols with partial device independence among three communicating parties. In these protocols, an untrusted tripartite entangled state is distributed to Alice, Bob¹, and Bob², who perform local measurements on their subsystems and apply one-way error correction to the outputs to generate a conference key. We again evaluate the conditional von Neumann entropy $H(\hat{A}_2|E)$ using our numerical method, with the key distinction that it is now calculated from tripartite correlations.

We start by presenting numerical bounds on the conditional entropy when the parties test the genuine tripartite steering inequalities derived in Ref. [37]. In the 2SDI scenario, where only Alice's devices are trusted, suppose that each party has three measurement settings with binary outcomes. To detect genuine tripartite entanglement, the parties can evaluate the following 2SDI steering inequality:

$$\begin{aligned} S_{2SDI} = & -1 + 0.1831(\langle \sigma_Z^A B_2^1 \rangle + \langle \sigma_Z^A B_2^2 \rangle + \langle B_2^1 B_2^2 \rangle) \\ & + 0.2582(\langle \sigma_X^A B_0^1 B_0^2 \rangle - \langle \sigma_Y^A B_0^1 B_1^2 \rangle) \\ & - \langle \sigma_Y^A B_1^1 B_0^2 \rangle - \langle \sigma_X^A B_1^1 B_1^2 \rangle \leq 0, \end{aligned} \quad (16)$$

where σ_Z^A represents Alice's Pauli σ_Z measurement, $\{B_0^1, B_1^1, B_2^1\}$ are the observables of Bob¹, and so on. A violation of this inequality certifies the presence of genuine tripartite entanglement among the three parties. The Greenberger-Horne-Zeilinger (GHZ) state $(|000\rangle + |111\rangle)/\sqrt{2}$ achieves the maximal violation of 0.5820 when all three observables for both Bob¹ and Bob² are also chosen as σ_X , σ_Y , σ_Z , correspondingly. The measurement outcomes obtained when all three parties choose their third

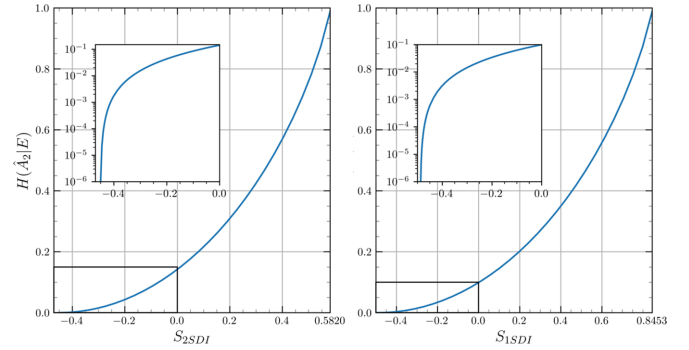


FIG. 5. Lower bounds on the conditional von Neumann entropy $H(\hat{A}_2|E)$ in terms of the 2SDI genuine tripartite steering inequality violation S_{2SDI} (left) and the 1SDI inequality violation S_{1SDI} (right). Calculations are performed with eight-point Gauss-Radau quadrature. The 2SDI curve is obtained at relaxation level 1 + $B^1 B^2 Z$, with each SDP solved in approximately 1 s. The 1SDI curve corresponds to relaxation level 1, with each SDP requiring less than 1 s to solve. In the insets, we show close-up views of the regions where the inequalities are not violated.

measurement setting, i.e., when all parties perform the σ_Z measurement, can be used to generate a conference key.

Besides, in the 1SDI scenario, where both Alice and Bob¹ are trusted, the parties can test a similar inequality under an analogous measurement configuration:

$$\begin{aligned} S_{1SDI} = & -1 - 0.1547\langle \sigma_Z^A \sigma_Z^{B^1} \rangle + \frac{1}{3}(\langle \sigma_Z^{B^1} B_2^2 \rangle + \langle \sigma_Z^A B_2^2 \rangle \\ & + \langle \sigma_X^A \sigma_X^{B^1} B_0^2 \rangle - \langle \sigma_X^A \sigma_Y^{B^1} B_1^2 \rangle \\ & - \langle \sigma_Y^A \sigma_Y^{B^1} B_0^2 \rangle - \langle \sigma_Y^A \sigma_X^{B^1} B_1^2 \rangle) \leq 0. \end{aligned} \quad (17)$$

The GHZ state maximally violates this inequality by 0.8453 when the three observables of Bob² are taken as σ_X , σ_Y , σ_Z , respectively. The correlation terms that appear in both Eqs. (16) and (17) are the stabilizers of the tripartite GHZ state. Their coefficients arise from the dual problems of the SDPs used to test whether the observed assemblages in partially DI scenarios admit a biseparable model [37].

The resulting numerical bounds on the conditional entropy $H(\hat{A}_2|E)$ as functions of the inequality violations are shown in Fig. 5. Interestingly, a nonzero conditional entropy can be obtained without violating the genuine steering inequalities above, indicating that genuine tripartite entanglement is not a prerequisite for certifying privacy. Similar observations have been made in the fully device-independent setting [45,62], and our results demonstrate that this behavior likewise manifests in steering regimes. What is more, the fidelity thresholds at which the conditional entropies become positive closely coincide with the GHZ entanglement detection thresholds, rather than the GME detection thresholds, associated with these steering inequalities. For the 2SDI inequality, the obtained fidelity threshold matches the known value $3/7$, whereas in the 1SDI case we observe a slightly higher threshold (≈ 0.368) than the value 0.25 reported in Ref. [37]. This is expected given that the inequality used here is tailored to witness GME and the corresponding inequality for entanglement detection would take a different form.

We then consider the usage of tripartite Bell inequalities while enforcing extra assumptions on partial device characterization. For conciseness and practical relevance, we present numerical rates of the cryptographic protocols when the parties share a three-qubit GHZ state and test the Holz-Kampermann-Bruß (HKB) inequality [83], the parity CHSH inequality [76], the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [84], and the genuine tripartite steering inequalities Eqs. (16) and (17) introduced above. Note that the MABK inequality is regarded as unsuitable for conference key agreement, since Alice's measurement settings that yield large violation are not aligned with the key generation measurement [75,76,85]. Nonetheless, it remains useful for random number generation tasks. More details on these Bell inequalities and the dependence of conditional entropies on their violations are presented in Appendix B, which also provides analytical conjectured expressions for some numerical results.

In our simulation, the noise is modeled either as local depolarization, $\mathcal{E}_l(\rho) = p\rho + (1-p)I_2/2$, applied identically to each single qubit, or as global depolarization, $\mathcal{E}_g(|\text{GHZ}\rangle\langle\text{GHZ}|) = p|\text{GHZ}\rangle\langle\text{GHZ}| + (1-p)I_8/8$. For comparison, we also evaluate the protocol rates based on the CHSH inequality [86], considering in this case a locally or globally depolarized Bell state $\mathcal{E}_g(|\Phi^+\rangle\langle\Phi^+|) = p|\Phi^+\rangle\langle\Phi^+| + (1-p)I_4/4$. The bit error rate between each pair of parties for the GHZ or Bell states is given by $e_b = (1-p^2)/2$ under local depolarization, and by $e_b = (1-p)/2$ under global depolarization.

The asymptotic conference key rates [see Eq. (3)] as functions of the depolarization parameter p are shown in Fig. 6. For comparison, we also include the concatenated conference key rates of the CHSH-based protocol, implemented as two sequential 1SDI-QKD sessions between Alice and the untrusted Bob¹, and then between Alice and the untrusted Bob². The overall conference key rate hence acquires a factor of 1/2. The conference key rates reach their maximum in the limit of maximal inequality violations in all cases. From the plots, we observe that the genuine tripartite steering inequalities yield the highest conference key rate, as expected from the tomographically complete measurements performed by each party. Interestingly, the asymmetry of the parity CHSH inequality leads to a higher 1SDI conference key rate when Bob² with a single input is untrusted, compared to the case where Bob¹ with two inputs is untrusted. We note that the latter case agrees with the DI conference key rate employing the parity CHSH inequality up to numerical precision, and the same holds for the 2SDI case [see Fig. 9(a) in Appendix B 2].

3. Tripartite randomness expansion

In addition to QCKA, we also explore the applicability of partially DI-RE protocols involving three communicating parties. Each round of such protocols commences with the parties using an initial random seed to determine their inputs, followed by corresponding local measurements on a shared tripartite state. Randomness is then extracted from the outputs of one or more parties associated with a certain input, for instance, from a single party's output $\hat{A}_{x^*}$ or from a joint output

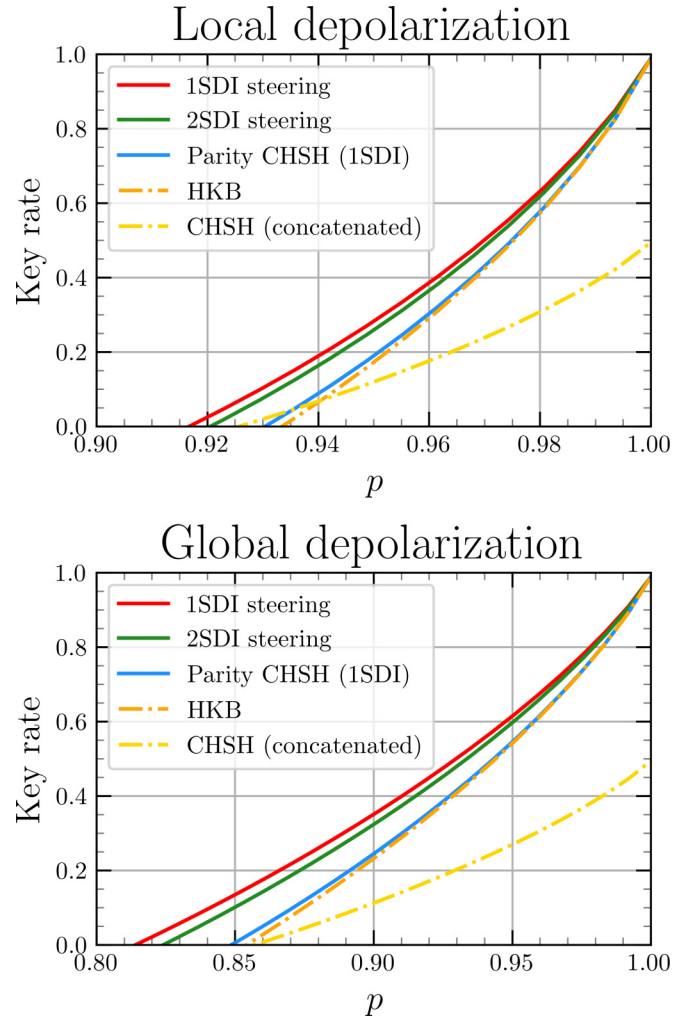


FIG. 6. Asymptotic conference key rates vs the depolarization parameter p for tripartite partially DI-QCKA protocols based on the two genuine steering inequalities, the parity CHSH inequality, the HKB inequality, and concatenated bipartite 1SDI-QKD protocols based on the CHSH inequality. Rates identical to the corresponding DI cases are indicated by dash-dotted lines.

$\hat{A}_{x^*}\hat{B}_{y^*}^1$. The amount of certified randomness is quantified by the conditional von Neumann entropy of these outcomes in the presence of Eve and is lower bounded as in Eqs. (6) and (8). The observed value of a steering or Bell inequality enters the corresponding SDP as a constraint.

Specifically, when Alice extracts randomness from her output $\hat{A}_{x^*}$ in response to the input x^* , the asymptotic one-outcome randomness expansion rate after subtracting the input randomness is given by [62]

$$R_{\text{out}} \geq H(\hat{A}_{x^*}|E) - c\gamma - h(\gamma), \quad (18)$$

where γ denotes the probability of selecting a test round and c is the number of random input bits for the corresponding inequality test. For instance, $c = 3 \log_2 3$ for the two genuine steering inequalities, since each party inputs a random trit to select three measurement settings. One can further consider a scenario where all parties are colocated and aim to quantify the global randomness of their joint measurement outcomes.

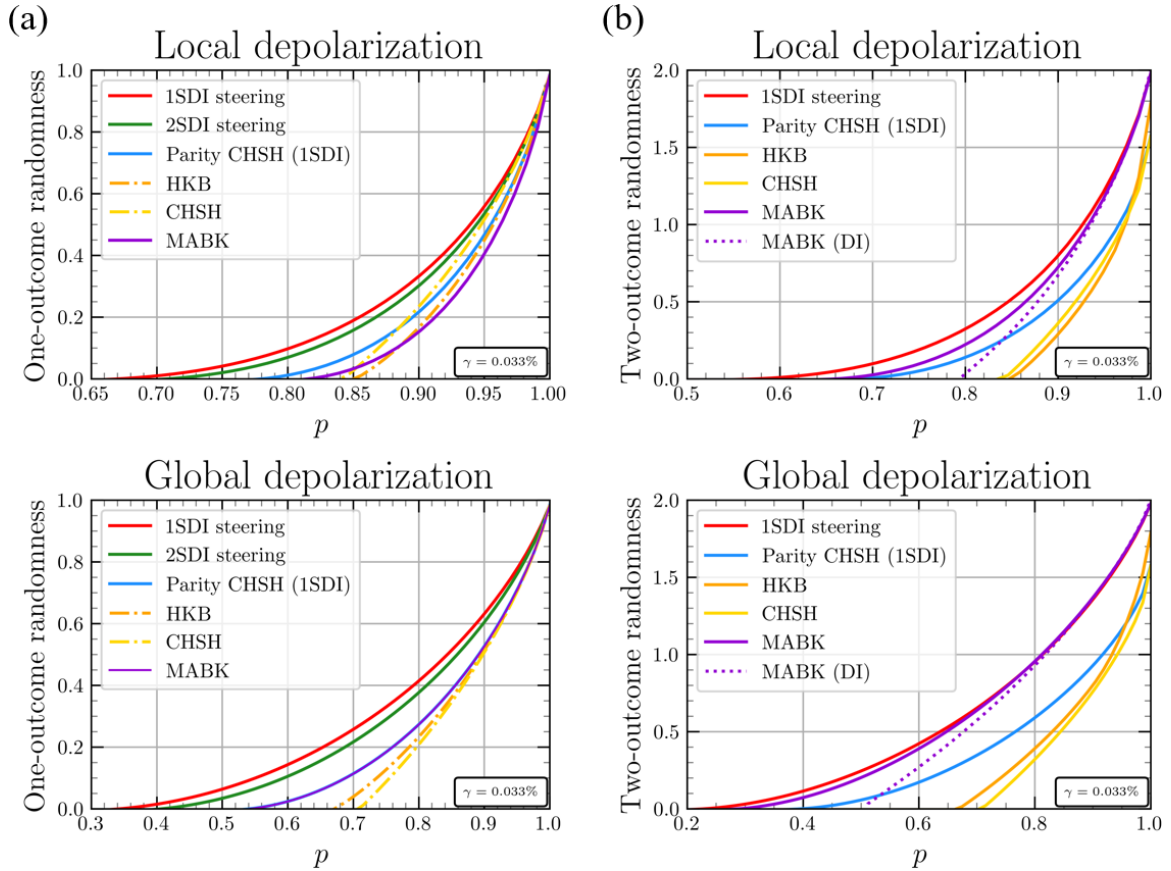


FIG. 7. Asymptotic performances of different partially DI-RE protocols vs the depolarization parameter p . (a) One-outcome randomness expansion rates for protocols based on the two genuine steering inequalities, the parity CHSH inequality, the HKB inequality, the CHSH inequality, and the MABK inequality. Under global depolarization, rates from the parity CHSH and MABK inequalities differ only by a fixed offset of $\gamma = 0.033\%$. (b) Two-outcome randomness expansion rates for 1SDI protocols. Assuming one Bob's device is untrusted, the randomness is extracted from Alice and another trusted Bob's joint outcomes. The analytical result for the MABK inequality in the fully DI regime is also shown. Here, $\gamma = 0.033\%$ is the probability of selecting a test round. Rates identical to their corresponding DI cases are indicated by dash-dotted lines.

Similarly, when Alice and Bob¹ extract randomness from their joint outputs, the spot-checking two-outcome randomness expansion rate is given by

$$R_{2\text{out}} \geq H(\hat{A}_x^* \hat{B}_{y_1}^1 | E) - c\gamma - h(\gamma). \quad (19)$$

In what follows, we set $\gamma = 0.033\%$, in accordance with a recent DI-RE experimental implementation [87].

Within the same depolarization model, Fig. 7(a) benchmarks the one-outcome randomness expansion rates of partially DI-RE protocols based on different inequalities, while Fig. 7(b) presents the 1SDI randomness rates extracted from Alice and another trusted Bob's joint outcomes. The rates associated with the parity CHSH inequality are computed by treating the single-input Bob² as the only untrusted party. As before, we observe that the genuine steering inequalities yield the highest rates and the strongest robustness. For the MABK inequality, the resulting rates are considerably higher than those in the fully DI case, revealing that GME is not a prerequisite in partially DI-RE protocols based on this inequality. More details are provided in Appendix B 1.

Moreover, under global depolarization, the one-outcome randomness expansion rates from the parity CHSH and MABK inequalities differ only by a fixed offset of $\gamma = 0.033\%$, due to the extra random input bit in the MABK testing. After removing this offset, the two rate curves agree pointwise up to 10^{-6} . Another point worth mentioning is that, unlike in the fully DI-RE protocols [62], the rates associated with the parity CHSH inequality are generally higher than those obtained using the HKB inequality. This arises from treating Bob with a single input in the parity CHSH scenario as the sole untrusted party (see Appendix B 2 for further discussions). These results highlight the potential advantage of partially DI cryptographic protocols in terms of performance when compared with their fully DI counterparts.

V. CONCLUSION

In this work, we investigated an asymmetric cryptographic scenario where only a subset of the communicating parties' devices are trusted, while the others remain untrusted. This hybrid setting underscores the interplay between experimental amenability and security requirements, yielding a framework

of practical relevance in asymmetric quantum networks. Combined with the best available numerical technique [44], we adopted a computationally efficient semidefinite relaxation hierarchy to numerically benchmark the performance of partially DI quantum cryptography schemes across bipartite, multipartite, and high-dimensional regimes. Our results reveal that relaxing partial trust in device-dependent protocols leaves the overall performance unchanged, whereas introducing partial trust into DI protocols can, in certain cases, largely enhance the achievable privacy. These findings provide insights into the trade-off between device trustworthiness and cryptographic security, paving the way for scalable implementations in such asymmetric quantum architectures.

Future research is expected to analyze partially device-independent quantum cryptographic protocols in more practical settings. This includes accounting for detector imperfections by incorporating data-processing approaches [18,20] and for finite-size effects through generalizations of the entropy accumulation theorem [56–58]. Analytical proofs supporting the numerical observations presented here would also be highly desirable, for instance, by adapting techniques developed in Refs. [62,85]. Moreover, it would be interesting to either explore the ultimate performance limits of partially DI schemes, or unify DI, partially DI, and device-dependent frameworks into a hierarchically rigorous structure.

ACKNOWLEDGMENTS

This work has been supported by the National Natural Science Foundation of China (Grants No. 62375252, No. 11874346, and No. 12174375), the National Key R&D Program of China (Grant No. 2019YFA0308700), the Anhui Initiative in Quantum Information Technologies (Grant No. AHY060200), the Quantum Science and Technology-National Science and Technology Major Project (Grants No. 2021ZD0301100, No. 2021ZD0301400, and No. 2024ZD0302200), and the Zhejiang Provincial Natural Science Foundation of China (Grant No. LQ24A050005).

DATA AVAILABILITY

The data that support the findings of this article are openly available [88].

APPENDIX A: PROOF OF Γ BEING POSITIVE SEMIDEFINITE

In this Appendix, we prove that the block matrix defined in Eq. (9),

$$\Gamma = \sum_{i,j} |i\rangle\langle j|_R \otimes \text{Tr}_{BE}[\rho_{ABE}(I_A \otimes E_j^\dagger E_i)],$$

is positive semidefinite. Here, Γ acts on the ancillary register R and the system of the trusted party A , where $\dim R = |S|$. Let an arbitrary vector $|v\rangle = \sum_{i,n} v_{in} |i\rangle_R |n\rangle_A$ be given, where $\{|n\rangle_A\}_{n=1}^{\dim A}$ is an orthonormal basis of system A . Then,

$$\begin{aligned} \langle v|\Gamma|v\rangle &= \sum_{i,j,m,n} v_{in}^* v_{jm} \langle n|_A \text{Tr}_{BE}[\rho_{ABE}(I_A \otimes E_j^\dagger E_i)] |m\rangle_A \\ &= \sum_{m,n} \langle n|_A \text{Tr}_{BE} \left[\rho_{ABE} \left(I_A \otimes \left(\sum_j v_{jm}^* E_j \right) \right)^\dagger \right] \end{aligned}$$

$$\begin{aligned} &\left(\sum_i v_{in}^* E_i \right) \Big) |m\rangle_A \\ &= \sum_{m,n} \langle n|_A \text{Tr}_{BE}[\rho_{ABE}(I_A \otimes T_m^\dagger T_n)] |m\rangle_A, \end{aligned}$$

where we have defined

$$T_n := \sum_i v_{in}^* E_i, \quad \text{for } n = 1, \dots, \dim A.$$

Using the identity $\text{Tr}_{BE}[X_{ABE}]Y_A = \text{Tr}_{BE}[X_{ABE}(Y_A \otimes I_{BE})]$, we can rewrite the previous line as a full trace:

$$\begin{aligned} \langle v|\Gamma|v\rangle &= \sum_{m,n} \text{Tr}[\text{Tr}_{BE}[\rho_{ABE}(I_A \otimes T_m^\dagger T_n)] |m\rangle\langle n|_A] \\ &= \sum_{m,n} \text{Tr}[\text{Tr}_{BE}[\rho_{ABE}(I_A \otimes T_m^\dagger T_n)] (|m\rangle\langle n|_A \otimes I_{BE})] \\ &= \sum_{m,n} \text{Tr}[\rho_{ABE}(|m\rangle\langle n|_A \otimes T_m^\dagger T_n)]. \end{aligned}$$

Collecting the sums gives

$$\langle v|\Gamma|v\rangle = \text{Tr} \left[\rho_{ABE} \left(\sum_m |m\rangle_A \otimes T_m^\dagger \right) \left(\sum_n |n\rangle_A \otimes T_n \right)^\dagger \right].$$

Denote $Q := \sum_m |m\rangle_A \otimes T_m^\dagger$, and then the above expression becomes $\text{Tr}[\rho_{ABE} Q Q^\dagger]$. Since $\rho_{ABE} \geq 0$ and $Q Q^\dagger \geq 0$, their product under the trace is nonnegative, thus $\langle v|\Gamma|v\rangle = \text{Tr}[\rho_{ABE} Q Q^\dagger] \geq 0$. Because this holds for arbitrary $|v\rangle$, we conclude Γ is positive semidefinite, and is hence Hermitian. The extension to other partially DI scenarios follows in a straightforward manner.

APPENDIX B: BELL INEQUALITIES AND THEIR CONDITIONAL ENTROPIES

In this Appendix, we summarize the Bell inequalities examined in this work—including MABK, parity CHSH, HKB, and CHSH inequalities—and the corresponding one-outcome and two-outcome entropy bounds applied to benchmark DI-QCKA and DI-RE protocols.

1. MABK inequality

The MABK inequality for three parties, Alice, Bob¹, and Bob² reads [84]

$$\begin{aligned} S_M &= \langle A_0 B_0^1 B_1^2 \rangle + \langle A_0 B_1^1 B_0^2 \rangle + \langle A_1 B_0^1 B_0^2 \rangle - \langle A_1 B_1^1 B_1^2 \rangle \\ &\leq 2 \stackrel{\text{GME}}{\leq} 2\sqrt{2} \stackrel{\text{Q}}{\leq} 4. \end{aligned} \quad (\text{B1})$$

If one observes a violation $S_M < 2$, then entanglement is certified in a DI fashion. A stronger violation, $S_M < 2\sqrt{2}$, further certifies GME. The maximum quantum value $S_M^Q = 4$ can be achieved by the three-qubit GHZ state $(|000\rangle + |111\rangle)/\sqrt{2}$ with the following measurement settings:

$$\begin{aligned} A_0 &= B_0^1 = -B_0^2 = \sigma_Y, \\ A_1 &= B_1^1 = -B_1^2 = \sigma_X. \end{aligned} \quad (\text{B2})$$

In the fully DI regime, the one-outcome conditional entropy of Alice's outcome $\hat{A}_0$ in terms of the inequality

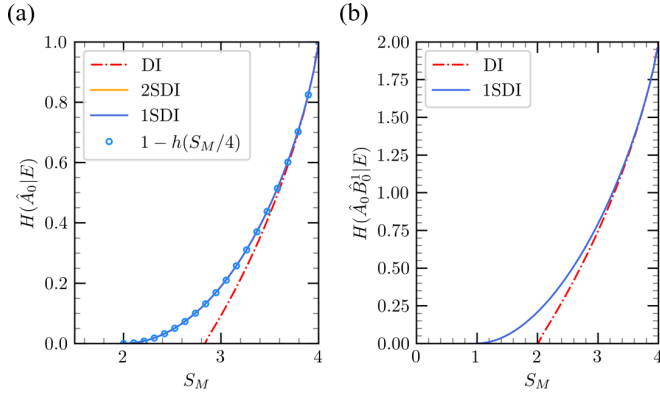


FIG. 8. Lower bounds on the conditional entropies in partially DI scenarios as functions of the MABK inequality violation. (a) Numerical results for the one-outcome entropy $H(\hat{A}_0|E)$ in the 1SDI (blue) and 2SDI (orange) cases. Calculations are performed with eight-point Gauss-Radau quadrature. The 2SDI curve is obtained at relaxation level $1 + B^1 B^2$, while the 1SDI curve corresponds to relaxation level 1. In both cases, each SDP is solved in less than 1 s. The two curves coincide and precisely reproduce the expression $1 - h(S_M/4)$. (b) Numerical results for the two-outcome entropy $H(\hat{A}_0 \hat{B}_0^1|E)$ (blue) with Bob² as the untrusted party. Calculations employ the same number of quadrature nodes and relaxation level 1, with each SDP requiring approximately 3 s to solve. For comparison, the fully DI entropy bounds [Eqs. (B3) and (B4)] are shown in dash-dotted lines. Results associated with other outputs are identical.

violation is tightly bounded by [74]

$$H(\hat{A}_0|E) \geq 1 - h\left(\frac{1 + \sqrt{S_M^2/8 - 1}}{2}\right). \quad (\text{B3})$$

Hence, GME is necessary for nonzero one-outcome conditional entropy in DI MABK scenario. Additionally, the two-outcome conditional entropy admits an analytical lower bound [85]:

$$H(\hat{A}_0 \hat{B}_0^1|E) \geq 2 - H(\{1 - 3f(S_M), f(S_M), f(S_M), f(S_M)\}), \quad (\text{B4})$$

where $H(\cdot)$ is the Shannon entropy of the corresponding probability distribution and $f(S_M) = 1/4 - \sqrt{3(S_M^2 - 4)}/24$.

Nonetheless, the entropy bounds in the partially DI scenario exhibit remarkably distinct features. Here, Alice's measurements are assumed to be precisely $A_0 = \sigma_Y$ and $A_1 = \sigma_X$, which enters the objective functions and constraints of the SDPs [see Eq. (7)]. By applying the numerical method introduced in Sec. III, we obtain numerical lower bounds on the conditional entropies, plotted in Fig. 8. The computed one-outcome entropies $H(\hat{A}_0|E)$ in both the 1SDI and 2SDI scenarios coincide up to six decimals. Crucially, the numerical curves both match a conjectured expression $1 - h(S_M/4)$. In addition, we observe that the two-outcome entropy $H(\hat{A}_0 \hat{B}_0^1|E)$ in the 1SDI scenario becomes positive once $S_M < 1$, whereas in the fully DI case the threshold is $S_M = 2$.

We note that the partially DI one-outcome entropies become already nonzero as soon as $S_M < 2$, whereas the DI

counterpart demands the MABK violation to reach the GME threshold $2\sqrt{2}$. This distinction can be illustrated by a heuristic example. In the fully DI case, consider the shared state $I_2 \otimes |\Phi^+\rangle\langle\Phi^+|$, where Alice is uncorrelated with the Bobs, and take her measurements to be $A_0 = A_1 = I$. In this configuration, the MABK violation can still reach $2\sqrt{2}$ even though Alice's system is separable [85]. One can see that, because Alice's measurements are untrusted in the DI setting, a violation above the GME threshold is necessary to ensure that Alice is indeed entangled with the rest parties. In contrast, in the partially DI scenario Alice's measurements are characterized to be two complementary Pauli observables, which rules out the above strategy. This suggests that the complementarity of Alice's measurements makes any MABK violation sufficient to certify Alice's entanglement with the other parties, removing the requirement of GME to ensure certifiable privacy. A formal proof of this assertion remains to be established and is left for future work.

2. Parity CHSH inequality

We next consider the parity CHSH inequality, where the asymmetry in the parties' inputs leads to a pronounced contrast between the DI and the partially DI entropies. The parity CHSH inequality reads [76]

$$S_{\text{PC}} = \langle A_1 B_-^1 B_0^2 \rangle + \langle A_0 B_+^1 \rangle \leq 1 \leq \frac{Q}{\sqrt{2}}, \quad (\text{B5})$$

where $B_{\pm}^1 = (B_0^1 \pm B_1^1)/2$. The maximum quantum value $S_{\text{PC}}^Q = \sqrt{2}$ can be achieved by the following measurements on the three-qubit GHZ state:

$$\begin{aligned} A_0 &= \sigma_Z, & A_1 &= \sigma_X, \\ B_+^1 &= \sigma_Z/\sqrt{2}, & B_-^1 &= \sigma_X/\sqrt{2}, \\ B_0^2 &= \sigma_X. \end{aligned} \quad (\text{B6})$$

Unlike the MABK inequality, the parity CHSH and the following inequalities enforce that Alice performs a σ_Z measurement at maximal violation. This essential difference enables these inequalities to support conference key generation, whereas the MABK inequality can only facilitate random number generation.

The one-outcome DI entropy in terms of the inequality violation is tightly bounded by [76]

$$H(\hat{A}_0|E) \geq 1 - h\left(\frac{1 + \sqrt{S_{\text{PC}}^2 - 1}}{2}\right). \quad (\text{B7})$$

So far, only a numerical bound on the two-outcome DI entropy is given in Ref. [62].

Note that Bob² has only a single measurement input. When Bob² is treated as the sole untrusted party in the 1SDI scenario, higher conditional entropies can be certified from the inequality violation compared to the fully DI case, as

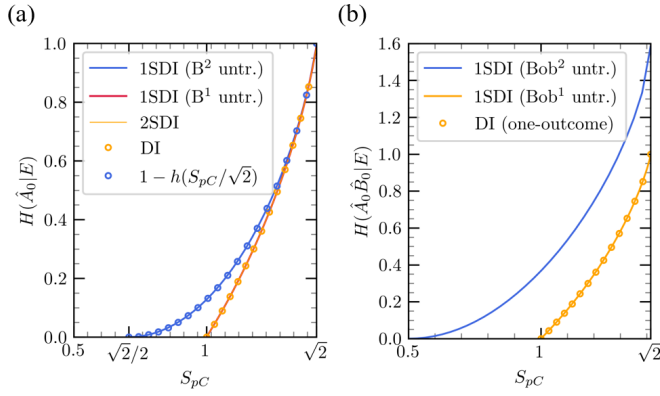


FIG. 9. Lower bounds on the conditional entropies in partially DI scenarios as functions of the parity CHSH inequality violation. (a) Numerical results for the one-outcome entropy $H(\hat{A}_0|E)$ in the 1SDI (either Bob¹ or Bob² is untrusted) and 2SDI cases. Calculations are performed with eight-point Gauss-Radau quadrature. The 2SDI curve is obtained at relaxation level $1 + B^1B^2$, while the 1SDI curves correspond to relaxation level 1. Each SDP is solved in less than 1 s. The 1SDI curve with Bob² untrusted (blue) reproduces the expression $1 - h(S_{PC}/\sqrt{2})$. The 1SDI curve with Bob¹ untrusted (red) and the 2SDI curve (orange) nearly match the DI result [Eq. (B7)], with deviations less than 10^{-6} except for the last few points limited by the finite number of Gauss-Radau nodes. (b) Numerical results for the two-outcome entropy with either Bob¹ or Bob² as the untrusted party. The entropies are evaluated over the joint outcome of two trusted parties. The same number of quadrature nodes and relaxation level 1 are used, with each SDP solved in approximately 2 s. The curve corresponding to Bob¹ untrusted reproduces the DI one-outcome entropy.

illustrated in Fig. 9. Specifically, the one-outcome entropy matches the conjectured expression $1 - h(S_{PC}/\sqrt{2})$ up to 10^{-6} . Moreover, when Bob¹ (with two measurement inputs) is treated as the untrusted party, the resulting 1SDI one-outcome entropies agree with the DI results given in Eq. (B7). The same holds for the 2SDI entropies. As for the two-outcome entropy, nonzero values already appear for $S_{PC} < 1/2$, with the 1SDI and DI two-outcome entropies attaining the same maximum at the maximal inequality violation, confirming the tightness of our results. Interestingly, the 1SDI two-outcome entropy with Bob¹ untrusted reproduces the DI one-outcome entropy in Eq. (B7). This is because, when Bob¹ is the only untrusted party, Alice and Bob² can effectively be regarded as a single composite party. Under this grouping, the parity CHSH inequality reduces to the bipartite CHSH inequality scaled by a factor of $1/2$, and the resulting two-outcome entropy thus recovers Eq. (B7) [or Eq. (15) with S_C replaced by $2S_{PC}$].

3. HKB inequality

The tripartite HKB inequality reads [83]

$$S_H = \langle A_1 B_+^1 B_+^2 \rangle - \langle A_0 B_-^1 \rangle - \langle A_0 B_-^2 \rangle - \langle B_-^1 B_-^2 \rangle \leq 1 \stackrel{\text{GME}}{\leq} \sqrt{2} \stackrel{\text{Q}}{\leq} 3/2. \quad (\text{B8})$$

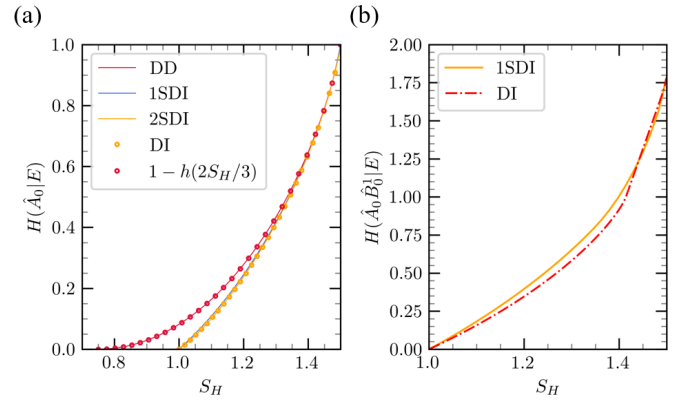


FIG. 10. Lower bounds on the conditional entropies in partially DI scenarios as functions of the HKB inequality violation. (a) Numerical results for the one-outcome entropy $H(\hat{A}_0|E)$ in the 1SDI, 2SDI, and fully DD cases. Calculations are performed with eight-point Gauss-Radau quadrature. The 2SDI curve is obtained at relaxation level $1 + B^1B^2$, while the 1SDI curves correspond to relaxation level 1, and each SDP is solved in less than 1 s. The DD curve is calculated in a similar manner by tracing out only Eve in the block matrices [see Eq. (13)], and is obtained at relaxation level 1 with each SDP solved in about 1 s. We find that the DD entropies precisely reproduce the expression $1 - h(2S_H/3)$. The 2SDI and 1SDI curves deviate slightly from the DI bound in Eq. (B10), with the largest discrepancy being on the order of 10^{-2} . (b) Numerical results for the two-outcome entropy with either Bob¹ or Bob² as the untrusted party. The same number of quadrature nodes and relaxation level 1 are used, with each SDP solved in approximately 3 s. For comparison, the DI two-outcome entropy conjectured in Ref. [62] is also reproduced in the dash-dotted line.

The maximum quantum value $S_H^Q = 3/2$ is attained by the three-qubit GHZ state with the following measurements:

$$A_0 = \sigma_Z, \quad A_1 = \sigma_X, \\ B_+^1 = B_+^2 = \frac{\sqrt{3}}{2}\sigma_X, \quad B_-^1 = B_-^2 = -\frac{1}{2}\sigma_Z. \quad (\text{B9})$$

A tight lower bound on the one-outcome DI entropy was derived in Ref. [62], which also provides a conjecture for the two-outcome counterpart. The one-outcome expression reads

$$H(\hat{A}_0|E) \geq 1 - h\left(\frac{S_H + 1 + \sqrt{S_H^2 + 2S_H - 3}}{4}\right). \quad (\text{B10})$$

Figure 10 shows the numerical lower bounds on the conditional entropies in terms of the HKB inequality violation. We observe that, unlike the other inequalities, the 1SDI and 2SDI one-outcome entropies deviate from the DI bound in Eq. (B10) by up to 10^{-2} , even though the curves share the same starting and ending points. Moreover, the device-dependent entropies exceed those in the 1SDI scenario and match the conjectured expression $1 - h(2S_H/3)$ with six decimal accuracy. This is not entirely unexpected, as imposing more assumptions on the devices should generally lead to higher entropies. Nevertheless, this peculiar behavior observed for the HKB inequality warrants further investigation.

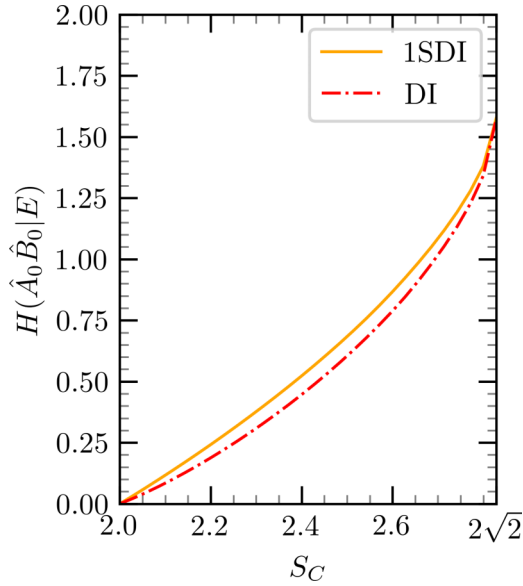


FIG. 11. Lower bounds on the two-outcome conditional entropies in 1SDI and DI scenarios as functions of the CHSH inequality violation. The 1SDI curve is obtained at the relaxation level $1 + BZ + ZZ$, with each SDP taking about 10 s to solve. The DI curve is computed using the NPA hierarchy at level $2 + ABZ$, including all monomials appearing in the objective function. Each SDP in this case requires about 1 min to solve.

4. CHSH inequality

Finally, we review the renowned CHSH inequality for two parties, Alice and Bob, which reads [86]

$$S_C = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2 \leq 2\sqrt{2}. \quad (\text{B11})$$

The maximum quantum value $S_C^Q = 2\sqrt{2}$ is attained by the two-qubit Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ with the following measurements:

$$\begin{aligned} A_0 &= \sigma_Z, & A_1 &= \sigma_X, \\ B_0 &= (\sigma_Z + \sigma_X)/\sqrt{2}, & B_1 &= (\sigma_Z - \sigma_X)/\sqrt{2}. \end{aligned} \quad (\text{B12})$$

The DI bound on the conditional one-outcome entropy is given in Eq. (15), and it agrees with the 1SDI results up to at least six decimal places, as shown in Fig. 4. Furthermore, we computed the 1SDI two-outcome entropy using an eight-point Gauss-Radau quadrature and a relaxation level of $1 + BZ + ZZ$. The resulting values, shown in Fig. 11, are observed to be higher than the numerical DI results.

- [1] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
- [3] 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).
- [4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [5] C. Portmann and R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.* **94**, 025008 (2022).
- [6] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [7] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A* **78**, 042333 (2008).
- [8] 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).
- [9] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors, *New J. Phys.* **13**, 073024 (2011).
- [10] P. Ye, W. Chen, G.-W. Zhang, F.-Y. Lu, F.-X. Wang, G.-Z. Huang, S. Wang, D.-Y. He, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Induced-photorefractive attack against quantum key distribution, *Phys. Rev. Appl.* **19**, 054052 (2023).
- [11] M. Fadeev, A. Ponomova, Q. Peng, A. Huang, R. Shakhovoy, and V. Makarov, Optical-pumping attack on a quantum key distribution laser source, *Opt. Express* **33**, 47001 (2025).
- [12] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [13] 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).
- [14] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.* **11**, 045021 (2009).
- [15] 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).
- [16] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, *et al.*, Experimental quantum key distribution certified by Bell's theorem, *Nature (London)* **607**, 682 (2022).
- [17] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, A device-independent quantum key distribution system for distant users, *Nature (London)* **607**, 687 (2022).
- [18] 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).

- [19] 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, *Nat. Commun.* **12**, 2880 (2021).
- [20] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Device-independent quantum key distribution with random postselection, *Phys. Rev. Lett.* **128**, 110506 (2022).
- [21] Y.-Z. Zhen, Y. Mao, Y.-Z. Zhang, F. Xu, and B. C. Sanders, Device-independent quantum key distribution based on the Mermin-Peres magic square game, *Phys. Rev. Lett.* **131**, 080801 (2023).
- [22] T. Le Roy-Deloison, E. P. Lobo, J. Pauwels, and S. Pironio, Device-independent quantum key distribution based on routed Bell tests, *PRX Quantum* **6**, 020311 (2025).
- [23] B.-W. Lu, C.-W. Yang, R.-Q. Wang, B.-F. Gao, Y.-Z. Zhen, Z.-G. Wang, J.-K. Shi, Z.-Q. Ren, T. A. Hahn, E. Y.-Z. Tan, *et al.*, Device-independent quantum key distribution over 100 km with single atoms, *Science* **391**, 592 (2026).
- [24] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, *Phys. Rev. A* **84**, 010302(R) (2011).
- [25] K. T. Goh, J.-D. Bancal, and V. Scarani, Measurement-device-independent quantification of entanglement for given Hilbert space dimension, *New J. Phys.* **18**, 045022 (2016).
- [26] M. Ioannou, P. Sekatski, A. A. Abbott, D. Rosset, J.-D. Bancal, and N. Brunner, Receiver-device-independent quantum key distribution protocols, *New J. Phys.* **24**, 063006 (2022).
- [27] M. Ioannou, M. A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A. A. Abbott, P. Sekatski, J.-D. Bancal, *et al.*, Receiver-device-independent quantum key distribution, *Quantum* **6**, 718 (2022).
- [28] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [29] 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(R) (2012).
- [30] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, *Rev. Mod. Phys.* **92**, 015001 (2020).
- [31] H. J. Kimble, The quantum internet, *Nature (London)* **453**, 1023 (2008).
- [32] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
- [33] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature (London)* **589**, 214 (2021).
- [34] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, *et al.*, Implementation of a 46-node quantum metropolitan area network, *npj Quantum Inf.* **7**, 134 (2021).
- [35] J.-L. Liu, X.-Y. Luo, Y. Yu, C.-Y. Wang, B. Wang, Y. Hu, J. Li, M.-Y. Zheng, B. Yao, Z. Yan, *et al.*, Creation of memory-memory entanglement in a metropolitan quantum network, *Nature (London)* **629**, 579 (2024).
- [36] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Multipartite Einstein-Podolsky-Rosen steering and genuine tripartite entanglement with optical networks, *Nat. Phys.* **11**, 167 (2015).
- [37] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. S. Ribeiro, and S. P. Walborn, Detection of entanglement in asymmetric quantum networks and multipartite quantum steering, *Nat. Commun.* **6**, 7941 (2015).
- [38] K. Chen and H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, *Quantum Inf. Comput.* **7**, 689 (2007).
- [39] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, *New J. Phys.* **19**, 093012 (2017).
- [40] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network, *Phys. Rev. X* **11**, 041016 (2021).
- [41] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, *Adv. Quantum Technol.* **3**, 2000025 (2020).
- [42] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).
- [43] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
- [44] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, *Quantum* **8**, 1445 (2024).
- [45] L. Wooltorton, P. Brown, and R. Colbeck, Genuine multipartite entanglement is not necessary for standard device-independent conference key agreement, *Phys. Rev. Lett.* **135**, 220803 (2025).
- [46] G. Carrara, H. Kampermann, D. Bruß, and G. Murta, Genuine multipartite entanglement is not a precondition for secure conference key agreement, *Phys. Rev. Res.* **3**, 013264 (2021).
- [47] E. Biham and T. Mor, Security of quantum cryptography against collective attacks, *Phys. Rev. Lett.* **78**, 2256 (1997).
- [48] R. Renner and J. I. Cirac, De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, *Phys. Rev. Lett.* **102**, 110504 (2009).
- [49] C. A. Miller and Y. Shi, Universal security for randomness expansion from the spot-checking protocol, *SIAM J. Comput.* **46**, 1304 (2017).
- [50] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A* **461**, 207 (2005).
- [51] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, *New J. Phys.* **20**, 113014 (2018).
- [52] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
- [53] R. Bhavsar, S. Ragy, and R. Colbeck, Improved device-independent randomness expansion rates using two sided randomness, *New J. Phys.* **25**, 093035 (2023).
- [54] C. Roch i Carceller, J. Pauwels, S. Pironio, and A. Tavakoli, Prepare-and-measure scenarios with photon-number constraints, *Phys. Rev. Lett.* **135**, 140802 (2025).
- [55] B. Ulu, N. Brunner, and M. Weilenmann, Device-independent quantum key activation, *Phys. Rev. Lett.* **135**, 190801 (2025).
- [56] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, *Nat. Commun.* **9**, 459 (2018).
- [57] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, *Commun. Math. Phys.* **379**, 867 (2020).

- [58] T. Metger and R. Renner, Security of quantum key distribution from generalised entropy accumulation, *Nat. Commun.* **14**, 5272 (2023).
- [59] H. Zhou, Numerical framework for semi-device-independent quantum random-number generators, *Phys. Rev. A* **107**, 052402 (2023).
- [60] M. F. Pusey, Negativity and steering: A stronger Peres conjecture, *Phys. Rev. A* **88**, 032313 (2013).
- [61] N. D'Alessandro, C. Roch i Carceller, and A. Tavakoli, Semidefinite relaxations for high-dimensional entanglement in the steering scenario, *Phys. Rev. Lett.* **134**, 090802 (2025).
- [62] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß, Boosting device-independent cryptography with tripartite nonlocality, *Quantum* **7**, 980 (2023).
- [63] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [64] D. Bruß, Optimal eavesdropping in quantum cryptography with six states, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [65] P. Wittek, Algorithm 950: Ncpol2sdpa-sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables, *ACM Trans. Math. Softw.* **41**, 1 (2015).
- [66] G. Sagnol and M. Stahlberg, PICOS: A Python interface to conic optimization solvers, *J. Open Source Softw.* **7**, 3915 (2022).
- [67] The MOSEK optimization suite 11.0.29, 2025, <https://docs.mosek.com/latest/pythonapi/index.html>.
- [68] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, Computing secure key rates for quantum cryptography with untrusted devices, *npj Quantum Inf.* **7**, 158 (2021).
- [69] E. Woodhead, Semi device independence of the BB84 protocol, *New J. Phys.* **18**, 055010 (2016).
- [70] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d -level systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [71] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, *Phys. Rev. A* **82**, 030301(R) (2010).
- [72] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, *Sci. Adv.* **3**, e1701491 (2017).
- [73] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, Quantum key distribution overcoming extreme noise: Simultaneous subspace coding using high-dimensional entanglement, *Phys. Rev. Appl.* **15**, 034003 (2021).
- [74] J. Ribeiro, G. Murta, and S. Wehner, Fully device-independent conference key agreement, *Phys. Rev. A* **97**, 022307 (2018).
- [75] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Comment on “Fully device-independent conference key agreement”, *Phys. Rev. A* **100**, 026301 (2019).
- [76] J. Ribeiro, G. Murta, and S. Wehner, Reply to “comment on ‘Fully device-independent conference key agreement’”, *Phys. Rev. A* **100**, 026302 (2019).
- [77] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [78] E. Woodhead and S. Pironio, Secrecy in prepare-and-measure Clauser-Horne-Shimony-Holt tests with a qubit bound, *Phys. Rev. Lett.* **115**, 150501 (2015).
- [79] O. Nieto-Silleras, S. Pironio, and J. Silman, Using complete measurement statistics for optimal device-independent randomness evaluation, *New J. Phys.* **16**, 013035 (2014).
- [80] P.-S. Lin, D. Rosset, Y. Zhang, J.-D. Bancal, and Y.-C. Liang, Device-independent point estimation from finite data and its application to device-independent property estimation, *Phys. Rev. A* **97**, 032309 (2018).
- [81] In order to facilitate the key rate calculation, the experimental probability distributions are projected onto the closest ones satisfying the no-signaling constraints [80]. The DI key rate is calculated using the BFF method and the NPA hierarchy at a level $2 + ABZ + AZZ$, with $m = 12$.
- [82] The key rate is calculated at a level $1 + BZ$, with $m = 12$ also.
- [83] T. Holz, H. Kampermann, and D. Bruß, Genuine multipartite Bell inequality for device-independent conference key agreement, *Phys. Rev. Res.* **2**, 023251 (2020).
- [84] N. D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [85] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß, Entropy bounds for multiparty device-independent cryptography, *PRX Quantum* **2**, 010308 (2021).
- [86] 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 (1969).
- [87] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, *et al.*, Device-independent randomness expansion against quantum side information, *Nat. Phys.* **17**, 448 (2021).
- [88] J.-H. Wei, Partially-device-independent-quantum-cryptography-in-asymmetric-networks, GitHub repository, 2025, <https://github.com/JunHao-Wei/Partially-device-independent-quantum-cryptography-in-asymmetric-networks>.