Upper Bounds on Device-Independent Quantum Key Distribution Rates in Static and Dynamic Scenarios

Eneet Kaur,[1,*] Karol Horodecki,[2,3,†] and Siddhartha Das[4,5,‡]

[1] *Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

[2] *Institute of Informatics, National Quantum Information Centre in Gdańsk, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*

[3] *International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, Gdansk 80-308, Poland*

[4] *Centre for Quantum Information & Communication (QuIC), École polytechnique de Bruxelles, Université libre de Bruxelles, Brussels B-1050, Belgium*

[5] *Center for Security, Theory and Algorithmic Research (CSTAR), Centre for Quantum Science and Technology (CQST), International Institute of Information Technology, Hyderabad, Gachibowli, Telangana 500032, India*

(Received 7 October 2021; revised 23 March 2022; accepted 24 June 2022; published 10 November 2022)

In this work, we develop upper bounds on key rates for device-independent quantum key distribution (DI-QKD) protocols and devices. We study the reduced cc-squashed entanglement and show that it is a convex functional. As a result, we show that the convex hull of the currently known bounds is a tighter upper bound on the device-independent key rates of the standard Clauser-Horne-Shimony-Holt (CHSH)-based protocol. We further provide tighter bounds for DI-QKD key rates achievable by any protocol applied to the CHSH-based device. This bound is based on reduced relative entropy of entanglement optimized over decompositions into local and nonlocal parts. In the dynamical scenario of quantum channels, we obtain upper bounds for device-independent private capacity for the CHSH-based protocols. We show that the device-independent private capacity for the CHSH-based protocols on depolarizing and erasure channels is limited by the secret key capacity of dephasing channels.

DOI: 10.1103/PhysRevApplied.18.054033

I. INTRODUCTION

Quantum key distribution is a way of establishing the key—a secure, uniformly random bitstring between distant honest parties, that can be used for one-time pad encryption. The history of development of the quantum key distribution can be divided in two stages. Security of the first protocols such as BB84 [1] were based on the trust towards the manufacturer. The devices were assumed to be working according to their specification. The eavesdropper was assumed only to interfere with the channel connecting the honest parties. In the second stage, taking its origins in Ekert's paper [2] this assumption was dropped leading to the *device-independent* quantum cryptography. In the latter approach security of a device is not based on the assumptions about its inner workings, but only on the statistics of its inputs and outputs [3–6]. The adversary in this scenario is assumed to obey the laws of quantum mechanics. This approach has dramatically increased the security level of the quantum key distribution, which is known to be vulnerable to imperfections of the implementation [7]. Indeed, device-independent cryptography can lead to establishing the secure key even if the adversary has manufactured the device herself in any malicious way.

As in Ekert's work [2], quantum device-independent key distribution is based on testing the statistics via the so-called Bell inequalities [8]. In the generic quantum device-independent (QDI) protocol, the honest parties randomly choose to generate the raw key bit or to test the inputs and outputs. If the tested statistics imply high violation of some Bell inequality, they could not have had predefined values before they were generated. It was however hard to put this idea into practice, due to notorious problems with its implementation that should close the so-called *loopholes* evading the security scenario. One of such loopholes was the so-called detection-efficiency loophole: low-efficiency detectors, which disallow for the mentioned argument of the nonpreexistence of statistics [9,10]. The other, to mention just two of several, was assuring a proper distance between the honest parties, so that their inputs and outputs do not influence each other during measurement (so-called no-signaling loophole) [11]. Fortunately, these fundamental problems have been overcome

*e2kaur@uwaterloo.ca
†karol.horodecki@ug.edu.pl
‡das.seed@iiit.ac.in

in the sequence of the so-called loophole-free Bell test experiments [12–14].

The (QDI) approach got advanced meanwhile both in theory [15–17] and experiment [18,19]. Recently it was shown that some of the latter so-called loophole-free experiments had small but nonzero key rate [20]. This fact was then confirmed in three different proof-of-principle experiments achieving nonzero key rates [21–23]. The obtained key rates are considerably smaller than in the device-dependent case, which corresponds to early theoretical results [5]. There it has opened the problem of achievable key rates in a QDI setting. After the mentioned results of Refs. [15–17], the problem of achievable key rates has recently drawn much attention [24–26], where advanced techniques to lower bound the device-independent key rate achievable by one-way classical communication has been proposed. Considerable focus is given to the possibility of obtaining a nonzero key rate for devices driven from the experiment with detectors having low detection efficiency. In order to close the gap between theory and experiment, recent proposals go beyond the standard scenario with the setting $(2, 3, 2, 2)$ of two inputs (one binary and one trinary) and two binary outputs [20, 24,27], including drawing the key from more than two outputs [20].

In parallel, the initial—call it *device-dependent approach*—was getting maturity. On the practical side, the point-to-point or relay-based QKD were achieved commercially and experimentally (see Ref. [28,29] and references therein). From a theoretical perspective, the limitations in the form of upper bounds on the key rate were developed in various device-dependent scenarios [30–36] (see Ref. [37] for an overview).

Until recently, no analog of the upper bounds in the quantum device-independent scenario has been found. Therefore, as a complementary approach to the described lower bounds on the QDI key, in this paper we focus on the upper bounds to device-independent quantum key distribution rates. A result in this direction has been given in Ref. [5], in the case of the nonsignaling adversary, that is the one which is constrained only by the no faster than light communication principle. Now, a number of recent papers are tackling this problem [38–43] most of which concerns, as we do, the quantum adversary [44]. By quantum adversary we mean the one whose state of memory and operations can be described within the theory of quantum mechanics. In this paper, we not only find tighter limitations on the performance of device-independent quantum key distribution, but also provide a unified view on the previous bounds exhibiting hidden connections. Although our bounds are quite generic, applicable to various scenarios, we illustrate them with an example of the $(2, 3, 2, 2)$ scenario.

After a seminal result of Ref. [38] for the quantum adversary, three approaches were taken: (i) that of Ref. [40] where the bound is proposed via reduced entanglement measures, (ii) that of Ref. [41] where the intrinsic information is proposed as an upper bound via Ref. [45] (iii) that of Ref. [42] where classical attack is proposed via the so-called intrinsic information. In Ref. [42], a strong result was provided. We refer to the bound obtained in Ref. [42], as the FBJLKA bound and the bound obtained in Ref. [41] as the AFL bound. Namely, certain quantum states exhibiting nonlocality, have a *zero* QDI key under standard protocols. The key rate considered there is obtained by protocols based on projective measurements and announcing publicly the inputs. It is easy to observe a direct analogy between this result and a previously obtained upper bound in a case when Eve is limited only by no-signaling communication [39]. There the key achieved by a single measurement done in parallel is shown to be zero for certain quantum nonlocal devices (for any Bell inequality that can be used for testing). Noticing this connection will be crucial to our methods in going beyond the FBJŁKA bound. Indeed, one of our main results state that a convex hull of two known bounds is also an upper bound on the QDI key. This result originates from the technique called convexification introduced in Ref. [39].

The most common DI-QKD protocols use only a single measurement for key generation. In particular, its honest implementation is based on distributing the two-qubit Werner states (mixtures of a maximally entangled state with the maximally mixed state). The testing against the eavesdropper is based on the CHSH inequality [46]. The approaches of Refs. [41,42] provide different upper bounds for such a protocol. The AFL bound works in regime when the Werner state is close to the maximally entangled state, while the second works very well in the opposite regime—when it is close to the maximally mixed state. This is because the first attack is quantum (by a mixture of Bell states and tuned measurements) while the second exploits errors, and works when such errors in the Werner state occurs. It was therefore not clear how to achieve a single bound, which works in both regimes. In this work, we show that the two bounds are instances of the optimization of a single convex quantity. This allows us to obtain a bound that performs better than the above-introduced bounds.

II. MAIN RESULTS

In this section, we outline the three main results of this paper. For technical details, we refer to the appropriate sections. Formally a quantum device is given by its quantum representation $\mathrm{Tr}[M_a^x \otimes M_b^y \rho]$ where $\{M_a^x\}_a$ and $\{M_b^y\}_b$ are positive operator-valued measures (POVMs) for each input to the device (x, y), and ρ is a bipartite state. We denote such a device as $(\rho, \mathcal{M})$ where $\mathcal{M} = \{M_a^x \otimes M_b^y\}_{a,b}^{x,y}$. The measurements and the states are assumed to be controlled by an eavesdropper.

A QKD protocol consists of several rounds of accessing the device $(\rho, \mathcal{M})$ and obtaining the raw data in the form of the measurement inputs and outputs of the device. This data is then postprocessed to obtain the final key. The final key is such that Eve has vanishing small knowledge about the key. The postprocessing consists of local operations and classical communication between Alice and Bob. The key rate of a protocol is given by the final length of the key divided by the total number of rounds n. In this work, we consider independent and identical devices (IID). This implies that during each of the rounds of the protocols, the underlying device is given by $(\rho, \mathcal{M})$.

A device-independent QKD protocol involves learning about the device to prove the security of the generated key. We can divide the protocols based on the information the protocol learns about the device. In the first protocol, we consider the honest parties learn only about certain parameters of the device, such as the level of violation of a Bell inequality $\omega(\rho, \mathcal{M})$ and the rate of the error in the outputs of the key rounds, also referred to as the raw key, $P_{\text{err}}(\rho, \mathcal{M})$. We denote the device-independent key rate for such protocols as $K^{\text{IID}}_{\text{DI,par}}(\rho, \mathcal{M})$ (see Ref. [41] for this approach). The second category, considered in Ref. [38,42] is based on the protocols in which the parties perform a full tomography of the device. We denote the DI key rate for such protocols as $K^{\text{IID}}_{\text{DI,dev}}(\rho, \mathcal{M})$.

In DI-QKD protocols, we assume that an eavesdropper controls the device. The honest parties (Alice and Bob) while accessing a device cannot differentiate between two devices $(\rho, \mathcal{M})$ and $(\sigma, \mathcal{N})$ if the observed statistics are equivalent. We denote this equivalence by $(\rho, \mathcal{M}) = (\sigma, \mathcal{N})$.

As the first main result, given in Sec. IV, we provide tighter bounds for the aforementioned protocols. The bound we provide is given in terms of reduced relative entropy of entanglement optimized over decompositions into local and nonlocal part.

We develop on the results of Ref. [40] going beyond states that are positive under partial transposition (PPT) [47,48]. In the theorem given below, LHV denotes the set of devices with locally realistic hidden variable models. We arrive at the following upper bound for general DI-QKD protocols.

Theorem 1. *The maximal DI-QKD rate $K^{\text{IID}}_{\text{DI}}(\rho, \mathcal{M})$ of a device $(\rho, \mathcal{M})$ is upper bounded as*

$$K^{\text{IID}}_{\text{DI,dev}}(\rho, \mathcal{M}) \leq (1-p) \inf_{(\sigma^{\text{NL}}, \mathcal{N}) = (\rho^{\text{NL}}, \mathcal{M})} E_R(\sigma^{\text{NL}}) + p \inf_{(\sigma^{\text{L}}, \mathcal{N}) = (\rho^{\text{L}}, \mathcal{M})} E_R(\sigma^{\text{L}}), \quad (1)$$

where $E_R(\rho)$ is the relative entropy of entanglement [49] of the bipartite state ρ,

$$\rho = (1-p)\rho^{\text{NL}} + p\rho^{\text{L}} \quad (2)$$

such that $(\sigma^{\text{L}}, \mathcal{N}), (\rho^{\text{L}}, \mathcal{M}) \in$ LHV.

We then prove an analogous theorem. The maximal DI-QKD rate $K^{\text{IID}}_{\text{DI,par}}(\rho, \mathcal{M})$ of a device $(\rho, \mathcal{M})$, where the parameters considered are the CHSH violation ω [2] and the quantum bit error rate (QBER), is upper bounded as

$$K^{\text{IID}}_{\text{DI,par}}(\rho, \mathcal{M}) \leq (1-p) \inf_{\omega(\sigma^{\text{bnl}}, \mathcal{N}) = \omega(\rho^{\text{bnl}}, \mathcal{M})} E_R(\sigma^{\text{bnl}}), \quad (3)$$

where $\rho = (1-p)\rho^{\text{bnl}} + p\rho^{\text{bl}}$ and ρ^{bl} denotes state satisfying CHSH inequality and ρ^{bnl} denotes the state-violating CHSH inequality (The letters bnl correspond to bipartite non-local and bl corresponds to bipartite local) [46]. We plot the upper bounds in Fig. 2. Here, $\omega(\sigma^{\text{bnl}}, \mathcal{N}) = \omega(\rho^{\text{bnl}}, \mathcal{M})$, is used to denote that the CHSH violations observed for the two devices is equal.

We now discuss the second main result of our work, given in Sec. V. Consider a set up in which Alice and Bob are connected by a channel. Alice's device prepares a bipartite quantum state and transmits it through the channel. Now, on surface this situation might seem similar to the situation we encountered before, wherein Alice and Bob are sharing a noisy quantum state. However, a crucial difference is that Alice's device can prepare a perfect Bell state but during transmission the state will get corrupted because of the channel noise. The noise prevalent in the channel will fundamentally limit the DI key that Alice and Bob can share. This is a generalization of the setup considered in Ref. [40]. The device for such a set up is given by $(\Lambda, \rho, \mathcal{M})$, where Λ is a channel connecting Alice to Bob. This could include an optical fiber for instance. We provide upper bounds on the device-independent key rate of the device $(\Lambda, \rho, \mathcal{M})$. We allow for the protocols in this set up to have two types of classical communication. The device is allowed to communicate after each input and output round. We also allow the honest parties (Alice and Bob) to communicate with each other after each input and output round. This communication involves error correction or parameter estimation part of the protocol.

The DI-QKD capacity of the device $(\Lambda, \rho, \mathcal{M})$ under the assumption of its IID uses assisted with i-way communication between allies outside the device and j-way communication between the input-output rounds within the device, is given by [40]

$$\mathcal{P}_i^{\text{IDI}_j}(\Lambda, \rho, \mathcal{M}) := \inf_{\varepsilon > 0} \limsup_{n \to \infty} \mu_{i,n}^{\text{IDI}_j, \varepsilon}(\Lambda, \rho, \mathcal{M}), \quad (4)$$

where $\mu_{i,n}^{\text{IDI}_j, \varepsilon}(\Lambda, \rho, \mathcal{M})$ is the maximum key rate optimized over all viable CLOCC protocols $\hat{\mathcal{P}}$ over the IID uses of device, and also includes a minimization over the possible IID devices IDI_j as well as a minimization over all ε approximate devices given by $(\Lambda', \sigma, \mathcal{N}) \approx_\varepsilon (\Lambda, \rho, \mathcal{M})$. We define the IID-device-independent variants IDI_j for

$j \in \{0,1,2\}$, where the devices are IID and are not allowed memory or communication from one round to the next (see Ref. [40] and Sec. V for details on different adversarial models). By CLOCC protocols, we mean that the Alice and Bob can communicate with each other and perform only classical operations on their devices. This informally means that the statistics of the two devices are approximately equal. We require this minimization over all devices since Alice and Bob do not trust the underlying devices. We have

$$\mu_{i,n}^{\mathrm{IDI}_j,\varepsilon}(\Lambda,\rho,\mathcal{M}) := \sup_{\hat{P}\in\mathrm{CLOPC}_i} \inf_{\substack{(\Lambda',\sigma,\mathcal{N})\in\mathrm{IDI}_j \\ (\Lambda',\sigma,\mathcal{N})\approx_\varepsilon(\Lambda,\rho,\mathcal{M})}} \kappa_n^\varepsilon(\hat{P},(\Lambda',\sigma,\mathcal{N})), \tag{5}$$

where κ_n^ε is the rate of achieved ε-perfect key and classical labels from local classical operations in $\hat{P} \in \mathrm{CLOPC}_i$ are possessed by the allies (Alice and Bob).

Consider now a class of channels Λ that are simulable via LOCC and the respective Choi states as the resource [50,51].

That is,

$$\Lambda_{A\to B}(\rho_A) = \mathcal{L}_{AA'\to B}\left(\Phi^\Lambda_{A'B}\otimes\rho_A\right), \tag{6}$$

where $\mathcal{L}_{AA'\to B}$ is a LOCC channel, with the classical communication being from A to B and $\Phi^\Lambda_{A'B} := \Lambda(\Phi^+_{A'A})$ is the Choi state of the channel, with $\Phi^+_{A'B} := (1/d)\sum_{i,j=0}^{d-1}|i,i\rangle\langle j,j|_{A'B}$ denoting a maximally entangled state of Schmidt rank $d = \min\{|A'|,|B|\}$. The above equation informally implies that any quantum communication via the channel Λ is equivalent to sharing the Choi state Φ^Λ followed by local operations and classical communication. The following upper bounds hold

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\Lambda,\rho,\mathcal{M}) \le \inf_{\substack{(\Lambda',\sigma,\mathcal{N})\in\mathrm{IDI}_j \\ (\Lambda',\sigma,\mathcal{N})=(\Lambda,\rho,\mathcal{M})}} E_R(\Phi^{\Lambda'}), \tag{7}$$

where $\Phi^{\Lambda'} := \Lambda'(\Phi^+)$ is the Choi state of the channel Λ'. We also restrict Λ' to be covariant channels.

In Fig. 3, we plot the upper bounds on the DI-QKD rates for the devices $(\Lambda,\rho,\mathcal{M})$ for Λ being qubit channels—depoloarizing $\mathcal{D}^p$, dephasing $\mathcal{P}^p$, and erasure $\mathcal{E}^p$, where actions of these channels are given as $\mathcal{P}^p(\rho) = (1-p)\rho + p\sigma_Z\rho\sigma_Z$, $\mathcal{D}^p(\rho) = (1-p)\rho + p\frac{1}{2}\mathbb{1}$, $\mathcal{E}^p(\rho) \equiv (1-p)\rho + p|e\rangle\langle e|$, where $|e\rangle\langle e|$ is the erasure symbol, orthonormal to the support of the input state and $p \in [0,1]$. The relative entropy of entanglement of the Choi states of the erasure and dephasing channels are also the device-dependent QKD capacities of respective channels [34]. We make a crucial observation that the dephasing channel can simulate the device $(\Lambda,\rho,\mathcal{M})$ with Λ as the erasure channel or depolarizing channel in a device-independent way for protocols using the CHSH violation and QBER as the parameters to identify the device. This suggests that the outcomes of the device will have statistics that can be explained by the dephasing channel even when the actual channel present inside the device is erasure or depolarizing.

As our third main result, we study a bound called *reduced* cc-*squashed entanglement*. The upper bounds presented below apply only to the class of standard protocols that use only certain inputs for generating key. In such DI-QKD protocols the key rounds and the parameter estimation rounds are separated. This implies that the final key is generated from outputs of specified inputs. The number of key-generating inputs can be varied depending on the protocol, however usually the key is taken only from a single input. To study upper bounds on the DI-QKD rates for such protocols, we begin with introducing an entanglement measure, similar to the squashed entanglement, which is implicitly used in Ref. [41] (also see Lemma 7 of Ref. [52]):

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\rho_{AB},M) := \inf_{\Lambda_E} I(A:B|E)_{M\otimes\Lambda_E.(\psi^\rho)} \tag{8}$$

It is a function of a pair of POVMs $M := M_a^{\hat{x}}\otimes M_a^{\hat{y}}$ and a bipartite quantum state. The $\hat{x}$ and $\hat{y}$ corresponds to the key-generating rounds. It computes the infimum over channels Λ_E acting on the purification ψ^ρ_{ABE} of the state ρ_{AB}, of the *conditional mutual information* of resulting extension of ρ measured with M on system AB. We call it *cc-squashed entanglement* where CC stands for classical-classical registers of the measured system AB.

We further consider its reduced versions (*reduced CC-squashed entanglement*), where reduction is due to the infimum on the set of allowed attacking strategies of the eavesdropper while manufacturing the device. As in the case of IID DI key rate there are two versions of reduced cc-squashed entanglement:

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})) := \inf_{\substack{\omega(\sigma,\mathcal{N})=\omega(\rho,\mathcal{M}) \\ P_{\mathrm{err}}(\sigma,\mathcal{N})=P_{\mathrm{err}}(\rho,\mathcal{M}(\hat{x},\hat{y}))}} E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma_{AB},\mathcal{M}(\hat{x},\hat{y})), \tag{9}$$

$$E_{\mathrm{sq,dev}}^{\mathrm{CC}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})) := \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma_{AB},\mathcal{M}(\hat{x},\hat{y})). \tag{10}$$

In the above definitions, $(\rho_{AB},\mathcal{M})$ corresponds to the honest device in consideration and $(\hat{x},\hat{y})$ corresponds to the key-generation inputs. We can also consider σ to be infinite dimensional and any issues regarding this fact has been tackled in Ref. [52]. In the first definition, we have the infimum over all devices compatible to certain parameters observed in the protocol. In the second definition,

we have the infimum over all devices that give the distribution $p(a,b|x,y) = \mathrm{Tr}(\mathcal{M}_a^x \otimes \mathcal{M}_b^y \rho)$. It is clear that by definition $E^{\mathrm{CC}}_{\mathrm{sq,par}} \leq E^{\mathrm{CC}}_{\mathrm{sq,dev}}$. This is because the former involves the infimum over a larger set of dishonest device. We denote the DI-QKD rate for protocols with single key-generation inputs $\hat{x}$ and $\hat{y}$ as $K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev/par}}(\rho,\mathcal{M})$. Using the proof techniques in Refs. [40,45], we can see (Theorem 5 and Corollary 5) that the above quantities upper bound the DI-QKD rate:

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev/par}}(\rho,\mathcal{M}) \leq E^{\mathrm{CC}}_{\mathrm{sq,dev/par}}(\rho,\mathcal{M}). \tag{11}$$

We prove that the bound is convex, and outperforms both the limitations presented in Refs. [41,42] in a certain regime of noise. We then show that in the case when testing in the DI-QKD protocol is done by estimating the CHSH inequality and the QBER, the cc-squashed entanglement and its reduced version is an upper bound. We further argue, that the bounds studied in Refs. [41,42] are in fact *particular instances of the optimization* that takes place in computing of the reduced cc-squashed entanglement. That is, the upper bounds *plotted* in Refs. [41,42] are upper bounds on $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y}))$. We denote the plotted functions as $I_{AL}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y}))$ and $I_{FBJL+}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y}))$, respectively. That means, if $E^{\mathrm{CC}}_{\mathrm{sq,par}}$ was plotted, it would be lesser than both the bounds $I_{AL}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y}))$ and $I_{FBJL+}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y}))$ given in Refs. [41,42], respectively. Formally, for any device $(\rho,\mathcal{M})$ and input $\mathcal{M}(\hat{x},\hat{y})$, there is

$$E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})) \leq I_{AL}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})), \tag{12}$$

$$E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})) \leq I_{FBJL+}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})), \tag{13}$$

$$E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})) \leq E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho_{AB},\mathcal{M}(\hat{x},\hat{y})). \tag{14}$$

Based on the above inequalities and some of the desirable properties like convexity of the cc-squashed entanglement with respect to the states, we obtain our third main result. In what follows we narrow considerations to $(\mathcal{M},(\hat{x},\hat{y}))$ being *projective*, as the bound for Werner states presented in Ref. [42] applies only to this case. Our third main result is encapsulated in theorem below.

Theorem 2. *For a Werner state ρ^W_{AB} and $\mathcal{M}$ consisting of projective measurements $P^x_a \otimes P^y_b$, and a pair of inputs $(\hat{x},\hat{y})$ used to generate the key, there is*

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}(\rho^W_{AB},\mathcal{M}) \leq \mathrm{Conv}(I_{AL}(\rho^W_{AB},\mathcal{M}(\hat{x},\hat{y})), I_{FBJL+}(\rho^W_{AB},\mathcal{M}(\hat{x},\hat{y}))), \tag{15}$$

where $\mathrm{Conv}(F_1,F_2)$ *is the convex hull of the plots of functions F_i, and $K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}(\rho^W_{AB},\mathcal{M})$ is defined with respect to $\omega(\rho^W,\mathcal{M})$ and $P_{\mathrm{err}} = P(a \neq b|\hat{x}\hat{y})$.*

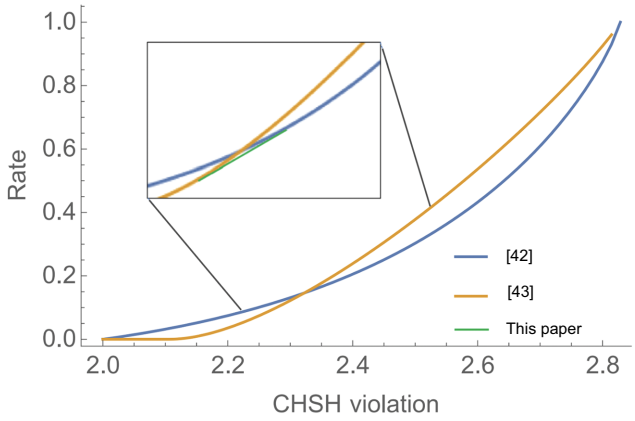

FIG. 1. In this figure, we show the plots for standard device-independent CHSH protocol obtained in Refs. [41,42], and the upper bound given in Theorem 2, which is the convex hull of the former bounds, depicted in green.

We plot the upper bound obtained from the aforementioned theorem in Fig. 1. The above result stems from the technique provided in Ref. [39] where a similar upper bound obtained via the method called convexification was given in the scenario with nonsignaling adversary.

We also extend the definition of $E^{\mathrm{CC}}_{\mathrm{sq}}$ for multiple measurements. We then prove that the reduced version of this quantity is an upper bound on the DI-QKD rate for protocols with multiple key-generating inputs. We note that for extension to multiple measurements, the function introduced is tuned to protocols in which the measurements are announced by Alice and Bob and hence are known to the eavesdropper. We could in principle, on similar grounds, also consider upper bounds for protocols in which the measurements are not known to the eavesdropper.

III. NOTATION AND DEFINITIONS

In this section we provide the notation used throughout the paper along with a relevant definition including that of device-dependent and device-independent secure key rate in the IID setting. We also give an intuitive explanation of the latter definitions.

We begin with recalling the definition of key and device-dependent key rate of a quantum state. A quantum state representing (ideal) secure key of length K is a pair of bitstrings drawn from a uniform distribution, which are decoupled from the state of adversary:

$$\tau_{ABE}(K) := \frac{1}{K}\sum_{i=0}^{K-1} |ii\rangle\langle ii|_{AB} \otimes \sigma_E. \tag{16}$$

Ideal security is hard to achieve in practice. Instead we are interested in designing protocols that uses n copies of an input state ρ_{AB} achieving ϵ security and take the limit of small $\epsilon \to 0$ when $n \to \infty$. By protocol $\mathcal{P}$ we mean a

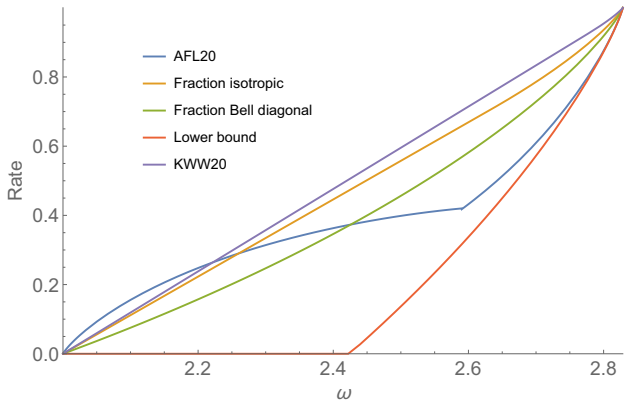

FIG. 2. In this plot, we depict the bounds on the amount of DI key that can be obtained from a CHSH-based device. The yellow line and green line corresponds to the upper bounds obtained from Eq. (3). The blue line corresponds to the bound obtained in Appendix B of Ref. [41]. The purple line corresponds to the bound obtained in Ref. [38]. The red line corresponds to the lower bounds obtained in Ref. [60].

quantum map from the set of local operations and classical communication $\mathcal{P} \in \text{LOCC}$ such that acting on $\rho_{AB}^{\otimes n}$ produce output close by ϵ to $\tau_{ABE}(n\kappa_n^\epsilon)$. We note that κ_n^ϵ is the key rate (private bits per copy) and $n\kappa_n^\epsilon$ gives the total number of private bits readily accessible from the ideal key state τ_{ABE}. More formally, a protocol $\mathcal{P}$ acting on n input states ρ_{AB} has *rate* κ_n^ϵ if it outputs state ρ_{ABE}^{out} that satisfies ϵ-security condition:

$$\left\| \rho_{ABE}^{\text{out}} - \tau_{ABE}(n\kappa_n^\epsilon) \right\|_1 \leq \epsilon, \tag{17}$$

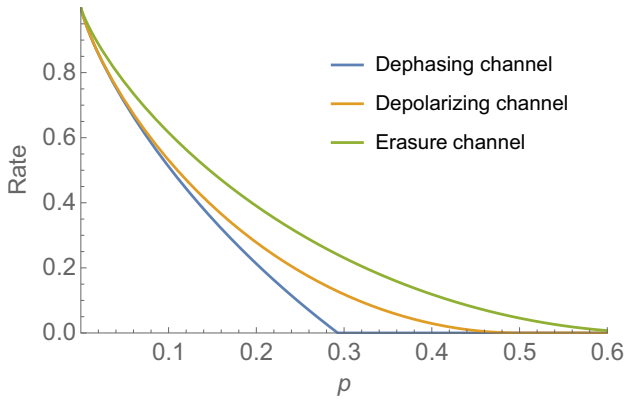

FIG. 3. In the above figure, we plot upper bounds on the device-dependent QKD capacities of depolarizing channel (yellow line), dephasing channel (blue line), and erasure channel (green line). We notice that the upper bounds for erasure and dephasing channels are achievable device-dependent QKD rates (capacities). We then notice that for the CHSH protocols, the upper bounds on the DI-QKD capacities of channels is limited by the device-dependent QKD capacity of dephasing channels.

where $\|\cdot\|_1$ denotes the trace-norm distance. The device-dependent key rate of a quantum state ρ_{AB} reads then [45, 53–56]:

$$K_{\text{DD}}(\rho_{AB}) := \inf_{\epsilon>0} \limsup_{n\to\infty} \sup_{\mathcal{P}\in\text{LOCC}} \kappa_n^\epsilon(\mathcal{P}(\rho_{AB}^{\otimes n})). \tag{18}$$

In the above the $\limsup_{n\to\infty}$ reflects the fact that it is enough that the protocol is able to produce ϵ-secure output only on an infinite *subsequence* of natural numbers n of copies of the input states (e.g., only for $n = 2^k$ for some natural k). The infimum over ϵ standing in front reflects the fact that a given amount of key is achievable only if with increasing n there are protocols $\mathcal{P}$ that achieve better and better ϵ security with $\epsilon \to 0$.

We are ready to introduce the notation and facts needed to recall the device-independent key rate, and its relation to the device-dependent one. Like in the device-dependent scenario the central object is a quantum state, in the device-independent one the central object is a (quantum) device. Informally it is a pair of a bipartite state ρ and a family of maps $\mathcal{M}$ parametrized by inputs (x, y) and outputs of the device (a, b). The maps acting on a state yield a conditional probability distribution representing the device.

Formally a quantum device is given by its quantum representation $\text{Tr}[M_a^x \otimes M_b^y \rho]$ where $\{M_a^x\}_a$ and $\{M_b^y\}_b$ are POVMs for each input to the device (x, y), and ρ is a bipartite state. We denote such a device as $(\rho, \mathcal{M})$ where $\mathcal{M} = \{M_a^x \otimes M_b^y\}_{a,b}^{x,y}$. Let LHV denote the set of states with locally realistic hidden variable models under a given set of measurements.

We denote the IID device-independent key rate of a quantum device as $K_{\text{DI}}^{\text{IID}}$. By IID we mean that the devices are independent and identical in each round of the protocol. We then consider various types of protocols for DI-QKD rate. In the first case, single inputs are used for key generation. There are a further two variants of such a protocol. The first quantifies the key achieved by protocols in which the honest parties perform test based only on certain parameters of the device. These parameters include the level of violation of a Bell inequality $\omega(\rho, \mathcal{M})$ and the rate of the error of the raw key data $P_{\text{err}}(\rho, \mathcal{M})$. We denote the device-independent key rate for such protocols as $K_{\text{DI,par}}^{\text{IID},(\hat{x},\hat{y})}(\rho, \mathcal{M})$ (see Ref. [41] for this approach). The second, considered in Ref. [38,42] is based on the protocols in which the parties perform a full tomography of the device. We denote the DI key rate for such protocols as $K_{\text{DI,dev}}^{\text{IID},(\hat{x},\hat{y})}(\rho, \mathcal{M})$.

Let $\mathcal{D}(\mathcal{H}_{AB})$ denote the set of states defined on the $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are the separable Hilbert spaces associated with the quantum systems A and B, respectively. Let $\mathbb{1}_A$ denote the identity operator on $\mathcal{H}_A$ and $|A|$ denote the dimension of $\mathcal{H}_A$ ($\dim(\mathcal{H}_A)$). Let Φ_{AB}^+

denote a maximally entangled state,

$$\Phi_{AB}^{+} := \frac{1}{d} \sum_{i,j=0}^{d-1} |i,i\rangle \langle j,j|_{AB} \tag{19}$$

for $d = \min\{|A|, |B|\}$ and an orthonormal basis $\{|i\rangle\}_i$. Let ϑ be the partial transposition map with respect to a fixed basis, i.e., $\vartheta(\rho_{AB}) = \rho_{AB}^{\Gamma_B}$. The set of separable states $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ is denoted as $\mathrm{SEP}(A;B)$.

Consider a setup, wherein Alice and Bob, two spatially separated parties, have to extract a secret key. We assume that in this setup, the devices are untrusted. That is, Alice and Bob do not trust the quantum states, nor do they trust their measurement devices. The untrusted measurement of the device is given by $\mathcal{M} \equiv \{M_a^x \otimes M_b^y\}_{a,b|x,y}$, where $a \in \mathcal{A}$, $b \in \mathcal{B}$, and $\mathcal{A}, \mathcal{B}$ denote the finite set of measurement outcomes. The measurement outcomes, i.e., ouputs of the device, are secure from adversary and assumed to be in the possession of the receiver, Alice or Bob. Also, $x \in \mathcal{X}, y \in \mathcal{Y}$, where $\mathcal{X}, \mathcal{Y}$ denote the finite set of measurement choices. The joint probability distribution is given as $p(a,b|x,y) = \mathrm{Tr}[M_a^x \otimes M_b^y \rho]$ for measurement $\mathcal{M}$ on bipartite state ρ_{AB} defined on the separable Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The quantum systems A, B can be finite or infinite dimensional. The number of inputs x, y and corresponding outputs a, b of local measurements by Alice and Bob are arbitrary in general.

Let $\omega(\rho, \mathcal{M})$ denote the violation of the given Bell inequality $\mathcal{B}$ by state ρ_{AB} when the measurement settings are given by $\mathcal{M}$. Let $P_{\mathrm{err}}(\rho, \mathcal{M})$ denote the expected QBER. In the standard protocols, it is a probability that the raw key of Alice differs from the raw key of Bob. Both the Bell violation, as well as the QBER are a function of the probability distribution of the box. If under local measurements $\mathcal{M}$, a state ρ exhibits a locally realistic hidden variable model then we write $\rho \in \mathrm{LHV}(\mathcal{M})$. If $\{p(a,b|x,y)\}_{a,b|x,y}$ obtained from $(\rho, \mathcal{M})$ and $(\sigma, \mathcal{N})$ are the same, we write $(\sigma, \mathcal{N}) = (\rho, \mathcal{M})$. In most DI-QKD protocols, instead of using the statistics of the *full* correlation, we use the Bell violation and the QBER to test the level of security of the observed statistics. In this way, the protocols coarse grain the statistics and we use only partial information of the full statistics to extract the device-independent key. In this context, the notation $(\sigma, \mathcal{N}) = (\rho, \mathcal{M})$ also implies that $\omega(\sigma, \mathcal{N}) = \omega(\rho, \mathcal{M})$ and $P_{\mathrm{err}}(\sigma, \mathcal{N}) = P_{\mathrm{err}}(\rho, \mathcal{M})$. When conditional probabilities associated with $(\rho, \mathcal{M})$ and $(\sigma, \mathcal{N})$ are ε close to each other, then we write $(\rho, \mathcal{M}) \approx_\varepsilon (\sigma, \mathcal{N})$. For our purpose, it suffices to consider the distance

$$d(p, p') = \sup_{x,y} \|p(\cdot|x,y) - p'(\cdot|x,y)\|_1 \leq \varepsilon. \tag{20}$$

The device-independent (DI) distillable key rate of a device is informally defined as the supremum over the finite key rates κ achievable by the best protocol on any device compatible with $(\rho, \mathcal{M})$, within an appropriate asymptotic block-length limit and security parameter. There are at least two definitions of compatibility. One is assuming full knowledge of the honest device reflected by the description of the device $(\rho, \mathcal{M})$. The other, as it was mentioned, is assuming only the knowledge of some parameters of the honest device. It is reflected only by a set of parameters. In standard protocols these are the level of violation of a certain Bell inequality, i.e., $\omega(\rho, \mathcal{M})$ and the quantum bit error rate $P_{\mathrm{err}}(\rho, \mathcal{M})$.

For our purpose, we constrain ourselves to the situation when the compatible devices are supposedly IID (independent and identically distributed). Although the class of attacks of the quantum adversary may be much larger, including non-IID attack, for our purpose it is sufficient to consider IID attacks. The reason for this is that any possible attack by the eavesdropper serves as a strategy for an upper bound. For our work, the choice of strategy is an IID attack.

In order to define formally the device-independent key in the IID setting, we need the following relations:

$$(\rho, \mathcal{M}) \approx_\varepsilon (\sigma, \mathcal{N}), \tag{21}$$

$$\omega(\rho, \mathcal{M}) \approx_\varepsilon \omega(\sigma, \mathcal{N}), \tag{22}$$

$$P_{\mathrm{err}}(\rho, \mathcal{M}) \approx_\varepsilon P_{\mathrm{err}}(\sigma, \mathcal{M}), \tag{23}$$

where Eq. (21) implies Eqs. (22) and (23). Formally, the definition of device-independent distillable key rate in IID setting, is given as

Definition 1 ([40])**.** *The maximum device-independent key rate of a device $(\rho, \mathcal{M})$ with IID behavior is defined as follows.*

$$K_{\mathrm{DI}}^{\mathrm{IID}}(\rho, \mathcal{M}) := \inf_{\varepsilon > 0} \limsup_{n \to \infty} \sup_{\hat{\mathcal{P}}} \inf_{(21)} \kappa_n^\varepsilon(\hat{\mathcal{P}}((\sigma, \mathcal{N})^{\otimes n})), \tag{24}$$

where κ_n^ε is the key rate achieved for any security parameter ε, block length or number of copies n, and measurements $\mathcal{N}$.

Here, $\hat{\mathcal{P}}$ is a protocol composed of classical local operations and public (classical) communication (CLOPC) acting on n identical copies of $(\sigma, \mathcal{N})$, which, composed with the measurement, results in a quantum local operations and public (classical) communication (QLOPC) protocol.

Before going on with the known facts, let us comment on the form of the above definition. We can see, that it is very similar to the the definition of device-independent key given in Eq. (18), with two crucial differences. First a minor one: the supremum is taken over protocols that consist of classical LOCC operations (CLOCC). That is having only classical inputs and outputs (the ones coming from n copies of a device). A major modification of the

definition device-dependent key comes with the presence of additional infimum over devices $(\sigma,\mathcal{N})$ that are ϵ close to the honest one $(\rho,\mathcal{M})$. This infimum reflects the fact that the device $(\rho,\mathcal{M})$ is not trusted, and can be replaced by any other pair of state σ and measurements $\mathcal{N}$, that yield enough close-by conditional probability distribution $(\sigma,\mathcal{N})$. Additionally, what is more, the protocol $\mathcal{P}$ acts on the dishonest device $(\sigma,\mathcal{N})$.

As discussed above, a large class of device-independent quantum key distribution protocols, rely on the Bell violation and the QBER of the device $p(a,b|x,y)$. For such protocols, we can define the device-independent key distillation protocol as follows.

Definition 2 (cf. [41])**.** *The maximal device-independent key rate of a device $(\rho,\mathcal{M})$ with IID behavior, Bell violation $\omega(\rho,\mathcal{M})$ and QBER $P_{\text{err}}(\rho,\mathcal{M})$, is defined as*

$$K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M},\omega,P_{\text{err}}) := \inf_{\varepsilon>0} \limsup_{n\to\infty} \sup_{\hat{\mathcal{P}}} \inf_{(22),(23)} \kappa_n^{\varepsilon}(\hat{\mathcal{P}}((\sigma,\mathcal{N})^{\otimes n})). \tag{25}$$

The difference between the above definition and that of $K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M})$ is only by the fact that the infimum is taken over the parameters: Bell violation $\omega(\rho,\mathcal{M})$ and the quantum bit error rate $P_{\text{err}}(\rho,\mathcal{M})$. Hence in the case of $K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M})$ the set of inputs to the protocol (i.e., the dishonest devices) is less than the corresponding one over which infimum is taken in the definition of $K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M},\omega,P_{\text{err}})$. Thus by property of the infimum, we obtain that by definition there is $K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M},\omega,P_{\text{err}}) \leq K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M})$.

Finally we also recall here the fact, which is used later in Sec. VI, that the maximal device-independent key distillation rate $K_{\text{DI}}(\rho,\mathcal{M})$ for the device $(\rho,\mathcal{M})$ is upper bounded by the maximal device-dependent key distillation rate $K_{\text{DD}}(\sigma)$ for all $(\sigma,\mathcal{N})$ such that $(\sigma,\mathcal{N}) = (\rho,\mathcal{M})$ (see Ref. [40]), i.e.,

$$K_{\text{DI}}(\rho,\mathcal{M}) \leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_{\text{DD}}(\sigma), \tag{26}$$

where K_{DD} is given in Eq. (18).

IV. BOUNDS ON DEVICE-INDEPENDENT KEY DISTILLATION RATE OF STATES

In this section, we provide tighter bounds for protocols considered in Ref. [38] and go beyond the results presented in Ref. [40]. (The latter were restricted only to states with positive partial transposition.) The bound we provide is given in terms of reduced relative entropy of entanglement optimized over decompositions into local and nonlocal part.

Proposition 1. *The maximal device-independent key rate $K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M},\omega,P_{\text{err}})$ of a device $(\rho,\mathcal{M})$ with IID behavior, Bell violation $\omega(\rho,\mathcal{M})$ and QBER $P_{\text{err}}(\rho,\mathcal{M})$ is upper bounded as*

$$K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M},\omega,P_{\text{err}}) \leq \inf_{\substack{\omega(\mathcal{N},\rho)=\mathcal{N},\sigma) \\ P_{\text{err}}(\mathcal{N},\rho)=P_{\text{err}}(\mathcal{M},\sigma)}} K_{\text{DD}}(\sigma). \tag{27}$$

Proof :

$$K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M},\omega,P_{\text{err}}) \leq \inf_{\varepsilon>0} \inf_{\substack{\omega(\mathcal{N},\rho)\approx\mathcal{N},\sigma) \\ P_{\text{err}}(\mathcal{N},\rho)\approx P_{\text{err}}(\mathcal{M},\sigma)}} \limsup_{n\to\infty} \sup_{\hat{\mathcal{P}}} \kappa_n^{\varepsilon}(\hat{\mathcal{P}}((\mathcal{N},\sigma)^{\otimes n})) \tag{28}$$

$$\leq \inf_{\varepsilon>0} \inf_{\substack{\omega(\mathcal{N},\rho)=\mathcal{N},\sigma) \\ P_{\text{err}}(\mathcal{N},\rho)=P_{\text{err}}(\mathcal{M},\sigma)}} \limsup_{n\to\infty} \sup_{\hat{\mathcal{P}}} \kappa_n^{\varepsilon}(\hat{\mathcal{P}}((\mathcal{N},\sigma)^{\otimes n})) \tag{29}$$

$$= \inf_{\substack{\omega(\mathcal{N},\rho)=\mathcal{N},\sigma) \\ P_{\text{err}}(\mathcal{N},\rho)=P_{\text{err}}(\mathcal{M},\sigma)}} \inf_{\varepsilon>0} \limsup_{n\to\infty} \sup_{\hat{\mathcal{P}}} \kappa_n^{\varepsilon}(\hat{\mathcal{P}}((\mathcal{N},\sigma)^{\otimes n})) \tag{30}$$

$$\leq \inf_{\substack{\omega(\mathcal{N},\rho)=\mathcal{N},\sigma) \\ P_{\text{err}}(\mathcal{N},\rho)=P_{\text{err}}(\mathcal{M},\sigma)}} K_{\text{DD}}(\sigma) \tag{31}$$

The first inequality follows from Observation 5 of Ref. [40]. The second inequality follows from restricting the infimum over the set of strategies. The equality follows from commuting the infimums. The last inequality follows from the definition of device-dependent key distillation rate. ■

Observation 1. *For entanglement measures* Ent*, which upper bounds the maximum device-dependent key distillation rate, i.e., $K_{\text{DD}}(\rho) \leq \text{Ent}(\rho)$ for a density operator ρ, we have,*

$$K_{\text{DI}}(\rho,\mathcal{M}) \leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_{\text{DD}}(\sigma) \tag{32}$$

$$\leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} \text{Ent}(\sigma). \tag{33}$$

Some well-known entanglement measures that upper bound $K_{\text{DD}}(\rho)$ are the relative entropy of entanglement $E_R(\rho)$, regularized relative entropy of entanglement $E_R^{\infty}(\rho)$, squashed entanglement $E_{\text{sq}}(\rho)$ (see Refs. [30,32,57]).

We develop the results of Ref. [40] going beyond states that are positive under partial transposition (PPT). We arrive at the following main result.

Theorem 3. *The maximal device-independent key rate $K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M})$ of a device $(\rho,\mathcal{M})$ is upper bounded as*

$$K_{\text{DI}}^{\text{IID}}(\rho,\mathcal{M}) \leq (1-p) \inf_{(\sigma^{\text{NL}},\mathcal{N})=(\rho^{\text{NL}},\mathcal{M})} E_R(\sigma^{\text{NL}}) + p \inf_{(\sigma^{\text{L}},\mathcal{N})=(\rho^{\text{L}},\mathcal{M})} E_R(\sigma^{\text{L}}), \tag{34}$$

where

$$\rho = (1-p)\rho^{\mathrm{NL}} + p\rho^{\mathrm{L}} \tag{35}$$

such that $\sigma^{\mathrm{L}}, \rho^{\mathrm{L}} \in \mathrm{LHV}$ *and* $\sigma^{\mathrm{NL}}, \rho^{\mathrm{NL}} \notin \mathrm{LHV}$ *for respective local measurements.*

Proof : The main idea behind the proof is to construct an alternative state with flagged local and nonlocal parts, followed by construction of flagged POVM elements. The flagged strategy reproduces the exact statistics as the original strategy. With this construction, we can use the decomposition of relative entropy for flagged state as the sum of the relative entropies for the constituent states.

Let us begin with the device $\{\rho, \mathcal{M}\}$ such that

$$\rho_{AB} = (1-p)\rho^{\mathrm{NL}} + p\rho^{\mathrm{L}}. \tag{36}$$

We have from Eq. (26) that

$$K_{\mathrm{DI}}(\rho, \mathcal{M}) \leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_{\mathrm{DD}}(\sigma). \tag{37}$$

Let us now construct a strategy $\left\{\sigma^{\mathrm{NL}}, N_a^x \otimes N_b^y\right\}$ such that $(\sigma^{\mathrm{NL}}, N_a^x \otimes N_b^y) = (\rho^{\mathrm{NL}}, M_a^x \otimes M_b^y)$. We also construct another strategy $\left(\sigma^{\mathrm{L}}, \Lambda_a^x \otimes \Lambda_b^y\right)$ such that $(\sigma^{\mathrm{L}}, \Lambda_a^x \otimes \Lambda_b^y) = (\rho^{\mathrm{L}}, M_a^x \otimes M_b^y)$. Combining the above deductions, we can define a strategy

$$\begin{aligned}\sigma_{ABR_1R_2} = (1-p)\sigma_{AB}^{\mathrm{NL}} \otimes |0\rangle\langle 0|_{R_1} \otimes |0\rangle\langle 0|_{R_2} \\ + p\sigma_{\mathrm{L}} \otimes |1\rangle\langle 1|_{R_1} \otimes |1\rangle\langle 1|_{R_2},\end{aligned} \tag{38}$$

$$\tilde{\Lambda}_a^x = N_a^x \otimes |0\rangle\langle 0|_{R_1} + \Lambda_a^x \otimes |1\rangle\langle 1|_{R_1}, \tag{39}$$

$$\tilde{\Lambda}_b^y = N_b^y \otimes |0\rangle\langle 0|_{R_2} + \Lambda_b^y \otimes |1\rangle\langle 1|_{R_2}. \tag{40}$$

We then see $(\rho, \mathcal{N}) = (\sigma, \tilde{\Lambda}_a^x \otimes \tilde{\Lambda}_b^y)$. We then obtain

$$K_{\mathrm{DI}}(\rho, \mathcal{M}) \leq K_{\mathrm{DD}}(\sigma) \tag{41}$$

$$\leq E_R(\sigma) \tag{42}$$

$$= (1-p)E_R(\sigma^{\mathrm{NL}}) + pE_R(\sigma^{\mathrm{L}}). \tag{43}$$

Since the strategies $\left(\sigma^{\mathrm{L}}, \Lambda_a^x \otimes \Lambda_b^y\right)$ and $\left(\sigma^{\mathrm{NL}}, N_a^x \otimes N_b^y\right)$ are arbitrary strategies, we obtain

$$\begin{aligned}K_{\mathrm{DI}}(\rho, \mathcal{M}) \leq (1-p) \inf_{(\rho^{\mathrm{NL}},\mathcal{M})=(\sigma^{\mathrm{NL}},\mathcal{N})} E_R(\sigma^{\mathrm{NL}}) \\ + p \inf_{(\rho^{\mathrm{L}},\mathcal{M})=(\sigma^{\mathrm{L}},\mathcal{N})} E_R(\sigma^{\mathrm{L}}).\end{aligned} \tag{44}$$

■

Similarly, when we are interested only in the two parameters, namely Bell violation ω and QBER P_{err}, of the device $(\rho, \mathcal{M})$, then we have the following upper bound on the DI-key distillation rate.

Proposition 2. *The maximal device-independent key distillation rate* $K_{\mathrm{DI}}(\rho, \mathcal{M}, \omega, P_{\mathrm{err}})$ *for the device* $(\rho, \mathcal{M})$ *and a linear Bell functional* $\omega(\rho, \mathcal{M})$ *and QBER* $P_{\mathrm{err}}(\rho, \mathcal{M})$ *is upper bounded by*

$$\begin{aligned}K_{\mathrm{DI}}(\rho, \mathcal{M}, \omega, P_{\mathrm{err}}) \leq p \inf_{\substack{\omega(\sigma^{\mathrm{L}},\mathcal{N})=\omega(\rho^{\mathrm{L}},\mathcal{M}) \\ P_{\mathrm{err}}(\sigma^{\mathrm{L}},\mathcal{N})=P_{\mathrm{err}}(\rho^{\mathrm{L}},\mathcal{M})}} E_R(\sigma^{\mathrm{L}}) \\ + (1-p) \inf_{\substack{\omega(\sigma^{\mathrm{NL}},\mathcal{N})=\omega(\rho^{\mathrm{NL}},\mathcal{M}) \\ P_{\mathrm{err}}(\sigma^{\mathrm{NL}},\mathcal{N})=P_{\mathrm{err}}(\rho^{\mathrm{NL}},\mathcal{M})}} E_R(\sigma^{\mathrm{NL}}),\end{aligned} \tag{45}$$

where $\rho = p\rho^{\mathrm{L}} + (1-p)\rho^{\mathrm{NL}}$ *and* $\rho^{\mathrm{L}} \in \mathrm{LHV}$ *and* $\sigma^{\mathrm{NL}}, \rho^{\mathrm{NL}} \notin \mathrm{LHV}$ *(for respective local measurements).*

For the proof, we refer to Appendix B.

Remark 1. *The above proposition is general, since the Bell functionals typically take the form of a scalar product, and hence are linear [8]. For example, the tight Bell inequalities corresponds to a test if a behavior is in or outside of the polytope of local behaviors. However, in principle, one could design a nonlinear Bell functional such as the ones which are designed to characterize in some way the set of quantum behaviors [see Eqs. (33) and (34) [8]].*

We now define a CHSH protocol considered in Ref. [58]. In this protocol, Alice's device has three inputs, i.e., $x \in \{0, 1, 2\}$ and Bob's device has two inputs, i.e., $y \in \{0, 1\}$. Alice and Bob's output are binary, i.e., $a, b \in \{0, 1\}$. This device is then defined by the distribution $\{p(a, b|x, y)\}$. The protocol uses a coarse graining of the distribution. That is, for each distribution, we define the CHSH violation ω and the QBER $p(a \neq b|x = 0, y = 1)$ as q. For such protocols $\mathcal{P}_{\mathrm{CHSH}}$, the relevant statistics of the device are ω and q. In the following, we use $\omega(\rho, \mathcal{N})$ to denote the CHSH violation observed by the quantum strategy $\rho, \mathcal{N}$. We have the following corollary.

Corollary 1. *The maximal device-independent key rate* $K_{\mathrm{DI}}^{\mathrm{IID}}(\rho, \mathcal{M})$ *of a device* $(\rho, \mathcal{M})$ *under* CHSH *protocol* $\mathcal{P}_{\mathrm{CHSH}}$*, is upper bounded as*

$$K_{\mathrm{DI}}^{\mathrm{IID}}(\rho, \mathcal{M}, \mathcal{P}_{\mathrm{CHSH}}) \leq (1-p) \inf_{\omega(\sigma^{\mathrm{NL}},\mathcal{N})=\omega(\rho^{\mathrm{NL}},\mathcal{M})} E_R(\sigma^{\mathrm{NL}}), \tag{46}$$

where

$$\rho = (1-p)\rho^{\mathrm{NL}} + p\rho^{\mathrm{L}}, \tag{47}$$

and $\rho^{\mathrm{L}} \in \mathrm{L}$ *and* $\sigma^{\mathrm{NL}}, \rho^{\mathrm{NL}} \notin \mathrm{L}$ *(for respective local measurements and CHSH inequality).*

Proof : To see the proof, we construct a strategy $\left\{\rho_{\mathrm{SEP}}, N_a^x \otimes N_b^y\right\}$ that reproduces $-2 \leq \omega \leq 2$ and any value of q. For this, choose $\rho_{\mathrm{SEP}} = |00\rangle\langle 00|$. Choose the following projective measurements:

$$N_a^1 = \alpha_1 \sigma_x + \alpha_2 \sigma_z, \tag{48}$$

$$N_a^2 = \omega_1 \sigma_x + \omega_2 \sigma_z, \tag{49}$$

$$N_b^1 = \sigma_z, \tag{50}$$

$$N_b^2 = \zeta_1 \sigma_x + \zeta_2 \sigma_z, \tag{51}$$

where $|\omega_1|^2 + |\omega_2|^2 = 1$, $|\alpha_1|^2 + |\alpha_2|^2 = 1$, and $|\zeta_1|^2 + |\zeta_2|^2 = 1$. The CHSH violation ω observed from the strategy given above is

$$\omega = \alpha_2(1 + \zeta_2) + \omega_2(1 - \zeta_2). \tag{52}$$

If $|\omega| \leq 1$, then choose $\omega_2 = 0, \zeta_2 = 0$ and $\alpha_2 = \omega$. If $1 \leq |\omega| \leq 2$, choose $\omega_2 = 0, \zeta_2 = 1$ and $\alpha_2 = \omega/2$. This recovers the observed CHSH violation. For QBER, the appropriate measurements are N_a^0, N_b^1. We see that any value q of QBER can be obtained by choosing N_a^0 as σ_x with probability $2q$ and σ_z with probability $1 - 2q$. Since the relative entropy of entanglement of $|00\rangle\langle 00|$ is 0, we have the proof. ■

Remark 2. *All bound entangled states satisfy CHSH inequality [59] and hence have zero device-independent key rate for CHSH-based protocols. It is interesting to note that there exists bound entangled states from which private key can be distilled [32], however even these states are useless for device-independent secret key distillation for CHSH-based protocols. That the same can be extended to all Bell inequalities is a matter of recently posed conjecture [41]—revised Peres conjecture.*

A. Numerics for CHSH protocols

We now plot the results of Corollary 1. We first consider the device to be an honest device with the underlying state being an isotropic state. The honest measurements are $M_a^0 = \sigma_z, M_a^1 = (\sigma_z + \sigma_x)/\sqrt{2}, M_a^2 = (\sigma_z - \sigma_x)/\sqrt{2}, M_b^0 = \sigma_z, M_b^1 = \sigma_x$, where σ_x and σ_z are Pauli-x and Pauli-z operators, respectively. A device having the above honest realization is called a CHSH-based device. Let us now consider the observed CHSH violation to be ω. Then, we can construct an isotropic state as

$$\rho^{\nu} = (1 - \nu)|\Phi^+\rangle\langle\Phi^+| + (\nu/4)\mathbb{1}, \tag{53}$$

where the parameter ν is related to the CHSH violation as, $\omega = 2\sqrt{2}(1 - \nu)$. We then have

$$\rho^{\omega} = \frac{\omega}{2\sqrt{2}}|\Phi^+\rangle\langle\Phi^+| + \frac{2\sqrt{2} - \omega}{8\sqrt{2}}\mathbb{1}. \tag{54}$$

The relative entropy of entanglement for the isotropic state is given by

$$E_R(\rho^{\omega}) = \lambda \log_2 \lambda + (1 - \lambda)\log_2(1 - \lambda) + 1, \tag{55}$$

$$\lambda = \frac{\omega}{2\sqrt{2}} + \frac{2\sqrt{2} - \omega}{8\sqrt{2}} \tag{56}$$

$$= \frac{3\omega}{8\sqrt{2}} + \frac{1}{4}. \tag{57}$$

Now, we express ρ^{ω} as

$$\rho^{\omega} = p\rho^{\omega_1} + (1 - p)\rho^{\omega_2}, \tag{58}$$

where $2\sqrt{2} \geq \omega_1 > 2$ and $2 \geq \omega_2 \geq 0$ and $\omega = p\omega_1 + (1 - p)\omega_2$.

We then have the following optimization:

$$K_{\mathrm{DI}}^{\mathrm{IID}}(\rho^{\omega}, \mathcal{M}, \mathcal{P}_{\mathrm{CHSH}}) = \min_{p,\omega_1} pE_R(\rho^{\omega_1}), \tag{59}$$

$$\omega = p\omega_1 + (1 - p)\omega_2, \tag{60}$$

$$0 \leq p \leq 1, \tag{61}$$

$$2 \leq \omega_1 < 2\sqrt{2}, \tag{62}$$

$$0 \leq \omega_2 \leq 2. \tag{63}$$

By performing this optimization, we can obtain the bound given in Fig. 2.

Another approach that we can take is to consider the quantum strategy taken in Ref. [60]. For this strategy the attacking quantum state is

$$\rho = \frac{1 + C}{2}|\Phi^+\rangle\langle\Phi^+| + \frac{1 - C}{2}|\Phi^-\rangle\langle\Phi^-|, \tag{64}$$

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \tag{65}$$

$$\left|\Phi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \tag{66}$$

$$C = \sqrt{\left(\frac{\omega}{2}\right)^2 - 1}. \tag{67}$$

With this strategy we obtain a tighter upper bound as plotted in Fig. 2. This strategy is particularly interesting as the attacking state does not allow for a decomposition between a local and a nonlocal part. The fractional bound reduces to relative entropy of entanglement of the state.

V. BOUNDS ON DEVICE-INDEPENDENT KEY DISTILLATION RATE THROUGH CHANNELS

A simple realistic model of a physical box depicting device-independent secret key generator (assumed to be an honest device from perspective of manufacturer) between allies, is describable by a tuple $(\widetilde{\Omega}, \rho, \mathcal{M})$. Tuple for device constitutes of measurement setting $\{M_a^x \otimes M_b^y\}$, a source state $\rho_{A'B'}$, and a bipartite quantum distribution channel $\widetilde{\Omega}_{A'B'\to AB}$, where a relay station inputs bipartite quantum state and each output of the channel Ω is transmitted to a designated receiver. The dimensions of the quantum systems A', B', A, B can be arbitrary in general as the device can use an arbitrary bipartite quantum channel $\widetilde{\Omega}$. Quantum states from the source undergo quantum dynamical evolution (quantum channels) before they are measured to yield outputs at the ends of Alice and Bob, who are designated parties or allies. Quantum channels can represent noisy transmission via optical fibers, space, etc. or local time evolution (e.g., [61,62]). In general, the bipartite distribution channel $\widetilde{\Omega}_{A'B'\to AB}$ is of the form $\Lambda^1_{A''\to A} \otimes \Lambda^2_{B''\to B} \circ \Omega_{A'B'\to A''B''}$, where $\Omega_{A'B'\to A''B''}$ allows for the joint operation on the bipartite source state and $\Lambda^1_{A''\to A}, \Lambda^2_{B''\to B}$ transmit A'', B'' to the ends A, B where local measurements (temporally sync between Alice and Bob) take place to yield classical outputs a, b to Alice and Bob, respectively. In general, adversarial manufacturer can design the device such that it can perform any physical actions between the rounds and is only required to provide two pairs of classical input-outputs, a pair to each designated party, while adversary is limited only by the laws of quantum mechanics (which includes no signaling).

The probability distribution $p_{(\widetilde{\Omega},\rho,\mathcal{M})}(a, b|x, y)$ associated with an honest device $(\widetilde{\Omega}, \rho, \mathcal{M})$ is given by

$$p(a, b|x, y) = \mathrm{Tr}[M_a^x \otimes M_b^y(\widetilde{\Omega}(\rho))]. \tag{68}$$

An honest device $(\widetilde{\Omega}, \rho, \mathcal{M})$ constituting channels has same characterization and conditions as an honest device $(\widetilde{\Omega}(\rho), \mathcal{M})$, which is the ideal situation where time evolution or noisy transmission of the source state $\widetilde{\Omega}(\rho)$ before measurement at the ends of Alice and Bob is not considered (see Sec. IV), i.e., in principle $(\widetilde{\Omega}, \rho, \mathcal{M}) = (\widetilde{\Omega}(\rho), \mathcal{M})$. If $\{p(a, b|x, y)\}$ obtained from the devices $(\widetilde{\Omega}, \rho, \mathcal{M})$ and $(\widetilde{\Omega}', \rho', \mathcal{M}')$ are the same, then we write $(\widetilde{\Omega}, \rho, \mathcal{M}) = (\widetilde{\Omega}', \rho', \mathcal{M})$. The Hilbert-space dimensions associated with systems involved in the device $(\widetilde{\Omega}', \rho', \mathcal{M}')$ need not be the same as their counterpart systems associated with the honest device $(\widetilde{\Omega}, \rho, \mathcal{M})$. When the two devices $(\widetilde{\Omega}, \rho, \mathcal{M})$ and $(\widetilde{\Omega}', \rho', \mathcal{M}')$ are ε close to each other in the trace-norm distance, we write $(\widetilde{\Omega}, \rho, \mathcal{M}) \approx_\varepsilon (\widetilde{\Omega}', \rho', \mathcal{M}')$.

The device-independent secret key agreement protocols can allow i-way communication for $i \in \{0, 1, 2\}$ depending on whether two allies, Alice and Bob, are allowed to perform i-way classical communication outside the devices [40]. This classical communication includes error correction and parameter estimation rounds. A two-way LOPC (LOPC_2) is a general LOPC channel where both Alice and Bob can send classical communication to each other over authenticated public channel, one-way LOPC (LOPC_1) is a restricted class of LOPC where only one party is allowed to transmit classical communication to the other (while the other remains barred from sending classical communication), and zero-way LOPC ($\mathrm{LOPC}_0 = \mathrm{LO}$) is a very restricted class of LOPC where both parties can perform only local operations and are barred from any classical communication. Therefore, $\mathrm{LO} \subset \mathrm{LOPC}_1 \subset \mathrm{LOPC}_2$. We note that in practice, there is also a need for (classical) communication to agree upon the protocol, and for other purposes like verification and testing.

Apart from the classical communication between Alice and Bob during the key distillation protocol, there also exists the possibility of the classical communication in the device. This classical communication can be based on the inputs from the previous rounds, that can be used by the device to prepare the source state to be measured in the coming round [40]. DI_j denotes the devices where the channel $\widetilde{\Omega}$ is IID, memory is allowed, and use j-way (classical) communication between the input-output rounds for $j \in \{0, 1, 2\}$. This j-way communication can take place either before the inputs are given or after the outputs are obtained. The DI_j devices can share memory locally at Alice and Bob across each round enabling the capability of adversary [40]. We provide definitions and related observations in Appendix C.

While these assumptions of restraining adversarial capabilities may drift from appropriate physical model of device independence, they may provide upper bounds on more capable adversarial models. For the purpose of deriving fundamental limitations, we can accept the trade-off that comes with simplistic assumptions on device-independence protocols. In particular, we can further restrict the adversary such that the device itself is assumed to be IID. We define the IID-device independent variants IDI_j for $j \in \{0, 1, 2\}$, where the devices are IID and are not allowed memory or communication from one round to the next (e.g., see Ref. [40]). Based on these observations, we generalize Definition 1 for the DI-QKD setups with channels in the following way.

Definition 3. *The device-independent secret key agreement (or private) capacity of the device* $(\widetilde{\Omega}, \rho, \mathcal{M})$ *under the assumption of its IID uses assisted with i-way communication between allies outside the device and j-way communication between the input-output rounds within the*

device, is given by

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega},\rho,\mathcal{M}) := \inf_{\varepsilon>0}\limsup_{n\to\infty}\mu_{i,n}^{\mathrm{IDI}_j,\varepsilon}(\widetilde{\Omega},\rho,\mathcal{M}), \quad (69)$$

where $\mu_{i,n}^{\mathrm{IDI}_j,\varepsilon}(\rho,\widetilde{\Omega},\mathcal{M})$ *is the maximum key rate optimized over all viable privacy protocols over the IID uses of device, while also including a minimization over the possible IID devices* IDI_j *that are compatible with the honest device. We have*

$$\mu_{i,n}^{\mathrm{IDI}_j,\varepsilon}(\widetilde{\Omega},\rho,\mathcal{M}) := \sup_{\hat{P}\in \mathrm{CLOPC}_i}\ \inf_{\substack{(\mathcal{N},\widetilde{\Omega}',\sigma)\in \mathrm{IDI}_j\\ (\mathcal{N},\widetilde{\Omega}',\sigma)\approx_\varepsilon(\mathcal{M},\widetilde{\Omega},\rho)}} \kappa_n^\varepsilon(\hat{P},(\mathcal{N},\widetilde{\Omega}',\sigma)), \quad (70)$$

where κ_n^ε *is the rate of achieved* ε*-perfect key and classical labels from local classical operations in* $\hat{P}\in CLOPC_i$ *are possessed by the allies (Alice and Bob).*

Another direct consequence of the IID device-independence assumptions is the following lemma.

Lemma 1. *For any two IID devices,* $(\widetilde{\Omega},\rho,\mathcal{M})$ *and* $(\widetilde{\Omega}',\sigma,\mathcal{N})$*, that are* IDI_j *and compatible to each other, we have*

$$(\widetilde{\Omega}',\sigma,\mathcal{N}) = (\widetilde{\Omega},\rho,\mathcal{M}) \implies \mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega}',\sigma,\mathcal{N}) = \mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega},\rho,\mathcal{M}). \quad (71)$$

The aforementioned definitions are a more realistic variant and generalization of the definitions presented in Ref. [40]. We obtain the definitions in Ref. [40] if we assume bipartite distribution channel $\widetilde{\Omega}=\mathrm{id}_{A'\to A}\otimes\Lambda_{B'\to B}$ and restrict minimization over compatible devices consisting of a channel of the form $\widetilde{\Omega}'=\mathrm{id}\otimes\Lambda'$, where id denotes the identity channel, in the definitions aforementioned.

Lemma 2. *The device-independent secret key capacity* $\mathcal{P}_i^{\mathrm{IDI}_j}$ *of an honest device* $(\widetilde{\Omega},\rho,\mathcal{M})$ *when* $\widetilde{\Omega}_{A'B'\to AB}=\Lambda^1_{A'\to A}\otimes\Lambda^2_{B'\to B}$ *is upper bounded by*

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega},\rho,\mathcal{M}) \le \inf_{\substack{(\widetilde{\Omega}',\sigma,\mathcal{N})\in \mathrm{IDI}_j\\ (\widetilde{\Omega}',\sigma,\mathcal{N})=(\widetilde{\Omega},\rho,\mathcal{M})}} \min\{\mathcal{P}^{\mathrm{DD}}_{\max\{i,j\}}(\Lambda'^1),\mathcal{P}^{\mathrm{DD}}_{\max\{i,j\}}(\Lambda'^2)\}, \quad (72)$$

where $\mathcal{P}_i^{\mathrm{DD}}(\Lambda)$ *is the* $LOPC_i$*-assisted private capacity of the point-to-point channel* Λ *(see, e.g., Refs. [35,37], and Appendix C 1) and* $\widetilde{\Omega}'=\Lambda'^1\otimes\Lambda'^2$.

Corollary 2. *It follows that for all* $i,j\in\{0,1,2\}$*, we have*

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega},\rho,\mathcal{M}) \le \min\{\mathcal{P}_2^{\mathrm{DD}}(\Lambda^1),\mathcal{P}_2^{\mathrm{DD}}(\Lambda^2)\}. \quad (73)$$

Furthermore, if the point-to-point channels Λ^1,Λ^2 *are PPT channels, we have*

$$\mathcal{P}_2^{\mathrm{IDI}_j}(\widetilde{\Omega},\rho,\mathcal{M}) \le \min\left\{\begin{matrix}\mathcal{P}_2^{\mathrm{DD}}(\Lambda^1),\mathcal{P}_2^{\mathrm{DD}}(\Lambda^2),\\ \mathcal{P}_2^{\mathrm{DD}}(\vartheta\circ\Lambda^1),\mathcal{P}_2^{\mathrm{DD}}(\vartheta\circ\Lambda^2)\end{matrix}\right\}, \quad (74)$$

where ϑ *is a partial transposition map, i.e.,* $\vartheta(\rho)=\rho^\Gamma$.

We now restrict to the case of telecovariant channels, which can be defined as in Refs. [50,63] and employed in Ref. [34] in the context of secret key agreement protocols over point-to-point quantum channels. The action of these channels can be simulated via teleportation protocol using resource states as the respective Choi states of the channels (see Ref. [64] and Appendix C for details).

The lemma below follows from the observation that the private capacity of telecovariant channels are upper bounded by the relative entropy of entanglement of the Choi state of the channel [34].

Lemma 3. *Consider a telecovariant distribution channel* $\widetilde{\Omega}_{A'B'\to AB}=\Lambda^1_{A'\to A}\otimes\Lambda^2_{B'\to B}$*, where both point-to-point channels* Λ^1 *and* Λ^2 *are telecovariant. The device-independent secret key capacity* $\mathcal{P}_i^{\mathrm{IDI}_j}$ *of an honest device* $(\widetilde{\Omega},\rho,\mathcal{M})$ *with such a telecovariant distribution channel* $\widetilde{\Omega}_{A'B'\to AB}=\Lambda^1_{A'\to A}\otimes\Lambda^2_{B'\to B}$ *is upper bounded by*

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega},\rho,\mathcal{M}) \le \inf_{\substack{(\widetilde{\Omega}',\sigma,\mathcal{N})\in \mathrm{IDI}_j\\ (\widetilde{\Omega}',\sigma,\mathcal{N})=(\widetilde{\Omega},\rho,\mathcal{M})}} \min\{E_R(\Phi^{\Lambda'^1}),E_R(\Phi^{\Lambda'^2})\}, \quad (75)$$

where $\widetilde{\Omega}'=\Lambda'^1\otimes\Lambda'^2$ *and* $\Phi^{\Lambda'_1}$ *and* $\Phi^{\Lambda'_2}$ *are the Choi states of the channels* Λ'^1 *and* Λ'^2*, respectively. We assume that the channels* Λ'^1 *and* Λ'^2 *are covariant channels.*

A. Some practical prototypes

Let us now focus on three widely considered noise models for the qubit systems: dephasing channel $\mathcal{P}^p$, depolarizing channel $\mathcal{D}^p$, and erasure channel $\mathcal{E}^p$. The actions of these telecovariant channels on the density operators ρ of a qubit system are given as follows.

1. Dephasing channel: $\mathcal{P}^p(\rho)\equiv(1-p)\rho+p\sigma_Z\rho\sigma_Z$, where σ_Z is the Pauli-Z operator.
2. Depolarizing channel: $\mathcal{D}^p(\rho)\equiv(1-p)\rho+p\frac{1}{2}\mathbb{1}$.
3. Erasure channel: $\mathcal{E}^p(\rho)\equiv p\rho+(1-p)|e\rangle\langle e|$, where $|e\rangle\langle e|$ is the erasure symbol, orthonormal to the support of the input state.

Let us now consider that Alice and Bob carry out the CHSH protocol over the channel $\mathrm{id}_{A'\to A}\otimes\Lambda_{B'\to B}$. As discussed above, for CHSH protocols, the relevant statistics are the CHSH violation $\omega(\rho,\mathcal{M})$ and QBER $P_{\mathrm{err}}(\rho,\mathcal{M})$. Thus, for CHSH protocols, the infimum in Eq. (75) is reduced to the tuples $\left(\tilde{\Omega}',\sigma,\mathcal{N}\right)$ that satisfy the CHSH statistics.

We first consider the honest device $\left(\rho,\mathrm{id}_{A'\to A}\otimes\mathcal{D}^p_{B'\to B},\mathcal{M}\right)$. Let $\mathcal{M}$ be an arbitrary but honest measurement considered in the CHSH protocol. Then, the CHSH violation observed by Alice and Bob is given as

$$\omega(\mathcal{D}^p(\rho),\mathcal{M})=(1-p)\omega(\rho,\mathcal{M})+p\omega\left(\frac{1}{4}\mathbb{1},\mathcal{M}\right) \tag{76}$$

$$=(1-p)\omega(\rho,\mathcal{M}). \tag{77}$$

$$\leq(1-p)\max_{\mathcal{M}}\omega(\rho,\mathcal{M})\equiv\omega^\star \tag{78}$$

Here, $\omega(\mathcal{D}^p(\rho),\mathcal{M})$ corresponds to the CHSH violation observed from the statistics obtained if the state $\mathcal{D}^p(\rho)$ is measured by $\mathcal{M}$. The second equality follows from $\omega(\mathcal{M},\frac{1}{4}\mathbb{1})=0$. The QBER associated with the state is $(1-p)P_{\mathrm{err}}(\rho,\mathcal{M})+\frac{1}{2}p$. We thus obtain the limits on the statistics that Alice and Bob would obtain on carrying out a CHSH protocol with the device $\left(\mathrm{id}_{A'\to A}\otimes\mathcal{D}^p_{B'\to B},\rho,\mathcal{M}\right)$.

We now construct a strategy $\left(\mathrm{id}_{A'\to A}\otimes\mathcal{P}^q_{B'\to B},\Phi,\mathcal{M}\right)$, where Φ is a maximally entangled state. By appropriate choice of parameter q and the measurements M^0_a,M^1_a,M^1_b,M^2_b, we can replicate the CHSH violation and P_{err} obtained from carrying out a CHSH protocol with the device $\left(\mathrm{id}_{A'\to A}\otimes\mathcal{D}^p_{B'\to B},\rho,\mathcal{M}\right)$. The noise of the dephasing channel q is chosen as $(1-C)/2$, where $C=\sqrt{(\omega^*/2)^2-1}$. The measurements are given as $M^{1,2}_a=(\sigma_z/\sqrt{1+C^2})\pm(C/\sqrt{1+C^2})\sigma_x$, $M^1_b=\sigma_z$, $M^2_b=\sigma_x$. With this strategy, we obtain the Bell violation $\omega^\star$. For replicating the statistics of QBER, with prob P_{err}, Alice chooses $A_0=\sigma_z$, else she randomly chooses a bit. This strategy has been previously used in Ref. [60] to show tightness of the obtained lower bounds for one-way CHSH protocols. With this strategy, we can replicate the statistics obtained from CHSH protocols performed over depolarizing channels.

Combining the above observations with Eq. (75), we then obtain the following:

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\mathrm{id}_A\otimes\mathcal{D}^p)\leq\min\left\{E_R(\mathcal{P}^{(1-C)/2}(\Phi)),E_R(\mathcal{D}^p(\Phi))\right\} \tag{79}$$

$$\leq\min\left\{1-H\left(\frac{1-C}{2}\right),1-H\left(\frac{3p}{4}\right)\right\}. \tag{80}$$

We also see that the maximum CHSH violation $\omega^\star$ obtained from the depolarizing channel with noise p is $(1-p)2\sqrt{2}$. Substituting $C=\sqrt{\left((1-p)2\sqrt{2}/2\right)^2-1}$ in Eq. (80), we obtain

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\mathrm{id}_A\otimes\mathcal{D}^p)\leq\min\left\{1-H\left(\frac{1}{2}\left(1-\sqrt{1-4p+2p^2}\right)\right),1-H(3p/4)\right\}. \tag{81}$$

We thus obtain that for CHSH protocols, the DI secret key capacity of depolarizing channels is strictly less than the private capacity of the depolarizing channel as can be seen in Fig. 3. Here, we use the upper bounds on the two-way (LOCC-assisted) device-dependent secret-key-agreement capacities for depolarizing and dephasing qubit channels obtained in Ref. [34].

Next, let us consider the erasure channel. Let $\mathcal{M}$ be a set of four measurements. The CHSH violation observed is

$$\omega(\mathcal{E}^p(\rho),\mathcal{M})=(1-p)\omega(\rho,\mathcal{M})+p\omega(|e\rangle\langle e|,\mathcal{M}) \tag{82}$$

$$=(1-p)\omega(\rho,\mathcal{M}). \tag{83}$$

$$\leq(1-p)\max_{\mathcal{M}}\omega(\rho,\mathcal{M})\equiv\omega^\star \tag{84}$$

We thus see that the upper bound on CHSH violation by erasure channel of noise p and the depolarizing channel p are exactly the same. However, the QBER obtained by carrying out the CHSH protocol across the erasure channel and depolarizing channel can be different. We then observe that any value of QBER can be observed by changing the measurement setting with the dephasing channel, as detailed before in the numerics for depolarizing channel. For erasure channels the QBER is zero, so we choose the measurement settings such that the QBER obtained from dephasing channel is also zero. We note that the measurement setting M^0_a that is used to tune the QBER, does not influence the CHSH value that is decided by the values M^1_a,M^2_a,M^1_b, and M^2_b. We thus obtain

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\mathrm{id}_A\otimes\mathcal{E}^p) \tag{85}$$

$$\leq\min\left\{E_R(\mathcal{P}^{(1-C)/2}(\Phi)),E_R(\mathcal{E}^p(\Phi))\right\} \tag{86}$$

$$\leq\min\left\{1-H\left(\frac{1-C}{2}\right),1-p\right\} \tag{87}$$

$$\leq\min\left\{1-H\left(\frac{1}{2}(1-\sqrt{1-4p+2p^2})\right),1-p\right\}. \tag{88}$$

That is, for CHSH protocols, the DI secret key capacity of erasure channels is strictly less than the private capacity of the erasure channels as can be seen in Fig. 3.

It is interesting to observe that in the above analysis, the violation of the CHSH inequality had a vital role in

limiting the CHSH DI capacity across various example channels. Due to the structure of the dephasing channel, which was the attacking channel, the QBER did not end up influencing the upper bounds.

We thus observe that the dephasing channel can simulate the device $(\mathrm{id}\otimes\Lambda,\rho,\mathcal{M})$ with erasure channel or depolarizing channel in a device-independent way for CHSH protocols. This suggests that the outcomes of the device will have statistics that can be explained by the dephasing channel even when the actual channel present inside device is erasure or depolarizing. Hence, it may be in the interest of the manufacturer to use the dephasing channel instead of the other two channels.

VI. UPPER BOUND VIA cc-SQUASHED ENTANGLEMENT

In this section, we study a bound called *reduced* cc-*squashed entanglement*. We prove that the bound is convex, and outperforms both the limitations presented in Refs. [41,42] in a certain regime of noise. In Sec. VI, we introduce an entanglement measure, which we call cc-squashed entanglement and denote as $E_{\mathrm{sq}}^{\mathrm{CC}}$. It does not have a traditional form [65], as it is a function of a *pair* of arguments: a state ρ and measurement $M=M_a\otimes M_b$, i.e., pair of POVMs with outcomes $\{a\}$ and $\{b\}$. We then observe that, this measure is (i) convex (see Lemma 4) and that (ii) (due to known results [45,52]) it upper bounds the device-dependent key of a classical-classical-quantum (CCQ) state $M\otimes\mathrm{id}\,\psi^{\rho}$, where ψ^{ρ} is a purification of ρ to the system of the eavesdropper.

In Sec. VI B by minimizing the cc-squashed entanglement over devices $(\sigma,\mathcal{N})$ that have compatible statistics with honest device $(\rho,\mathcal{M})$ we obtain definition of reduced cc-squashed entanglement measures. There are two versions of them. One comes from the compatibility constraint $(\sigma,\mathcal{N})=(\rho,\mathcal{M})$, and reads

$$E_{\mathrm{sq,dev}}^{\mathrm{CC}}(\rho,\mathcal{M}):=\inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})}E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma,\mathcal{N}(\hat{x},\hat{y})),\tag{89}$$

where $(\hat{x},\hat{y})$ is a pair of inputs from which the raw key is generated in standard DI-QKD protocols [so that $\mathcal{M}(\hat{x},\hat{y})=M_a\otimes M_b$]. We show that it upper bounds the IID device-independent key obtained via measurements $(\hat{x},\hat{y})$, which is defined via minimization over devices satisfying $(\sigma,\mathcal{N})=(\rho,\mathcal{M})$ and is denoted as $K_{\mathrm{DI,dev}}^{\mathrm{IID}}$. Most of the proofs in Sec. VI B are shown for the $K_{\mathrm{DI,dev}}^{\mathrm{IID}}$, as they are simple to state. By analogy to these proofs, we obtain similar properties for the second version of the reduced cc-squashed entanglement, which is more relevant for further considerations. It reads

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho,\mathcal{M}(\hat{x},\hat{y})):=\inf_{\substack{\omega(\sigma,\mathcal{N})=\omega(\rho,\mathcal{M})\\ P_{\mathrm{err}}(\sigma,\mathcal{N})=P_{\mathrm{err}}(\rho,\mathcal{M})}}E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma,\mathcal{N}(\hat{x},\hat{y})).\tag{90}$$

In particular we show that this function is (i) convex, and (ii) upper bounds the IID device-independent key obtained from single input $(\hat{x},\hat{y})$ upon testing that involves estimation of ω and P_{err}. The latter quantity is denoted as $K_{\mathrm{DI,par}}^{\mathrm{IID}}$.

Finally in Sec. VI C we apply the above results to show that the $E_{\mathrm{sq,par}}^{\mathrm{CC}}$ is a lower bound to the plots of the bounds given in Refs. [41,42]. Hence it is tighter bound on $K_{\mathrm{DI,par}}^{\mathrm{IID}}$ (see Theorem 5). Since the bound is convex, we obtain that in the case of Werner states, the convex hull of the plots of the bounds of Refs. [41,42] is an upper bound on the device-independent key rate $K_{\mathrm{DI,par}}^{\mathrm{IID}}$ (see Theorem 2). Due to the observation, which we state below, the convex combination of the plots is an alternative bound shown in Fig. 1.

We argue below, that the convex hull of two plots of the functions is below the convex combination of these plots treated as sets of points. In our applications the two plots will be the ones given in Refs. [41,42] as upper bounds for $K_{\mathrm{DI,par}}^{\mathrm{IID}}$.

Observation 2. *For two functions $f_1,f_2:[0,\infty)\to R_+$, let $g:[0,\infty)\to R_+$ be the largest convex function, which is less than or equal to the* $\min(f_1,f_2)$. *Then, for any $p\in[0,1]$ and $x_1,x_2\in[0,\infty)$ such that $f_1(x_1)\leq f_2(x_1)$ and $f_1(x_2)\geq f_2(x_2)$, there is*

$$g(px_1+(1-p)x_2)\leq pf_1(x_1)+(1-p)f_2(x_2).\tag{91}$$

Proof : We have the following chain of the (in)equalities, which we explain below:

$$\begin{aligned}g(px_1+(1-p)x_2)&\leq pg(x_1)+(1-p)g(x_2)\\&\leq p\min(f_1(x_1),f_2(x_1))+(1-p)\min(f_1(x_2),f_2(x_2))\end{aligned}\tag{92}$$

$$=pf_1(x_1)+(1-p)f_2(x_2)\tag{93}$$

The first inequality is due to convexity of g. The second is by assumption, that g is below the minimum of f_1 and f_2. The equality holds because of the assumption that for x_1, f_1 is less than or equal to f_2 and for x_2 it is converse. ■

A. cc-squashed entanglement and its properties

In what follows, we define an entanglement measure that takes as an input a bipartite state and a pair M_{AB} of POVMs $\{M_a\}_a$ and $\{M_b\}_b$, which act on systems locally, $M_{AB}:=M_a\otimes M_b$.

Definition 4. *A cc-squashed entanglement of a bipartite state ρ_{AB} reads $E_{\mathrm{sq}}(\rho_{AB},M)$ is defined as follows:*

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\rho,M):=\inf_{\Lambda:E\to E'}I(A:B|E')_{M_{AB}\otimes\Lambda_E\psi^{\rho}_{ABE}},\tag{94}$$

where M_{AB} is a pair of POVMs $M=M_a\otimes M_b$, and $\psi^{\rho}_{ABE}:=|\psi^{\rho}\rangle\langle\psi^{\rho}|_{ABE}$ is a state purification of ρ_{AB}.

Following Ref. [30], we observe first the following.

Observation 3. *For a bipartite state ρ_{AB} and a pair of POVMs $M = M_a \otimes M_b$, there is*

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\rho_{AB}, M) = \inf_{\rho_{ABE}=\mathrm{Ext}(\rho_{AB})} I(A:B|E)_{M\otimes \mathrm{id}_E\, \rho_{ABE}}, \quad (95)$$

where $\mathrm{Ext}(\rho_{AB})$ *is an arbitrary state extension of* ρ_{AB} *to system E, i.e.,* ρ_{ABE} *is a state such that* $\mathrm{Tr}_E[\rho_{ABE}] = \rho_{AB}$.

Proof : Following Ref. [30]: to see that Eq. (94)≤(95) we note that every extension can be obtained from the purifying system by an appropriate channel. Indeed, we first note that $|\psi\rangle_{ABEE''}$, which purifies ρ_{ABE} is related by an isometry to any state purification $|\psi^{\rho}\rangle$ of ρ_{AB}. Hence, a channel performing this isometry and tracing out E'' generates an extension ρ_{ABE}. Thus, the infimum in Eq. (94), which varies over Λ_E acting on ψ^{ρ} can be seen as optimization over the set of arbitrary extensions measured by M on AB, as it is the case in Eq. (95). Note that we use the fact that measurements M are the same in both formulas, and the extension in Eq. (95) is taken before the measurement.

Conversely, we have also Eq. (94)≥(95), because application of a channel on system E of a purified state ψ^{ρ}, results in an extension $\rho_{ABE'}$. ■

Owing to the above observation, we can see that the cc-squashed entanglement is convex, as stated in the lemma below.

Lemma 4. *For a pair of measurements M, two states* ρ_{AB} *and* ρ'_{AB}, $0 < p < 1$, *there is*

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\bar{\rho}_{AB}, M) \leq pE_{\mathrm{sq}}^{\mathrm{CC}}(\rho_{AB}, M) + (1-p)E_{\mathrm{sq}}^{\mathrm{CC}}(\rho'_{AB}, M), \quad (96)$$

where $\bar{\rho}_{AB} = p\rho_{AB} + (1-p)\rho'_{AB}$.

Proof : Consider first two tripartite extensions of the form:

$$\rho_1 := \rho_{ABE}, \quad (97)$$

$$\rho_2 := \rho'_{ABE} \quad (98)$$

of ρ_{AB} and ρ'_{AB}, respectively. Consider then the state of the following form:

$$\rho_{ABEF} = M \otimes \mathrm{id}_{EF}(p\rho_1 \otimes |0\rangle\langle 0|_F + (1-p)\rho_2 \otimes |1\rangle\langle 1|_F). \quad (99)$$

Note that it is a measured extension of the state $\bar{\rho}_{AB}$. Indeed, by linearity of the partial trace, tracing out over systems F and E we obtain the p-weighted mixture of states ρ_{AB} and ρ'_{AB}, measured by M, which is the measured state $\bar{\rho}_{AB}$.

By Observation 3 we can use the definition of $E_{\mathrm{sq}}^{\mathrm{CC}}$ based on extensions rather than channels. In what follows we go along similar lines to Refs. [30,39].

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\bar{\rho}_{AB}, M) = \inf_{\rho_{ABE}=\mathrm{Ext}(\bar{\rho}_{AB})} I(A:B|E)_{M\otimes \mathrm{id}_E\, \rho_{ABE}} \leq I(A:B|EF)_{\rho_{ABEF}} \quad (100)$$

$$= pI(A:B|E)_{M\otimes \mathrm{id}_E\, \rho_1} + (1-p)I(A:B|E)_{M\otimes \mathrm{id}_E\, \rho_2} \quad (101)$$

In the above we first narrow the infimum to a particular extension ρ_{ABEF}. The equality follows from the fact that system F is classical, and conditioning over such a system yields an average value of the conditional mutual information. We also have used linearity of measurement M:

$$\rho_{ABEL} = pM \otimes \mathrm{id}_{EF}\, \rho_1 \otimes |0\rangle\langle 0| + (1-p)M \otimes \mathrm{id}_{EF}\, \rho_2 \otimes |1\rangle\langle 1|, \quad (102)$$

to separate terms in Eq. (101). Since the extensions ρ_1 and ρ_2 were arbitrary, we can also take infimum over them, obtaining

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\bar{\rho}_{AB}, M) \leq p \inf_{\rho_{ABE}=\mathrm{Ext}(\rho_{AB})} I(A:B|E)_{M\otimes \mathrm{id}_E\, \rho_{ABE}} + (1-p) \inf_{\rho'_{ABE}=\mathrm{Ext}(\rho'_{AB})} I(A:B|E)_{M\otimes \mathrm{id}_E\, \rho'_{ABE}}. \quad (103)$$

Again by Observation 3 on the rhs we have $pE_{\mathrm{sq}}^{\mathrm{CC}}(\rho_{AB}, M) + (1-p)E_{\mathrm{sq}}^{\mathrm{CC}}(\rho'_{AB}, M)$, hence the assertion follows. ■

Following Ref. [45, Theorem 3.5] and Ref. [52, Lemma 7] we obtain the following.

Theorem 4 ([45])**.** *For a bipartite state* ρ, *its purified state* ψ^{ρ}, *and a pair of measurements M, there is*

$$K_{\mathrm{DD}}(M \otimes \mathrm{id}\, \psi^{\rho}) \leq E_{\mathrm{sq}}^{\mathrm{CC}}(\rho, M). \quad (104)$$

Proof : The proof boils down to invoking Ref. [45, Theorem 3.5] and Ref. [52, Lemma 7] for a tripartite CCQ state $\rho_{\mathrm{CCQ}} := M \otimes \mathrm{id}\, \psi^{\rho}$, and noticing that $I(A:B\downarrow E)_{\rho_{\mathrm{CCQ}}} = E_{\mathrm{sq}}^{\mathrm{CC}}(\rho, M)$. ■

B. Reduced cc-squashed entanglement

In this section we use the cc-squashed entanglement to define its reduced version and prove the convexity of the latter, and that it bounds the $K^{\mathrm{IID}}_{\mathrm{DI,dev/par}}$.

To see the application of the cc-squashed entanglement we need the following fact.

Lemma 5. *The IID quantum device-independent key achieved by protocols using single pair of measurements $(\hat{x},\hat{y})$ applied to $\mathcal{M}$ of a device $(\rho,\mathcal{M})$, is upper bounded as follows:*

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev}}(\rho,\mathcal{M}) := \inf_{\epsilon>0}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}}\inf_{(\sigma,\mathcal{N})\approx_\epsilon(\rho,\mathcal{M})} \kappa_n^{\epsilon,(\hat{x},\hat{y})}(\mathcal{P}(N(\sigma)^{\otimes n}) \leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_{\mathrm{DD}}(\mathcal{N}(\hat{x},\hat{y})\otimes \mathrm{id}\,\psi^\sigma), \tag{105}$$

where $N\equiv\mathcal{N}(\hat{x},\hat{y})$ is a single pair of measurements induced by inputs $(\hat{x},\hat{y})$ on $\mathcal{N}$ and where $\kappa_n^{\varepsilon(\hat{x},\hat{y})}$ is the rate of achieved ε-perfect key and classical labels from local classical operations in $\hat{P}\in$ CLOPC are possessed by the allies (Alice and Bob).

Proof :

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev}}(\rho,\mathcal{M}) = \inf_{\epsilon>0}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}}\inf_{(\sigma,\mathcal{N})\approx_\epsilon(\rho,\mathcal{M})} \kappa_n^{\epsilon,(\hat{x},\hat{y})}(\mathcal{P}(N(\sigma)^{\otimes n})) \tag{106}$$

$$\leq \inf_{\epsilon>0}\inf_{(\sigma,\mathcal{N})\approx_\epsilon(\rho,\mathcal{M})}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}} \kappa_n^{\epsilon,(\hat{x},\hat{y})}(\mathcal{P}(N(\sigma)^{\otimes n})) \tag{107}$$

$$\leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})}\inf_{\epsilon>0}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}} \kappa_n^{\epsilon,(\hat{x},\hat{y})}(\mathcal{P}(N(\sigma)^{\otimes n})) = \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_{\mathrm{DD}}(\mathcal{N}(\hat{x},\hat{y})\otimes \mathrm{id}\,\psi^\sigma). \tag{108}$$

In the above we first use the max-min inequality for sup and limsup [40]. We then narrow infimum to devices that ideally mimic the device $(\rho,\mathcal{M})$. We further notice that the key $\kappa_n^{\epsilon,(\hat{x},\hat{y})}(\mathcal{P}(N(\sigma)^{\otimes n}))$, where the supremum is taken over LOPC protocols, equals the device-dependent key of a tripartite CCQ state $N\otimes \mathrm{id}\,\psi_\sigma$. ■

The LOPC protocols considered in the above definition consist of the error correction and parameter amplification in the DI-QKD protocols over the CCQ state $\mathcal{N}(\hat{x},\hat{y})\otimes \mathrm{id}\psi^\sigma$. We assume that the test rounds and the key generation rounds are known to Eve due to classical communication carried out by Alice and Bob. We should specify that the distinction in the rounds was not known prior to the preparation of the device. This knowledge becomes available to the eavesdropper after Alice and Bob have performed the measurements and classically communicated with each other. This extra knowledge of distinction between test rounds and key generation rounds is instrumental in obtaining tighter upper bounds for DI-QKD protocols.

Due to Theorem 4, Ref. [52, Lemma 7], and the above lemma we have immediate corollary.

Corollary 3. *The IID quantum device-independent key achieved by protocols using single pair of measurements $(\hat{x},\hat{y})$ applied to $\mathcal{M}$ of a device $(\rho,\mathcal{M})$, is upper bounded as follows:*

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev}}(\rho,\mathcal{M}) \leq \inf_{(\sigma,\mathcal{N})\equiv(\rho,\mathcal{M})} E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,\mathcal{N}(\hat{x},\hat{y})) \tag{109}$$

$$=: E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M}(\hat{x},\hat{y})). \tag{110}$$

Observation 4. *If two quantum devices $(\rho,\mathcal{M})$ and $(\sigma,\mathcal{N})$ are such that $(\rho,\mathcal{M})=(\sigma,\mathcal{N})$ then*

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev}}(\rho,\mathcal{M}) = K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,dev}}(\sigma,\mathcal{N}), \tag{111}$$

$$E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M}(\hat{x},\hat{y})) = E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\sigma,\mathcal{N}(\hat{x},\hat{y})) \tag{112}$$

for any valid choice of $(\hat{x},\hat{y})$.

We now pass to study the upper bounds provided in Refs. [41,42]. We first note that in Ref. [41] conditions of equal CHSH value ω and QBER P_{err} are considered instead of equality of attacking and honest device. It is straightforward to adopt the above corollary to this case.

Corollary 4. *The IID quantum device-independent key achieved by protocols using a single pair of measurements $(\hat{x},\hat{y})$ applied to $\mathcal{M}$ of a device $(\rho,\mathcal{M})$, is upper bounded as follows:*

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}(\rho,\mathcal{M}) := \inf_{\epsilon>0}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}}\inf_{\substack{\omega(\sigma,\mathcal{N})\approx_\epsilon\omega(\rho,\mathcal{M})\\ P_{\mathrm{err}}(\sigma,\mathcal{N})\approx_\epsilon P_{\mathrm{err}}(\rho,\mathcal{M})}} \kappa_n^{\epsilon,(\hat{x},\hat{y})}(\mathcal{P}(N(\sigma)^{\otimes n})) \tag{113}$$

$$\leq \inf_{\substack{\omega(\sigma,\mathcal{N})=\omega(\rho,\mathcal{M})\\ P_{\mathrm{err}}(\sigma,\mathcal{N})=P_{\mathrm{err}}(\rho,\mathcal{M})}} E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,N) =: E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y})), \tag{114}$$

where $N=\mathcal{N}(\hat{x},\hat{y})$ is a single pair of measurements induced by inputs $(\hat{x},\hat{y})$ on $\mathcal{N}$.

We show that $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$ is equal to the bound [41, Eq. (19)] in Appendix D 1.

Observation 5. *If two quantum devices* $(\rho,\mathcal{M})$ *and* $(\sigma,\mathcal{N})$ *are such that* $\omega(\rho,\mathcal{M})=\omega(\sigma,\mathcal{N})$ *and* $P_{\mathrm{err}}(\rho,\mathcal{M})=P_{\mathrm{err}}(\sigma,\mathcal{N})$ *then*

$$K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}(\rho,\mathcal{M})=K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}(\sigma,\mathcal{N}), \tag{115}$$

$$E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))=E^{\mathrm{CC}}_{\mathrm{sq,par}}(\sigma,\mathcal{N}(\hat{x},\hat{y})), \tag{116}$$

for any valid choice of $(\hat{x},\hat{y})$. *This is to say that* $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$ *is a function explicitly depending on only two parameters* ω *and* P_{err}.

The quantity defined in Eq. (113) $K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}$ depends on the choice of Bell inequality and its violation ω and quantum bit error rate P_{err}. For further considerations one can assume that P_{err} is computed as $P(a\neq b|\hat{x},\hat{y})$, as the key is generated by $(\hat{x},\hat{y})$, however ω remains a free parameter. In any case, not to overload the notation, we refrain from decorating definition of $K^{\mathrm{IID},(\hat{x},\hat{y})}_{\mathrm{DI,par}}$ by ω, and make ω explicitly known from the context if needed (e.g., see Theorem 6).

It will appear crucial for the main Theorem 2 to prove that $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$ is convex, which we show in the lemma below.

Lemma 6. *The* $E^{\mathrm{CC}}_{\mathrm{sq,par}}$ *is convex, i.e., for every device* $(\bar{\rho},\mathcal{M})$ *and an input pair* $(\hat{x},\hat{y})$ *there is*

$$\begin{aligned}E^{\mathrm{CC}}_{\mathrm{sq,par}}(\bar{\rho},\mathcal{M}(\hat{x},\hat{y}))\leq p_1E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho_1,\mathcal{M}(\hat{x},\hat{y}))\\ +p_2E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho_2,\mathcal{M}(\hat{x},\hat{y})),\end{aligned} \tag{117}$$

where $\bar{\rho}=p_1\rho_1+p_2\rho_2$ *and* $p_1+p_2=1$ *with* $0\leq p_1\leq 1$.

Proof : Let us fix two strategies $(\sigma_1,\mathcal{N}_1)$ and $(\sigma_2,\mathcal{N}_2)$ such that $\omega(\sigma_i,\mathcal{N}_i)=\omega(\rho_i,\mathcal{M})$ and $P_{\mathrm{err}}(\sigma_i,\mathcal{N}_i)=P_{\mathrm{err}}(\rho_i,\mathcal{M})$. Consider also a state $\bar{\sigma}=p_1\sigma_1\otimes|00\rangle\langle 00|_{A'B'}+p_2\sigma_2\otimes|11\rangle\langle 11|_{A'B'}$, and a joint strategy $\mathcal{N}=\mathcal{N}_1\otimes|00\rangle\langle 00|_{A'B'}+\mathcal{N}_2\otimes|11\rangle\langle 11|_{A'B'}$. We note then that by linearity of ω, there is

$$\omega(\bar{\sigma},\mathcal{N})=\omega\left(\sum_i p_i\,\mathrm{Tr}\,\mathcal{N}_i\sigma_i\right)= \tag{118}$$

$$\sum_i p_i\omega(\sigma_i,\mathcal{N}_i)=\sum_i p_i\omega(\rho_i,\mathcal{M})=\omega(\bar{\rho},\mathcal{M}), \tag{119}$$

where in the prelast equality we use the fact that strategies $(\sigma_i,\mathcal{N}_i)$ reproduces statistics of $(\rho_i,\mathcal{M})$, respectively. Analogously we obtain

$$P_{\mathrm{err}}(\bar{\sigma},\mathcal{N})=P_{\mathrm{err}}(\bar{\rho},\mathcal{M}). \tag{120}$$

This implies that

$$E^{\mathrm{CC}}_{\mathrm{sq,par}}(\bar{\rho},\mathcal{M}(\hat{x},\hat{y}))\leq E^{\mathrm{CC}}_{\mathrm{sq}}(\bar{\sigma},\mathcal{N}(\hat{x},\hat{y})) \tag{121}$$

since infimum over strategies is less than the value of the function taken in the particular strategy described above by $(\bar{\sigma},\mathcal{N})$. We use further convexity of the $E^{\mathrm{CC}}_{\mathrm{sq}}$ function proved in Lemma 4 to get

$$\begin{aligned}E^{\mathrm{CC}}_{\mathrm{sq,par}}(\bar{\rho},\mathcal{M}(\hat{x},\hat{y}))\leq p_1E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_1\otimes|00\rangle\langle 00|_{A'B'},\mathcal{N}(\hat{x},\hat{y}))\\ +p_2E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_2\otimes|11\rangle\langle 11|_{A'B'},\mathcal{N}(\hat{x},\hat{y})).\end{aligned} \tag{122}$$

We further note that by definition of $\mathcal{N}$ there is

$$E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_1\otimes|00\rangle\langle 00|_{A'B'},\mathcal{N}(\hat{x},\hat{y}))=E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_1,\mathcal{N}_1(\hat{x},\hat{y})). \tag{123}$$

Indeed, $\mathcal{N}(\hat{x},\hat{y})(\sigma_1\otimes|00\rangle\langle 00|)=\mathcal{N}_1(\hat{x},\hat{y})\sigma_1\otimes|00\rangle\langle 00|$. Below we have a slight change in notation. From here on instead of $I(A:B|E)_\rho$, we use $I(A;B|E)[\rho]$. We also represent the purification ψ^σ_{ABE} as $\psi^{ABE}(\sigma)$. Hence, denoting by $\psi(\sigma)$ a purification of a state σ we get

$$\begin{aligned}&E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_1\otimes|00\rangle\langle 00|_{A'B'},\mathcal{N}(\hat{x},\hat{y}))\\ &=E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_1\otimes|00\rangle\langle 00|_{A'B'},\mathcal{N}_1(\hat{x},\hat{y})\otimes\mathrm{id}_{A'B'})\\ &=\inf_{\Lambda:E\to E'}I(AA':BB'|E')[(\mathcal{N}_1(\hat{x},\hat{y})\otimes\mathrm{id}_{A'B'}\otimes\Lambda_E)\\ &\psi^{ABA'B'E}(\sigma_1\otimes|00\rangle\langle 00|_{A'B'})]\\ &=\inf_{\Lambda:E\to E'}I(AA':BB'|E')[(\mathcal{N}_1(\hat{x},\hat{y})\otimes\mathrm{id}_{A'B'}\otimes\Lambda_E)\\ &\psi^{ABE}(\sigma_1)\otimes|00\rangle\langle 00|_{A'B'})]\\ &=\inf_{\Lambda:E\to E'}I(A:B|E')[\mathcal{N}_1(\hat{x},\hat{y})\otimes\Lambda_E\psi^{ABE}(\sigma_1)]\\ &=E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma_1,\mathcal{N}(\hat{x},\hat{y})).\end{aligned} \tag{124}$$

In the second last equality we use the fact that $I(AA':BB'|E')[\rho_{\mathrm{CCQ}}\otimes|00\rangle\langle 00|_{A'B'}]$ with $\rho_{\mathrm{CCQ}}:=(\mathcal{N}_1(\hat{x},\hat{y})\otimes\mathrm{id}_{A'B'}\otimes\Lambda_E)\psi^{ABE}(\sigma_1)$ equals just $I(A:B|E')[\rho_{\mathrm{CCQ}}]$ since the pure state $|00\rangle\langle 00|_{A'B'}$ does not alter the von Neumann entropies involved in definition of the conditional mutual

information. Similarly,

$$E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma_2 \otimes |11\rangle\langle 11|_{A'B'}, \mathcal{N}(\hat{x},\hat{y})) = E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma_2, \mathcal{N}_2(\hat{x},\hat{y})). \tag{125}$$

Hence, there is

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\bar{\rho}, \mathcal{M}(\hat{x},\hat{y})) \leq p_1 E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma_1, \mathcal{N}_1(\hat{x},\hat{y})) + p_2 E_{\mathrm{sq}}^{\mathrm{CC}}(\sigma_2, \mathcal{N}_2(\hat{x},\hat{y})). \tag{126}$$

Now, since strategies $(\sigma_i, \mathcal{N}_i)$ were arbitrary within their constraints, we obtain

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\bar{\rho}, \mathcal{M}(\hat{x},\hat{y})) \leq p_1 E_{\mathrm{sq,par}}^{\mathrm{CC}}(\sigma_1, \mathcal{N}_1(\hat{x},\hat{y})) + p_2 E_{\mathrm{sq,par}}^{\mathrm{CC}}(\sigma_2, \mathcal{N}_2(\hat{x},\hat{y})), \tag{127}$$

hence the assertion follows. ■

C. Application of the reduced squashed entanglement

We now observe that the upper bounds *plotted* in Refs. [41,42] are upper bounds on $E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y}))$. We denote the plotted functions as $I_{AL}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y}))$ and $I_{FBJL+}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y}))$, respectively. That means, if $E_{\mathrm{sq,par}}^{\mathrm{CC}}$ was plotted, it would be below both the bounds given in these articles.

Theorem 5. *For any device* $(\rho, \mathcal{M})$ *and input* $\mathcal{M}(\hat{x},\hat{y})$*, there is*

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})) \leq I_{AL}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})), \tag{128}$$

$$E_{\mathrm{sq,dev}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})) \leq I_{FBJL+}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})), \tag{129}$$

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})) \leq E_{\mathrm{sq,dev}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})). \tag{130}$$

Proof : Let us first note that the last inequality from the above follows from the fact, that the set over which infimum is taken in definition of $E_{\mathrm{sq,dev}}^{\mathrm{CC}}$ is contained in the set over which infimum is taken in definition of $E_{\mathrm{sq,par}}^{\mathrm{CC}}$.

To obtain Eq. (128), observe that the bound calculated in Ref. [41] is

$$I(A;B|E)_{M_A \otimes M_B \otimes \mathrm{id}_E \psi^{\sigma}_{ABE}}, \tag{131}$$

where $M_A = \sigma_z$, $M_B = \sigma_z$ with probability $1 - 2P_{\mathrm{err}}$ and a random bit with probability $2P_{\mathrm{err}}$. Here, ψ^{σ} is the purification of the state

$$\sigma = \frac{1+C}{2}|\Phi^+\rangle\langle\Phi^+|_{AB} + \frac{1-C}{2}|\Phi^-\rangle\langle\Phi^-|_{AB}, \tag{132}$$

$$\left|\Phi^{\pm}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \tag{133}$$

$$C = \sqrt{\left(\frac{\omega}{2}\right)^2 - 1}. \tag{134}$$

We then obtain the following set of inequalities:

$$E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho, \mathcal{M}(\hat{x},\hat{y})) \equiv \inf_{\substack{\omega(\sigma,\mathcal{N})=\omega(\rho,\mathcal{M}) \\ P_{\mathrm{err}}(\sigma,\mathcal{N})=P_{\mathrm{err}}(\rho,\mathcal{M})}} \inf_{\Lambda: E \to E'} I(A:B|E')_{M_{AB} \otimes \Lambda_E \psi^{\sigma}_{ABE}} \tag{135}$$

$$\leq I(A;B|E)_{M_A \otimes M_B \otimes \mathrm{id}_E \psi^{\sigma}_{ABE}}. \tag{136}$$

This follows by choosing particular strategies as specified above, where we choose the state given in Eq. (132), and by choosing $\Lambda_{E \to E'}$ as identity.

For the plot I_{FBJL+}, we first note that the FBJŁKA bound [42] works for the protocols where the measurements are projective and announced after the protocol. If we then fix a single measurement $(\hat{x},\hat{y})$, we can consider this to be known to Eve. In principle, in this case, Alice and Bob need not to announce the test rounds, as they can use a sublinear amount of private key needed for authentication to encrypt this information. However whenever test rounds (and so key rounds) are available to Eve, she can measure all her shares as if they were key rounds. This strategy will lead to the same bound as if Alice and Bob publicly announced testing and/or key rounds.

The device $p(ab|xy)$ against which the honest parties (implicitly) perform test in Ref. [42], is quantum, hence it is expected to be $(\rho, \mathcal{M})$ for some honest realization via measuring $\mathcal{M}$ on ρ promised by provider (e.g., a Werner state of some dimension, and the measurements of CHSH inequality). But it can be in fact equal to any $(\sigma, \mathcal{N})$ such that $(\sigma, \mathcal{N}) = (\rho, \mathcal{M})$. The idea of Ref. [42] is to represent the device $p(ab|xy)$ as convex combination of local and nonlocal part, where the local part is a mixture of local conditional distributions, i.e.,

$$p(ab|xy) = \sum_{i=0}^{k-1} p_i P_{\mathrm{L}}^{(i)}(ab|xy) + q P_{\mathrm{NL}}(ab|xy), \tag{137}$$

where $\sum_{i=0}^{k-1} p_i + q = 1$ for some natural k, $\{P_{\mathrm{L}}^{(i)}(ab|xy)\}_i$ is a set of local conditional distributions and $P_{\mathrm{NL}}(ab|xy)$

is the nonlocal part of the device $p(ab|xy)$. In what follows, for the clarity of argument we first assume that P_{L}^{i} are deterministic. That is, for every i and x, y $P_D^{(i)}(ab|xy) = \delta_{(a,b),(a_i^x,b_i^y)}$. That is, for every input the outcomes are (a_i^x, b_i^y) with probability 1. We further relax this assumption to local distributions in Remark 4.

Since the devices in the above convex combination are quantum, they admit quantum representation so that there exist collections of measurements $\mathcal{N}_{\mathrm{L}}^{(i)} = \{N_a^{x,(i)} \otimes N_b^{y,(i)}\}_{x,y}$ and $\mathcal{N}_{\mathrm{NL}} = \{N_a^{x,(\mathrm{NL})} \otimes N_b^{y,(\mathrm{NL})}\}_{x,y}$ and states σ_i as well as σ_{NL} such, that

$$\begin{aligned} P_D^{(i)}(ab|xy) &= \mathrm{Tr}\,\mathcal{N}_{\mathrm{L}}^{(i)}\sigma_i \\ P_{\mathrm{NL}}(ab|xy) &= \mathrm{Tr}\,\mathcal{N}_{\mathrm{NL}}\sigma_{\mathrm{NL}} \end{aligned} \tag{138}$$

We can then define a strategy, which realizes splitting of a device $p(ab|xy)$ into the above devices. To this end let us define

$$\sigma_{ABA'B'} = \sum_{i=0}^{k-1} p_i\sigma_i \otimes |ii\rangle\langle ii|_{A'B'} + q\sigma_{\mathrm{NL}}|kk\rangle\langle kk|_{A'B'} \tag{139}$$

and

$$\mathcal{N} = \sum_{i=0}^{k-1} \mathcal{N}_{\mathrm{L}}^{(i)} \otimes |ii\rangle\langle ii|_{A'B'} + \mathcal{N}_{\mathrm{NL}} \otimes |kk\rangle\langle kk|_{A'B'}. \tag{140}$$

By definition there is $(\sigma, \mathcal{N}) = \mathrm{Tr}\left(\sum_i p_i \mathcal{N}_{\mathrm{L}}^{(i)}\sigma_{\mathrm{L}}^{i} + q\mathcal{N}_{\mathrm{NL}}\sigma_{\mathrm{NL}}\right) = \sum_i p_i P_D^{(i)}(ab|xy) + qP_{\mathrm{NL}}(ab|xy) = (\mathcal{M}, \rho)$.

We are ready to define an *extension* of the state $\sigma_{ABA'B'}$ to systems EE' of Eve, which realizes distribution $p(abe|x,y)$ as defined in Ref. [42, Eq. (3)], given Eve learns (x,y).

$$\begin{aligned} \sigma_{ABA'B'EE'} = &\sum_{i=0}^{k-1} p_i\sigma_i \otimes |ii\rangle\langle ii|_{A'B'} \otimes \sigma_i^E \otimes |i\rangle\langle i|_{E'} \\ &+ q\sigma_{\mathrm{NL}} \otimes |kk\rangle\langle kk|_{A'B'} \otimes |?\rangle\langle ?|_E \otimes |k\rangle\langle k|_{E'}, \end{aligned} \tag{141}$$

where $\sigma_i^E = \sigma_i$ for all $i \in \{0, \ldots, k-1\}$.

Given the system E' is in state $|i\rangle\langle i|$ with $i \in \{0, \ldots, k\}$, the state of Alice and Bob collapses to σ_{AB}^k or σ_{NL}, respectively. Then, either $i = k$ so she learns $|?\rangle\langle ?|$, i.e., nothing from E, or $i < k$ and Eve measures $\sigma_i^E = \sigma_i$ according to $\mathcal{N}_{\mathrm{L}}^{(i)}(x,y)$ and learn the (deterministic) outputs of Alice and Bob a_i^x, b_i^y. Note here, that due to the fact that outputs of Alice and Bob are deterministic, Eve can learn them from a copy of the state σ_i, given she performs the same measurement as they do.

In particular, if the key-generation input is single, equal to $(\hat{x}, \hat{y})$, Alice, Bob, and Eve can generate from $\sigma_{ABA'B'EE'}$ a distribution $p(abe|\hat{x}\hat{y})$, where $e \in \mathcal{A} \times \mathcal{B} \cup \{?\}$, where $\mathcal{A}$ and $\mathcal{B}$ are the alphabets of outputs of Alice and Bob's device given input $(\hat{x}, \hat{y})$. Further, as proposed in Ref. [42], depending on the state of the system E', Eve applies a particular postprocessing map $\Lambda_{E|E'}^{\mathrm{post}} : E \to E''$ on her classical outputs $\delta_{(a_i^x,b_i^y),e}$ and symbol "?" mapping them to symbols $\{\bar{e}\}$ in order to minimize the value of $I(A : B|E'')_{p(ab\bar{e}|\hat{x}\hat{y})}$ on such obtained distribution $p(ab\bar{e}|\hat{x}\hat{y})$.

It is known, that any extension of a bipartite quantum state can be obtained by a CPTP map applied to its purifying system. Hence, there exists a map Λ_E^{ext} which produces from a purification of σ_{AB} denoted as $|\psi_{ABE}^{\sigma}\rangle$, the extension in state $\sigma_{ABA'B'EE'}$. This map composed with the measurement $\mathcal{N}_{\mathrm{L}}^{i}(\hat{x}, \hat{y})$ on the Eve system, followed by $\Lambda_{E|E'}^{\mathrm{post}}$ and tracing out register E' results in desired final distribution $p(ab\bar{e}|\hat{x}\hat{y})$.

To summarize, the distribution $p(ab\bar{e}|\hat{x}\hat{y})$ can be obtained by applying $\mathcal{N}(\hat{x}, \hat{y})$ on systems AB and $\Lambda_E^{\mathrm{tot}} := \mathrm{Tr}_{E'} \circ \Lambda_{E|E'}^{\mathrm{post}} \circ \mathcal{N}_{\mathrm{L}}(\hat{x}, \hat{y})_{E|E'} \circ \Lambda_E^{\mathrm{ext}}$ on system E of the purification $|\psi_{ABE}^{\sigma}\rangle$ of σ_{AB}. Here by $\mathcal{N}_{\mathrm{L}}(\hat{x}, \hat{y})_{E|E'}$ we mean that given E' is in state $|i\rangle$, $\mathcal{N}_{\mathrm{L}}^{(i)}(\hat{x}, \hat{y})$ is measured on system E. We thus have

$$\begin{aligned} I(A : B|E'')_{p(ab\bar{e}|\hat{x}\hat{y})} &= I(A : B|E)_{\mathcal{N}(\hat{x},\hat{y}) \otimes \Lambda_E^{\mathrm{tot}}|\psi_{ABE}^{\sigma}\rangle} \\ &\geq \inf_{\Lambda : E \to E''} I(A : B|E'')_{\mathcal{N}(\hat{x},\hat{y}) \otimes \Lambda|\psi_{ABE}^{\sigma}\rangle} \\ &= E_{\mathrm{sq}}(\sigma, \mathcal{N}(\hat{x}, \hat{y})) \\ &\geq \inf_{(\sigma,\mathcal{N}) = (\rho,\mathcal{M})} E_{\mathrm{sq}}(\sigma, \mathcal{N}(\hat{x}, \hat{y})) \\ &\equiv E_{\mathrm{sq,dev}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x}, \hat{y})). \end{aligned} \tag{142}$$

It suffices to note that the plot of I_{FBJL+} visualizes the values of the function $I(A : B|E'')_{p(ab\bar{e}|\hat{x}\hat{y})}$ attained on the distribution $p(ab\bar{e}|\hat{x}, \hat{y})$. Hence due to the above inequalities we obtain

$$I_{FBJL+}(\rho, \mathcal{M}(\hat{x}, \hat{y})) \geq E_{\mathrm{sq,dev}}^{\mathrm{CC}}(\rho_{AB}, \mathcal{M}(\hat{x}, \hat{y})). \tag{143}$$

■

We show in Appendix D 2, how to fit our results to exactly reproduce the results of Ref. [42].

As a corollary there comes the following fact.

Corollary 5. *For any device $(\rho, \mathcal{M})$ and a pair of inputs generating the key $(\hat{x}, \hat{y})$, there is*

$$K_{\mathrm{DI,par}}^{\mathrm{IID},(\hat{x},\hat{y})}(\rho, \mathcal{M}) \leq E_{\mathrm{sq,par}}^{\mathrm{CC}}(\rho, \mathcal{M}(\hat{x}, \hat{y})) \tag{144}$$

$$\leq \min\{I_{AL}(\rho, \mathcal{M}(\hat{x}, \hat{y})), I_{FBJL+}(\rho, \mathcal{M}(\hat{x}, \hat{y}))\} \tag{145}$$

Proof : It holds due to Corollary 4 and Theorem 5. ■

We are ready to state the main Theorem of this section. In what follows we narrow considerations to $(\mathcal{M}, (\hat{x}, \hat{y}))$ being *projective*, as the bound for Werner states presented in Ref. [42] applies only to this case.

Theorem 6. *For a Werner state ρ_{AB}^{W} and $\mathcal{M}$ consisting of projective measurements $P_a^x \otimes P_b^y$, and a pair of inputs $(\hat{x}, \hat{y})$ used to generate the key, there is*

$$K_{\mathrm{DI,par}}^{\mathrm{IID},(\hat{x},\hat{y})}(\rho_{AB}^{W}, \mathcal{M}) \leq \mathrm{Conv}(I_{AL}(\rho_{AB}^{W}, \mathcal{M}(\hat{x}, \hat{y})), I_{FBJL+}(\rho_{AB}^{W}, \mathcal{M}(\hat{x}, \hat{y}))), \tag{146}$$

where $\mathrm{Conv}(F_1, F_2)$ *is the convex hull of the plots of functions* F_i, *and* $K_{\mathrm{DI,par}}^{\mathrm{IID},(\hat{x},\hat{y})}(\rho_{AB}^{W}, \mathcal{M})$ *is defined with respect to* $\omega = CHSH$ *and* $P_{\mathrm{err}} = P(a \neq b|\hat{x}\hat{y})$.

Proof : For the proof it suffices to note that by Corollary 5 we have

$$\begin{aligned} K_{\mathrm{DI,par}}^{\mathrm{IID},(\hat{x},\hat{y})}(\rho_{AB}^{W}, \mathcal{M}) &\leq E_{\mathrm{sq,par}}^{\mathrm{CC}}(\sigma, \mathcal{M}(\hat{x}, \hat{y})) \\ &\leq \min\{I_{AL}(\sigma_{AB}, \mathcal{M}(\hat{x}, \hat{y})), I_{FBJL+} \\ &\quad \times (\sigma_{AB}, \mathcal{M}(\hat{x}, \hat{y}))\}. \end{aligned} \tag{147}$$

Now, by Lemma 6 the $E_{\mathrm{sq,par}}^{\mathrm{CC}}$ is convex. It is also below the plots of $I_{AL}(\sigma_{AB}, \mathcal{M}(\hat{x}, \hat{y}))$ and $I_{FBJL+}(\sigma_{AB}, \mathcal{M}(\hat{x}, \hat{y})$, due to the above inequality. As such, it must be below their convex hull. It also upper bounds the key, hence the key must be below the convex hull of the plots of I_{AL} and I_{FBJL+} as well. ■

We extend out approach to a greater number of measurements in Appendix E.

VII. DISCUSSION

We develop tighter bounds on the DI-QKD rate in the case of protocols with single measurement for generating the raw key. Extending this result for more measurements (see lower bounds studied in Ref. [20]), would be the next step. We also develop tighter bounds based on the relative entropy of entanglement for the general DI-QKD protocols. The upper bounds developed in this work are essential to understand the fundamental limitations of CHSH-based DI-QKD protocols. Our findings suggest that protocols that consider the full correlation or only one of the parties announces the inputs could potentially offer an improvement over key rates in device-independent protocols. It is, therefore, worthwhile to explore more general protocols. Developing further on the relative entropic bound, we use it to derive tighter limitations on the DI-QKD rate of bipartite states and setups with quantum channels. This line of approach can be helpful in the development of device-independent internet. In this case, it may be of interest to the manufacturer to know the equivalence of dephasing, erasure, and the depolarizing noises for the device-independent key. This can be particularly useful in choosing the error-correction codes to encode quantum information in the context of quantum repeaters. Our techniques can be generalized to the multipartite case and will form a future direction.

ACKNOWLEDGMENTS

KH thanks Anubhav Chaturvedi for discussion and Tamoghna Das for valuable insight in the topic of upper bounds on device-independent quantum key distribution rates. We thank Marek Winczewski for correcting the initial plot of Fig. 1.

Part of this work is performed at the Institute for Quantum Computing (IQC), University of Waterloo, which is supported by Innovation, Science and Economic Development Canada. EK acknowledges support by NSERC under the Discovery Grants Program, Grant No. 341495. We acknowledge partial support by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. MAB/2018/5, co-financed by EU within Smart Growth Operational Programme). The "International Centre for Theory of Quantum Technologies" project (Contract No. MAB/2018/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3). SD acknowledges Individual Fellowship at Université libre de Bruxelles; this project receives funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 801505.

APPENDIX A: OBSERVATIONS RELATED TO THE DI-QKD RATE

Definition 5. *In this section we present some observations, which follow from the definition of* $K_{\mathrm{DI}}^{\mathrm{IID}}$, *that can be of independent interest.*

The maximum device-independent key distillation rate $K_{\mathrm{DI}}^{\mathrm{IID}}$ *of a bipartite state* ρ_{AB} *is given by*

$$K_{\mathrm{DI}}^{\mathrm{IID}}(\rho) = \sup_{\mathcal{M}} K_{\mathrm{DI}}^{\mathrm{IID}}(\rho, \mathcal{M}). \tag{A1}$$

Observation 6. *We note that there may exist states* ρ *for which* $K_{\mathrm{DI}}^{\mathrm{IID}}(\rho) = 0$ *but* $K_{\mathrm{DI}}^{\mathrm{IID}}(\rho^{\otimes k}) > 0$ *for some* $k \in \mathbb{N}$.

A bipartite state ρ that is positive under partial transposition (PPT), i.e., $\rho^{\Gamma} \geq 0$, is called a PPT state. Similarly, a point-to-point channel Λ is called a PPT channel if $\Lambda \circ \vartheta$ is also a quantum channel [47,48], where ϑ is a partial transposition map, i.e., $\vartheta(\rho) = \rho^{\Gamma}$. There exists bipartite

entangled states, which are PPT [51,66,67]. However, all PPT states are useless for the task of entanglement distillation via LOCC even if they are entangled [47,48,51].

A direct consequence of Lemma 7 is the following corollary (see Ref. [40] for the proof argument made for $\leq$).

Corollary 6. *For any bipartite state ρ that is PPT, we have* $K_{\mathrm{DI}}^{\mathrm{IID}}(\rho) = K_{\mathrm{DI}}^{\mathrm{IID}}(\rho^{\Gamma})$.

The following lemma follows from the definition of $K_{\mathrm{DI}}^{\mathrm{IID}}$ (see Ref. [40] for the proof argument made for $\leq$):

Lemma 7. *The maximum device-independent key rate $K_{\mathrm{DI}}^{\mathrm{IID}}$ of a device $(\rho_{AB}, \mathcal{M})$ is equal to the maximum device-independent key rate of a device $(\sigma, \mathcal{N})$ when $(\rho, \mathcal{M}) = (\sigma, \mathcal{N})$:*

$$(\rho, \mathcal{M}) = (\sigma, \mathcal{N}) \implies K_{\mathrm{DI}}^{\mathrm{IID}}(\rho, \mathcal{M}) = K_{\mathrm{DI}}^{\mathrm{IID}}(\sigma, \mathcal{N}). \tag{A2}$$

APPENDIX B: PROOF FOR PROPOSITION 2

First, we can write $\rho = p\rho_1 + (1-p)\rho_2$. Let us fix two strategies $(\sigma_1, \mathcal{N}_1)$ and $(\sigma_2, \mathcal{N}_2)$ such that $\omega(\sigma_i, \mathcal{N}) = \omega(\rho_i, \mathcal{M})$ and $P_{\mathrm{err}}(\sigma_i, \mathcal{N}_i) = P_{\mathrm{err}}(\rho_i, \mathcal{M}_i)$. Consider also a state $\overline{\sigma} = p\sigma_1 \otimes |00\rangle\langle 00|_{A'B'} + (1-p)\sigma_2 \otimes |11\rangle\langle 11|_{A'B'}$, and a joint strategy $\mathcal{N} \equiv \mathcal{N}_1 \otimes |00\rangle\langle 00|_{A'B'} \otimes \mathcal{N}_2 \otimes |11\rangle\langle 11|_{A'B'}$. We note than that by linearity of ω, there is $\omega(\bar{\sigma}, \mathcal{N}) = \omega(\bar{\rho}, \mathcal{N})$. Analogously, we can also note that $P_{\mathrm{err}}(\bar{\sigma}, \mathcal{N}) = P_{\mathrm{err}}(\bar{\rho}, \mathcal{N})$. This implies, by the convexity of the relative entropy of entanglement, that

$$\inf_{\substack{\omega(\bar{\sigma},\mathcal{N})=\omega(\bar{\rho},\mathcal{N}) \\ P_{\mathrm{err}}(\bar{\sigma},\mathcal{N})=P_{\mathrm{err}}(\bar{\rho},\mathcal{N})}} E_R(\sigma) \leq E_R(\bar{\sigma}) \tag{B1}$$

$$\leq pE_R(\sigma_1) + (1-p)E_R(\sigma_2). \tag{B2}$$

Since the choice of σ_1 and σ_2 was arbitrary, we obtain

$$\inf_{\substack{\omega(\bar{\sigma},\mathcal{N})=\omega(\bar{\rho},\mathcal{N}) \\ P_{\mathrm{err}}(\bar{\sigma},\mathcal{N})=P_{\mathrm{err}}(\bar{\rho},\mathcal{N})}} E_R(\sigma) \leq E_R(\bar{\sigma}) \tag{B3}$$

$$\leq p \inf_{\substack{\omega(\sigma_1,\mathcal{N})=\omega(\rho_1,\mathcal{M}) \\ P_{\mathrm{err}}(\sigma_1,\mathcal{N})=P_{\mathrm{err}}(\rho_1,\mathcal{M})}} E_R(\sigma_1) \tag{B4}$$

$$+ (1-p) \inf_{\substack{\omega(\sigma_2,\mathcal{N})=\omega(\rho_2,\mathcal{M}) \\ P_{\mathrm{err}}(\sigma_2,\mathcal{N})=P_{\mathrm{err}}(\rho_2,\mathcal{M})}} E_R(\sigma_2). \tag{B5}$$

In particular, if we chose $\rho = p\rho^{\mathrm{L}} + (1-p)\rho^{\mathrm{NL}}$, we recover the statement of the proposition.

APPENDIX C: BOUNDS ON DI-QKD SETUPS WITH CHANNELS

In this section, we supplement the discussions and results in Sec. V. We provide upper bounds on the DI-QKD rates for the realistic scenarios by taking the dynamical processes (i.e., quantum channels) within the device into account.

For the dynamical devices, i.e., DI-QKD setups with consideration of channels inside the box, we have,

$$(\widetilde{\Omega}, \rho, \mathcal{M}) = (\widetilde{\Omega}', \rho', \mathcal{M}') \iff p_{(\widetilde{\Omega},\rho,\mathcal{M})} = p_{(\widetilde{\Omega}',\rho',\mathcal{M}')}, \tag{C1}$$

$$(\widetilde{\Omega}, \rho, \mathcal{M}) \approx_{\varepsilon} (\widetilde{\Omega}', \rho', \mathcal{M}') \iff p_{(\widetilde{\Omega},\rho,\mathcal{M})} \approx_{\varepsilon} p_{(\widetilde{\Omega}',\rho',\mathcal{M}')}. \tag{C2}$$

If an honest device $(\widetilde{\Omega}, \rho, \mathcal{M})$ constituting channels is being used just for a single round (where the bipartite distribution channel $\widetilde{\Omega}$ is called just once) then it is the same as an honest device $(\widetilde{\Omega}(\rho), \mathcal{M})$, which is the ideal situation where time evolution or noisy transmission of the source state $\widetilde{\Omega}(\rho)$ before measurement at the ends of Alice and Bob is not considered (see Sec. IV). That is $(\widetilde{\Omega}, \rho, \mathcal{M}) = (\widetilde{\Omega}(\rho), \mathcal{M})$ for a single round where the device uses the channel just once.

Definition 6. *The device-independent secret key agreement (or private) capacity of the device $(\widetilde{\Omega}, \rho, \mathcal{M})$ assisted with i-way communication between allies outside the device and j-way communication between the input-output rounds within the device, is given by*

$$\mathcal{P}_i^{\mathrm{DI_j}}(\widetilde{\Omega}, \rho, \mathcal{M}) := \inf_{\varepsilon>0} \limsup_{n\to\infty} \mu_{i,n}^{\mathrm{DI_j},\varepsilon}(\widetilde{\Omega}, \rho, \mathcal{M}), \tag{C3}$$

where $\mu_{i,n}^{\mathrm{DI_j},\varepsilon}(\widetilde{\Omega}, \rho, \mathcal{M})$ is the maximum key rate optimized over all viable privacy protocols with security parameter ε, while also including a minimization over the possible devices DI_j that are compatible with the honest device.

Definition 7. *The device-independent capacities $\mathcal{P}_i^{\mathrm{DI_j}}$ and $\mathcal{P}_i^{\mathrm{IDI}_j}$ of a bipartite distribution channel $\widetilde{\Omega}$ for the device DI_i and IDI_j, respectively, are defined as*

$$\mathcal{P}_i^{\mathrm{DI_j}}(\widetilde{\Omega}) := \sup_{\rho,\mathcal{M}} \mathcal{P}_i^{\mathrm{DI_j}}(\widetilde{\Omega}, \rho, \mathcal{M}), \tag{C4}$$

$$\mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega}) := \sup_{\rho,\mathcal{M}} \mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega}, \rho, \mathcal{M}). \tag{C5}$$

Remark 3. *We note that*

$$\mathcal{P}_i^{\mathrm{DI_j}}(\widetilde{\Omega}, \rho, \mathcal{M}) \leq \mathcal{P}_i^{\mathrm{IDI}_j}(\widetilde{\Omega}, \rho, \mathcal{M}) \tag{C6}$$

as

$$\mu_{i,n}^{\mathrm{DI_j},\varepsilon}(\widetilde{\Omega}, \rho, \mathcal{M}) \leq \mu_{i,n}^{\mathrm{IDI}_j,\varepsilon}(\widetilde{\Omega}, \rho, \mathcal{M}). \tag{C7}$$

1. Bounds on DI-QKD rates in terms of private capacities of the channels

The main objective of a device-dependent private protocol is to distribute secret keys between two or more trusted allies over quantum channels in the presence of a quantum eavesdropper (e.g., see Ref. [37]). Traditionally, the secret key agreement between Alice and Bob is over $\mathrm{id}_{A'\to A'}\otimes\Lambda_{A\to B}$, where the notion is that Alice transmits a part of composite system in joint state over channel $\Lambda_{A\to B}$ to Bob. It is assumed that the system A' does not undergo noisy evolution. Alice and Bob are allowed to use channels n times and make use of adaptive strategy by interleaving each call of channel with LOPC_i. In the end of the protocol, Alice and Bob perform LOPC_i to distill the secret key between them. However, in practice, even local systems with Alice could undergo noisy quantum evolution. Therefore, we need to consider quantum and private communication over bipartite quantum distribution channels of the form $\Lambda^1\otimes\Lambda^2$ rather than restricting to the bipartite quantum distribution channels of the form $\mathrm{id}\otimes\Lambda^2$.

Let us now consider a device-dependent quantum communication protocol where the goal is for a relay station to transfer prepared entangled state to two allies, Alice and Bob, such that Alice and Bob can distill secret keys between themselves, which is secure from a quantum eavesdropper and the relay station. We can assume that an arbitrary bipartite state $\rho_{A'B'}$ is available at relay station to Charlie. Charlie may operate bipartite quantum distribution channel $\Omega_{A'B'\to A''B''}$ on the state $\rho_{A'B'}$, and is an untrusted party. Charlie then transmits quantum systems A'', B'' in the joint state $\Omega(\rho)$ to trusted allies Alice and Bob, respectively, over quantum channels $\Lambda^1_{A''\to A}, \Lambda^2_{B''\to B}$. In general, all three parties can perform i'-way LOPC ($\mathrm{LOPC}_{i'}$) among themselves in an adaptive strategy, where $i'\in\{0,1,2\}$. Charlie can make n uses of channel $\widetilde{\Omega}=\Lambda^1\otimes\Lambda^2\circ\Omega$ interleaved with $\mathrm{LOPC}_{i'}$ between each round (i.e., each call of the channel). At the end of the protocol, the goal is for Alice and Bob to get the state from which secret key is readily accessible upon local measurements. The secret key distillable at the end of Alice and Bob can be ε close to the ideal secret key.

Definition 8. *The device-dependent privacy distribution capacity $\mathcal{R}_{i'}$ over a bipartite quantum distribution channel $\widetilde{\Omega}$ assisted with i'-way communication ($\mathrm{LOPC}_{i'}$) among Charlie, Alice, and Bob for $i'\in\{0,1,2\}$ is defined as*

$$\mathcal{R}_{i'}(\widetilde{\Omega}):=\inf_{\varepsilon>0}\limsup_{n\to\infty}\nu^{\varepsilon}_{i',n}(\widetilde{\Omega}), \tag{C8}$$

where $\nu^{\varepsilon}_{i',n}(\widetilde{\Omega})$ is the maximum ε-perfect key rate obtained among all possible repeatable privacy protocols (assisted with i'-way communication $\mathrm{LOPC}_{i'}$ among the relay station and the trusted allies) that uses channel $\widetilde{\Omega}$ n times.

Device-dependent privacy distribution capacity over $\mathrm{id}_{A'\to A'}\otimes\Lambda_{A\to B}$, where Alice herself is at the relay station and sender to Bob, with LOPC_i assistance reduces to device-dependent LOPC_i-assisted private capacity $\mathcal{P}^{\mathrm{DD}}_i(\Lambda)$ over point-to-point quantum channel Λ.

Observation 7. *The device-dependent privacy distribution capacity R_i over a bipartite quantum distribution channel $\widetilde{\Omega}=\Lambda^1\otimes\Lambda^2$ is upper bounded by the device-dependent private capacity over point-to-point channels Λ^1 and Λ^2, i.e.,*

$$\mathcal{R}_i(\widetilde{\Omega})\le\min\{\mathcal{P}^{\mathrm{DD}}_i(\Lambda^1),\mathcal{P}^{\mathrm{DD}}_i(\Lambda^2)\}. \tag{C9}$$

The protocol for the privacy distribution over $\Lambda^1\otimes\Lambda^2$ reduces to secret key agreement protocols over Λ^1 or Λ^2 if we assume $\Lambda^2=\mathrm{id}$ with Bob at relay station as sender or $\Lambda^1=\mathrm{id}$ with Alice at the relay station as the sender, respectively. Under such reduction of the protocol, a lesser amount of information is leaked to a quantum eavesdropper as a part of a noisy evolution becomes noiseless.

Lemma 8. *The device-independent secret key capacities $\mathcal{P}^{\mathrm{DI_j}}_i$ and $\mathcal{P}^{\mathrm{IDI}_j}_i$ of a device $(\widetilde{\Omega},\rho,\mathcal{M})$ in terms of optimized privacy distribution capacity $\mathcal{R}_{\max\{i,j\}}$ are*

$$\mathcal{P}^{\mathrm{DI_j}}_i(\widetilde{\Omega},\rho,\mathcal{M})\le\inf_{\substack{(\widetilde{\Omega}',\sigma,\mathcal{N})\in\mathrm{IDI}_j\\(\widetilde{\Omega}',\sigma,\mathcal{N})=(\widetilde{\Omega},\rho,\mathcal{M})}}\mathcal{R}_{\max\{i,j\}}(\widetilde{\Omega}'), \tag{C10}$$

$$\mathcal{P}^{\mathrm{IDI}_j}_i(\widetilde{\Omega},\rho,\mathcal{M})\le\inf_{\substack{(\widetilde{\Omega}',\sigma,\mathcal{N})\in\mathrm{IDI}_j\\(\widetilde{\Omega}',\sigma,\mathcal{N})=(\widetilde{\Omega},\rho,\mathcal{M})}}\mathcal{R}_{\max\{i,j\}}(\widetilde{\Omega}'). \tag{C11}$$

We omit the proof of the above lemma as proof arguments are similar to the proof of Ref. [40, Eqs. (47) and (49)].

2. Telecovariant channels

Definition 9. *Let G be a group with unitary representation $g\to U^g_A$ on $\mathcal{H}_A$ and $g\to V^g_B$ on $\mathcal{H}_B$. A quantum channel $\Lambda_{A\to B}$ is covariant with respect to the unitary group $\{\mathcal{U}_g\}_{g\in\mathcal{G}}$ if*

$$V^g_B\Lambda(\cdot)V^{g\dagger}_B=\Lambda\left(U^g_A(\cdot)U^{g\dagger}_A\right). \tag{C12}$$

If a quantum channel $\Lambda_{A\to B}$ satisfies Eq. (C12) such that the unitary group G is a one design, i.e.,

$$\frac{1}{|G|}\sum_{g\in G}U^g_A\rho_A U^{g\dagger}_A=\frac{1}{|A|}\mathbb{1}_A\quad\forall\rho_A, \tag{C13}$$

then $\Lambda_{A\to B}$ is said to be telecovariant.

A channel that is covariant with respect to one-design unitaries can be simulated via LOCC and the Choi state of the channel as a shared resource state [64]. That is,

$$\Lambda_{A\to B}(\rho_A) = \mathcal{L}_{AA'\to B}\left(\Phi^{\Lambda}_{A'B}\otimes\rho_A\right), \tag{C14}$$

where $\mathcal{L}_{AA'\to B}$ is a LOCC channel, with the classical communication being from A to B and $\Phi^{\Lambda}_{A'B}:=\Lambda(\Phi^{+}_{A'A})$ is the Choi state of the channel. The above equation informally implies that any quantum communication via the channel Λ is equivalent to sharing the Choi state Φ^{Λ} followed by local operations and classical communication.

APPENDIX D: ON RELATION TO PRIOR RESULTS

This section is devoted to relating our results to the ones obtained in Refs. [38,41,42]. We show that $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$ is equal to the bound [41, Eq. (19)]. We then show how our Theorem 5 relates to the approach of Ref. [42]. Finally we discuss the relation of our approach to that of Ref. [38].

1. Comparison with the approach of [41]

In this section, we argue that the $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$ is equal to the bound [41, Eq. (19)]. Before that we invoke the notation of Ref. [41], where $(\sigma_{ABE},\mathcal{M}(\hat{x},\hat{y}))\in\hat{\Sigma}(\omega^*,Q^*)$ iff $\mathrm{tr}_E(\sigma_{ABE},\mathcal{M}(\hat{x},\hat{y})\otimes\mathrm{id}_E)=q(ab|\hat{x}\hat{y})$ where $\omega(q(ab|\hat{x}\hat{y}))=\omega^*$ and $P_{\mathrm{err}}(q(ab|\hat{x}\hat{y}))=Q^*$.

The bound of Ref. [41] reads

$$\mathcal{I}_{\mathrm{par}}(\omega^*,Q^*,\hat{x},\hat{y}) := \inf_{\sigma\in\hat{\Sigma}(\omega^*,Q^*)} I(A;B\downarrow E)_{\sigma(\hat{x},\hat{y})}, \tag{D1}$$

where the quantity $I(A:B\downarrow E):=\inf_{\Lambda:E\to E'} I(A:B|E')_{\sigma(\hat{x},\hat{y})}$ is computed on a state σ_{ABE} measured with $\mathcal{M}(\hat{x},\hat{y})$ on AB for some measurements $\mathcal{M}$.

The equivalence is encapsulated in the following theorem.

Theorem 7. *Let $(\rho,\mathcal{M})$ be a quantum device with parameters ω^*,Q^* where Q^* is computed based on the inputs $(\hat{x},\hat{y})$. Then there is*

$$E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y})) = \mathcal{I}(\omega^*,Q^*,\hat{x},\hat{y}) \tag{D2}$$

for any choice of the inputs $(\hat{x},\hat{y})$.

Proof : In what follows we can fix $(\hat{x},\hat{y})$ arbitrarily. We first prove that for any quantum realization $(\rho,\mathcal{M})$ of a device with parameters ω^*,Q^*, there is $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$ is a lower bound to $\mathcal{I}(\omega^*,Q^*,\hat{x},\hat{y})$. To this end, let us assume that the infimum in $\mathcal{I}$ is achieved for a pair $(\widetilde{\sigma}_{ABE},\widetilde{\mathcal{M}}(x,y))\in\hat{\Sigma}(\omega^*,Q^*)$. We then observe that for $\widetilde{\rho}_{AB}:=\mathrm{tr}_E\widetilde{\sigma}_{ABE}$, there is

$$\mathcal{I}_{\mathrm{par}}(\omega^*,Q^*,\hat{x},\hat{y}) = I(A:B\downarrow E)_{(\widetilde{\sigma}_{ABE},\widetilde{\mathcal{M}}(\hat{x},\hat{y}))} \tag{D3}$$

$$\geq E^{\mathrm{CC}}_{\mathrm{sq}}(\widetilde{\rho}_{AB},\widetilde{\mathcal{M}}(\hat{x},\hat{y})) \tag{D4}$$

$$\geq \inf_{\substack{\omega(\sigma,\mathcal{N})=\omega(\widetilde{\rho},\widetilde{\mathcal{M}})\\ P_{\mathrm{err}}(\sigma,\mathcal{N}(\hat{x},\hat{y}))=P_{\mathrm{err}}(\widetilde{\rho},\widetilde{\mathcal{M}}(\hat{x},\hat{y}))}} E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,\mathcal{N}(\hat{x},\hat{y})) \tag{D5}$$

$$\geq \inf_{\substack{\omega(\sigma,\mathcal{N})=\omega(\rho,\mathcal{M})\\ P_{\mathrm{err}}(\sigma,\mathcal{N}(\hat{x},\hat{y}))=P_{\mathrm{err}}(\rho,\mathcal{M}(\hat{x},\hat{y}))}} E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,\mathcal{N}(\hat{x},\hat{y})) \tag{D6}$$

$$= E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y})), \tag{D7}$$

where the first inequality comes from the fact, that channels $\Lambda:E\to E'$ in definition of $E^{\mathrm{CC}}_{\mathrm{sq}}$ are acting on a purification of $\widetilde{\rho}_{AB}=\mathrm{tr}_E\widetilde{\sigma}_{ABE}$ hence can achieve a lower value than channels acting on system E of $\widetilde{\sigma}_{ABE}$. The next inequality is just by taking infimum, while the last is due to the fact that $(\rho_{AB},\mathcal{M}),(\widetilde{\rho}_{AB},\widetilde{\mathcal{M}})\in\hat{\Sigma}(\omega^*,Q^*)$.

We prove now the converse inequality. Let $(\sigma_{AB},\mathcal{N})$ be a pair achieving infimum in definition of the $E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y}))$. In particular there is $\omega(\sigma,\mathcal{N})=\omega(\rho,\mathcal{M})=\omega^*$ by assumption and $P_{\mathrm{err}}(\sigma,\mathcal{N})=P_{\mathrm{err}}(\rho,\mathcal{M})=Q^*$. And hence $(\psi^{\sigma},\mathcal{N})\in\hat{\Sigma}(\omega^*,Q^*)$. We have then

$$E^{\mathrm{CC}}_{\mathrm{sq,par}}(\rho,\mathcal{M}(\hat{x},\hat{y})) = E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,\mathcal{N}(\hat{x},\hat{y})) \tag{D8}$$

$$= I(A:B\downarrow E)_{(\psi^{\sigma},\mathcal{N}(\hat{x},\hat{y}))} \tag{D9}$$

$$\geq \inf_{\sigma'\in\hat{\Sigma}(\omega^*,Q^*)} I(A:B\downarrow E)_{\sigma'(\hat{x},\hat{y})} \tag{D10}$$

$$= \mathcal{I}_{\mathrm{par}}(\omega^*,Q^*,\hat{x},\hat{y}), \tag{D11}$$

hence the assertion follows. ■

In Ref. [41] [see Eq. (18) there] there is also defined a quantity, which is equivalent to $E^{\mathrm{CC}}_{\mathrm{sq,dev}}$. It reads in our notation

$$\mathcal{I}_{\mathrm{dev}}(p(ab|\hat{x}\hat{y})) := \inf_{\sigma\in\Sigma(p(ab|\hat{x}\hat{y}))} I(A;B\downarrow E)_{\sigma(\hat{x},\hat{y})}, \tag{D12}$$

where $\sigma_{ABE}\in\Sigma(p(ab|\hat{x}\hat{y}))$ iff there exists a measurement $\mathcal{M}$ such that $\mathrm{tr}_E(\sigma_{ABE}\mathcal{M}\otimes\mathrm{id}_E)=p(ab|xy)$. Analogous proof to the above, with $\hat{\Sigma}$ replaced by Σ and optimization over ω and P_{err} reduced to optimization over compatible devices, leads to the following equivalence.

Theorem 8. *For any quantum realization* $(\rho, \mathcal{M})$ *of a device* $p(ab|xy)$ *and pair of inputs* $(\hat{x}, \hat{y})$*, there is*

$$\mathcal{I}_{\text{dev}}(p(ab|\hat{x}\hat{y})) = E^{\text{CC}}_{\text{sq,dev}}(\rho, \mathcal{M}(\hat{x}, \hat{y})). \tag{D13}$$

2. Correspondence with Ref. [42]

In this section we present two remarks showing how to fit our approach to *exactly* reproduce results of Ref. [42] (however not necessarily in optimal way with respect to finding upper bounds on the key rate). We first extend the proof of Theorem 5 to the case of splitting into local rather than deterministic devices.

Remark 4. *In the case where the devices in Eq. (137) are not deterministic, one can explicitly specify* σ_i *and* $\mathcal{N}^{(i)}_{\text{L}}$ *as it is explained below, with all other parts of the proof of Theorem 5 unchanged. For each* $i \in \{0, \ldots, k-1\}$*, there exists a splitting of* $P^{(i)}_{\text{L}}(ab|xy)$ *into deterministic devices*

$$P^{(i)}_{\text{L}}(ab|xy) = \sum_j q^{(i)} P^{(ij)}_D(a|x) P^{(ij)}_D(b|y). \tag{D14}$$

We can then explicitly realize the deterministic devices as

$$P^{(ij)}_D(a|x) = \text{Tr}\, \sigma^{(ij)}_A \mathcal{N}^x_{a,\text{L}}, \tag{D15}$$

where $\sigma^{(ij)}_A = \otimes_{l=1}^{|\mathcal{X}|} |a^{(ij)}_l\rangle\langle a^{(ij)}_l|_{A_l}$*, and*

$$\mathcal{N}^x_{a,\text{L}} = \{P_{A_x} \otimes \text{id}_{A_{l\neq x}}\}, \tag{D16}$$

$$\mathcal{N}^y_{b,\text{L}} = \{P_{B_y} \otimes \text{id}_{B_{l\neq y}}\}, \tag{D17}$$

where P_l *projects system* A_l *(or* B_l*, respectively) onto computational basis. Having defined analogously* $P_D(b|y)$*, we can define the state* $\sigma_{ABA'B'}$ *as follows:*

$$\sigma_{ABA'B'} = \sum_{i=0}^{k-1} p_i \left(\sum_j q^{(i)}_j \sigma^{(ij)}_A \otimes \sigma^{(ij)}_B \right) \otimes |ii\rangle\langle ii|_{A'B'} + q\sigma_{\text{NL}} \otimes |kk\rangle\langle kk|_{A'B'}, \tag{D18}$$

where $\sum_j q^{(i)}_j \sigma^{(ij)}_A \otimes \sigma^{(ij)}_B =: \sigma_i$*.*
With

$$\mathcal{N}^{(i)}_{\text{L}}(x, y) = \mathcal{N}^x_{a,\text{L}} \otimes \mathcal{N}^y_{b,\text{L}} \tag{D19}$$

for all $i \in \{0, \ldots, k-1\}$ *already defined, and* $\mathcal{N}$ *defined as in Eq. (140), we have again* $(\sigma_{ABA'B'}, \mathcal{N}) = \text{Tr}(\sum_i p_i \mathcal{N}^{(i)}_{\text{L}} \sigma_i + q\mathcal{N}_{\text{NL}} \sigma_{\text{NL}}) = (\mathcal{M}, \rho)$*.*

We can also define extension of the state $\sigma_{ABA'B'}$ *to Eve's systems* $E_A E_B$ *as shown below.*

$$\begin{aligned}\sigma_{ABA'B'E_AE_BE'} = \sum_{i=0}^{k-1} \sum_j & p_i q^{(i)}_j \sigma^{(ij)}_A \otimes \sigma^{(ij)}_B \otimes |ii\rangle\langle ii|_{A'B'} \\ & \otimes \sigma^{(ij)}_{E_A} \otimes \sigma^{(ij)}_{E_B} \otimes |i\rangle\langle i|_{E'} + q\sigma_{\text{NL}} \\ & \otimes |kk\rangle\langle kk|_{A'B'} \\ & \otimes |?\rangle\langle ?|_{E_A} \otimes |?\rangle\langle ?|_{E_B} \otimes |k\rangle\langle k|_{E'},\end{aligned} \tag{D20}$$

where $\sigma^{(ij)}_{E_A} = \sigma^{(ij)}_A$ *and* $\sigma^{(ij)}_{E_B} = \sigma^{(ij)}_B$*. Note, that given knowledge of* (x, y) *Eve can measure* $\mathcal{N}^{(i)}_{\text{L}}(x, y)$ *on her systems* $E_A E_B$ *and learn the outcomes of Alice and Bob.*

We have therefore specified a tripartite quantum state, from which Alice, Bob, and Eve generate the distribution $p(abe|xy)$ *as it is specified in Ref. [42, Eq. (3)]. In this distribution Eve is fully correlated to the outcomes of local devices, and is fully uncorrelated (having symbol "?") with the nonlocal device. The remaining part of the proof of Theorem 5 is the same as shown before.*

In the remark below we argue that our approach presented in Theorem 5 is slightly more general than that of Ref. [42].

Remark 5. *In fact the register* E' *is not used in Ref. [42]. There, the distribution* $P(ab\bar{e}|\hat{x}\hat{y})$ *depends only from the outputs* (a, b) *and "?" and not on the number of a deterministic device that produces this output. The system* E' *appeared in our discussion as a mean to realize the condition of Ref. [42] that Eve should obtain the outputs of Alice and Bob in the case when the device shared by them is local. Whether one can achieve this goal without additional information held by the index i is possible, we leave as an open problem. We also keep system* E' *and its use in the description (proof of Theorem 5) due to the fact that it shows that Eve has more knowledge, that may lead to potentially tighter upper bounds.*

3. Comparison with the intrinsic nonlocality of Ref. [38]

As the second conclusion from the above theorem there comes the fact that for any family of plots of the upper bound via the average intrinsic information given in Ref. [42], the device-independent key is below their convex hull.

As we see above $E^{\text{CC}}_{\text{sq,dev}}(\rho, \mathcal{M}, p(x, y)$ as well as intrinsic nonlocality [38] are based on conditional mutual information where the Eve system is an extension system of underlying strategy. For completeness, we give here the definition of the quantum intrinsic nonlocality as introduced in Ref. [38].

Definition 10. *The quantum intrinsic nonlocality of a correlation $p(a,b|x,y)$ is defined as*

$$N^{Q}(p(a,b|x,y)) = \sup_{p(x,y)} \inf_{\rho_{\bar{A}\bar{B}XYE}} I(\bar{A};\bar{B}|XYE)_{\rho}, \tag{D21}$$

where

$$\rho_{\bar{A}\bar{B}XYE} = \sum_{x,y,a,b} p(x,y)p(a,b|x,y)|a\rangle\langle a|_{\bar{A}} \otimes |b\rangle\langle b|_{\bar{B}} \otimes |x\rangle \times \langle x|_X \otimes |y\rangle\langle y|_Y \otimes \rho_E^{a,b,x,y}. \tag{D22}$$

Here, $p(a,b|x,y)\rho_E^{a,b,x,y} = \mathrm{Tr}_{AB}\left[(\Lambda_a^x \otimes \Lambda_b^y)\rho_{ABE}\right]$ and ρ_{ABE} is the extension of ρ_{AB}.

The major differences between the two quantities is as follows: the intrinsic nonlocality is a function of the device $\{p(a,b|x,y)\}$ while $E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y))$ is a function of the compatible ρ_{CCQ} states. For most DI-QKD protocols, the testing rounds are only relevant while choosing the compatible strategies, but have no further role to play in the key generation protocol. This distinction between the testing and key-generation rounds can be exploited via $E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y))$ to upper bounds the key rate for protocols with *specific* inputs. The presence of $p(x,y)$ in the definition of the intrinsic nonlocality does not allow for this clear distinction of the key-generation and testing rounds. Another major difference is that with $E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y))$ we allow for a flexibility on the channels that Eve can act upon her extension systems. That is, Eve's actions on the extensions can be dependent on the measurements performed by Alice and Bob. These two differences in the structure of the quantities are vital to obtain tighter bounds.

4. EXTENSION TO MORE MEASUREMENTS

One can consider the function $E^{\mathrm{CC}}_{\mathrm{sq}}$ for multiple measurements defined as follows.

Definition 11. *The cc-squashed entanglement of the collection of measurements $\mathcal{M}$ measured with distribution $p(x,y)$ of the inputs reads*

$$E^{\mathrm{CC}}_{\mathrm{sq}}(\rho_{AB},\mathcal{M},p(x,y)) := \sum_{x,y} p(x,y)E^{\mathrm{CC}}_{\mathrm{sq}}(\rho_{AB},M_{x,y}). \tag{E1}$$

Similarly to Observation 3 we have that

$$E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{M},p(x,y)) = \sum_{x,y} p(x,y) \inf_{\rho_{ABE}=\mathrm{Ext}(\rho_{AB})} I(A:B|E)_{M_{x,y}\otimes \mathrm{id}_E\,\rho_{ABE}} \tag{E2}$$

We note here that the extensions ρ_{ABE} can be different for different choices for (x,y). We then note a general fact that a convex combination of convex functions is a convex function itself.

Lemma 9. *Let $\{f_i\}$ be the set of convex functions. Then for every distribution $\{p_i\}$ the function $\sum_i p_i f_i$ is convex.*

Proof : Let $x = px_1 + (1-p)x_2$ then,

$$\sum_i p_i f_i(x) \le \sum_i p_i(pf_i(x_1) + (1-p)f_i(x_2)) = p\sum_i p_i f_i(x_1) + (1-p)\sum_i p_i f_i(x_2). \tag{E3}$$

■

From the above lemma it follows that due to convexity of $E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,M)$ the function $E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{M},p(x,y))$ is convex. Further, due to convexity of the latter function we have that the analogously defined reduced version of this function

$$E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y)) := \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,\mathcal{N},p(x,y)) \tag{E4}$$

is also convex (via analogous lemma to Lemma 6).

It will appear crucial to notice, that in DI-QKD it is assumed, that the distribution of inputs $p(x,y)$ is drawn from a private shared randomness held by Alice and Bob, which is independent of the device $(\rho,\mathcal{M})$. (In most cases $p(x,y)$ is the uniform distribution. Otherwise sharing private correlations in order to choose inputs based on these correlations would imply sharing private key. It would be then no sense to run a DI-QKD, given Alice and Bob already share the key in the form of these correlations.) Due to this "free-will" assumption, it is not known to Eve for each run which (x,y) was chosen by Alice and Bob. This means that *a priori* Eve does not have access to systems E_xE_y of an extension of the form

$$\sum_{x,y} p(x,y)M_{x,y}\,\mathrm{id}_E\,\rho_{ABE}^{(x,y)} \otimes |xy\rangle\langle xy|_{E_xE_y}, \tag{E5}$$

where $\rho_{ABE}^{(x,y)}$ is an extension of ρ_{AB} for each (x,y). However, under assumption that *Alice and Bob make the announcements for the choice of measurements and Eve subsequently learns this measurement* [42], Eve can have access to the extensions given in Eq. (E5). To obtain these extensions, we can assume that the eavesdropper can act on its quantum system by a map $\Lambda_{E\to E_xE_y}$, which is dependent on the measurements (x,y). It is crucial for further considerations that Eve has access to the above extension. To make this assumption explicit we consider the following QDI key rate:

$$K^{\mathrm{IID,broad}}_{\mathrm{DI,dev}}(\rho,\mathcal{M},p(x,y)) := \inf_{\epsilon>0}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}}\inf_{(\sigma,\mathcal{N})\approx_\epsilon(\rho,\mathcal{M})} \kappa^\epsilon_n\left(\mathcal{P}\left(\left[\sum_{x,y}p(x,y)N_{xy}\otimes \mathrm{id}_E(\psi^\sigma_{ABE}\otimes|xy\rangle\langle xy|_{E_xE_y})\right]^{\otimes n}\right)\right), \tag{E6}$$

where by *broad* we mean that (x,y) are broadcasted, and made explicit by adding systems E_xE_y to Eve.

We denote the action of broadcasting the values of (x,y) (creating systems E_xE_y) as $\mathcal{C}$. This allows us to state the following technical lemma.

Lemma 10. *The function* $E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{C}\circ\sum_{x,y}p(x,y)M_{x,y})$ *is convex in the second argument, i.e.,*

$$E^{\mathrm{CC}}_{\mathrm{sq}}\left(\rho,\mathcal{C}\circ\sum_{x,y}p(x,y)M_{x,y}\right)\le\sum_{x,y}p(x,y)E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,M_{x,y}). \tag{E7}$$

Proof : We can write

$$E^{\mathrm{CC}}_{\mathrm{sq}}\left(\rho,\mathcal{C}\circ\sum_{x,y}p(x,y)M_{x,y}\right)\le\inf_{\Lambda_{EE_xE_y}} I(A;B|EE_xE_y)_{\Lambda_{EE_xE_y}(\rho_{ABEE_xE_y})}. \tag{E8}$$

Here, the inequality follows by fixing a particular class of extension. We take an arbitrary extension of the underlying quantum state, allow for flag registers and arbitrary quantum channels on Eve's system. We construct a particular extension of ρ measured by $\sum_{x,y}p(x,y)M_{x,y}$ as follows:

$$\rho_{ABEE_xE_y}:=\sum_{x,y}p(x,y)M_{x,y}\otimes\mathrm{id}_{EE_xE_y}\,\sigma_{ABE}\otimes|xy\rangle\langle xy|_{E_xE_y}, \tag{E9}$$

where σ_{ABE} is an arbitrary extension of the state ρ. The map $\Lambda_{EE_xE_y}$ is arbitrary. The access to the registers E_xE_y is assured by application of a broadcasting map $\mathcal{C}$ after performing the measurement. It is straightforward to see that upon tracing out E,E_x,E_y we obtain ρ measured by a convex combination of $M_{x,y}$. Now, let us choose a particular map of the form

$$\tilde{\Lambda}_{EE_xE_y}=\sum_{x,y}\tilde{\Lambda}^{x,y}_E\otimes|xy\rangle\langle xy|_{E_xE_y}, \tag{E10}$$

where $\tilde{\Lambda}^{x,y}_E$ is arbitrary. We then obtain

$$E^{\mathrm{CC}}_{\mathrm{sq}}\left(\rho,\mathcal{C}\circ\sum_{x,y}p(x,y)M_{x,y}\right) \tag{E11}$$

$$\le I(A;B|EE_xE_y)_{\tilde{\Lambda}_{EE_xE_y}(\rho_{ABEE_xE_y})} \tag{E12}$$

$$=\sum_{x,y}p(x,y)I(A;B|E)_{M_{x,y}\otimes\tilde{\Lambda}^{x,y}_E(\sigma_{ABE})}, \tag{E13}$$

where $\tilde{\Lambda}_{EE_xE_y}(\rho_{ABEE_xE_y})=\sum_{x,y}p(x,y)M_{x,y}\otimes\tilde{\Lambda}^{x,y}_E\otimes\mathrm{id}_{E_xE_y}\,\sigma_{ABE}\otimes|xy\rangle\langle xy|_{E_xE_y}$. Since $\tilde{\Lambda}^{x,y}_E$ is an arbitrary map, we obtain

$$E^{\mathrm{CC}}_{\mathrm{sq}}\left(\rho,\mathcal{C}\circ\sum_{x,y}p(x,y)M_{x,y}\right) \tag{E14}$$

$$\le\sum_{x,y}p(x,y)\inf_{\Lambda^{x,y}_E}I(A;B|E)_{M_{x,y}\otimes\Lambda^{x,y}_E(\rho_{ABE})} \tag{E15}$$

$$=\sum_{x,y}p(x,y)E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,M_{x,y}). \tag{E16}$$

This concludes the proof. ■

We note now, that $E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{M},p(x,y))$ is an upper bound for a distillable key of the state $\sum_{x,y}p(x,y)M_{x,y}\otimes\mathrm{id}_E\,|\psi^\rho\rangle\langle\psi^\rho|_{ABE}\otimes|xy\rangle\langle xy|_{E_xE_y}$.

Theorem 9. *For a bipartite state* ρ *and a set of measurements* $\mathcal{M}$*, performed with probabilities* $p(x,y)$ *on it, there is*

$$K_{\mathrm{DD}}\left(\sum_{x,y}p(x,y)M_{x,y}\otimes\mathrm{id}_E\,|\psi_\rho\rangle\langle\psi_\rho|\otimes|xy\rangle\langle xy|_{E_xE_y}\right)\le E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{M},p(x,y)). \tag{E17}$$

Proof : The proof follows from Ref. [45, Theorem 3.5] (also see Ref. [52, Lemma 7]) for a tripartite CCQ state $\rho_{\mathrm{CCQ}}:=\sum_{x,y}p(x,y)M_{x,y}\otimes\mathrm{id}\,|\psi_\rho\rangle\langle\psi_\rho|\otimes|xy\rangle\langle xy|_{E_xE_y}$, and noticing that $K_{\mathrm{DD}}(\rho_{\mathrm{CCQ}})\le I(A:B\downarrow E)_{\rho_{\mathrm{CCQ}}}=E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{C}\circ\sum_{x,y}p(x,y)M_{x,y})\le\sum_{x,y}p(x,y)E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,M_{x,y})\equiv E^{\mathrm{CC}}_{\mathrm{sq}}(\rho,\mathcal{M},p(x,y))$, where the last inequality follows from Lemma 10. ■

We are ready to formulate the analog of Corollary 3.

$$K^{\mathrm{IID,broad}}_{\mathrm{DI,dev}}(\rho,\mathcal{M},p(x,y)) \equiv \inf_{\epsilon>0}\limsup_{n}\sup_{\mathcal{P}\in\mathrm{LOPC}}\inf_{(\sigma,\mathcal{N})\approx_\epsilon(\rho,\mathcal{M})}$$
$$\kappa^{\epsilon}_{n}\left(\mathcal{P}\left(\left[\sum_{x,y}p(x,y)N_{xy}\otimes \mathrm{id}_E(|\psi_\sigma\rangle\langle\psi_\sigma|\otimes|xy\rangle\langle xy|_{E_xE_y})\right]^{\otimes n}\right)\right) \tag{E18}$$

$$\leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} E^{\mathrm{CC}}_{\mathrm{sq}}(\sigma,\mathcal{N},p(x,y)) =: E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y)), \tag{E19}$$

where N_{xy} are measurements induced by (x,y) on $\mathcal{N}$, respectively.

Proof : It follows from similar lines as the proof of Lemma 5 to show that

$$K^{\mathrm{IID,broad}}_{\mathrm{DI,dev}}(\rho,\mathcal{M},p(x,y)) \leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_{\mathrm{DD}}$$
$$\left(\sum_{x,y}p(x,y)M_{x,y}\otimes \mathrm{id}_E\,|\psi_\rho\rangle\langle\psi_\rho|\otimes|xy\rangle\langle xy|_{E_xE_y}\right). \tag{E20}$$

The assertion follows then from Theorem 9. ■

Let us note, that the above bound is in principle tighter than the one considered in Ref. [42], as it is stated in the Theorem below.

Theorem 10. *The function $E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y))$ is (i) a convex upper bound on $K^{\mathrm{IID,broad}}_{\mathrm{DI,dev}}(\rho,\mathcal{M},p(x,y))$ and (ii) a lower bound to the upper bound given in Ref. [42, Eq. (5)].*

Proof : The first part of the proof follows from Corollary 7. The convexity of this upper bound is already observed, as analogous to the one of $E^{\mathrm{CC}}_{\mathrm{sq,par}}$ proved in Lemma 6. We focus now on showing that this function is a lower bound to the upper bound given in Ref. [42].

Let us first restrict the attacks to such that the channel Λ involved in the definition of the $E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y))$ is a POVM, i.e., has only classical outputs, denoted as Λ^{cl}_E. In such a case we have

$$E^{\mathrm{CC}}_{\mathrm{sq,dev}}(\rho,\mathcal{M},p(x,y)) \leq \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})}\sum_{x,y}p(x,y)\inf_{\Lambda^{\mathrm{post}}_E\circ\Lambda^{cl}_E} I(A:B|E)[N_{xy}\otimes\Lambda^{\mathrm{post}}_E\circ\Lambda^{cl}_E|\psi_\sigma\rangle] \tag{E21}$$

$$= \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})}\sum_{x,y}p(x,y)\inf_{\Lambda^{cl}_E} I(A:B\downarrow E)[N_{xy}\otimes\Lambda^{cl}_E|\psi_\sigma\rangle]$$
$$\leq \sum_{x,y}p(x,y)I(A:B\downarrow E)[\tilde{N}_{xy}\otimes\tilde{\Lambda}^{cl}_E|\psi_{\tilde{\sigma}}\rangle] \tag{E22}$$

$$\equiv \sum_{p(x,y)}p(x,y)I(A:B\downarrow EE')[p(abei|xy)] \tag{E23}$$

$$\leq \sum_{p(x,y)}p(x,y)I(A:B\downarrow E)[p(abe|xy)], \tag{E24}$$

where $I(A:B\downarrow E)[p(abe|xy)]$ is the *intrinsic information* of the distribution $p(abe|xy)$. (In the last line we obtain the bound given in Ref. [42, Eq. (5)].)

The first inequality is due to restriction of the infimum to that over POVMs with classical outputs only. The first equality follows from using the definition of intrinsic information, which absorbs minimization over channels $\Lambda^{\mathrm{post}}_E$. The inequality (E22) follows from (i) fixing a particular choice of the attack $(\tilde{\mathcal{N}},\tilde{\sigma}) := (\mathcal{N},\sigma)$, where σ is given in Eq. (D18) and $\mathcal{N}$ is defined via Eqs. (D16), (D17) and (140) (ii) by choosing $\tilde{\Lambda}^{\mathrm{ext}}_E$ such that it produces extension $\sigma_{ABA'B'E_AE_BE'}$ given in Eq. (D20), when acting on system E of $|\psi^\sigma\rangle_{ABE}$. (iii) The choice of a channel $\tilde{\Lambda}^{cl}_E := \mathcal{N}^{(i)}_{\mathrm{L}}(x,y)_{E|E'}\circ\tilde{\Lambda}^{\mathrm{ext}}_E$ where measurements $\mathcal{N}^{(i)}_{\mathrm{L}}(x,y) = \mathcal{N}^{x}_{a,\mathrm{L}}\otimes\mathcal{N}^{y}_{b,\mathrm{L}}$ are given in Eq. (D19). This is possible for Eve because, as discussed earlier, Alice and Bob broadcast the input choices (x,y). This choice results in classical systems EE' holding pairs (e,i) with $e\in\mathcal{A}\times\mathcal{B}\cup\{?\}$ and $i\in\{0,\ldots,k\}$, where $e=(a,b)$, i.e., the outputs of Alice and Bob given input x,y has been chosen. We thus observe in Eq. (E23), that the minimized conditional information is equal to the intrinsic information of such obtained distribution $p(abei|xy)$.

The last inequality is due to the fact, that we first trace out register E', so that the channel involved in the definition of the intrinsic information does not depend on i (the information from which local device Eve obtains the outputs). This narrows the infimum over channels in the definition of intrinsic information, hence the quantity under consideration can only go up. As a result the intrinsic information is a function of distribution $p(abe|xy)$, as it is obtained in Ref. [42, Eq. (5)]. (See Remark 5 in this context.) ■

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Bangalore, India, 1984), p. 175.

[2] Artur K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] Dominic Mayers and Andrew Chi-Chih Yao, *Quantum Cryptography with Imperfect Apparatus* (IEEE Computer Society, Palo Alto, CA, USA, 1998), p. 503.

[4] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier, in *Automata, Languages and Programming* (Springer Berlin Heidelberg, 2006), p. 72.

[5] Antonio Acín, Nicolas Gisin, and Lluis Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[6] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[7] Vadim Makarov, Controlling passively quenched single photon detectors by bright light, New J. Phys. **11**, 065003 (2009).

[8] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[9] Philip M. Pearle, Hidden-variable example based upon data rejection, Phys. Rev. D **2**, 1418 (1970).

[10] Emilio Santos, Critical analysis of the empirical tests of local hidden-variable theories, Phys. Rev. A **46**, 3646 (1992).

[11] John Stewart Bell, Atomic-cascade photons and quantum-mechanical nonlocality, Commen. At. Mol. Phys. **9**, 121 (1980).

[12] Marissa Giustina, *et al.*, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[13] Lynden K. Shalm, *et al.*, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[14] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter, Event-Ready Bell Test using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes, Phys. Rev. Lett. **119**, 010402 (2017).

[15] Umesh Vazirani and Thomas Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[16] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).

[17] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, Simple and tight device-independent security proofs, SIAM J. Comput. **48**, 181 (2019).

[18] C. Teo, J. Minář, D. Cavalcanti, and V. Scarani, Analysis of a proposal for a realistic loophole-free bell test with atom-light entanglement, Phys. Rev. A **88**, 053848 (2013).

[19] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature **526**, 682 (2015).

[20] Rene Schwonnek, Koon Tong Goh, Ignatius W. Primaatmaja, Ernest Y. Z. Tan, Ramona Wolf, Valerio Scarani, and Charles C. W. Lim, Robust device-independent quantum key distribution with random key basis, Nat. Commun. **12**, 2880 (2021).

[21] Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff, Rene Schwonnek, Florian Fertig, Sebastian Eppelt, Valerio Scarani, Charles C. W. Lim, and Harald Weinfurter, Experimental device-independent quantum key distribution between distant users, Nature **4**, 687 (2022).

[22] 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, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J-D. Bancal, Device-independent quantum key distribution, ArXiv:2109.14600 (2021).

[23] Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, Ming-Han Li, Yang Liu, Jingyun Fan, Feihu Xu, Qiang Zhang, and Jian-Wei Pan, High-speed device-independent quantum key distribution against collective attacks, ArXiv:2110.01480 (2021).

[24] Ernest Y-Z. Tan, René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja, and C. C-W. Lim, Computing secure key rates for quantum cryptography with untrusted devices, npj Quantum Inf. **7**, 158 (2021).

[25] Peter Brown, Hamza Fawzi, and Omar Fawzi, Computing conditional entropies for quantum correlations, Nat. Commun. **12**, 575 (2021).

[26] 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, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J-D. Bancal, Device-independent quantum key distribution, ArXiv:2109.14600 (2021).

[27] Junior R. Gonzales-Ureta, Ana Predojević, and Adán Cabello, Device-independent quantum key distribution based on Bell inequalities with more than two inputs and two outputs, Phys. Rev. A **103**, 052436 (2021).

[28] R. Horodecki, Quantum information, Acta Phys. Pol. A **139**, 197 (2021).

[29] Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan, Large scale quantum key distribution: Challenges and solutions [invited], Opt. Express **26**, 24260 (2018).

[30] Matthias Christandl and Andreas Winter, Squashed entanglement: An additive entanglement measure, J. Math. Phys. **45**, 829 (2004).

[31] Remigiusz Augusiak and Paweł Horodecki, Multipartite secret key distillation and bound entanglement, Phys. Rev. A **80**, 042307 (2009).

[32] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim, General paradigm for distilling classical key from quantum states, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[33] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[34] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[35] Mark M. Wilde, Marco Tomamichel, and Mario Berta, Converse bounds for private communication over quantum channels, IEEE Trans. Inf. Theory **63**, 1792 (2017).

[36] Stefan Bäuml, Siddhartha Das, and Mark M. Wilde, Fundamental Limits on the Capacities of Bipartite Quantum Interactions, Phys. Rev. Lett. **121**, 250504 (2018).

[37] Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki, Universal Limitations on Quantum Key Distribution over a Network, Phys. Rev. X **11**, 041016 (2021).

[38] Eneet Kaur, Mark M. Wilde, and Andreas Winter, Fundamental limits on key rates in device-independent quantum key distribution, New J. Phys. **22**, 023039 (2020).

[39] Marek Winczewski, Tamoghna Das, and Karol Horodecki, Limitations on device independent secure key via squashed non-locality, ArXiv:1903.12154v5 (2019).

[40] Matthias Christandl, Roberto Ferrara, and Karol Horodecki, Upper Bounds on Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **126**, 160501 (2021).

[41] Rotem Arnon-Friedman and Felix Leditzky, Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture, IEEE Trans. Inf. Theory **67**, 6606 (2021).

[42] Máté Farkas, Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński, and Antonio Acín, Bell Nonlocality is not Sufficient for the Security of Standard Device-Independent Quantum Key Distribution Protocols, Phys. Rev. Lett. **127**, 050503 (2021).

[43] Eneet Kaur, LSU Doctoral Dissertations, 5208 (2020).

[44] We note here, that the key rate in the scenario with a nonsignaling adversary are lower than in the quantum device-independent scenario. Hence the latter one seems to be more practical and so we focus on it. Indeed, as of now, no postquantum theory, which subsides quantum mechanics is known that could help a nonsignaling adversary to be practically more powerful than the quantum one.

[45] Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner, in *Theory of Cryptography* (Springer Berlin Heidelberg, 2007), p. 456.

[46] 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).

[47] E. M. Rains, Bound on distillable entanglement, Phys. Rev. A **60**, 179 (1999).

[48] E. M. Rains, A semidefinite program for distillable entanglement, IEEE Trans. Inf. Theory **47**, 2921 (2001).

[49] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying Entanglement, Phys. Rev. Lett. **78**, 2275 (1997).

[50] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[51] Micał Horodecki, Paweł Horodecki, and Ryszard Horodecki, Mixed-State Entanglement and Distillation: Is There a "Bound" Entanglement in Nature?', Phys. Rev. Lett. **80**, 5239 (1998).

[52] Karol Horodecki, Marek Winczewski, and Siddhartha Das, Fundamental limitations on the device-independent quantum conference key agreement, Phys. Rev. A **105**, 022604 (2022); see also arXiv:2111.02467.

[53] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. Lond. A **461**, 207 (2005).

[54] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim, Secure Key from Bound Entanglement, Phys. Rev. Lett. **94**, 160502 (2005).

[55] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim, General paradigm for distilling classical key from quantum states, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[56] M. Christandl, The structure of bipartite quantum states—insights from group theory and cryptography, ArXiv:quant-ph/0604183 (2006).

[57] Matthias Christandl, The structure of bipartite quantum states-insights from group theory and cryptography, Ph.D. thesis, ArXiv:quant-ph/0604183 (2006).

[58] Antonio Acín, Serge Massar, and Stefano Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers, New J. Phys. **8**, 126 (2006).

[59] Lluís Masanes, Asymptotic Violation of Bell Inequalities and Distillability, Phys. Rev. Lett. **97**, 050503 (2006).

[60] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[61] Siddhartha Das, Sumeet Khatri, and Jonathan P. Dowling, Robust quantum network architectures and topologies for entanglement distribution, Phys. Rev. A **97**, 012335 (2018).

[62] Siddhartha Das, Sumeet Khatri, George Siopsis, and Mark M. Wilde, Fundamental limits on quantum dynamics based on entropy change, J. Math. Phys. **59**, 012205 (2018).

[63] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, General teleportation channel, singlet fraction, and quasidistillation, Phys. Rev. A **60**, 1888 (1999).

[64] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti, Realization schemes for quantum instruments in finite dimensions, J. Math. Phys. **50**, 042101 (2009).

[65] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[66] Asher Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[67] R. Simon, Peres-Horodecki Separability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2726 (2000).