Upper Bounds on Device-Independent Quantum Key Distribution

Christandl, Matthias; Ferrara, Roberto; Horodecki, Karol

Published in:
Physical Review Letters

DOI:
10.1103/PhysRevLett.126.160501

Publication date:
2021

Document version
Publisher's PDF, also known as Version of record

Document license:
Other

Citation for published version (APA):
Upper Bounds on Device-Independent Quantum Key Distribution

Matthias Christandl*
QMATH, Department of Mathematical Sciences, University of Copenhagen,
Universitetsparken 5, 2100 Copenhagen Ø, Denmark

Roberto Ferrara†
Lehr- und Forschungseinheit für Nachrichtentechnik, Technische Universität München, 80333 Munich, Germany

Karol Horodecki‡
Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics,
University of Gdańsk, 80-308 Gdańsk, Poland and International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-952 Gdańsk, Poland

(Received 28 November 2020; accepted 25 March 2021; published 21 April 2021)

Quantum key distribution (QKD) is a method that distributes a secret key to a sender and a receiver by the transmission of quantum particles (e.g., photons). Device-independent quantum key distribution (DIQKD) is a version of QKD with a stronger notion of security, in that the sender and receiver base their protocol only on the statistics of input and outputs of their devices as inspired by Bell’s theorem. We study the rate at which DIQKD can be carried out for a given bipartite quantum state distributed between the sender and receiver or a quantum channel connecting them. We provide upper bounds on the achievable rate going beyond upper bounds possible for QKD. In particular, we construct states and channels where the QKD rate is significant while the DIQKD rate is negligible. This gap is illustrated for a practical case arising when using standard postprocessing techniques for entangled two-qubit states.

DOI: 10.1103/PhysRevLett.126.160501

Introduction.—Quantum key distribution (QKD) offers the possibility to distribute a perfectly secure key among two parties via quantum communication [1]. The parties can later use this key for perfectly secure communication. Whereas theoretically, the security of QKD is very well understood, the experimental implementations remain challenging. This is because it is difficult to verify that the theoretical models and the experimental implementations fit together. In practice, the exploitation of differences between model and implementation are known as side channels, and it is here that quantum communication opens a can of worms [2]. QKD is thus dependent on the exact known specifications of the devices used: it is device dependent.

Ekert’s scheme for QKD merely verified by the violation of a Bell inequality opens up the possibility of device-independent QKD (DIQKD), as the violation of a Bell inequality can be argued by the obtained correlations alone (under the assumption of appropriate timing of the signals). In recent years, DIQKD has been put on a firm footing [3–12]. However, it should be said that a device purchased from an adversarial vendor emphasizes other types of loopholes, for instance, the hidden storage and later unwanted release of the bits generated [13–15].

Whereas security proofs for both QKD and DIQKD are involved, e.g., since channel noise needs to be estimated and the eavesdropper might carry out non-i.i.d. attacks, upper bounds on the optimal rate can be obtained with a Shannon-theoretic approach. In the case of QKD, the corresponding rates are the key rate $K(\rho)$ of a bipartite state $\rho$ shared among the communicating parties [16,17] and the private capacity $P(\Lambda)$ of a quantum channel $\Lambda$ [18]. Interestingly, these rates can indeed be achieved in the actual QKD setting, e.g., by use of the postselection technique [19]. For the first upper bounds on DIQKD rates see Ref. [20].

In this Letter, we consider the natural DIQKD variants $K^{\text{DI}}(\rho)$ and $P^{\text{DI}}(\Lambda)$. Since DIQKD has a higher security demand than QKD, one has the trivial bounds $K^{\text{DI}}(\rho) \leq K(\rho)$ and $P^{\text{DI}}(\Lambda) \leq P(\Lambda)$.

Our main results are upper bounds on the DIQKD rates that go beyond the bounds implied by QKD, thereby pointing out a fundamental difference between standard and device-independent QKD. We illustrate the bounds with an example where the QKD rate is constant but, remarkably, the DIQKD rate is vanishingly low. In the following we introduce the setting before presenting and illustrating the main results.

Communication rates in quantum cryptography.—Every QKD and DIQKD protocol consists of preparing, exchanging, and measuring quantum particles, followed by the
postprocessing of the measurement data resulting in the final key. Note that these are not necessarily separate stages, but may be interwoven. Most QKD protocols, however, can be modeled as an establishment of $n$ independent copies of a bipartite quantum state $\rho$ between the communicating parties Alice and Bob, followed by a protocol consisting of local operations and public communication (LOPC). For simplicity, we will assume that all Hilbert spaces are finite dimensional. This protocol results in a final key secret against an eavesdropper holding the purification of $\rho^{\otimes n}$ and a copy of all classical communication. When maximizing over possible LOPC protocols, one obtains the key rate $K(\rho)$.

If Alice and Bob have control over their measurement apparatuses, there exist effective methods to verify that they indeed have $n$ independent copies of $\rho$, even if the adversary interferes with the quantum communication. Thus $K(\rho)$ also has the practical relevance as a QKD rate and not only information-theoretic meaning [19].

Instead of modeling the distribution of the quantum particles by a density matrix $\rho$, one might also model it as arising from a quantum channel $\Lambda$, a completely positive trace-preserving linear map. This scenario, which results in the private capacity $C(\Lambda)$ is more general but more cumbersome to treat. Therefore, we will focus on the density matrix paradigm, yet also state our results in the channel paradigm.

Note that in most practical protocols, the QKD paradigm, yet also state our results in the channel paradigm.

In DIQKD, measurements are performed on single copies of $\rho$ by positive operator valued measures (POVMs) $\{A^a_x\}_a$ and $\{B^b_y\}_b$. We denote the measurement choices by $x$ and $y$, respectively, and the outcomes by $a$ and $b$. If an eavesdropper does not interfere with the measurement, this results in $n$ independent and identical samples of the conditional probability distribution

$$p(a,b|x,y) := \text{tr}[\rho^{\otimes n} (A^a_x \otimes B^b_y)]p].$$

Classical postprocessing then leads to the final secret key against an eavesdropper who holds the purification of the state $\rho^{\otimes n}$ as well as a transcript of all public communication. We note that the distribution of the measurement choice $p(x,y) = p(x)p(y)$ is usually fixed (e.g., uniform) so that the samples are actually drawn from the distribution $p(a,b,x,y) = p(a,b|x,y)p(x,y)$, rather than from $p(a,b,x,y)$. The choice of measurements and their distribution is denoted by $M$. We denote the corresponding QKD rate when maximizing over POVMs by $K^{(1)}(\rho)$, indicating that the measurement acts on one copy of the state. Note that

$$K^{(1)}(\rho) \leq K(\rho).$$

In DIQKD, in contrast to QKD, Alice and Bob know neither the measurement operators performed by their apparatus nor the states measured. In particular, even though they can verify that they have $n$ independent copies of $p(a,b|x,y)$, it might not be possible to infer that the underlying quantum process respects the independent nature. Namely, it might not be possible to prove that the measurements $\{A^a_x\}_a$ and $\{B^b_y\}_b$ were indeed carried out independently on independent copies of $\rho$, rather than some more complicated procedure. Even assuming that the device indeed performed $n$ independent independent measurements on an identical quantum state, leading to what we call the DIQKD rate

$$K^{\text{DI}}(\rho)$$

leaves open the possibility for different measurements as we will explain in the following. We emphasize that it is possible, yet unproven, that this rate can be achieved in a realistic DIQKD setting, as recent research indicates [8,21] (cf. research on quantum de Finetti theorems [22–24]).

Since knowing less about the apparatus can only decrease the rate, we have

$$K^{\text{DI}}(\rho) \leq K^{(1)}(\rho) \leq K(\rho). \quad (1)$$

In the following, we will provide upper bounds that improve on this bound and exploit them to present a gap between $K^{\text{DI}}(\rho)$ and $K(\rho)$.

**Upper bounds on DIQKD.**—Assume now that the POVMs $\{A^a_x\}_a$ and $\{B^b_y\}_b$ are optimal for $K^{\text{DI}}(\rho)$ (such POVMs exist by compactness, since the Hilbert spaces are finite-dimensional). Note that there might exist a different state $\rho'$ and different measurements $\{A'^a_x\}_a$ and $\{B'^b_y\}_b$ leading to the same distribution

$$p(a,b|x,y) := \text{tr}[\rho^{\otimes n} (A^a_x \otimes B^b_y)]p].$$

In this case, we write $(M,\rho) \equiv (M',\rho')$. We thus see that the maximal achievable key rate for $\rho$ is also achievable for $\rho'$. We thus have

$$K^{\text{DI}}(\rho) \leq K^{\text{DI}}(\rho').$$

Combining this bound with Eq. (1) we find that

$$K^{\text{DI}}(\rho) \leq \sup_{(M,\rho) \equiv (M',\rho')} \inf_{(M',\rho')} K(\rho'). \quad (2)$$

A proof based on the formal definitions of the involved rates is given in the Supplemental Material [25].

We will now give a construction of examples, where $(M,\rho) \equiv (M',\rho')$. For this, note that transposing Bob’s system does not change the probabilities

$$\text{tr}[\rho^{\otimes n} (A^a_x \otimes B^b_y)]p].$$

Here, $T$ denotes the transpose and $\Gamma$ the partial transpose. The density matrix $\rho$ can lose the property of being positive
semidefinite after partial transposition. For the equation above to be valid, we thus require $\rho^T \succeq 0$, in which case $\rho$ is said to be PPT (positive under partial transposition). PPT states are the only known examples of bound-entangled states, that is, entangled states from which no pure entanglement can be extracted at a positive rate [26]. Still, they form a rich class of states, including states from which a secret key can be extracted at positive rates [17,27] (similar results are known for channels [28–30]). There are even examples of PPT entangled states that violate Bell inequalities [31]. When restricting to PPT states $\rho$, we therefore find

$$K_{\text{Di}}(\rho) \leq \min\{K(\rho^T), K(\rho)\}. \quad (3)$$

To see the significance of the above result, it is important to note, that there are PPT states for which $K(\rho^T)$ is low [17,32]. This implies a gap via the above inequality and therefore a fundamental difference between device-dependent and device-independent secrecy.

We now provide an example of states exhibiting this gap. Aimed at constructions with relatively few qubits, we further develop the results of Refs. [32,33] (see also the Supplemental Material). In general, this gap holds for all those examples of PPT states that are close to private bits, but that after partial transposition become close to separable states [17,32–35].

**Examples.**—We consider the $2d \times 2d$ dimensional states from Ref. [32] which are of the form

$$\rho_d := \frac{1}{2} \left[ \begin{array}{cccc} (1-p)\sqrt{XX^\dagger} & 0 & 0 & (1-p)X \\ 0 & pY & 0 & 0 \\ 0 & 0 & pY & 0 \\ (1-p)X^\dagger & 0 & 0 & (1-p)\sqrt{X^\dagger X} \end{array} \right],$$

with $X$ and $Y$ to be chosen later, satisfying $\|X\|_1 = \|Y\|_1 = 1$. The qubit systems are called the key systems and the qudits are called the shield systems. By the privacy-squeezing technique of Ref. [27], this state has at least as much key as the key obtained by measuring

$$\rho_{\text{Bell}} := \frac{1}{2} \left[ \begin{array}{cccc} (1-p) & 0 & 0 & (1-p) \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ (1-p) & 0 & 0 & (1-p) \end{array} \right],$$

which is a Bell diagonal state. A lower bound on this key is given by the Devetak-Winter protocol [16], which was also derived in Eq. (22) of Ref. [36] and reads

$$K_D(\rho_{\text{Bell}}) \geq 1 - H\left[\left(1 - p \frac{p}{2} \frac{p}{2}\right)\right],$$

where $H$ is the Shannon entropy.

In order for $\rho_d$ to be PPT, we choose $Y = (1/d) \sum_{i=0}^{d-1} |ii\rangle\langle ii|$ and $X = 1/(d\sqrt{d}) \sum_{i=0}^{d-1} u_{ij}|ij\rangle\langle ji|$, with $u_{ij}$ being complex numbers of modulus $(1/\sqrt{d})$ such that $U = \sum_{ij} u_{ij}|j\rangle\langle i|$ is a unitary matrix [33]. In particular, one can take $U$ to be the Fourier transform or (if $d$ is a power of two) a tensor power of the Hadamard matrix. We also choose $p = 1/(\sqrt{d} + 1)$. To conclude, we derived the lower bound $K(\rho_d) \geq 1 - H[(\sqrt{d} - 1/2)/\sqrt{d} + 1]$, while the upper bound $K(\rho_d) \leq 1/(\sqrt{d} + 1)$ was computed as part of Ref. [37], Supplemental Material, Corollary 40. See also Theorem 2 in the Supplemental Material, where Ref. [38] is used.

A quick check reveals that $K(\rho_d) > K(\rho_d^T)$ for all $d \geq 24$, i.e., for all states $\rho_d$ with at least three qubits and a qutrit in the shield at each side. In particular, $\rho_d$ is thus a 12 qubit state, which proves the separation between the device-dependent and the device-independent key. For 20 qubits of shield per side, we arrive at a state which has $K(\rho_{20}) \geq 0.98$ and $K(\rho_{20}^T) \leq 1/(2^{10} + 1) \sim 10^{-3}$.

**Remark.**—At first, this does not seem to be a practical example. Note, however that using the common subroutine advantage distillation on $\rho_{20}^T$ yields the same lower and upper bounds as $\rho_{20}$. Our results thus directly concern the amount of key distilled after advantage distillation [39] on the key part of 20 copies of $\rho_2$ if we make sure that the other 20 qubits of shield do not get in the hands of the eavesdropper. In particular, we see that whereas in QKD, the obtained bit in this setting is secure, the upper bound tells us that this bit is not secure in a device-independent setting. Therefore the state, and particularly any of its parts, including the shield, cannot be tested independently of the device. The quantum operation of removing a system (in our case, the shield) from the reach of the eavesdropper is based on trust in the quantum memories and cannot be certified by classical correlations alone.

**Device-independent entanglement measures.**—Implicit in the upper bound on $K(\rho^T)$ was the use of the relative entropy of entanglement $E_r$. In this context, it is therefore natural to introduce device-independent entanglement measures. In analogy to Eq. (2), for any entanglement measure $E$ we define

$$E^\downarrow(\rho) := \sup_{A_M} \inf_{\{X,\sigma\} = (M,\rho)} E(\sigma) \leq E(\rho). \quad (4)$$

where we use the down arrow to indicate the optimization over Eve’s implementation of the device, in close analogy to the down arrow used in the intrinsic information [40], where also an optimization over Eve’s action is carried out.
Notice that $E^\dagger(\langle \psi | \langle \psi |) = E(\langle \psi | \langle \psi |)$ because all pure states are self-testable [41]. If $E$ is either the distillable key $K$ or an upper bound on it, it then follows that

$$K^{\text{DI}} \leq K^\dagger \leq E.$$  \hfill (5)

In particular, for $E$ being the squashed entanglement $E_{sq}$ or the relative entropy of entanglement $E_r$, we obtain

$$K^{\text{DI}} \leq \min\{E_{sq}^\dagger, E_r^\dagger\}.$$  

In the example above, the relative entropy bound was implicitly used together with $E_r^\dagger(\rho) \leq E_r(\rho^T)$ for PPT states $\rho$. Note that fixing a choice of $M$ in $E_r^\dagger$ also produces a device-independent entanglement measure of a distribution.

**Device-independent private capacity.**—The ideas presented so far can also be applied to the private capacity $P(\Lambda)$ of a channel $\Lambda$. They are thus useful in the most general setting, where, for instance, the optical fiber itself is modeled and not only the states produced when using the optical fiber.

There are different natural versions of the private capacity depending on whether assistance by public communication is restricted to being one-way ($P_1$) or whether general two-way communication is allowed ($P_2$). In the information-theoretic setting, the setting without public communication ($P_0$) is also meaningful. With increased power comes increased rate, and thus

$$P_0 \leq P_1 \leq P_2.$$  

The device-independent private capacity also has three analogous versions $P^{\text{DI}}_i$, $i = 0$, 1, 2 corresponding to whether two-way, one-way, or no public communication is given to Alice and Bob outside the devices. Additionally, there will be different classes of adversarial devices, depending on whether we consider adversaries that, besides the quantum channel, use two-, one-, or no-way public communication inside the devices to produce the state to be measured. Arguably, allowing less classical communication in the device than the one used by Alice and Bob is physically unsound, but can be used as a mathematical tool to reach some upper bounds. Thus, we can restrict ourselves to adversarial devices that use no public communication, which can only make the rates larger. Similarly, we also consider i.i.d. devices that do not use memory between the input states of different channel uses.

Again, these are not realistic implementations of a device delivered by an adversary but merely a tool to provide upper bounds. Indeed, in practical scenarios the provided devices will often be from a cooperating rather than an adversarial party. These devices will use quantum memories at Alice and Bob and even classical communication outside the classical input-output rounds where communication is allowed, to maximize the key. In the Supplemental Material, we explore the various rates obtained when considering different classes of devices allowed to the adversary and the different variants of public communications that are allowed to the intended parties.

We now introduce the class of i.i.d. devices that use neither public communication nor memory between channel uses. A device for a channel $\Lambda$ from Alice to Bob is given by a tuple $(M, \rho, \Lambda)$ of measurements $M$ on Alice and Bob’s side, a bipartite state $\rho$ (half of which is the input to the channel), and a channel $\Lambda$. The conditional probability distribution is then obtained, as shown in Fig. 1, via

$$p(ab|x,y) = \text{tr}[(id \otimes \Lambda)(\rho) \cdot M^s_a \otimes M^r_b].$$

We again write $(\mathcal{N}, \sigma, \mathcal{N}') \equiv (M, \rho, \Lambda)$ for devices that produce the same distribution. As in the case of entanglement measures for states, we can use any channel entanglement measure $E(\Lambda)$ to define a device-independent version

$$E^\dagger(\Lambda) \equiv E^\dagger(\Lambda) := \sup_{M, \rho} \inf_{(\mathcal{N}, \sigma, \mathcal{N}') = (M, \rho, \Lambda)} E(\Lambda')$$  \hfill (6)

(see Refs. [42,43] for the channel generalizations of $E_{sq}$ and $E_r$, respectively, as well as Ref. [44] for the use of the latter). See also Ref. [45].

The above quantities give rise to quantities $P^\dagger_i$ which will be upper bounds on the actual device-independent privacy capacities. When combining them with an upper bound $P_i \leq E$ we obtain (here illustrated with $i = 2$)

$$P^{\text{DI}}_i(\Lambda) \leq P^\dagger_i(\Lambda) \leq E^\dagger(\Lambda).$$  \hfill (7)

Also here, we can now apply the partial transpose idea. In order to do so, we introduce the partial transpose map $\theta$ $[\theta(\rho) = \rho^T]$. If a channel $\Lambda$ is such that $\theta \circ \Lambda$ is also a channel (i.e., $\Lambda$ completely positive and completely copositive), then any device for $\Lambda$ can be transformed into a device for $\theta \circ \Lambda$ with the same statistics as shown in Fig. 1. The consequence is analogous to Eq. (3) (for $i = 2$):

$$P^{\text{DI}}_i(\Lambda) \leq P_2(\theta \circ \Lambda) \leq E(\theta \circ \Lambda).$$  \hfill (8)
This bound can be used to show that there is a gap between the private capacity and the device-independent private capacity, as there exist examples of channels for which $\mathcal{P}_1(\Lambda)$ is large, but $\mathcal{P}_2(\Theta \circ \Lambda)$ small [44].

Discussion.—We have derived general upper bounds on the generation of a device-independent key. For the sake of completeness, we provide a detailed definition of device-independent key rates [8,9] in the Supplemental Material. Using the upper bounds, we have shown that a gap can exist between the device-dependent (or standard) and device-independent distillable key. In fact, the gap can be shown to be maximally large, meaning that some states and channels support secret key generation, but at most a negligible amount of a device-independent secret key. The construction has been obtained for a class of states and channels that have zero distillable entanglement or quantum capacity and that are known as PPT states or channels. We leave it as an interesting challenge to lower the dimension of such examples.

Notice that the partial transpose approach has previously led to upper bounds on Bell nonlocality in terms of faithful measures of entanglement [35], taking inspiration on upper bounds on key repeater rates [32]. In Ref. [37], bounds on the key repeater rate were given beyond the use of the partial transpose idea, leading to a connection with distillable entanglement. We hope that a similar result can be obtained connecting the device-independent distillable key and private capacity to the distillable entanglement and the quantum capacity, respectively [37], potentially leading to bounds for non-PPT states and channels.

One may regard the gap $\Delta K(\rho,M) := K(\rho) - K^{\text{DI}}(\rho,M)$ as a measure of trust towards a device $(\rho,M)$ (and analogously for quantum channels). For example, $\Delta K$ is zero for the singlet with Clauser-Horne-Shimony-Holt testing, meaning that this device does not need to be trusted, and the same may hold for all pure states. However, this is not the case for some bound-entangled states for which our results prove that $\Delta K$ is nonzero. Obtaining similar results for the multipartite case of conference key agreement is an interesting open problem.

M. C. acknowledges financial support from the European Research Council (ERC Grant Agreement No. 337603 and 81876) and VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059). R. F. was supported by the Bundesministerium für Bildung und Forschung (BMBF) through Grant No. 16KIS0857 and thanks Jed Kaniewski for useful discussions. K. H. acknowledges the support of the National Science Centre grant Sonata Bis 5 UMO-2015/18/E/ST2/00327, and partial support by the Foundation for Polish Science through the IRAP project, cofinanced by the EU within the Smart Growth Operational Programme (Contract No. 2018/MAB/5).

Note added.—Recently, we became aware of the independent but closely related work [46], where a conjecture is formulated that bound-entangled states have a zero device-independent key against a quantum adversary [46] (see in this context the related results in case of nonsignaling adversaries [47]). Our work can be regarded as supporting evidence for this conjecture.

—christandl@math.ku.dk
—roberto.ferrara@tum.de
—khorodec@inf.ug.edu.pl

PHYSICAL REVIEW LETTERS 126, 160501 (2021)