# Upper bounds on key rates in device-independent quantum key distribution with qudits based on convex-combination attacks

Author: Neil Parker i Sánchez
Advisor: Dr. Enky Oudot
*ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, Avinguda Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona*

Advisor: Dr. Antoni García-Santiago
*Facultat de Física, Universitat de Barcelona, Diagonal 645, 08028 Barcelona, Spain.*
(Dated: January 13, 2024)

**Abstract:** Device-independent quantum key distribution (DIQKD) is the pinnacle of secure communication over an untrusted channel. Its security is based solely on the classical data observed by the honest parties attempting to establish a shared secret key. Despite DIQKD's unrivalled security, real-world implementations are subject to noise, which limits its effective range. Traditionally, DIQKD has been based on measurements performed on an entangled pair of qubits. In this work, we explore the use of higher-dimensional systems as a way to improve its resilience to noise. To do this, we consider convex-combination attacks, which provide easy-to-compute upper bounds on DIQKD key rates. Our results show that using higher-dimensional states only provides a small improvement in resilience to noise, which may not justify the added experimental complexity.

## I. INTRODUCTION

Cryptography is the study of secure communication. It aims to establish protocols that allow two honest parties (Alice and Bob) to exchange messages without an eavesdropper (Eve) being able to access them. During the twentieth century, with the development of long-distance communication, the need arose for a method of sharing secret information without physically meeting with the other party. The RSA (Rivest-Shamir-Adleman) public-key cryptosystem [1] was meant to solve this problem by having the recipient hold two large prime numbers and publicly announce their product. The product can then be used by anyone to encrypt a message, but the prime factors are needed to decrypt it. An eavesdropper therefore has to factor the product in order to decode the message. The security of this kind of protocol, which is used to this day, is based on the fact that factoring the product of two large prime numbers is a computationally hard problem. Nonetheless, as computational power increases and new technologies such as quantum computing emerge, this could soon change [2].

*Quantum key distribution* (QKD) offers a solution to this problem. In each round of a QKD protocol, Alice and Bob share a quantum system and perform measurements on it in order to generate a secret key known only by them. This key can then be used to encode a message. With QKD, the probability of Eve guessing the key does not depend on her computational power. Instead, the security of these protocols is based on the laws of physics. These guarantee that any attempt at eavesdropping will introduce errors and be detected by the honest parties [3]. In QKD, the underlying assumption is that the physical apparatus employed precisely conforms to its theoretical description based on quantum mechanics. This can be difficult to verify, and a small deviation can allow an eavesdropper to compromise the protocol.

*Device-independent quantum key distribution* (DIQKD) aims to remove all assumptions about the physical implementation of the protocol by basing its security solely on the observed correlations between the outcomes of Alice and Bob's measurements.

The key ingredient that makes DIQKD possible is a large violation of a *Bell inequality*. The simplest Bell inequality involves two parties (Alice and Bob), who are far apart and perform measurements on some apparatus. They can choose between two measurement settings indexed by $x, y \in \{1, 2\}$, and they each get one of two outcomes indexed by $a, b \in \{1, 2\}$. By doing this, they can find the probability distribution $p_{AB}(a, b|x, y)$. If their observed correlations come from a common source, then the joint probabilities can be expressed as $p^{\text{loc}}_{AB}(a, b|x, y) = \int_\lambda p(\lambda)p_A(a|\lambda, x)p_B(b|\lambda, y)\mathrm{d}\lambda$. Such distributions are called *local*. A Bell inequality is a linear combination $I = \sum_{a,b,x,y} c_{a,b,x,y}p_{AB}(a, b|x, y)$, which we refer to as the *Bell expression*, along with the maximum value of $I$ that can be achieved by a local distribution, which we call the *local bound* and label $C_b$. When giving a Bell inequality we write $I \leq C_b$. In the scenario described with two settings and outcomes there is only one relevant Bell inequality, which is the CHSH inequality [4]. The CHSH expression is $I := E(a_1, b_1) - E(a_1, b_2) + E(a_2, b_1) + E(a_2, b_2)$, where $E(a_x, b_y) = p(a = b|x, y) - p(a \neq b|x, y)$. Its local bound is 2. However, if measurements are performed on a shared quantum system, the maximum value of $I$ increases to $2\sqrt{2}$. This can be generalised to a larger number of parties, measurements, and outcomes, and shows that the correlations observed by performing measurements on a multipartite quantum system can be *non-local*.

Interestingly, if we assume that quantum mechanics is valid, the maximum violation of some Bell inequalities can only be achieved by certain states and measurements. This allows for *self-testing*. In other words, just by study-

ing the statistics of an experiment, one can characterise the physical system and measurements being used [5]. For QKD protocols using these states and measurements, no assumptions about their implementation are required, which makes them device-independent.

In any experimental implementation of DIQKD, there is always some noise that scales with distance. This limits the maximum observable Bell violation and can compromise the security of the protocol. There have been many studies on establishing how much noise is tolerable [6, 7], and experimental implementations have been demonstrated by Nadlinger *et al.* [8] and Zhang *et al.* [9]. However, robustness of DIQKD to noise must be improved in order to scale it up to longer distances. One way to do this is to explore higher-dimensional states, since most protocols are based on qubits.

The security of a QKD protocol is quantified by its *key rate* $r$, which is the number of secure key bits generated per round of the protocol. Traditionally, QKD is performed by having Alice and Bob share an entangled pair of qubits, which are two-level quantum systems. However, in this work we use more general $d$-level quantum systems, which we refer to as *qudits*. For this reason, we will use logarithms base $d$ instead of base 2 when calculating the key rate. Hence, its value will be given in $d$-its rather than bits. Additionally, in this work we focus on the *asymptotic* key rate (hereafter simply referred to as the key rate), for which the number of protocol rounds goes to infinity. In general, we want to find the minimum experimental requirements for the key rate to be positive and, in particular, the maximum amount of noise tolerable. To calculate the key rate, we must assume that the most powerful possible eavesdropper exploits any imperfections in the protocol due to noise. Even though significant progress has been made on this front during the last decade [10], such security proofs are difficult to perform and yield experimental requirements that can be lowered when considering more accurate characterisations of Eve's power. An alternative approach is to consider a specific attack on the protocol. This provides an upper bound on the key rate and hence a lower bound on the experimental requirements. In this paper we focus on the latter approach. We consider the attack proposed by Łukanowski *et al.* [7] and generalise it to protocols using higher-dimensional states to find an upper bound on their key rate and answer the question of whether they offer a significant advantage.

## II. SCENARIO

In each round of the protocols we consider, Alice performs a measurement according to a random variable $X$, indexed by $x \in \{1, \dots, m_A\}$. We call $x$ the measurement *setting*. She then obtains an *outcome* $a \in \{1, \dots, n_A\}$, corresponding to a random variable $A$. Similarly, Bob performs a measurement according to a random variable $Y$, indexed by $y \in \{1, \dots, m_B\}$, and obtains an outcome $b \in \{1, \dots, n_B\}$, corresponding to a random variable $B$.

After a certain number of rounds, the honest parties publicly announce some of their settings and outcomes. This allows them to determine $p^{\text{obs}}_{AB}(a, b|x, y)$. They can then distil a shared secret key through two kinds of public discussion, referred to as *privacy amplification* (PA) and *error correction* (EC). This communication can be either one-way (e.g. from Alice to Bob) or two-way. In this work, we only consider one-way communication.

From here on, we take the number of outcomes $n_A$ and $n_B$ to be equal to the dimension $d$ of Alice and Bob's shared system. We also set $m_A = 2$ and $m_B = 3$. The measurements corresponding to $x, y \in \{1, 2\}$ are chosen so as to maximise the violation of a Bell inequality. Bob's extra setting $y = 3$ is chosen to maximise the correlation of his outcomes with Alice's when she chooses $x = 2$. We refer to the pair $(x^*, y^*) = (2, 3)$ as the *key settings*. The rounds in which these settings are chosen are used to generate the shared secret key. In our focus on the asymptotic key rate, we operate under the assumption that the key settings are selected with a probability approaching certainty, that is, almost surely or with a probability of 1. This approach maximises the key rate, while simultaneously enabling Alice and Bob to accurately determine the complete probability distribution, a process facilitated by the infinite number of rounds.

## III. THE CONVEX-COMBINATION ATTACK

As stated before, we can consider a specific attack in order to obtain an upper bound on the key rate. An attack can broadly be defined as a method used by Eve to intercept the secret key. We consider *individual attacks*, in which Eve holds a higher-dimensional state involving Alice, Bob and herself such that the correlation observed by Alice and Bob is recovered on average. At the end of each round, Eve records an instance of a random variable $E$ based on a measurement she performs on this state, the outcome of which is correlated with Alice's and Bob's. This is fully described by a tripartite correlation $p_{ABE}(a, b, e|x, y)$ involving Eve that must satisfy

$$\sum_e p_{ABE}(a, b, e|x, y) = p^{\text{obs}}_{AB}(a, b|x, y) \ \forall x, y. \tag{1}$$

For any such attack, the following expression provides an upper bound on the key rate [11, 12]

$$r \leq H(A|E, x = x^*) - H(A|B, x = x^*, y = y^*) =: r_{\text{ub}} \tag{2}$$

where $H(A|E, x = x^*)$ is the conditional entropy of Alice's outcomes given Eve's, and $H(A|B, x = x^*, y = y^*)$ is the conditional entropy of Alice's outcomes given Bob's. Henceforth, we omit the measurement settings, which we take to be the key settings. $H(Y|X)$ can be understood as $X$'s ignorance of $Y$'s outcomes. We refer to $H(A|E)$ as the *PA-term*, and to $H(A|B)$ as the *EC-term*. On the one hand, the PA-term can be interpreted as the number of bits per round available to Alice after she compresses

her outcomes so that they are no longer correlated with Eve's. On the other hand, the EC-term can be seen as the number of bits that Alice must publicly announce to ensure that Bob has a key that perfectly matches hers.

Specifically, we consider *convex-combination* (CC) attacks [7]. These are individual attacks in which Eve distributes, in each round, either a local bipartite correlation $p_{AB}^{\mathcal{L}}$ with probability $q^{\mathcal{L}}$, or a non-local one $p_{AB}^{\mathcal{NL}}$ with probability $q^{\mathcal{NL}} = 1 - q^{\mathcal{L}}$. These must satisfy

$$q^{\mathcal{L}} p_{AB}^{\mathcal{L}}(a,b|x,y) + q^{\mathcal{NL}} p_{AB}^{\mathcal{NL}}(a,b|x,y) = p_{AB}^{\text{obs}}(a,b|x,y) \tag{3}$$

$\forall a,b,x,y$. Since the space of local correlations $\mathcal{L}$ is a polytope, each local correlation $p_{AB}^{\mathcal{L}}(a,b|x,y)$ within it can be decomposed as a convex combination of its vertices $p_{AB}^{\mathcal{L},(i)}$, which are local deterministic strategies. That is, $p_{AB}^{\mathcal{L}}(a,b|x,y) = \sum_i \gamma_i p_{AB}^{\mathcal{L},(i)}(a,b|x,y)$ with $\gamma_i \in [0,1]\,\forall i$. Therefore, in each round, Eve can distribute the deterministic strategy $p_{AB}^{\mathcal{L},(i)}$ with probability $q_i^{\mathcal{L}} = \gamma_i q^{\mathcal{L}}$. By keeping track of which deterministic strategies she distributes, she gains perfect knowledge of Alice's and Bob's outcomes in the local rounds. On the contrary, we make the overpessimistic assumption that Eve has no knowledge of the outcomes in the non-local rounds. If she did, this would only improve the attack and lead to a tighter upper bound on the key rate [7].

Eve's goal can be expressed in terms of the following linear optimisation problem [7]:

$$\begin{aligned} &\text{Find a vector} && \mathbf{q} \coloneqq (\mathbf{q}^{\mathcal{L}}, q^{\mathcal{NL}}) \\ &\text{that maximises} && q^{\mathcal{L}} \equiv (1,1,\ldots,1,0)\cdot\mathbf{q} \\ &\text{subject to} && (1,1,\ldots,1)\cdot\mathbf{q} = 1 \\ & && \mathbf{0} \le \mathbf{q} \le \mathbf{1} \\ & && \mathbf{q}\cdot(\mathbf{p}_{\mathbf{AB}}^{\mathcal{L}}, p_{AB}^{\mathcal{NL}}) = p_{AB}^{\text{obs}} \end{aligned} \tag{4}$$

where $\mathbf{p}_{\mathbf{AB}}^{\mathcal{L}} = \{p_{AB}^{\mathcal{L},(i)}\}_i$ is the set of all local deterministic strategies, $p_{AB}^{\mathcal{NL}}$ is the chosen non-local correlation, and $p_{AB}^{\text{obs}}$ is the observed correlation.

Geometrically, once $p_{AB}^{\mathcal{NL}}$ is fixed, this corresponds to finding the point along the segment connecting $p_{AB}^{\mathcal{NL}}$ and $p_{AB}^{\text{obs}}$ that lies on the boundary of $\mathcal{L}$, as shown in Fig. 1.

As noted above, certain non-local correlations uniquely identify a state and measurements. Nevertheless, if there is some amount of noise, $p_{AB}^{\text{obs}}$ inevitably deviates from this behaviour. We account for noise by using the *finite visibility* model [7]. In this model, we assume that Alice and Bob succeed in sharing the intended state with probability $V \in [0,1]$, and that otherwise their outcomes are uniformly random. If $p_{AB}^{\text{ideal}}$ is the noise-free correlation they intend to share, then the correlation they observe is

$$p_{AB}^{\text{obs}}(a,b|x,y) = V p_{AB}^{\text{ideal}}(a,b|x,y) + \frac{1-V}{d^2} \tag{5}$$

where $d$ is the dimension of their shared quantum system.

In this work, we assume that the non-local correlation used by Eve is the same as the noise-free correlation used by Alice and Bob, i.e. $p_{AB}^{\mathcal{NL}} = p_{AB}^{\text{ideal}}$. We do this in order to find an upper bound on the key rate in the full range of visibilities $V \in [0,1]$. If Eve were to use a non-local correlation different from Alice and Bob's, then in the limit of $V \to 1$ the CC attack would become unfeasible. In particular, we consider two non-local correlations, which are those that maximally violate the inequalities introduced by Salavrakos *et al.* [13] and Collins *et al.* [14], respectively. We refer to the latter as the CGLMP-inequality.

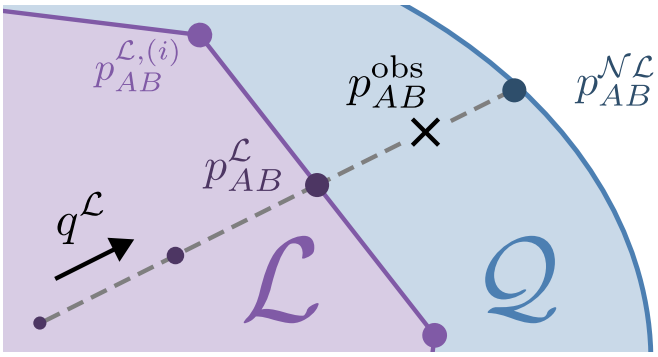


FIG. 1. Diagram of the local set of correlations $\mathcal{L}$, which is a polytope, and the quantum set $\mathcal{Q}$, which contains $\mathcal{L}$. Eve distributes a combination of a local correlation $p_{AB}^{\mathcal{L}} \in \mathcal{L}$ and a non-local one $p_{AB}^{\mathcal{NL}} \in \mathcal{Q} \setminus \mathcal{L}$, resulting in $p_{AB}^{\text{obs}}$. Therefore, $p_{AB}^{\mathcal{L}}$ must lie on the segment connecting $p_{AB}^{\mathcal{NL}}$ and $p_{AB}^{\text{obs}}$. To maximise the local weight, $p_{AB}^{\mathcal{L}}$ must be as close as possible to $p_{AB}^{\text{obs}}$, that is, on the boundary of $\mathcal{L}$.

Salavrakos' inequality is tailored to be maximally violated by the maximally entangled state $|\psi_{\max}\rangle = (1/\sqrt{d})\sum_{q=1}^{d}|qq\rangle$ when using optimal measurements, which we refer to as the CGLMP-optimal measurements [13]. These measurements also lead to the maximal violation of the CGLMP-inequality by this state [14]. However, a larger violation can be achieved by another state, which we refer to as the CGLMP state [15].

## IV. UPPER BOUNDS

As mentioned previously, our goal is to find the point along the segment connecting $p_{AB}^{\mathcal{NL}}$ and $p_{AB}^{\text{obs}}$ that lies on the boundary of $\mathcal{L}$. To identify non-locality, we use the CGLMP-inequality, since it coincides with a facet of the local polytope [16]. This inequality is expressed as [14]

$$\begin{aligned} I_d = \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \Big\{ & p(A_1 = B_1 + k) \\ & + p(B_1 = A_2 + k + 1) + p(A_2 = B_2 + k) \\ & + p(B_2 = A_1 + k) - p(A_1 = B_1 - k - 1) \\ & - p(B_1 = A_2 - k) - p(A_2 = B_2 - k - 1) \\ & - p(B_2 = A_1 - k - 1) \Big\} \le 2 =: C_b \end{aligned} \tag{6}$$

where

$$p(A_x = B_y + k) \coloneqq \sum_{j=1}^{d} p_{AB}(j, j+k \bmod d|x, y). \quad (7)$$

First, we consider the maximally entangled state $|\psi_{\max}\rangle$ as the noise-free quantum state, and the CGLMP-optimal measurements. These measurements lead to the maximal value of $I_d$ achievable by this state, which we write as $I_d^{\max}$, and for which there is an explicit expression (see Appendix VII A for details).

For the CC attack to work, Eq. (3) must be satisfied. Furthermore, in the finite visibility scenario, $p_{AB}^{\text{obs}}(a, b|x, y)$ takes the form given in Eq. (5). By combining these expressions, we get

$$p_{AB}^{\mathcal{L}}(a, b|x, y) = \tilde{V} p_{AB}^{\mathcal{NL}}(a, b|x, y) + \frac{1 - \tilde{V}}{d^2} \quad (8)$$

where $\tilde{V} \coloneqq \left(V - (1 - q^{\mathcal{L}})\right)/q^{\mathcal{L}}$. Note that $\tilde{V} \in [0, 1]$. Hence, maximising $q^{\mathcal{L}}$ corresponds to maximising $\tilde{V}$ such that $p_{AB}^{\mathcal{L}}(a, b|x, y)$ is local. The result of this maximisation is the *local visibility* $V^{\mathcal{L}}$. The local weight is thus

$$q^{\mathcal{L}} = \frac{1 - V}{1 - V^{\mathcal{L}}} \quad (9)$$

if $V \geq V^{\mathcal{L}}$ and $q^{\mathcal{L}} = 1$ otherwise. We show in Appendix VII A that $I_d^{\mathcal{L}} = \tilde{V} I_d^{\mathcal{NL}}$. By setting $I_d^{\mathcal{L}} = C_b$ in this expression, we get $\tilde{V} = C_b/I_d^{\max}$. Hence, if the probability distribution obtained by setting $\tilde{V} = C_b/I_d^{\max}$ in Eq. (9) is local, then this value of $\tilde{V}$ must be maximal, since any larger value would imply a Bell inequality violation. We can verify that this probability distribution is local by checking that it can be decomposed as a convex-combination of deterministic strategies. We do this via linear programming up to $d = 10$. We conjecture that this is true $\forall d \geq 2$, and hence $V^{\mathcal{L}} = C_b/I_d^{\max}$ $\forall d \geq 2$. This allows us to determine the maximum local weight using Eq. (9). Since the conditional entropy $H(A|E)$ is 1 in the non-local rounds and 0 in the local rounds, the PA-term is $H(A|E) = 1 - q^{\mathcal{L}}$. Computing the conditional Shannon entropy for $p_{AB}^{\text{obs}}$ gives us the EC-term

$$H(A|B) = -\frac{1 + (d-1)V}{d} \log_d \left(1 + (d-1)V\right) - \frac{(d-1)(1-V)}{d} \log_d (1 - V) + 1. \quad (10)$$

By subtracting these two terms, we get the following upper bound on the key rate:

$$r_{\text{ub}} = \frac{1 + (d-1)V}{d} \log_d \left(1 + (d-1)V\right) + \frac{(d-1)(1-V)}{d} \log_d (1 - V) - \frac{1 - V}{1 - 2/I_d^{\max}}. \quad (11)$$

In the case of the CGLMP state, we use linear programming to solve the problem described in Eq. (4) in order to find the local weight $q^{\mathcal{L}}$. To do this, we first need to find $p_{AB}^{\mathcal{NL}}$. To this end, we define the Bell operator $\hat{\mathcal{B}}_d$ corresponding to the CGLMP-inequality defined in Eq. (6), where we use the measurements that achieve the best known violation of this inequality [13]. We then optimise the phases of these measurements to maximise the largest eigenvalue of $\hat{\mathcal{B}}_d$, and use the associated eigenstate as the non-local state (which is precisely the CGLMP state). Finally, we find the probabilities $p_{AB}^{\mathcal{NL}}$ corresponding to these optimal measurements. Once $p_{AB}^{\mathcal{NL}}$ is known, we can calculate the EC-term $H(A|B)$ for a given visibility and find the local weight $q^{\mathcal{L}}$ via linear programming, which allows us to calculate the PA-term, which is $H(A|E) = 1 - q^{\mathcal{L}}$ as previously stated. As before, the difference of these two terms provides an upper bound on the key rate.

## V. RESULTS AND DISCUSSION

The upper bounds obtained for both the maximally entangled state and the CGLMP state are very close. With the CGLMP state, they are marginally lower and therefore the resilience to noise is slightly worse (see Fig. 2). This is due to a larger EC-term, since Alice's and Bob's outcomes are less correlated than when using the maximally entangled state. This leads to an overall decrease in the key rate (see Figs. 5 and 6 in Appendix VII B for further details).

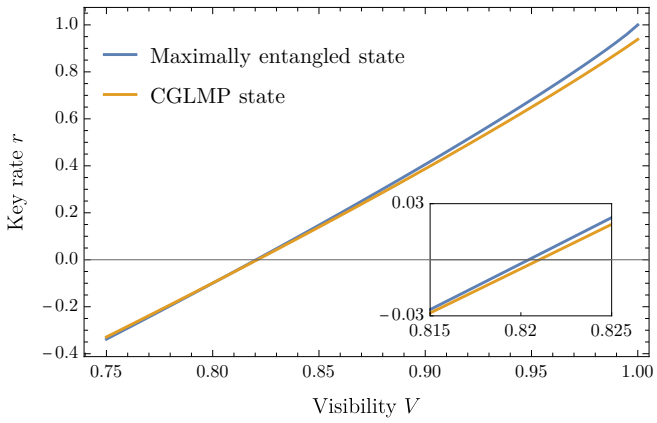


FIG. 2. CC-based upper bounds on the key rate in terms of the visibility for the maximally entangled and CGLMP states for dimension $d = 3$. For $V \gtrsim 0.805$, the upper bound is higher with the maximally entangled state. The critical visibilities at which $r_{\text{ub}} = 0$ are 0.82043 for the maximally entangled state and 0.82101 for the CGLMP state.

The value of $V$ at which $r_{\text{ub}} = 0$, known as the *critical visibility* $V_{\text{crit}}$, is a useful quantity for measuring resilience to noise. For $V \leq V_{\text{crit}}$, no secure communication is possible. Hence, it is desirable to have a low $V_{\text{crit}}$. For the maximally entangled state, we can calculate $V_{\text{crit}}$ for any dimension $d$ using Eq. (2) (see Fig. 3). For the CGLMP state, we computed $V_{\text{crit}}$ numerically up to $d = 8$ (see Table I in Appendix VII B).

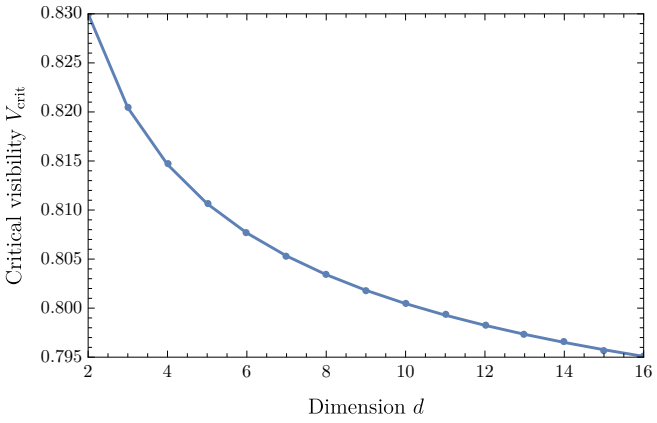


FIG. 3. Critical visibility $V_{\text{crit}}$ obtained by means of Eq. (11) as a function of the dimension $d$ for protocols using the maximally entangled state. The critical visibility is 0.8300 for $d = 2$ and decreases with $d$. Eventually, as $d \to \infty$, $V_{\text{crit}}$ would reach a plateau around 0.7539.

Finally, we can study the asymptotic behaviour of $r_{\text{ub}}$ from Eq. (11) as $d \to \infty$. By taking the limit, we find

$$r_{\text{ub}}^{\infty} \coloneqq \lim_{d\to\infty} r_{\text{ub}} = \frac{(2 - \pi^2/(16\ \text{Catalan}))V - 1}{1 - \pi^2/(16\ \text{Catalan})} \tag{12}$$

where we used that $\lim_{d\to\infty} I_d^{\max} = 32\text{Catalan}/\pi^2 \simeq 2.970$ where Catalan $\simeq 0.9159$ is Catalan's constant [14]. By setting $r_{\text{ub}}^{\infty} = 0$ and solving for $V$ we find the critical visibility as $d \to \infty$, which is $V_{\text{crit}}^{\infty} = 1/(2 - \pi^2/(16\ \text{Catalan})) \simeq 0.7539$. Since $I_d^{\text{obs}} = V I_d^{\max}$, we have $I_d^{\text{crit},\infty} = V_{\text{crit}}^{\infty} I_d^{\max} \simeq 2.239$. Therefore, if $I_d^{\text{obs}} \lesssim 2.239$, no key exchange is possible for protocols using the maximally entangled state.

## VI. CONCLUSIONS

We have shown that increasing the dimension of the shared quantum system in DIQKD protocols provides a small increase of the upper bounds on the key rates, which implies there could be a slight reduction in the visibility requirements of such protocols. Nonetheless, these improvements may not justify the added challenges associated with using higher-dimensional states, since the critical visibility reaches a plateau as $d \to \infty$ around 0.75.

This work could be extended by examining variations of the protocol we have presented. For example, it may be worth studying the use of more general non-local states. The effect of different preprocessing schemes on Alice's classical data—such as noisy preprocessing [17]—as well as two-way communication between Alice and Bob, could also be considered. Finally, in this work we have focused on the asymptotic key rate, with the number of protocol rounds going to infinity. It may also be worth studying the finite case to see if an improvement is achieved by increasing the dimension. For systems with dimension greater than 2, the gap between the lower and upper bounds on the key rate remains to be closed. This could be achieved by broadening our focus to coherent (or general) attacks in which Eve has a quantum memory which allows her to process the intercepted qudits collectively.

## ACKNOWLEDGMENTS

I'd like to thank my ICFO advisor, Dr. Enky Oudot, for his time, attention, ideas, and feedback, and also my UB advisor, Dr. Antoni García Santiago, for his guidance, advice, and comments. I appreciate everyone at the QIT group at ICFO for welcoming me, especially Dr. Antonio Acín for offering me an internship (for the second time), and Javier Rivera and Anna Steffinlongo for their crucial help. Lastly, I thank my friends and family, and in particular my father for proofreading this text.

[1] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120 (1978).
[2] P. W. Shor, SIAM Journal on Computing **26**, 1484 (1997), arxiv:quant-ph/9508027.
[3] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7 (2014).
[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Physical Review Letters **23**, 880 (1969).
[5] D. Mayers and A. Yao, Quantum Info. Comput. **4**, 273–286 (2004), arXiv:quant-ph/0307205.
[6] E. M. González-Ruiz *et al.*, in *Optica Quantum 2.0 Conference and Exhibition* (2023) p. QM3B.3, arXiv:2211.16472 [quant-ph].
[7] K. Łukanowski *et al.*, in *Quantum 2.0 Conference and Exhibition* (2022) p. QTu4C.1, arxiv:2206.06245 [quant-ph].
[8] D. P. Nadlinger *et al.*, Nature **607**, 682 (2022), arxiv:2109.14600 [quant-ph].
[9] W. Zhang *et al.*, Nature **607**, 687 (2022), arxiv:2110.00575 [quant-ph].
[10] P. Brown, H. Fawzi, and O. Fawzi, Nature Communications **12**, 575 (2021), arxiv:2007.12575 [quant-ph].
[11] I. Csiszar and J. Korner, IEEE Transactions on Information Theory **24**, 339 (1978).
[12] R. Ahlswede and I. Csiszar, IEEE Transactions on Information Theory **39**, 1121 (1993).
[13] A. Salavrakos *et al.*, Physical Review Letters **119**, 040402 (2017), arxiv:1607.04578 [quant-ph].
[14] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Physical Review Letters **88**, 040404 (2002), arxiv:quant-ph/0106024.
[15] A. Acin *et al.*, Physical Review A **65**, 052325 (2002), arxiv:quant-ph/0111143.
[16] L. Masanes, Quantum Information & Computation **3**, 345 (2003), arXiv:quant-ph/0210073 [quant-ph].
[17] M. Ho *et al.*, Physical Review Letters **124**, 230502 (2020), arxiv:2005.13015 [quant-ph].

## VII. APPENDIX

### A. Analytical derivation of the upper bound on the key rate using the maximally entangled state

The maximal value of the CGLMP expression $I_d$ given in Eq. (6) achievable by the maximally entangled state $|\psi_{\max}\rangle$ is [14]

$$I_d^{\max} = 4d \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \left(f_d(k) - f_d(-(k+1))\right), \tag{13}$$

where $f_d(k) \coloneqq 1/(2d^3 \sin^2[\pi(k+1/4)/d])$.

Using Eqs. (7) and (8), we find that

$$p^{\mathcal{L}}(A_x = B_y + k) = \frac{1-\tilde{V}}{d} + \tilde{V} p^{\mathcal{NL}}(A_x = B_y + k). \tag{14}$$

By substituting this into Eq. (6), we find that $I_d^{\mathcal{L}} = \tilde{V} I_d^{\mathcal{NL}}$. Similarly, we can see that $I_d^{\text{obs}} = V I_d^{\mathcal{NL}}$. This allows us to see that $V^{\mathcal{L}} = C_b / I_d^{\max}$, as explained in IV.

When using the maximally entangled state, the probabilities $p_{AB}^{\mathcal{NL}}(a,b|x,y)$ only depend on $x$, $y$, and the differences between the outcomes $a$ and $b$ modulo $d$ [13]. If Alice and Bob use the same measurement parameters for the key settings, then $p_{AB}(a,b|x^*,y^*) = \delta_{a,b}/d$. With this in mind, we can calculate the EC-term $H(A|B)$ and the PA-term $H(A|E)$. The conditional entropy of $Y$ given $X$ is defined as $H(Y|X) = \sum_{x\in\mathcal{X}} p(x) H(Y|X = x)$, where $H(X) = -\sum_{x\in\mathcal{X}} p(x) \log_d p(x)$ is the Shannon entropy. First, the EC-term can be written as

$$H(A|B) = \sum_{b=1}^{d} p_B^{\text{obs}}(b) H\left\{\frac{p_{AB}^{\text{obs}}(1,b)}{p_B^{\text{obs}}(b)}, \ldots, \frac{p_{AB}^{\text{obs}}(d,b)}{p_B^{\text{obs}}(b)}\right\} \tag{15}$$

where all probabilities are for the key settings. Since $p_{AB}^{\text{obs}}(a,b) = V p_{AB}^{\mathcal{NL}}(a,b) + (1-V)/d^2$ only depends on the difference between the outcomes $a$ and $b$ modulo $d$, and since $p_B^{\text{obs}}(b) = 1/d \ \forall b$,

$$\begin{aligned} H(A|B) &= H\left\{V + \frac{1-V}{d}, \frac{1-V}{d}, \ldots, \frac{1-V}{d}\right\} \\ &= -\frac{1+(d-1)V}{d} \log_d\left(1+(d-1)V\right) \\ &\quad - \frac{(d-1)(1-V)}{d} \log_d\left(1-V\right) + 1. \end{aligned} \tag{16}$$

For the PA-term, since Eve has perfect knowledge of Alice's outcomes in the local rounds and has no knowledge of the outcomes of the non-local rounds, we have $H(A|E,\mathcal{L}) = 0$ and $H(A|E,\mathcal{NL}) = 1$. Hence, $H(A|E) = q^{\mathcal{NL}} = 1 - q^{\mathcal{L}}$. Using Eq. (9) and the fact that $V^{\mathcal{L}} = C_b/I_d^{\max} = 2/I_d^{\max}$, we get

$$H(A|E) = 1 - \frac{1-V}{1-2/I_d^{\max}} \tag{17}$$

if $V \geq V^{\mathcal{L}}$ and $H(A|E) = 0$ otherwise.

### B. Additional figures and tables

In this section we present a few additional figures and tables. Fig. 4 shows a schematic of a DIQKD protocol, while Figs. 5 and 6 show the PA and EC-terms used for the calculation of the upper bounds, respectively. Finally, Table I shows the critical visibilities for dimensions ranging from 2 to 8, both for the maximally entangled and CGLMP states.

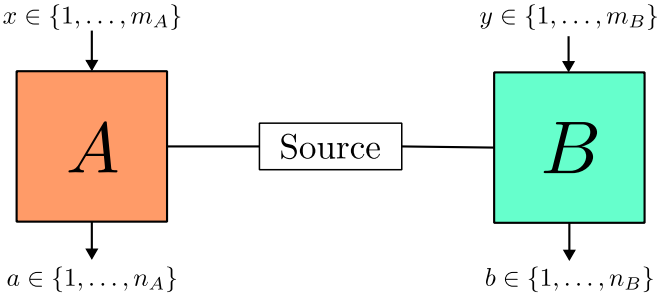


FIG. 4. Schematic of a DIQKD protocol in which Alice (Bob) has $m_A$ ($m_B$) settings and $n_A$ ($n_B$) outcomes.

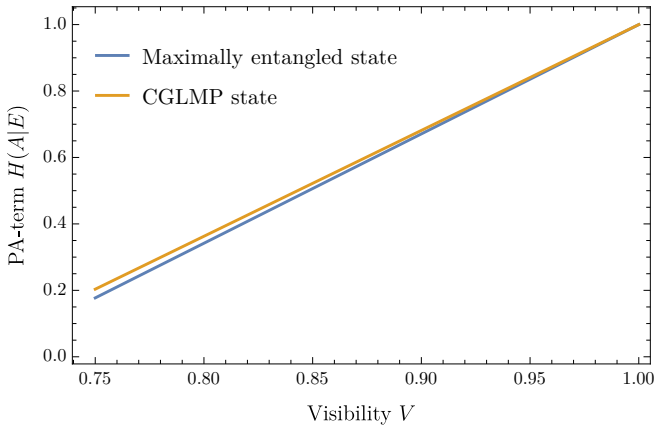


FIG. 5. PA-term in the CC-based upper bound on the key rate in terms of the visibility when using the maximally entangled and CGLMP states for dimension $d = 3$. For $V$ close to 1 the values are very close to each other in both cases.

| | $V_{\text{crit}}$ | |
|---|---|---|
| $d$ | Maximally entangled state | CGLMP state |
| 2 | 0.82999 | 0.82999 |
| 3 | 0.82043 | 0.82101 |
| 4 | 0.81464 | 0.81550 |
| 5 | 0.81064 | 0.81165 |
| 6 | 0.80766 | 0.80874 |
| 7 | 0.80532 | 0.80644 |
| 8 | 0.80341 | 0.80455 |

TABLE I. Critical visibilities for dimensions ranging from 2 to 8 when using a mixture of local deterministic strategies and the maximally entangled state or the CGLMP state.

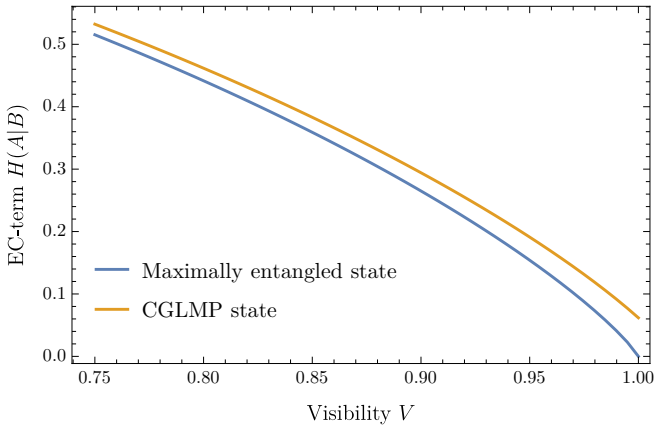


FIG. 6. EC-term in the CC-based upper bound on the key rate in terms of the visibility when using the maximally entangled and CGLMP states for dimension $d = 3$. For $V$ close to 1, the value of the EC-term is significantly larger with the CGLMP state. This is due to the fact that the outcomes are less correlated with the CGLMP state as opposed to the maximally entangled state. Therefore, more error correction will be needed when using the CGLMP state.

### C. GitHub repository

The MATLAB script we used to obtain the results presented in this paper is available on GitHub at https://github.com/neilps2000/DIQKD-CC-UB. The main script is `qudit_CC_UB.m`, which allows us to calculate an upper bound on the key rate and the critical visibility when using the maximally entangled state or the CGLMP state. The script `test_locality.m` allows us to verify that the correlations obtained with the finite visibility model using the maximally entangled state are local when the visibility is $V = C_b/I_d^{\max}$, where $C_b$ is the local bound of the CGLMP-inequality and $I_d^{\max}$ is the maximal violation of this inequality by the maximally entangled state for dimension $d$.