

Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement

Marcus Huber^{1,2,3} and Marcin Pawłowski^{1,4}

¹*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*

²*Institut de Ciències Fotoniques, 08860 Castelldefels, Barcelona, Spain*

³*Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Spain*

⁴*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, 80-952 Gdańsk, Poland*

(Received 31 January 2013; revised manuscript received 20 June 2013; published 11 September 2013)

We show that in device-independent quantum key distribution protocols the privacy of randomness is of crucial importance. For sublinear test sample sizes even the slightest guessing probability by an eavesdropper will completely compromise security. We show that a combined attack exploiting test sample and measurement choices compromises the security even with a linear-size test sample and otherwise device-independent security considerations. We explicitly derive the sample size needed to retrieve security as a function of the randomness quality. We demonstrate that exploiting features of genuinely higher-dimensional systems, one can reduce this weakness and provide device-independent security more robust against weak randomness sources.

DOI: [10.1103/PhysRevA.88.032309](https://doi.org/10.1103/PhysRevA.88.032309)

PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Hk, 03.67.Mn

I. INTRODUCTION

Quantum cryptography is one of the most prominent applications of quantum information theory. It enables a level of security in key distribution that is unparalleled in classical information theory, as a successful eavesdropping would violate fundamental laws of quantum physics. This is true at least in theoretically perfect settings. Specific attacks targeted at imperfect technical implementations, such as low-efficiency detectors, have shown that there is still a lot of room for improvement until the application is perfected. The original proposals, however, were still making a lot of strong assumptions on the systems used for cryptography. One can group these approaches in two classes. Prepare-and-measure quantum key distribution (QKD) utilizes the fact that measurement is not possible without disturbance in quantum physics (the first protocol was proposed in Ref. [1]). The strong assumption here is that one is in perfect control of the source and measurement apparatuses. Indeed it was shown that security can be compromised if the source of the information carriers or the measurement apparatuses used for interacting with them are manipulated [3,4]. In the second type of protocol entanglement is used to establish a secure key, which due to the limited shareability of quantum correlations provides security even if the source of entangled states is in the hands of an eavesdropper (the first such protocol was proposed in Ref. [2]). In this case, however, it is also possible to break the security of the protocols if the eavesdropper also has manipulated the measurement devices. Fortunately, using device-independent verification of entanglement, one can overcome this flaw, and recent works have focused on device-independent quantum key distribution (DIQKD) (see e.g. Refs. [5–8]).

All device-independent proposals so far have used assumptions about a perfectly uniform randomness being readily available. In Ref. [10] it was shown that even a slight imperfection in randomness generation leads to a possible loophole and even entanglement-based protocols can be compromised. This loophole, however, originates in the sublinear size of the test sample.

The attack of Eve in that paper assumes that Eve is responsible for the weak randomness and can use her knowledge of the

bias to guess with high probability in which rounds the security check will be performed and thus remain undetected. However, this is only one of the points where the randomness enters the protocol. The other is the choice of the measurement settings. As we will see, the bad quality of randomness used there has a big impact on the security. In this paper we generalize the attack from Ref. [10] and show that the security of the DIQKD can be compromised, even when using a linear test sample, if Eve exploits the min-entropy loss in both the choice of the settings and the test sample.

We show that below a certain threshold of randomness quality key generation is no longer possible with qubit protocols. Furthermore we propose a scheme that overcomes this weakness by considering genuinely high-dimensional entangled systems, which are readily available in quantum photonics (see, e.g., Refs. [11–16]).

This paper is structured as follows: First, we present the scenario that we are working in and the protocol that the parties are using. Then, we derive the minimal violation of the Bell inequality used as a security parameter as a function of min-entropy loss rate. Next, we prove the necessity of a feature that any QKD protocol must have in the presence of weak randomness: the linear size of the test sample. Then we find the sufficient size of the sample for Collins, Gisin, Linden, Massar, Popescu (CGLMP) inequality [17] testing. We end by discussing the implications of our work and the open problems.

II. THE SETTING

To start let us first specify the setting. Alice and Bob want to share a secure key. They implement a protocol under the following conditions: (1) a potentially compromised measurement apparatus, (2) a potentially compromised source of multidimensionally entangled quantum systems, (3) no preexisting secret key, (4) weak randomness, and (5) an authenticated classical channel. In condition 1, Alice and Bob have access to quantum measurement devices, which they cannot trust. However, following [9], we assume that the observables measured in the different runs commute. Condition 3 is very important. If Alice and Bob have some shared secret bits, they could use them as a randomness source

with perfect randomness. For condition 4, Alice and Bob have potentially compromised sources of randomness. Their min-entropy loss rate is L . We assume that the randomness generators of Alice and Bob can be correlated.

Now we specify the protocol that they are going to implement. It is the standard DIQKD setting. Two communicating parties are going to use the CGLMP [17] inequality violation as their security parameter. To estimate the violation each party has to randomly choose one of the settings $a = 0, 1$ for Alice and $b = 0, 1$ for Bob. To generate the key Bob will use a third setting $b = 2$, which gives him outcomes maximally correlated with Alice's when she chooses $a = 0$. The protocol has N runs. First, Bob randomly chooses a subset of fN runs where the parties estimate the parameter. In this subset he chooses settings $b = 0$ or 1 randomly. In the remaining $(1 - f)N$ runs he uses $b = 2$. Alice chooses $a = 0$ or 1 randomly in all the runs.

After the measurements for all the runs are complete Bob announces the cases which he used for parameter estimation. The parties announce the settings and outcomes for all of these runs and use them to estimate the value of the CGLMP inequality violation. In the remaining $(1 - f)N$ runs Alice announces when she has chosen $a = 1$, and the parties discard these runs. Only the cases when $a = 0$ and $b = 2$ are used to generate the key.

This protocol is quite standard for DIQKD apart from the fact that usually only a number of runs sublinear in N are used for the parameter estimation. The reason why we need a sample of linear size is the weak randomness in the possession of the parties. From [10] we already know that Alice and Bob cannot have any secure protocol with a smaller test sample under these conditions (and we give the explicit proof for the DIQKD scenario in Sec. A 1).

In order to analyze the protocol we take the same approach as Ref. [10] in quantifying the imperfection of the randomness using the min-entropy loss rate. Min-entropy is the measure of choice because any source generating the bits that has any type of randomness will also exhibit nonzero min-entropy. This measure makes our result completely general as it is quite easy to compute the min-entropy loss rate of any source specified using a different measure. For example, Santha-Vazirani (S-V) sources [18] have a min-entropy loss rate of $L = 1 + \log_2(\frac{1}{2} - \epsilon)$. Therefore our result can, in a straightforward manner, be applied to S-V sources. The same holds for sources which are bit fixing, biased, or described by some Renyi entropy [19]. On the other hand, if we would choose any other measure of randomness, relating it to others would be not possible; e.g., bit-fixing sources, which simply fix some fraction of the bits in advance and choose the rest at random, are indistinguishable from a fully deterministic source from an S-V point of view.

Let (M, b) denote an imperfect source of randomness that creates strings of length M , according to a probability distribution with min-entropy b . We quantify the bias of the source by the min-entropy loss rate denoted $L = \frac{M-b}{M}$.

III. THE MOST GENERAL ATTACK EXPLOITING BAD RANDOMNESS IN THE SIFTED KEY GENERATION

The protocol described above generates a sifted key, which can later be turned into the secret key via classical privacy amplification and error-correction procedures. Although these

procedures also require randomness, their analysis falls outside the scope of this paper, and we are interested in the most general attack on the “quantum” part of the protocol. First, let us focus on the randomness in the choice of the settings.

The min-entropy loss rate L is the resource that the adversary uses to attack the protocol. It can be directly related to her probability of guessing the settings in each round of the protocol. For clarity, we can divide the guessing into two parts. The first is deciding whether $b = 2$, or, in other words, whether this round is used for parameter estimation. The second is guessing the measurement settings in each round.

Eve's goal is to learn as much of the sifted key as possible while remaining undetected. When $b = 2$, then the adversary aims to maximize her correlations with Alice. If $b < 2$, her aim is to hide her interference. The limits of her resource make it impossible to know the value of b in every round. Since the strategy optimal for $b = 2$ gives her more information about the key than the one for $b < 2$, the optimal attack is to use the strategy for $b = 2$ even in some rounds used for parameter estimation provided that she can avoid detection.

The strategy optimal for $b = 2$ is to prepare a product state (its details are discussed later), but if L is large enough, we will see that it also becomes the optimal strategy for $b < 2$. In this case we have no hopes for security.

Our protocol has two important parameters: the amount of CGLMP violation and the fraction f of the rounds used for parameter estimation. Now we find the lower bounds for both of these as functions of L .

IV. BELL INEQUALITY VIOLATION AS A SECURITY CHECK

In the device-independent protocols the key ingredient is the parameter estimation phase where the parties estimate the violation of the Bell inequality. However, to test it some randomness is required. To our knowledge, in all the works on device-independent protocols it is assumed that this randomness is perfect. The attack presented in [10] used only the fact that weak randomness can let Eve choose a subset of runs that she knows is not used for parameter estimation. But weak randomness of the settings leads to an increase of the local bound, which, in turn, leads to another loophole in quantum cryptography [20]. Although, in addition to [20], there have been other works that studied the dependence of the local bound on the input randomness, either they have been restricted to Clauser-Horne-Shimony-Holt (CHSH) inequality [21], or the randomness was measured in terms of conditional Shannon entropy [22]. Therefore we need to adapt the methods from [22] to find the local bound on CGLMP as a function of the min-entropy loss rate.

We start by expressing CGLMP in a “normalized” form,

$$\begin{aligned} \frac{1}{4} [& P(A \leq B | a = 0, b = 0) + P(B \leq A | a = 0, b = 1) \\ & + P(A \leq B | a = 1, b = 1) \\ & + P(B < A | a = 1, b = 0)] \leq \frac{3}{4}, \end{aligned} \quad (1)$$

where a and b denote the settings of Alice and Bob, respectively, and A and B are their outcomes. This is a normalized variant of CGLMP first introduced in [23].

One approach to Bell inequalities is to treat them as nonlocal games. We can think of the parties receiving their inputs from

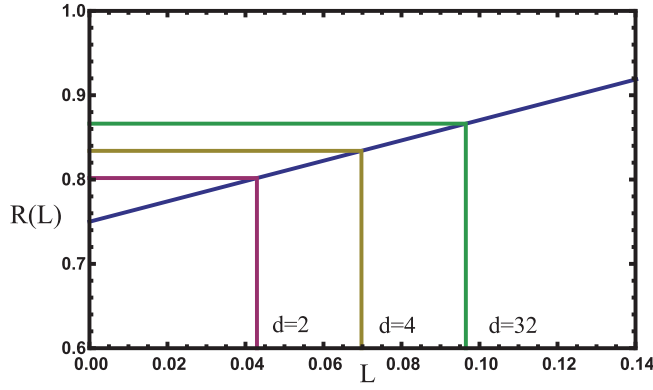


FIG. 1. (Color online) Here we plot the maximal expectation value of the normalized CGLMP inequality, with product states that are distributed by Eve, as a function of the min-entropy loss rate L . For comparative purposes we also include three exemplary violations by maximally entangled states of dimension $d = 2$, $d = 4$, and $d = 32$. It follows directly from this relation that if the min-entropy loss rate L exceeds ≈ 0.043 , there is no hope of a secure protocol using qubits.

the referee, who assures them that they are chosen according to uniform probability distribution. He can, however, be wrong or lying. What happens then is Alice and Bob play the game with the strategy optimized for the uniform distribution of settings even though they are not. Effectively, they are trying to violate inequality:

$$\begin{aligned} p_{00}P(A \leq B|a=0, b=0) + p_{01}P(B \leq A|a=0, b=1) \\ + p_{10}P(A \leq B|a=1, b=1) \\ + p_{11}P(B < A|a=1, b=0) \leq R, \end{aligned} \quad (2)$$

where p_{ij} is the probability of Alice getting setting i and Bob getting j . Furthermore, these probabilities change each round. In Sec. A 2 we give the details of the proof that the optimal violation that can be achieved with product states for a given min entropy loss rate L is given by

$$R(L) = \frac{3}{4} + \frac{L}{2(2 - \log_2 3)}. \quad (3)$$

This bound is plotted in Fig. 1, and it becomes the crucial local bound that Alice and Bob need to violate if they want to have a chance for security.

V. SECURITY CONSIDERATIONS

However, violating the local bound is only a necessary condition for the security. It is known [9] that the key rate in the DIQKD protocol with commuting observables secure against general attacks is lower bounded by

$$K \geq H_{\min}(A|E) - \frac{N_{\text{pub}}}{N_{\text{key}}}, \quad (4)$$

where $H_{\min}(A|E)$ is the min-entropy rate of Alice's bit of the key conditioned on Eve's information, N_{pub} is the amount of communication in the error-correction and privacy-amplification phases, and N_{key} is the length of the key. In Secs. A 3 and A 4 we show that the violation of the local bound in the CGLMP inequality implies $H_{\min}(A|E) > 0$, and indeed we can even infer a lower bound $H_{\infty}(A|E) \geq \frac{R_{\text{obs}} - R(L)}{2 \ln 2}$, where R_{obs} is the average value of the CGLMP measured by the parties.

Error correction and privacy amplification imply that whenever $a = 0$ and $b = 2$, the correlations are provably perfect. This forces Eve to use the states that give maximal correlation between the parties for settings $a = 0$ and $b = 2$ as the part of her strategy optimal for $b = 2$. This is in contrast to the attack proposed in [10], where in most of the rounds not used for parameter estimation Eve tries to decrease the correlations between Alice and Bob. This attack can remain undetected under the assumption of sublinear sample size.

If the violation of CGLMP is large enough, we know that we can have a secure protocol, but we still have to find out the size of the test sample f .

From the considerations presented earlier we know that the optimal strategy for Eve is to use the strategy optimal for $b < 2$ in kN rounds with $k \leq f$ and the strategy optimal for $b = 2$ in the rest of them. The strategy optimal for $b < 2$ is, obviously, to send the state that violates CGLMP the most for the given number of outcomes. The strategy optimal for $b = 2$ is to send the product state $|\psi\rangle$. Of course, the closer Eve wants to bring k to f , the more min-entropy loss L she has to induce:

$$L_N = \frac{\log_2 \binom{N}{fN} - \log_2 \binom{(1-k)N}{(1-f)N}}{\log_2 \binom{N}{fN}}, \quad (5)$$

which for large N approaches

$$L(k, f) = \lim_{N \rightarrow \infty} L_N = \frac{-f \log_2(f) - (1-k) \log_2(1-k) + (f-k) \log_2(f-k)}{h(f)}, \quad (6)$$

where $h(\cdot)$ is Shannon's binary entropy function.

At the same time the closer k is to f , the larger the Bell inequality violation that the parties can observe is. In $\frac{k}{f}$ of the rounds used to estimate CGLMP the state that violates it maximally for the given number of outcomes is distributed. Let us denote this violation by $R_Q(L, d)$. In the remaining $\frac{f-k}{f}$ rounds the state distributed is $|\psi\rangle$, and since it is a product

state, the maximal violation is $R(L)$. Therefore the violation observed can be at most

$$R_{\text{obs}} \leq \frac{k}{f} R_Q(L, d) + \frac{f-k}{f} R(L), \quad (7)$$

which implies

$$k \geq f \frac{R_{\text{obs}} - R(L)}{R_Q(L, d) - R(L)}. \quad (8)$$

$R_Q(L, d)$ is the maximal quantum violation of the CGLMP inequality with d outcomes and the min-entropy loss rate of the randomness of the settings L . There are no known methods of finding this value. However, we can always bound it by the algebraic bound: $R_Q(L, d) \leq 1$, which implies

$$k \geq f \frac{R_{\text{obs}} - R(L)}{1 - R(L)} = k(R_{\text{obs}}, L). \quad (9)$$

Plugging this into (6), we obtain

$$L \geq L(k(R_{\text{obs}}, L), f), \quad (10)$$

which can be solved for any value of L giving a lower and an upper bound on the fraction f of the rounds used for parameter estimation (Fig. 2). There is an upper bound due to the fact that f is the fraction of rounds to be tested with the CGLMP inequality. Here Eve needs to make sure that she restricts most of them to a sample space that she knows with certainty. Counterintuitively, if f is chosen to be too large, this task actually gets easier for Eve, aiding her attack.

Now we also need to discuss another lower bound for f . For $N \rightarrow \infty$ it will also be arbitrarily small due to infinite precision in the measurement of R_{obs} . But in every practical scenario we have to face the fact that we only have a limited number of runs and R_{obs} will always carry experimental error bars from its statistical deduction. So depending on the statistical fidelity which we aim for in a finite number of runs, we will have to choose a large enough fraction of N runs to guarantee that such precision is possible to attain in fN runs. This lower bound is easy to calculate for any specific implementation, but because it also depends on the experimental settings and errors, we do not present a detailed analysis of this lower bound. We

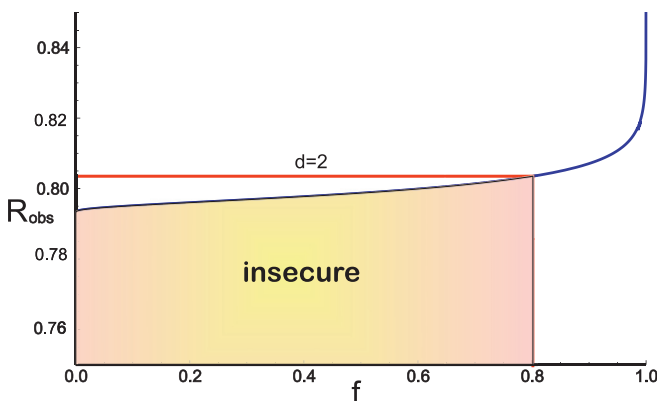


FIG. 2. (Color online) Here we depict the lower bound on the observed violation R_{obs} for different linear fractions f and for a fixed value of min-entropy loss rate $L = 0.03$. As in this case $R(L) = 0.786141$, we know we need to observe a strictly larger violation to provide security, and we see that if the violation is high enough, we can indeed choose any f . For qubits $d = 2$ the fundamental limit is $R_{\text{obs}} \leq 0.801777$, which fundamentally constrains $f \leq 0.723026$, whereas with $d = 4$ one can already reach $f \leq 0.999416$.

want to point out, however, that it can, in a realistic setting, be significantly larger than the upper bound on f for qubits.

VI. CONCLUSION AND OUTLOOK

In conclusion we have shown that even in DIQKD settings security can be compromised if the local randomness is not uniform. We explicitly derive the fundamental bounds on the randomness quality in this setting and, consequently, demonstrate that high-dimensional entanglement is indeed more powerful than mere qubit entanglement. Thus not only have we shed light on the role of randomness in the security of DIQKD protocols, but at the same time we have provided a clear example where the generation of high-order entanglement opens up new paths in quantum cryptography.

For the fundamental introduction of the protocol we have looked at an idealized scenario. We can, however, also apply the same reasoning without assuming perfect correlations (discussed in Sec. A 5) and even deal with attacks exploiting weak randomness in the error-correction and privacy-amplification phases (see Sec. A 6) and also considering different types of entropy loss in the randomness generators. The basis for the improvement of the protocol remains the same, however. A higher violation of Bell inequalities through higher dimensions increases the randomness of the outcomes and strengthens the protocols, while a higher number of outcomes increases the key rate. A full analysis of different scenarios is under preparation.

It should also be noted that this protocol is not necessarily only usable in situations where the randomness quality exceeds a bound for qubits. If the min-entropy loss rate assumed is small enough that the protocol would also potentially be achievable using qubit systems, it still pays off greatly to use the high-order entanglement due to the fact that with every measurement multiple bits of the key are generated [i.e., $\log_2(d)$ bits], and there is no downside once such high-dimensional entanglement is readily available. That is proven by numerous recent experimental results that achieve high-order entanglement up to $d \approx 50$ in Ref. [16], which provides more than five bits per measurement outcome. Also there exist different possibilities for implementing such high dimensions in photonic systems, e.g., in path (Ref. [12]) or a large family of orbital angular momentum modes (e.g., Ref [13]).

ACKNOWLEDGMENTS

We want to thank Sven Ramelow and the members of IQOQI Vienna for initial fruitful discussions. Furthermore we would like to thank Jan Bouda, Martin Plesch, Matej Pivoluska, and Andreas Winter for insightful comments on the manuscript. M.H. also acknowledges funding from the FP7-MarieCurie grant “Quacocos.” M.P. acknowledges support from UK EPSRC, FNP TEAM, ERC grant QUOLAPS, and NCN Grant No. 2012/05/E/ST2/02352.

APPENDIX

1. Impossibility of sublinear sample size

In the protocol we use a linear size of the test sample for both CGLMP correlations and the ones for $a = 0$ and

$b = 2$. One could ask if this is indeed necessary. Because the conditions on Eve's attack and the setting of our protocol are substantially different from the one presented in [10], we cannot use the attack presented there to prove the insecurity of the protocol. However, we can find an attack which works, with slight modifications in both settings. Let us start with the device-independent one.

If the test sample is of the size $N^{1-\alpha}$, then Eve can choose a number k such that $kN > N^{1-\alpha}$. Because we are interested in the limit of large N 's, k can be chosen arbitrarily small. Eve exploits the weak randomness of the parties to make sure that the $N^{1-\alpha}$ rounds for CGLMP inequality testing are taken from kN predetermined rounds. In these rounds Eve sends the state that Alice and Bob hope to have in all of them. In the rest of the rounds she prepares product state $|\psi\rangle = |x\rangle_{a=0}|x\rangle_{b=2}$, where the indices denote the bases.

In this case the CGLMP inequality violation is estimated only in the rounds where the state is entangled and, at the same time, the correlations for $a = 0$ and $b = 2$ are perfect in all the cases. This means that the parties will not detect Eve, while $H_\infty(A|E) < k$ can be made arbitrarily small for large N .

The min-entropy loss rate in this case can also be made arbitrarily small since

$$\lim_{N \rightarrow \infty} \frac{\log_2 \left(\frac{N}{N^{1-\alpha}} \right) - \log_2 \left(\frac{kN}{N^{1-\alpha}} \right)}{\log_2 \left(\frac{N}{N^{1-\alpha}} \right)} = 0. \quad (\text{A1})$$

The version of this attack for the prepare-and-measure scenario involves Eve not interacting in the kN rounds used to check the correlations and measuring the system in the $(1-k)N$ rounds in a random basis and sending the state that she got to Bob. It also leads to arbitrarily low min-entropy with arbitrarily good randomness.

2. Bell inequality violation as a security check

From [22] we know that the local bound for the CGLMP game played with imperfect randomness is $1 - r$, where

$$\begin{aligned} H_\infty &= -\log_2 \max_{a_1, \dots, a_M, b_1, \dots, b_M} P(a_1, \dots, a_M, b_1, \dots, b_M) = -\log_2 \max_{a_1, \dots, a_M, b_1, \dots, b_M} \prod_{i=1}^M P(a_i, b_i | a_{i-1}, \dots, a_M, b_{i-1}, \dots, b_M) \\ &\leq -\log_2 \prod_{i=1}^M \max_{a_i, b_i} P(a_i, b_i | a_{i-1}, \dots, a_M, b_{i-1}, \dots, b_M) = H_\Sigma \end{aligned} \quad (\text{A5})$$

and

$$L = \frac{2M - H_\infty}{2M} = 1 - \frac{H_\infty}{2M}, \quad (\text{A6})$$

we get

$$R \leq \frac{3}{4} + \frac{L}{2(2 - \log_2 3)} = R(L). \quad (\text{A7})$$

$r = \min_{a,b} P(a,b)$. The lowest amount of min-entropy for a particular value of r is attained by the distribution $(r, \frac{1-r}{3}, \frac{1-r}{3}, \frac{1-r}{3})$. This leads to the local bound in the terms of min-entropy,

$$R \leq \min\{3 \times 2^{-H_\infty(a,b)}, 1\}. \quad (\text{A2})$$

As soon as this value reaches the quantum bound, there is no possibility of the experimental verification that the measured state is not classical and no hopes for secure QKD. The quantum bound, however, depends on the dimension of the measurement system and approaches 1 as $d \rightarrow \infty$ [24]. This value is obtained by a min-entropy of $\log_2 3 \approx 1.585$; however, the critical value is smaller for any state of finite dimension. The quantum bound on the normalized CGLMP inequality [Eq. (1)] is 0.8177 for $d = 2$ and 0.8516 for $d = 5$ [23], which translates to critical min-entropies of 1.875 and 1.817, respectively.

For an experiment repeated many times, in the i th run the bound is $R_i = \min\{3 \times 2^{-H_\infty^i}, 1\}$, where H_∞^i is the min-entropy of the settings in the i th round conditioned on the events from the setting generation for the previous rounds. Let us see how big the average $R = \frac{1}{M} \sum_{i=1}^M R_i$ can be for a given sum of the entropies $H_\Sigma = \sum_{i=1}^M H_\infty^i$. Clearly, it is pointless for the adversary to set H_∞^i lower than $\log_2 3$ of any i as it does not increase the bound. In region $H_\infty \in [\log_2 3, 2]$ R is convex, so the optimal strategy is to use m instances of settings with entropy $\log_2 3$ and $M - m$ instances with entropy 2, where

$$\log_2 3m + 2(M - m) = H_\Sigma, \quad (\text{A3})$$

which gives $m = \frac{2M - H_\Sigma}{2 - \log_2 3}$. This will give the local bound

$$R \leq \frac{1}{M} \left(m + \frac{3}{4}(M - m) \right) = \frac{3}{4} + \frac{1 - \frac{H_\Sigma}{2M}}{2(2 - \log_2 3)}. \quad (\text{A4})$$

Because the total min-entropy of the source is

3. The sufficiency of the violation of the CGLMP inequality

Lemma 1. The violation of the local bound in the CGLMP inequality implies $H_{\min}(A|E) > 0$.

Proof. Let us assume that there exists a setting of Alice, say $a = 0$, such that $\max_A P(A|a = 0) = 1$, which corresponds to zero min-entropy. In such a case, instead of measuring

with the setting $a = 0$, Alice can always just return to the outcome which is certain without making any measurement at all. In other words, she can measure observable $\mathbb{1}$. In [25] it was shown that if all the observables for one party are compatible (can be measured simultaneously), then the no-signaling, quantum, and local bounds are the same. But $\mathbb{1}$ and any observable that is measured for $a = 1$ are compatible, so the local bound cannot be violated even by no-signaling theory. QED.

4. Lower bounding min-entropy of Eve

Theorem 1. In the scenario presented above $H_\infty(A|E) \geq \frac{R_{\text{obs}} - R(L)}{2 \ln 2}$, where R_{obs} is the average value of the CGLMP measured by the parties.

Proof. Let us take a setting of Alice, say $a = 0$, such that $\max_A P(A|a = 0) = p$ and consider a procedure similar to the one in Lemma 1 but with the outcome of the identity measurement set to the A for which this maximum is reached. From Lemma 1 we know that in this case the bound R cannot be violated. However, it still could be violated if for the $a = 0$ measurement an A_0 different than $\mathbb{1}$ is used.

If the value of CGLMP for the strategy with A_0 is

$$\begin{aligned} p_{00}P(A \leq B|a = 0, b = 0) + p_{01}P(B \leq A|a = 0, b = 1) \\ + p_{10}P(A \leq B|a = 1, b = 1) \\ + p_{11}P(B < A|a = 1, b = 0) = Q, \end{aligned} \quad (\text{A8})$$

then the value for the strategy with $\mathbb{1}$ is at least

$$\begin{aligned} p(p_{00}P(A \leq B|a = 0, b = 0) \\ + p_{01}P(B \leq A|a = 0, b = 1) \\ + p_{10}P(A \leq B|a = 1, b = 1) \\ + p_{11}P(B < A|a = 1, b = 0) \\ = Q - (1 - p)[p_{00}P(A \leq B|a = 0, b = 0) \\ + p_{01}P(B \leq A|a = 0, b = 1)], \end{aligned} \quad (\text{A9})$$

and this has to be less than or equal to R . Because the outcome probabilities are bounded by 1 and the setting probabilities are bounded by the exponent of min-entropy, we get

$$Q \leq R + (1 - p)2^{1-H_\infty} \quad (\text{A10})$$

or

$$p \leq 1 - 2^{H_\infty-1}(Q - R). \quad (\text{A11})$$

In an experiment repeated M times the min-entropy rate of Eve is

$$\begin{aligned} H_\infty(A|E) &= -\frac{1}{M} \log_2 \prod_{i=1}^M p_i = -\frac{1}{M} \sum_{i=1}^M \log_2 p_i \\ &\geq \frac{1}{M 2 \ln 2} \sum_{i=1}^M 2^{H_i} (Q_i - R_i) \\ &\geq \frac{1}{M 2 \ln 2} \sum_{i=1}^M Q_i - R_i \\ &\geq \frac{R_{\text{obs}} - R(L)}{2 \ln 2} = H(L), \end{aligned} \quad (\text{A12})$$

where in the last three inequalities we have used, respectively, the logarithm's power series expansion, the positivity of the min-entropy, and formula (A7). Bound $H(L)$ is far from optimal since the approximations made are pretty coarse. For a specific outcome alphabet much better bounds probably exist.

5. Nonperfect correlations

In the case where one does not assume perfect correlations of the measurement outcomes in the rounds where Alice uses basis 0 and Bob uses basis 2, due to noise in the system, the situation becomes a little more involved. Alice's basic strategy, as well as the improvement from higher dimensions, remains the same.

In this case Eve's resource is still L . If it is larger than zero, it means that some choices of the rounds where the correlations are tested are more probable than the others. Her choice of strategy for each is a pair of numbers: the guessing probability p and the Bell expression expectation value I . They are connected by the relation $p_G \leq f(I)$. It follows directly from (A11) that

$$p \leq f(I) = 1 - 2^{H_\infty-1}[I - R(L)]. \quad (\text{A13})$$

These numbers for each round have to be chosen in advance, and this choice depends on the probability distribution of the tested rounds. Whatever strategy Eve chooses, there is a choice for the test sample which is optimal, from Eve's point of view, for this strategy, and for each choice of the test sample there is an optimal strategy.

There are two factors that Eve has to consider when choosing her strategy: the observed Bell inequality violation and her average guessing probability of the bit of the key. Eve's target is to maximize the latter while keeping the former above a certain threshold. If $L < 1$, then there is some uncertainty in the choice of the test sample, and Eve cannot be sure that the choice will be optimal for her strategy. For every strategy we can list all the choices of the sample according to the value of Eve's target function in decreasing order. Her guessing probability is their weighted average, and the only constraint on the weights (which are the probabilities of choosing them as a sample) is that the largest is $p_{\text{max}} 2^{H_\infty} = 2^{M(1-L)}$, where M is the number of bits necessary for the description of the test sample. This means that the best distribution of the probabilities is (M, p_{max}) flat.

Because Eve's strategy is product, i.e., the numbers I and p_G are chosen in advance for each round and do not depend on the actual numbers produced by the generators, it is optimal for her to concentrate her knowledge of the choice of the sample on the information about particular rounds rather than on the relations between them. In other words, it is better for her to know that the sample will certainly be tested in round 1 and have a 50% probability of being tested in round 2 rather than knowing that the sample will certainly be tested in exactly one of these rounds, although the min-entropy is the same in both cases.

Therefore the most general strategy for Eve is to know a fraction a of all the rounds when the Bell inequality is definitely tested and a fraction b when it is definitely not tested. If the tested fraction is f , then, obviously, $a \leq f$ and $b \leq 1 - f$.

The min-entropy loss is

$$L = \frac{\log_2 \binom{N}{fN} - \log_2 \binom{(1-a-b)N}{(f-a)N}}{\log_2 \binom{N}{fN}}, \quad (\text{A14})$$

the observed Bell inequality violation is

$$R_{\text{obs}} \leq \frac{a}{f} \beta_{QM}(L) + \frac{f-a}{f} I, \quad (\text{A15})$$

and Eve's average guessing probability is

$$p_{av} = \frac{b}{1-f} + \frac{1-f-b}{1-f} p_G. \quad (\text{A16})$$

β_{QM} is the maximal quantum violation of CGLMP with min-entropy loss rate L . It comes from the rounds when Eve is sure that the testing takes place. In the rounds when she knows nothing she uses p_G and I related by (A13). These equations can again be numerically solved for any given pair of L and R_{obs} to optimize the strategy and calculate the lower and upper bounds for security considerations. The basic mechanism behind the advantage of higher-dimensional systems, however, remains the same. We plan to extensively survey these generalized scenarios, also including other types of randomness loss in future publications.

6. Error correction and privacy amplification

The final stages of every key distribution protocol are error correction (EC) and privacy amplification (PA). Their purpose is to provide Alice and Bob with a key whose copies are identical for both parties and completely unknown to Eve. These stages also require randomness, and so far in all the works it has been assumed that this randomness is perfect. If weak randomness is used, it opens another avenue for the eavesdropper's attacks. In the main text we mention this possibility and state that since EC and PA are purely classical procedures, they lie out of the scope of this paper. However, in a forthcoming work we plan to include them in our analysis and prove the following conjecture.

Conjecture 1. In the scenario discussed in this paper EC and PA are possible if

$$H(L) - H(A|B) > L, \quad (\text{A17})$$

where $H(L)$ is given by formula (A12), $H(A|B)$ is the conditional Shannon entropy rate of Alice's key conditioned on Bob's, and L is the min-entropy loss rate of their source.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984), pp. 175–179.
 - [2] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, *Nat. Commun.* **2**, 349 (2011).
 - [4] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, *Phys. Rev. Lett.* **107**, 170404 (2011).
 - [5] D. Mayers and A. Yao, in *Proceedings of the 39th IEEE Conference on Foundations of Computer Science, 1998* (IEEE, Piscataway, 1998), p. 503; [arXiv:quant-ph/9809039](#); *Quant. Inf. Comput.* **4**, 273 (2004).
 - [6] J. Barrett, L. Hardy, and A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005).
 - [7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
 - [8] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *New J. Phys.* **11**, 045021 (2009).
 - [9] Ll. Masanes, S. Pironi, and A. Acín, *Nat. Commun.* **2**, 238 (2011).
 - [10] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, *Phys. Rev. A* **86**, 062308 (2012).
 - [11] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, *Nature (London)* **412**, 3123 (2001).
 - [12] C. Schaeff, R. Polster, R. Lapkiewicz, R. Fickler, S. Ramelow, and A. Zeilinger, *Opt. Express* **20**, 16145 (2012).
 - [13] M. Krenn, R. Fickler, M. Huber, R. Lapkiewicz, W. Plick, S. Ramelow, and A. Zeilinger, *Phys. Rev. A* **87**, 012326 (2013).
 - [14] R. Fickler, R. Lapkiewicz, W. N. Plick, M. Krenn, C. Schaeff, S. Ramelow, and A. Zeilinger, *Science* **338**, 640 (2012).
 - [15] S. Zhao, L. Gong, Y. Li, H. Yang, Y. Sheng, X. Dong, F. Cao, and B. Zheng, [arXiv:1205.0851](#) [quant-ph].
 - [16] J. Romero, D. Giovannini, S. Franke-Arnold, S. M. Barnett, and M. J. Padgett, *Phys. Rev. A* **86**, 012334 (2012).
 - [17] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, *Phys. Rev. Lett.* **88**, 040404 (2002).
 - [18] M. Santha and U. Vazirani, in *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS-84)* (IEEE Computer Society, New York, 1984), p. 434.
 - [19] S. Vadhan, *Pseudorandomness: Foundations and Trends in Theoretical Computer Science* (Now Publishers Inc, Boston - Delft, 2012).
 - [20] J. Kofler, T. Paterek, and C. Brukner, *Phys. Rev. A* **73**, 022104 (2006).
 - [21] T. Lawson, N. Linden, and S. Popescu, [arXiv:1011.6245](#) [quant-ph].
 - [22] M. Pawłowski, K. Horodecki, P. Horodecki, and R. Horodecki, in *Quantum Cryptography and Computing*, edited by R. Horodecki, S. Kilin, and J. Kowalik (IOS Press, Amsterdam, 2010), pp. 224–230.
 - [23] S. Zohren and R. D. Gill, *Phys. Rev. Lett.* **100**, 120406 (2008).
 - [24] S. Zohren, P. Reska, R. D. Gill, and W. Westra, *Europhys. Lett.* **90**, 10002 (2010).
 - [25] M. Pawłowski and Č. Brukner, *Phys. Rev. Lett.* **102**, 030403 (2009).