Article:
Farkas, Mate (2024) Unbounded Device-Independent Quantum Key Rates from Arbitrarily Small Nonlocality. Physical Review Letters. 210803. ISSN 1079-7114

https://doi.org/10.1103/PhysRevLett.132.210803

Unbounded Device-Independent Quantum Key Rates from Arbitrarily Small Nonlocality

Máté Farkas*
Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom

(Received 26 October 2023; accepted 10 April 2024; published 22 May 2024)

Device-independent quantum key distribution allows for proving the security of a shared cryptographic key between two distant parties with potentially untrusted devices. The security proof is based on the measurement outcome statistics (correlation) of a Bell experiment, and security is guaranteed by the laws of quantum theory. While it is known that the observed correlation must be Bell nonlocal in order to prove security, recent results show that Bell nonlocality is in general not sufficient for standard device-independent quantum key distribution. In this work, we show that conversely, there is no lower bound on the amount of nonlocality that is sufficient for device-independent quantum key distribution. Even more so, we show that from certain correlations that exhibit arbitrarily small nonlocality, one can still extract unbounded device-independent key rates. Therefore, a quantitative relation between device-independent key rates and Bell nonlocality cannot be drawn in general. Our main technique comprises a rigorous connection between self-testing and device-independent quantum key distribution, applied to a recently discovered family of Bell inequalities with arbitrarily many measurement outcomes.

DOI: 10.1103/PhysRevLett.132.210803

Introduction.—Device-independent quantum key distribution (DIQKD) allows two distant parties to establish a secure cryptographic key without having to trust the devices they use in the protocol [1–4]. The security of the key is guaranteed solely by the laws of quantum physics. DIQKD solves two problems present in other types of key distribution protocols: it does not rely either on the hardness of computational problems (like most nonquantum key distribution schemes [5–7]), or on the characterization of the devices used in the protocol (like standard quantum key distribution schemes [8–10]). While the practicality of DIQKD still poses challenges, the first proof-of-principle experiments were carried out recently [11–13], demonstrating that DIQKD can be achieved with current technology. Remaining challenges include increasing the key rates and the distance over which the protocols can be implemented, noting that increasing the key rates naturally leads to an increase in the achievable distance as well [3,4].

This work is concerned with characterizing fundamental resources necessary for achieving high key rates. The key rate of a protocol is the number of secret bits that can be produced in a given round of the protocol, and we will compare key rates with *Bell nonlocality* [14], a naturally connected notion: in a DIQKD protocol, two parties measure a bipartite quantum system locally, and the final key is extracted from the measurement outcomes. It is known that DIQKD is possible only if these measurement outcome statistics demonstrate nonlocal correlations (i.e., they violate a Bell inequality) [1,2]. It is, however, less clear how the amount of nonlocality (or Bell inequality violation) relates to the achievable key rate. In fact, recently it was shown that nonlocality in itself is not sufficient for the security of a large class of DIQKD protocols [15]. That is, there exist correlations that violate a Bell inequality, but cannot be used for DIQKD using standard techniques. In this work, we show a somewhat opposing statement: one can extract unbounded key rates from certain correlations that violate Bell inequalities arbitrarily weakly. Furthermore, these protocols also only use standard techniques. Therefore, one can conclude that (standard) DIQKD key rates and Bell nonlocality are incomparable resources, and achieving large key rates does not necessarily imply a large amount of nonlocality.

Preliminaries.—Any DIQKD protocol starts with the measurement stage: two parties, Alice and Bob, locally measure their part of a fresh copy of a bipartite quantum state ρ defined on the tensor product of two Hilbert spaces, $\mathcal{H}_A \otimes \mathcal{H}_B$. Every time they measure, it constitutes a round of the protocol. In every round, they can decide to perform one of (finitely) many available measurements. For Alice, these measurement settings are denoted $x \in \{0, 1, \ldots, n_A - 1\} =: [n_A]$, and for Bob, $y \in [n_B]$. In each round they obtain a measurement outcome, labeled by $a \in [k_A]$ for Alice and $b \in [k_B]$ for Bob. Once they have obtained their respective outcomes, a new round begins with a fresh copy of ρ. They perform many rounds (in this

work we are interested in the asymptotic limit of infinitely many rounds) and record their settings and outcomes, which concludes the measurement stage.

After this, Alice and Bob estimate the *correlation*, that is, the joint probability distribution $p(a,b|x,y)$ of the outcomes conditioned on the measurement settings. The estimation is done by publicly announcing a small subset of their inputs and outputs, after which this subset of their data is discarded.

Quantum theory dictates that the correlation will be given by the Born rule,

$$p(a,b|x,y) = \mathrm{tr}\left[\left(A_a^x \otimes B_b^y\right)\rho\right], \tag{1}$$

where $\{A_a^x\}_a$ and $\{B_b^y\}_b$ represent positive-operator-valued measures (POVMs) for every x and y. It is important to note at this point that certain quantum correlations are *nonlocal*, i.e., roughly speaking they do not have a classical physical description [14]. The nonlocality of a correlation is witnessed by the violation of a *Bell inequality*, a linear inequality on the correlation that is satisfied by all classical correlations (classical correlations are said to be in the *local set*). It is an important prerequisite for a correlation to violate a Bell inequality in order for it to be useful for DIQKD [1,2].

Returning to the steps of a DIQKD protocol, once they have estimated the correlation, Alice and Bob decide whether the correlation is satisfactory for DIQKD (based on criteria that we will discuss next). If it is not, they abort the protocol. If the correlation passes the test, they employ privacy amplification and error correction on their remaining data (on the recorded inputs and outputs that were not discarded) [16–18]. This is done via public, but authenticated classical communication channels. At the end of the privacy amplification and error correction stage, Alice and Bob are each left with a string of bits that are perfectly random (as a result of privacy amplification) to any potential eavesdropper limited by the laws of quantum physics. Moreover, these strings of bits are exactly the same for Alice and Bob, as a result of error correction. The asymptotic key rate, r, is then defined as the length of this bit string, divided by the number of rounds, taking the limit of infinitely many rounds.

One of the seminal results of (device-independent) quantum key distribution is a universal lower bound on the achievable key rate from a given correlation. The bound quantifies the key rate that can be extracted from the outcomes of the "key settings" $\hat{x}$ on Alice's side and $\hat{y}$ on Bob's side, by performing privacy amplification and error correction via one-way communication from Alice to Bob. The bound is referred to as the Devetak-Winter rate [19], and in our context it is given by

$$r \geq H(A|E) - H(A|B), \tag{2}$$

where $H(A|E) = \inf_{|\psi\rangle,\{A_a^x\},\{B_b^y\}}\{H(A|E)_\sigma\}$ is the infimum over all states $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ that are a purification of a state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$, and over all POVMs A_a^x on $\mathcal{H}_A$ and B_b^y on $\mathcal{H}_B$ such that the state and the measurements are compatible with the observed correlation, $\mathrm{tr}[(A_a^x \otimes B_b^y)\rho] = p(a,b|x,y)$. Furthermore, $H(A|E)_\sigma$ is the conditional von Neumann entropy of the corresponding classical-quantum state

$$\sigma_{AE} = \sum_{a \in [k_A]} |a\rangle\langle a| \otimes \mathrm{tr}_{AB}\left[\left(A_a^{\hat{x}} \otimes \mathbb{I}_B \otimes \mathbb{I}_E\right)|\psi\rangle\langle\psi|\right], \tag{3}$$

and $H(A|B)$ is the conditional Shannon entropy of the distribution $p(a,b|\hat{x},\hat{y})$. Note that an analogous bound holds for the case of one-way communication from Bob to Alice, and that the bound on r only depends on the observed correlation $p(a,b|x,y)$. Furthermore, this bound is valid against the most powerful, so-called coherent eavesdropping attacks [20–22]. If Alice and Bob cannot establish a positive lower bound for their key rate, they abort the protocol.

The term $H(A|E)$ captures the cost of privacy amplification (any eavesdropper's uncertainty of Alice's outcome), while the term $H(A|B)$ captures the cost of error correction (Bob's uncertainty of Alice's outcome). Since $H(A|B)$ can be directly computed from the correlation, the difficulty in estimating the Devetak-Winter bound is in bounding $H(A|E)$. Indeed, various methods have been proposed to bound this quantity for arbitrary correlations (and not just based on Bell inequality violation). General analytic techniques are lacking, while numerical techniques scale rather badly in the number of settings and outcomes [23–27].

It is important to note that while from a given correlation bounding $H(A|E)$ is the main difficulty, a good bound on $H(A|E)$ does not necessarily imply good (or even positive) key rates. For this, correlations with small $H(A|B)$ need to be found. Indeed, constant-sized device-independent randomness has been established from a small amount of nonlocality [28,29], but the same has not been done for DIQKD.

Self-testing and DIQKD.—In this work, we analytically tackle the problem of bounding private randomness from a specific type of correlations. In particular, we expose a rigorous connection between DIQKD and a strong certification technique in Bell nonlocality called *self-testing* [30]. We say that a correlation $p(a,b|x,y)$ self-tests the pure quantum state $|\tilde{\psi}\rangle \in \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$ and the measurements $\tilde{A}_a^x$ on $\mathcal{H}_{\tilde{A}}$ and $\tilde{B}_b^y$ on $\mathcal{H}_{\tilde{B}}$, if for all quantum states ρ on some Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$ and all measurements A_a^x on $\mathcal{H}_A$ and B_b^y on $\mathcal{H}_B$ such that $p(a,b|x,y) = \mathrm{tr}[(A_a^x \otimes B_b^y)\rho]$, we have that for every purification $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ of ρ

there exist Hilbert spaces $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ and local isometries $V_A\colon \mathcal{H}_A \to \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{A'}$ and $V_B\colon \mathcal{H}_B \to \mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{B'}$ such that

$$(V_A \otimes V_B \otimes \mathbb{I}_E)(A_a^x \otimes B_b^y \otimes \mathbb{I}_E)|\psi\rangle = (\tilde{A}_a^x \otimes \tilde{B}_b^y)|\tilde{\psi}\rangle \otimes |\mathrm{aux}\rangle \tag{4}$$

for some state $|\mathrm{aux}\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_E$ and for all x, y, a, b. The primary aim of self-testing is to characterize quantum states and measurements solely from the observed correlation in a Bell experiment, and many examples of self-testing are known [30].

Our main technical observation linking self-testing and DIQKD is that whenever a correlation self-tests some quantum state and measurements, the parties can extract private randomness from their measurements. In fact, it is sufficient that the weaker form of Eq. (4),

$$(V_A \otimes V_B \otimes \mathbb{I}_E)(A_a^{\hat{x}} \otimes \mathbb{I}_B \otimes \mathbb{I}_E)|\psi\rangle = (\tilde{A}_a^{\hat{x}} \otimes \mathbb{I}_{\tilde{B}})|\tilde{\psi}\rangle \otimes |\mathrm{aux}\rangle, \tag{5}$$

holds for some fixed $\hat{x}$ and for all a. Equation (5) follows from Eq. (4) by fixing $x = \hat{x}$ and summing up over b, and note that further summing up over a, we obtain

$$(V_A \otimes V_B \otimes \mathbb{I}_E)|\psi\rangle = |\tilde{\psi}\rangle \otimes |\mathrm{aux}\rangle. \tag{6}$$

The reason why condition (4) is sufficient for certifying private randomness is because the term $H(A|E)$ in Eq. (2) can be computed analytically if the correlation is self-testing [or the weaker condition (5) holds] as follows. For all tripartite states $|\psi\rangle$ and measurements A_a^x compatible with the observed correlation, we have

$$\begin{aligned}
\sigma_{AE} &= \sum_a |a\rangle\langle a| \otimes \mathrm{tr}_{AB}[(A_a^{\hat{x}} \otimes \mathbb{I}_B \otimes \mathbb{I}_E)|\psi\rangle\langle\psi|] = \sum_a |a\rangle\langle a| \otimes \mathrm{tr}_{AB}\left[(V_A^\dagger V_A \otimes V_B^\dagger V_B \otimes I_E)(A_a^{\hat{x}} \otimes \mathbb{I}_B \otimes \mathbb{I}_E)|\psi\rangle\langle\psi|\right] \\
&= \sum_a |a\rangle\langle a| \otimes \mathrm{tr}_{\tilde{A}A'\tilde{B}B'}\left[(V_A \otimes V_B \otimes I_E)(A_a^{\hat{x}} \otimes \mathbb{I}_B \otimes \mathbb{I}_E)|\psi\rangle\langle\psi|(V_A^\dagger \otimes V_B^\dagger \otimes I_E)\right] \\
&= \sum_a |a\rangle\langle a| \otimes \mathrm{tr}_{\tilde{A}A'\tilde{B}B'}\left[\left((\tilde{A}_a^{\hat{x}} \otimes \mathbb{I}_{\tilde{B}})|\tilde{\psi}\rangle_{\tilde{A}\tilde{B}} \otimes |\mathrm{aux}\rangle_{A'B'E}\right)\left(\langle\tilde{\psi}|_{\tilde{A}\tilde{B}} \otimes \langle\mathrm{aux}|_{A'B'E}\right)\right] \\
&= \sum_a |a\rangle\langle a| \otimes \mathrm{tr}\left[(\tilde{A}_a^{\hat{x}} \otimes \mathbb{I}_{\tilde{B}})|\tilde{\psi}\rangle\langle\tilde{\psi}|_{\tilde{A}\tilde{B}}\right]\mathrm{tr}_{A'B'}(|\mathrm{aux}\rangle\langle\mathrm{aux}|_{A'B'E}) = \left[\sum_a p_A(a|\hat{x})|a\rangle\langle a|\right] \otimes \sigma_E,
\end{aligned} \tag{7}$$

where $\sigma_E = \mathrm{tr}_{A'B'}|\mathrm{aux}\rangle\langle\mathrm{aux}|_{A'B'E}$ is some fixed quantum state on $\mathcal{H}_E$, $p_A(a|\hat{x}) = \sum_b p(a,b|\hat{x},y)$ is Alice's marginal distribution, and we used the conditions (5) and (6). The conditional von Neumann entropy in Eq. (2) is then given by (for all states and measurements compatible with the correlation)

$$\begin{aligned}
H(A|E)_\sigma &= H(AE)_\sigma - H(E)_\sigma \\
&= H\left(\sum_a p_A(a|\hat{x})|a\rangle\langle a| \otimes \sigma_E\right) - H(\sigma_E) \\
&= H\left(\sum_a p_A(a|\hat{x})|a\rangle\langle a|\right) + H(\sigma_E) - H(\sigma_E) \\
&= H(\{p_A(a|\hat{x})\}_a) = H(A),
\end{aligned} \tag{8}$$

where we used that the von Neumann entropy is additive under the tensor product. Therefore, the entropy $H(A)$ of Alice's outcome from measurement $\hat{x}$ is private, that is, no eavesdropper can guess it better than random. Note that a similar argument is used in the proofs of Ref. [29].

In order to promote this device-independent randomness certification statement to device-independent quantum key distribution, we need a measurement on Bob's side such that its outcome is correlated with the outcome of setting $\hat{x}$ of Alice. Such a choice maximizes the Devetak-Winter bound in Eq. (2) by minimizing $H(A|B)$. While such a highly correlated measurement setting $\hat{y}$ might already be part of the setup that gives rise to the self-testing correlation, notice that adding an extra setting on Bob's side does not change the calculation for Alice's private randomness. In particular, Eq. (5) still holds, as deriving this equation does not refer to the extra setting on Bob's side, which also highlights the general utility of condition (5). Therefore, for every correlation certifying Eq. (5), one can aim to find the best possible measurement for Bob that maximizes the device-independent key rate, i.e., given $|\tilde{\psi}\rangle$ and $\{\tilde{A}_a^{\hat{x}}\}_a$ from condition (5), one can attempt to find a measurement $\{B_b^{\hat{y}}\}_b$ minimizing $H(A|B)$.

Unbounded key from arbitrarily small nonlocality.—Using the above techniques, we will now prove that from correlations arbitrarily close to the local set (and therefore violating any Bell inequality arbitrarily weakly) one can extract $\log(d)$ bits of device-independent key for any integer $d \geq 2$. For this purpose, we need to use Bell inequalities with d outcomes. Various recent works have looked at such scenarios (also in the context of DIQKD) [31–34], and a family of inequalities particularly suitable for our purposes was introduced in Ref. [35]. The inequalities are

parametrized by an integer $d \geq 2$ and *overlap matrix* O, whose elements are characterized by two orthonormal bases on $\mathbb{C}^d$, which we choose to be $\{|j\rangle\}_{j=0}^{d-1}$ and $\{|e_k\rangle\}_{k=0}^{d-1}$. The elements of the overlap matrix are then given by

$$O_{jk} = |\langle j|e_k\rangle|. \tag{9}$$

In the Bell scenario, Alice has 2 measurement settings with d outcomes each and Bob has d^2 settings with 3 outcomes each, and we denote the settings of Bob by the pair jk, where $j, k \in [d]$ (notice that we swapped the role of Alice and Bob compared to Ref. [35]). For every $d \geq 2$ and every overlap matrix such that $O_{jk} < 1$ for all j, k (equivalently, $O_{jk} > 0$ for all j, k) the authors of Ref. [35] construct a nontrivial Bell inequality, i.e., a Bell inequality that has a quantum violation:

$$\begin{aligned}\mathcal{B}_d = &\sum_{j,k=0}^{d-1} \sqrt{1-O_{jk}^2}\big[p(j,0|0,jk) - p(j,1|0,jk) \\ &+ p(k,1|1,jk) - p(k,0|1,jk)\big] \\ &- \frac{1}{2}\sum_{j,k=0}^{d-1}\big(1-O_{jk}^2\big)\big[p_B(0|jk) + p_B(1|jk)\big],\end{aligned} \tag{10}$$

where $p_B(b|jk)$ is Bob's marginal distribution.

Moreover, the authors of Ref. [35] show that the maximal quantum violation can be achieved by sharing a locally d-dimensional maximally entangled state $|\phi_d^+\rangle = (1/\sqrt{d})\sum_{j=0}^{d-1}|jj\rangle$, and Alice's measurements being $\{|j\rangle\langle j|\}_{j=0}^{d-1}$ for $x=0$ and $\{|e_k\rangle\langle e_k|\}_{k=0}^{d-1}$ for $x=1$ (together with appropriate measurements for Bob that we do not describe here for the sake of simplicity).

While the maximal violation of these inequalities does not provide a self-test in the usual sense, in Ref. [35] it is shown that for every state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ giving rise to the maximal violation, there exist local isometries $V_A\colon \mathcal{H}_A \to \mathbb{C}^d \otimes \mathcal{H}_{A'}$ and $V_B\colon \mathcal{H}_B \to \mathbb{C}^d \otimes \mathcal{H}_{B'}$ (with $\mathcal{H}_{A'}$ isometric to $\mathcal{H}_A$ and $\mathcal{H}_{B'}$ isometric to $\mathcal{H}_B$) such that

$$(V_A \otimes V_B)\rho(V_A^\dagger \otimes V_B^\dagger) = |\phi_d^+\rangle\langle\phi_d^+| \otimes \sigma_{A'B'} \tag{11}$$

for some quantum state $\sigma_{A'B'}$ on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$. Our new contribution to this certification is to show that the maximal violation implies that Alice's measurement corresponding to setting $x=0$ satisfies

$$V_A A_a^0 V_A^\dagger = |a\rangle\langle a| \otimes \tilde{A} \quad \forall\, a \in [d] \tag{12}$$

for some fixed operator $\tilde{A}$ on $\mathcal{H}_{A'}$ and that

$$V_B V_B^\dagger = \mathbb{I}_{\mathbb{C}^d} \otimes \tilde{B}, \tag{13}$$

for some fixed operator $\tilde{B}$ on $\mathcal{H}_{B'}$ [36]. Note that Eqs. (11)–(13) do not constitute self-testing in the usual sense: Eq. (11) is expressed in terms of mixed states, the state and measurement certification are decoupled, and only one measurement of Alice and none of Bob's measurements are certified. Nevertheless, using recent results on the general theory of self-testing [38], we can show that Eqs. (11)–(13) imply condition (5) [36]. Therefore—by the earlier arguments—the resulting conditional von Neumann entropy will again satisfy

$$H(A|E)_\sigma = H(A) = \log(d) \tag{14}$$

for the setting $\hat{x}=0$ of Alice [the specific value $\log(d)$ follows from the fact that $p_A(a|0) = (1/d)$ [35]]. Then, introducing a d-outcome measurement for Bob that is perfectly correlated to the $\hat{x}=0$ setting of Alice (e.g., in the ideal realization one can choose $B_b^{\hat{y}} = |b\rangle\langle b|$), we get a lower bound on the key rate,

$$r \geq H(A|E) - H(A|B) = \log(d) \tag{15}$$

for all $d \geq 2$ and for all overlap matrices with $O_{jk} > 0$. That is, we obtain a family of correlations that certify $\log(d)$ bits of secret key. Notice that while these correlations maximally violate a Bell inequality (the one characterized by d and O_{jk}), in some cases they might be arbitrarily close to the set of local correlations.

Exploiting precisely this fact, we now show that for every $d \geq 2$, there exist correlations arbitrarily close to the local set but still certifying $\log(d)$ bits of secret key. To do so, for every d we need to provide an overlap matrix O such that the correlation maximising the corresponding Bell inequality from Ref. [35] is arbitrarily close to the local set. Consider the trivial case of $|e_k\rangle = |k\rangle$ for all $k \in [d]$, leading to an overlap matrix $O_{jk} = \delta_{jk}$. The corresponding correlation that arises by measuring $|\phi_d^+\rangle$ with the measurements $\{|j\rangle\langle j|\}$ for both settings $x=0$ and $x=1$ is local (irrespective of the measurement choices of Bob), since Alice's measurements are compatible [39]. Now let us perturb $\{|e_k\rangle\}$ by a small unitary transformation in a way that leads to a nontrivial overlap matrix with all elements strictly positive. One particularly symmetric way to achieve this is by taking the generalized Pauli X operator

$$X = \sum_{j=0}^{d-1}|j+1\rangle\langle j| = \sum_{j=0}^{d-1}\omega_d^j|\chi_j\rangle\langle\chi_j| = \mathrm{e}^G, \tag{16}$$

where $\omega_d = \mathrm{e}^{(2\pi\mathrm{i}/d)}$ is the dth root of unity, $|\chi_j\rangle = (1/\sqrt{d})\sum_{k=0}^{d-1}\omega_d^{jk}|k\rangle$ is the Fourier basis and $G = \sum_{j=0}^{d-1}[(2\pi\mathrm{i}/d)j]|\chi_j\rangle\langle\chi_j|$. Then, consider the unitary operator parametrized by $\varepsilon \in [0,1]$,

$$U_\varepsilon := \sum_{j=0}^{d-1} \omega_d^{\varepsilon j} |\chi_j\rangle\langle\chi_j| = \mathrm{e}^{\varepsilon G}. \tag{17}$$

Clearly, $U_0 = \mathbb{I}$, and U_ε is continuous in ε, a consequence of the well-known fact that the map $t \mapsto \mathrm{e}^{tM}$ is continuous in t for any matrix M (see, e.g., [40], Chap. 2). Also, for every $\varepsilon \in (0, 1)$ we have that the overlap matrix of $\{|j\rangle\}_{j=0}^{d-1}$ and $\{U_\varepsilon|k\rangle\}_{k=0}^{d-1}$ is nontrivial, that is, all of its elements are strictly positive [36]. As such, by the above arguments, the correlation that arises by measuring $|\phi_d^+\rangle$ with the measurements $\{|j\rangle\langle j|\}_{j=0}^{d-1}$ and $\{U_\varepsilon|k\rangle\langle k|U_\varepsilon^\dagger\}_{k=0}^{d-1}$ (and the appropriate measurements for Bob) certifies $\log(d)$ bits of secure key for every $\varepsilon \in (0, 1)$ and every integer $d \geq 2$.

If we now choose ε to be arbitrarily small (but positive), the resulting correlation, $p_\varepsilon(a, b|x, y)$ gets arbitrarily close (e.g., in ℓ_1 norm) to the local correlation $p_{\varepsilon=0}(a, b|x, y)$, since the correlation is also continuous in ε (it is quadratic in $U_\varepsilon = \mathrm{e}^{\varepsilon G}$) [36]. Therefore, for any integer $d \geq 2$, for arbitrarily small $\varepsilon > 0$ the correlation $p_\varepsilon(a, b|x, y)$ certifies $\log(d)$ bits of device-independent key, but the correlation is arbitrarily close to the set of local correlations. That is, from arbitrarily small nonlocality, one can still certify unbounded (with increasing d) device-independent key.

Conclusion.—In this work, we exposed a rigorous connection between self-testing and DIQKD as well as device-independent randomness generation. Thanks to this connection and the latest developments in high-dimensional Bell nonlocality, we showed that unbounded device-independent key rates can be certified from correlations with arbitrarily small nonlocality. This result together with recent findings indicates that DIQKD and Bell nonlocality might be incomparable resources, and in the search for a fundamental quantum resource for DIQKD, the amount of nonlocality is not the right quantity to consider.

It is important to point out that the correlations in this work that are arbitrarily close to the local set cannot tolerate even arbitrarily small noise (naturally, as this noise would map the correlation into the local set). It would be a practically motivated further research direction to investigate the relation of robust self-testing and noise-robust DIQKD. On the fundamental side, further characterising what correlations allow for certifying the relations (5) would lead to insights on the correlations useful for DIQKD.

Note added.—Recently, the author became aware of the related independent work of Ref. [41]. The authors there derive new self-testing statements in the simplest Bell scenario and prove that constant DIQKD rates (1 bit) can be achieved from arbitrarily small nonlocality.

M. F. would like to thank Jędrzej Kaniewski and Laura Mančinska for fruitful discussions.

*mate.farkas@york.ac.uk

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[2] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[3] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, Quantum **7**, 932 (2023).
[4] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, npj Quantum Inf. **9**, 10 (2023).
[5] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
[6] V. S. Miller, in *Advances in Cryptology—CRYPTO '85 Proceedings* (Springer Berlin Heidelberg, Berlin, Heidelberg, 1986), pp. 417–426.
[7] N. Koblitz, Math. Comput. **48**, 203 (1987).
[8] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[10] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[11] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Nature (London) **607**, 682 (2022).
[12] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, Nature (London) **607**, 687 (2022).
[13] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **128**, 110506 (2022).
[14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[15] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, and A. Acín, Phys. Rev. Lett. **127**, 050503 (2021).
[16] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[17] R. Ahlswede and I. Csiszár, IEEE Trans. Inf. Theory **39**, 1121 (1993).
[18] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[19] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[20] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[21] R. Arnon-Friedman, *Device-Independent Quantum Information Processing: A Simplified Analysis* (Springer Nature, 2020), 10.1007/978-3-030-60231-4.
[22] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).
[23] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).
[24] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).
[25] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, npj Quantum Inf. **7**, 158 (2021).
[26] P. Brown, H. Fawzi, and O. Fawzi, Nat. Commun. **12**, 575 (2021).
[27] P. Brown, H. Fawzi, and O. Fawzi, arXiv:2106.13692.

[28] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[29] L. Wooltorton, P. Brown, and R. Colbeck, Phys. Rev. Lett. **129**, 150403 (2022).
[30] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).
[31] J. R. Gonzales-Ureta, A. Predojević, and A. Cabello, Phys. Rev. A **103**, 052436 (2021).
[32] N. Miklin, A. Chaturvedi, M. Bourennane, M. Pawłowski, and A. Cabello, Phys. Rev. Lett. **129**, 230403 (2022).
[33] Z.-P. Xu, J. Steinberg, J. Singh, A. J. López-Tarrida, J. R. Portillo, and A. Cabello, Quantum **7**, 922 (2023).
[34] J. Singh and A. Cabello, Phys. Rev. A **109**, 022204 (2024).
[35] G. Pereira Alves and J. Kaniewski, Phys. Rev. A **106**, 032219 (2022).
[36] See the Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.132.210803, which includes Ref. [37], for proofs of private randomness from weaker conditions, of the nontrivial overlaps of Eq. (17) with the computational basis, and of the fact that $p_e(a, b|x, y)$ gets arbitrarily close to the local set.
[37] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani, Phys. Rev. A **97**, 022104 (2018).
[38] P. Baptista, R. Chen, J. Kaniewski, D. R. Lolck, L. Mančinska, T. G. Nielsen, and S. Schmidt, arXiv:2310.12662.
[39] M. T. Quintino, T. Vértesi, and N. Brunner, Phys. Rev. Lett. **113**, 160402 (2014).
[40] B. C. Hall, *Lie Groups, Lie Algebras, and Representations* (Springer, New York, 2013).
[41] L. Wooltorton, P. Brown, and R. Colbeck, preceding Letter, Phys. Rev. Lett. **132**, 210802 (2024).