White Rose Research Online

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk
Universities of Leeds, Sheffield and York

Deposited via The University of York.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/212737/

Version: Published Version

Article:
Wooltorton, Lewis, Brown, Peter and Colbeck, Roger (2024) Device-Independent Quantum Key Distribution with Arbitrarily Small Nonlocality. Physical Review Letters. 210802. ISSN: 1079-7114

https://doi.org/10.1103/PhysRevLett.132.210802

Reuse
This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:
https://creativecommons.org/licenses/

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Device-Independent Quantum Key Distribution with Arbitrarily Small Nonlocality

Lewis Wooltorton,[1,2,*] Peter Brown,[3,†] and Roger Colbeck[1,‡]
[1]Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom
[2]Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1FD, United Kingdom
[3]Télécom Paris—LTCI, Inria, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

(Received 26 October 2023; accepted 19 April 2024; published 22 May 2024)

Device-independent quantum key distribution allows two users to set up shared cryptographic key without the need to trust the quantum devices used. Doing so requires nonlocal correlations between the users. However, in Farkas *et al.* [Phys. Rev. Lett. **127**, 050503 (2021)] it was shown that for known protocols nonlocality is not always sufficient, leading to the question of whether there is a fundamental lower bound on the minimum amount of nonlocality needed for any device-independent quantum key distribution implementation. Here, we show that no such bound exists, giving schemes that achieve key with correlations arbitrarily close to the local set. Furthermore, some of our constructions achieve the maximum of 1 bit of key per pair of entangled qubits. We achieve this by studying a family of Bell inequalities that constitute all self-tests of the maximally entangled state with a single linear Bell expression. Within this family there exist nonlocal correlations with the property that one pair of inputs yield outputs arbitrarily close to perfect key. Such correlations exist for a range of Clauser-Horne-Shimony-Holt values, including those arbitrarily close to the classical bound. Finally, we show the existence of quantum correlations that can generate both perfect key and perfect randomness simultaneously, while also displaying arbitrarily small Clauser-Horne-Shimony-Holt violation. This opens up the possibility of a new class of cryptographic protocol.

DOI: 10.1103/PhysRevLett.132.210802

Introduction.—Establishing shared or global randomness between two isolated parties is a task achievable using quantum theory [1–3], but inaccessible to classical physics without additional assumptions. Quantum key distribution (QKD), for example, can be performed by making measurements on a shared entangled state, and security is derived assuming the devices behave according to a physical model [4]. Meeting the practical requirements of a model can be challenging, and mismatches between the model and reality can lead to security problems (see, e.g., [5]). However, quantum theory allows us to bypass the majority of such mismatch issues: entangled quantum systems can exhibit input-output behaviors that are nonlocal [6,7], giving rise to device-independent approaches to QKD [2,8–13]. The same can be said about the related task of randomness expansion [14–19].

Given quantum correlations that exhibit *some* nonlocality, how much secure key can be extracted device independently? To achieve the highest security, we want to find a lower bound on the amount of key conditioned on the observed nonlocality. Such lower bounds have been found in a variety of scenarios, both analytically [10,20,21] and numerically [22–25].

A related question that has achieved less attention is for what range of nonlocality is device-independent quantum key distribution (DIQKD) possible? It has recently been shown that nonlocality is not a sufficient condition for DIQKD using standard protocols [26]. More precisely, [26] showed that there exist quantum correlations, arising from Werner states [27], with some nonlocality, for which an upper bound on the secret key rate vanishes. While the result of [26] does not encompass all possible protocols, it raises the question of whether there exists a minimum amount of nonlocality needed for any DIQKD implementation. A conclusive proof of existence, or contradiction, for such a bound is currently missing from the literature.

In this Letter, we show that no such bound exists. Contrasting the work of [26], we show one can find quantum correlations with arbitrarily small nonlocality that can be used for DIQKD with a key rate arbitrarily close to 1 bit per pair of shared entangled qubits (we refer to this as near-perfect DIQKD). This complements existing work showing the same holds for global randomness expansion (DIRE) [28,29], which we expand upon here. We also go one step further: there exist quantum correlations

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

with arbitrarily small nonlocality that can be used for both near-perfect DIQKD and maximum DIRE. To our knowledge this is the first example of such correlations to appear in the literature, and could open up the possibility for a new class of cryptographic protocols.

Our results are obtained by self-testing [30–34] quantum correlations close to the local boundary. We study a versatile family of bipartite Bell expressions that first appeared in [35], and encompass those used in the literature to certify secret key [21] and randomness [29,36]. These expressions are tangent hyperplanes to the boundary of the set of quantum correlators, and constitute all self-tests of the singlet with a single linear Bell expression, when considering two observers with binary inputs and outputs [35,37]. Moreover, to prove self-testing we reduce the problem to qubits via Jordan's lemma [38]; a self-contained reduction can be found in the Supplemental Material [39], which may be of independent interest.

Background.—We consider the minimal Bell scenario for DIQKD. Let two spacelike separated parties, Alice and Bob, each hold a device with inputs $x, y \in \{0, 1\}$ and outputs $a, b \in \{0, 1\}$. The devices are characterized by the joint distribution $p(ab|xy)$, which must be no signaling.

A quantum strategy refers to a joint state, $\rho_{\tilde{Q}_A\tilde{Q}_B}$, and sets of observables $\tilde{A}_x = \tilde{M}_{0|x} - \tilde{M}_{1|x}$, $\tilde{B}_y = \tilde{N}_{0|y} - \tilde{N}_{1|y}$, where $\{\tilde{M}_{a|x}\}_a$, $\{\tilde{N}_{b|y}\}_b$ are projective measurements (which can be assumed without loss of generality according to Naimark's dilation theorem [45]) on the physical Hilbert spaces $\mathcal{H}_{\tilde{Q}_A}$ or $\mathcal{H}_{\tilde{Q}_B}$ held by Alice and Bob. We consider an adversarial scenario in which Eve holds a purification $|\Psi\rangle_{\tilde{Q}_A\tilde{Q}_BE}$ of $\rho_{\tilde{Q}_A\tilde{Q}_B}$ and can set the quantum behavior of each device (i.e., which measurements each input corresponds to). Eve's aim is to establish nontrivial correlations between the classical register A holding Alice's outcomes and E, while remaining undetected. Such correlations will allow Eve to learn information about Alice's raw key when Alice measures, e.g., $X = x$; this is described by the postmeasurement classical-quantum state $\rho_{AE|X=x} = \sum_a |a\rangle\langle a|_A \otimes \rho_E^{a|x}$, where $\rho_E^{a|x} = \mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_B}[(\tilde{M}_{a|x} \otimes \mathbb{I}_{\tilde{Q}_BE})|\Psi\rangle\langle\Psi|]$ is the subnormalized state held by Eve conditioned on Alice getting a when x is measured. The global postmeasurement classical-classical-quantum state $\rho_{ABE|X=x,Y=y}$ is defined analogously, and the behavior is recovered via the Born rule $p(ab|xy) = \mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_BE}[(\tilde{M}_{a|x} \otimes \tilde{N}_{b|y} \otimes \mathbb{I}_E)|\Psi\rangle\langle\Psi|]$.

As we are restricting ourselves to binary inputs and outputs, the nonlocality of the resulting joint behavior can be quantified in terms of its Clauser-Horne-Shimony-Hold (CHSH) value [46], $I_{\mathrm{CHSH}} = \langle A_0(B_0 + B_1)\rangle + \langle A_1(B_0 - B_1)\rangle$, where $\langle A_xB_y\rangle$ are the correlators, $\langle A_xB_y\rangle = \sum_{ab}(-1)^{a+b}p(ab|xy)$, which equal $\mathrm{Tr}[(\tilde{A}_x \otimes \tilde{B}_y)\rho_{\tilde{Q}_A\tilde{Q}_B}]$ when the behavior is quantum. The local and quantum bounds are given by 2 and $2\sqrt{2}$, respectively, and it is well known that there is a unique quantum state and sets of measurements that achieve the quantum bound, up to local isometries. It is in this sense that the CHSH inequality *self-tests* the corresponding state (which is maximally entangled) and measurements.

We consider DIQKD protocols based on spot checking with two measurements per party and a single Bell inequality (see, e.g., [[4], Section 4.4] for an example using the CHSH inequality [47]). In order to compute the secret key rate the relevant quantities are the conditional von Neumann entropies $H(A|X = x, E)$ and $H(A|X = x, Y = y, B)$, where $X = x$ and $Y = y$ are the inputs used for key generation. The latter entropy, which is independent of Eve's system, captures the cost for Alice and Bob to reconcile their raw keys and can be estimated directly from the statistics. The former captures the randomness in Alice's raw key conditioned on Eve, and must be lower bounded in terms of the observed behavior P_{obs}, or some functions f_i of P_{obs} (for instance, f_i might be a Bell expression). The asymptotic secret key rate is then bounded by the Devetak-Winter formula [48]

$$r^{\mathrm{key}} \geq \max_{x,y}\big(\inf[H(A|X = x, E)_{\rho_{AE|X=x}}] - H(A|X = x, Y = y, B)_{\rho_{AB|X=x,Y=y}}\big), \tag{1}$$

where the infimum is taken over states and measurements compatible with $f_i(P_{\mathrm{obs}})$. Analogously, the global randomness rate is defined by the quantity $r^{\mathrm{global}} = \max_{x,y} \inf H(AB|X = x, Y = y, E)_{\rho_{ABE|X=x,Y=y}}$. The asymptotic rates can serve as a basis for rates with finite statistics using tools such as the entropy accumulation theorem [13,49,50].

To achieve a key rate arbitrarily close to 1 bit per entangled state shared, we consider the family of three parameter Bell inequalities from [35] whose maximal quantum violation self-tests a unique state and measurements (up to local isometries). In this case we consider a single functional $f = \langle B_{\theta,\phi,\omega}\rangle$ with observed value η, and denote the rate $R^{\mathrm{key}}_{\theta,\phi,\omega}(\eta)$. Achieving the quantum bound self-tests a pure (in fact, maximally entangled) state that therefore must be uncorrelated with Eve, allowing us to directly compute the entropy from the observed behavior. We find $H(A|X = 0, E) = 1$, and $H(A|X = Y = 0, B) = \epsilon$ for any epsilon $\epsilon \in (0, 2 - (3/4)\log(3)]$, giving a key rate $1 - \epsilon$ that tends to 1 as $\epsilon \to 0$, while at the same time having a CHSH value arbitrarily close to classical bound. We also use $R^{\mathrm{global}}_{\theta,\phi,\omega}(\eta)$ to denote the randomness rate based on the same functional.

Methods.—Our main results are derived from studying the family of self-testing Bell expressions in [35], also recently reported in [37]. We provide a new self-testing proof, and all claims are proven in the Supplemental Material [39].

Proposition 1.—Let $\theta, \phi, \omega \in \mathbb{R}$. Define the family of Bell expressions, labeled $\langle B_{\theta,\phi,\omega}\rangle$,

$$\cos(\theta+\phi)\cos(\theta+\omega)\langle A_0(\cos\omega B_0 - \cos\phi B_1)\rangle + \cos\phi\cos\omega\langle A_1(-\cos(\theta+\omega)B_0 + \cos(\theta+\phi)B_1)\rangle. \tag{2}$$

Then the following hold: (i) the local bounds are given by $\pm\eta^{\mathrm{L}}_{\theta,\phi,\omega}$, where $\eta^{\mathrm{L}}_{\theta,\phi,\omega}$ is defined as

$$\max_{\pm}\{\big|\cos(\theta+\omega)\cos(\omega)\big(\cos(\theta+\phi)\pm\cos(\phi)\big)\big| + \big|\cos(\theta+\phi)\cos(\phi)\big(\cos(\theta+\omega)\pm\cos(\omega)\big)\big|\}. \quad (3)$$

(ii) If

$$\cos(\theta+\phi)\cos(\phi)\cos(\theta+\omega)\cos(\omega) < 0, \quad (4)$$

then the quantum bounds are given by $\pm\eta^{\mathrm{Q}}_{\theta,\phi,\omega}$, where

$$\eta^{\mathrm{Q}}_{\theta,\phi,\omega} = \sin(\theta)\sin(\omega-\phi)\sin(\theta+\omega+\phi). \quad (5)$$

(iii) $\big|\eta^{\mathrm{Q}}_{\theta,\phi,\omega}\big| > \eta^{\mathrm{L}}_{\theta,\phi,\omega} \Leftrightarrow$ (4) holds.

(iv) If (4) holds, then up to local isometries there is a unique strategy that achieves $\langle B_{\theta,\phi,\omega}\rangle = \eta^{\mathrm{Q}}_{\theta,\phi,\omega}$:

$$\rho_{Q_A Q_B} = |\psi\rangle\langle\psi|, \text{ where } |\psi\rangle = \frac{|00\rangle + i|11\rangle}{\sqrt{2}},$$
$$A_0 = \sigma_X, \quad A_1 = \cos\theta\sigma_X + \sin\theta\sigma_Y,$$
$$B_0 = \cos\phi\sigma_X + \sin\phi\sigma_Y, \quad B_1 = \cos\omega\sigma_X + \sin\omega\sigma_Y. \quad (6)$$

Special cases of the above family have already found applications in device-independent (DI) cryptography. For example, it contains all bipartite expressions found in [29,36], which certify maximum global DI randomness. One can also recover the marginal-free subfamily of the tilted CHSH inequalities [28,51], which have found use in DIQKD [21,52] and robust self-testing of the singlet [53]. Moreover, it has been shown [35,37] that the family (2) constitute an infinite family of hyperplanes tangent to the boundary of the quantum set of correlations with uniform marginals, $\mathcal{Q}_{\mathrm{corr}}$, and constitute every self-test of the singlet with a single linear function of the correlators in this scenario. We discuss these connections in more detail in the Supplemental Material [39].

Perfect randomness from arbitrarily small nonlocality.—First we consider all strategies that certify maximum global randomness in this scenario using a maximally entangled state, certified by a single Bell expression. This contains the subfamily in [29], where the randomness versus nonlocality relationship was studied using a one parameter family of Bell expressions; here we review and extend this to a two parameter subfamily of (2).

Proposition 2.—For any $s \in (2, 3\sqrt{3}/2]$, there exists a tuple (θ,ϕ,ω) satisfying (4), along with a set of quantum correlations achieving $R^{\mathrm{global}}_{\theta,\phi,\omega}(\eta^{\mathrm{Q}}_{\theta,\phi,\omega}) = 2$ and $I_{\mathrm{CHSH}} = s$.

The subfamily self-tests σ_X for both Alice and Bob, along with $|\psi\rangle = (|+,y_+\rangle + |-,y_-\rangle)/\sqrt{2}$, where $|\pm\rangle(|y_\pm\rangle)$ are the eigenstates of σ_X (σ_Y). This is achieved by setting $\omega = \pi$, resulting in a two parameter family of Bell expressions

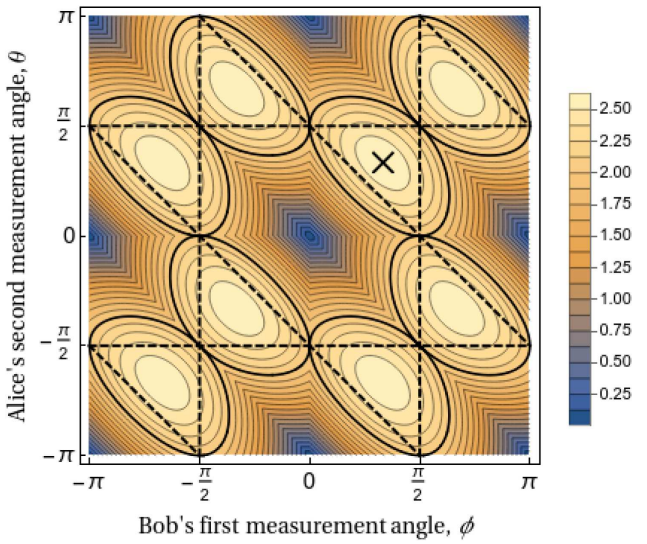

FIG. 1. Contour plot of nonlocality, measured using the maximum of the eight CHSH-type inequalities, for the strategies in Eq. (6) with $\omega = \pi$. The points inside the dashed triangles, excluding the boundary, can be used for perfect DIRE with a single linear Bell inequality: they satisfy (4) and have a value in $(2, 3\sqrt{3}/2]$ for one of the CHSH-type inequalities, with the maximum of I_{CHSH} indicated with the black cross at $\theta = \phi = \pi/3$. Approaching $\phi = -\pi/2$ or $\phi = \pi/2$ inside the corresponding region also allows arbitrarily good DIQKD. The black contours indicate $I_{\mathrm{CHSH}} = 2$ for at least one CHSH-type inequality.

certifying uniform randomness when $X = 0$, $Y = 1$, and (4) holds: $\cos(\theta+\phi)\cos(\theta)\langle A_0(B_0 + \cos(\phi)B_1)\rangle - \cos(\phi)\langle A_1(\cos(\theta)B_0 + \cos(\theta+\phi)B_1)\rangle$. Figure 1 shows the valid regions of (θ,ϕ) space for perfect randomness certification.

Near-perfect key from arbitrarily small nonlocality.—Next we turn our attention to DIQKD. We consider the key rate achievable using the strategies in Proposition 1, and which CHSH values are compatible.

Proposition 3.—For any $s \in (2, 5/2]$, and any $\epsilon \in (0, 2 - (3/4)\log(3)]$, there exists a tuple (θ,ϕ,ω) satisfying (4), along with a set of quantum correlations achieving $R^{\mathrm{key}}_{\theta,\phi,\omega}(\eta^{\mathrm{Q}}_{\theta,\phi,\omega}) = 1 - \epsilon$ and $I_{\mathrm{CHSH}} = s$.

This statement is achieved by self-testing σ_X for Alice and $\cos(\phi)\sigma_X + \sin(\phi)\sigma_Y$ for Bob, along with $|\psi\rangle$. One can then take ϕ arbitrarily close to $\pi/2$; we find $H(A|X=0,E) = 1$ from self-testing, and $H(A|X=0, Y=0, B) = H_{\mathrm{bin}}[(1+\sin(\phi))/2] \coloneqq \epsilon$, where H_{bin} is the binary entropy function. Hence in the limit $\phi \to \pi/2$, ϵ tends to 0 and we achieve perfect key. Moreover, at this limit point, we can choose (θ,ω) such that the CHSH interval $(2, 5/2]$ is achieved—see Fig. 2 for an illustration.

Interestingly, the limit point violates (4): at $\phi = \pi/2$ the Bell expression (2) becomes trivial (the local and quantum bounds coincide), and we cannot find a single Bell expression that can certify perfect key. The correlations

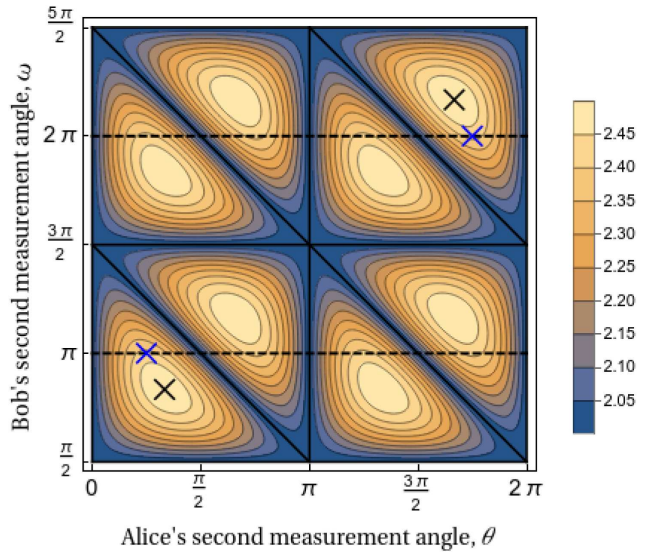

FIG. 2. Contour plot of nonlocality, measured using the maximum of the eight CHSH-type inequalities of the strategies in Eq. (6), at the limit $\phi = \pi/2$. All points on the graph are limit points of correlations that achieve arbitrarily perfect DIQKD with a single linear Bell inequality, including the contours with CHSH values equal to 2, which are shown as black triangles. The black dashed lines show where perfect DIRE can also be achieved, with the blue crosses denoting the maximum value of $I_{\mathrm{CHSH}} = 1 + \sqrt{2}$ at $\theta = \pi/4$, $\omega = \pi$ and $\theta = 7\pi/4$, $\omega = 2\pi$. The black crosses denote the global maximum of $I_{\mathrm{CHSH}} = 5/2$ at $\theta = \pi/3$, $\omega = 5\pi/6$ and $\theta = 5\pi/3$, $\omega = 13\pi/6$.

achieved in this limit [those resulting from the construction (6)] are nonlocal and were recently studied in [37], where it was shown such points correspond to nonexposed regions of $\mathcal{Q}_{\mathrm{corr}}$; our result shows the implications of this for DIQKD. At least two linear functionals are then required to uniquely identify the correlations, and, indeed, using all four correlators one can verify for various values of (θ, ω), the limit point satisfies the self-testing criteria of the singlet given by Wang *et al.* [54], and a one-parameter subfamily containing the point with $I_{\mathrm{CHSH}} = 5/2$ was studied in [[55], Section 3.4.1], including the nonexposed nature of the case with $I_{\mathrm{CHSH}} = 5/2$. We can therefore recover another statement similar to Proposition 3. We express this using $r^{\mathrm{key}}_{\theta,\phi,\omega}$, which is the quantity defined by Eq. (1) evaluated with functionals f_i constraining all four correlators to the values generated by the strategy in Eq. (6).

Proposition 4.—For any $s \in (2, 5/2]$, there exists a tuple (θ, ϕ, ω), along with a set of quantum correlations achieving $r^{\mathrm{key}}_{\theta,\phi,\omega} = 1$ and $I_{\mathrm{CHSH}} = s$.

In other words, if we constrain all four correlators rather than the Bell inequality of (2), then we achieve perfect key directly, rather than in a limit. However, the use of four correlators can have disadvantages in the case of finite statistics because for a fixed number of shared states larger error bars are present when estimating four quantities rather than one; see, e.g., [49,56].

Near-perfect key and randomness from arbitrarily small nonlocality.—Finally, we consider the possibility of using the same set of quantum correlations to generate perfect key from one input combination, and perfect randomness from another.

Proposition 5.—For any $s \in (2, 1 + \sqrt{2}]$ and any $\epsilon \in (0, H_{\mathrm{bin}}[(2 + \sqrt{2})/4])$, there exists a tuple (θ, ϕ, ω) satisfying (4), along with a set of quantum correlations achieving $R^{\mathrm{global}}_{\theta,\phi,\omega}(\eta^{\mathrm{Q}}_{\theta,\phi,\omega}) = 2$, $R^{\mathrm{key}}_{\theta,\phi,\omega}(\eta^{\mathrm{Q}}_{\theta,\phi,\omega}) = 1 - \epsilon$ and $I_{\mathrm{CHSH}} = s$.

This is obtained by simultaneously self-testing σ_X for Alice, and both $\cos(\phi)\sigma_X + \sin(\phi)\sigma_Y$ and σ_X for Bob, along with $|\psi\rangle$. Following the same arguments as before, we can fix $\omega = \pi$, and take ϕ arbitrarily close to $\pi/2$, resulting in a key rate of $1 - \epsilon$ and global randomness 2 for input choices $X = 0$, $Y = 0$ and $X = 0$, $Y = 1$ respectively. By varying θ, we can achieve the range of CHSH values $(2, 1 + \sqrt{2}]$, as shown in Fig. 2. For the same reasons discussed in the previous section, there also exists a nonlimiting statement when the full correlators are considered.

Proposition 6.—For any $s \in (2, 1 + \sqrt{2}]$, there exists a tuple (θ, ϕ, ω), along with a set of quantum correlations achieving $r^{\mathrm{global}}_{\theta,\phi,\omega} = 2$, $r^{\mathrm{key}}_{\theta,\phi,\omega} = 1$, and $I_{\mathrm{CHSH}} = s$.

Discussion.—We have shown that quantum theory allows perfect DI key to be shared between two users using correlations that are arbitrarily close to being local. However, we do not know that any correlation exhibiting nonlocality, can be used for DIQKD—for instance, as shown in [26], those that lie in the interior of $\mathcal{Q}_{\mathrm{corr}}$ and arise from measuring experimentally relevant states cannot generate key using standard protocols. The behaviors we use for our results are generated by the singlet, and lie on the self-testable boundary of $\mathcal{Q}_{\mathrm{corr}}$.

Similar statements hold for DI randomness generation, and we also showed the existence of quantum correlations that can simultaneously be used either to share key or generate maximum randomness, while being arbitrarily close to the local set. This is not only an intriguing feature of quantum theory, but opens up the possibility for new protocols exploiting this feature. For example, certifying global randomness implies 1 bit of blind randomness for Alice, in which she does not need to trust Bob [57–59]. This prompts an application to QKD postprocessing in which certified randomness from some outcomes could help replenish some of the private randomness consumed in others. We leave the study of such protocols, and other applications of this construction, to future investigation.

Although we achieve arbitrarily good key using a single Bell expression, getting perfect key is excluded. On the other hand, perfect key is possible by testing all four correlators. This raises the question of the minimum number of linear quantities required. It would be of further interest to find the robustness of the present constructions to noise. We leave these as problems for future investigation.

Finally, our Letter also highlights how, when given access to the full set of single Bell functionals that self-test the singlet in this scenario, one can find interesting relationships between cryptographic tasks and nonlocality. It would be interesting to find further applications. For example, it has been shown how use of the various subfamilies of Proposition 1 can boost practical DIQKD, DIRE, and robust self-testing [21,29,60,61]; given access to their generalizations, further improvements may be found by optimizing over the entire family of Bell expressions (2).

Note added.—During the writing up of this work we became aware of a related work [62] that also shows the possibility of key distribution with arbitrarily small nonlocality using an alternative approach.

This work was supported by EPSRC via the Quantum Communications Hub (Grant No. EP/T001011/1) and Grant No. EP/SO23607/1 and by the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, Grant agreement No. 101114043).

*Corresponding author: lewis.wooltorton@york.ac.uk
†Corresponding author: peter.brown@telecom-paris.fr
‡Corresponding author: roger.colbeck@york.ac.uk

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179, https://doi.org/10.1016/j.tcs.2014.05.025.
[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).
[4] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).
[5] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).
[6] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, England, 1987), 10.1017/CBO9780511815676.
[7] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Nonlocal correlations as an information-theoretic resource, Phys. Rev. A **71**, 022101 (2005).
[8] J. Barrett, L. Hardy, and A. Kent, No signalling and quantum key distribution, Phys. Rev. Lett. **95**, 010503 (2005).
[9] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Phys. Rev. Lett. **98**, 230501 (2007).
[10] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).
[11] J. Barrett, R. Colbeck, and A. Kent, Unconditionally secure device-independent quantum key distribution with only two devices, Phys. Rev. A **86**, 062326 (2012).
[12] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. **113**, 140501 (2014).
[13] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).
[14] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2007, also available as arXiv:0911.3814.
[15] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).
[16] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, J. Phys. A **44**, 095305 (2011).
[17] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC '14* (ACM, New York, NY, USA, 2014), pp. 417–426, https://doi.org/10.1145/2591796.2591843.
[18] C. A. Miller and Y. Shi, Universal security for randomness expansion from the spot-checking protocol, SIAM J. Comput. **46**, 1304 (2017).
[19] R. Colbeck and R. Renner, Free randomness can be amplified, Nat. Phys. **8**, 450 (2012).
[20] M. Ho, P. Sekatski, E.-Y. Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution, Phys. Rev. Lett. **124**, 230502 (2020).
[21] E. Woodhead, A. Acín, and S. Pironio, Device-independent quantum key distribution with asymmetric CHSH inequalities, Quantum **5**, 443 (2021).
[22] P. Brown, H. Fawzi, and O. Fawzi, Computing conditional entropies for quantum correlations, Nat. Commun. **12**, 575 (2021).
[23] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, Computing secure key rates for quantum cryptography with untrusted devices, npj Quantum Inf. **7**, 158 (2021).
[24] M. Masini, S. Pironio, and E. Woodhead, Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints, arXiv:2107.08894.
[25] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, arXiv:2106.13692.
[26] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, and A. Acín, Bell nonlocality is not sufficient

for the security of standard device-independent quantum key distribution protocols, Phys. Rev. Lett. **127**, 050503 (2021).
[27] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).
[28] A. Acín, S. Massar, and S. Pironio, Randomness versus nonlocality and entanglement, Phys. Rev. Lett. **108**, 100402 (2012).
[29] L. Wooltorton, P. Brown, and R. Colbeck, Tight analytic bound on the trade-off between device-independent randomness and nonlocality, Phys. Rev. Lett. **129**, 150403 (2022).
[30] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).
[31] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, J. Phys. A **45**, 455304 (2012).
[32] T. H. Yang and M. Navascués, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A **87**, 050102(R) (2013).
[33] J. Kaniewski, Self-testing of binary observables based on commutation, Phys. Rev. A **95**, 062323 (2017).
[34] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, Quantum **4**, 337 (2020).
[35] T. P. Le, C. Meroni, B. Sturmfels, R. F. Werner, and T. Ziegler, Quantum correlations in the minimal scenario, Quantum **7**, 947 (2023).
[36] L. Wooltorton, P. Brown, and R. Colbeck, Expanding bipartite Bell inequalities for maximum multi-partite randomness, arXiv:2308.07030.
[37] V. Barizien, P. Sekatski, and J.-D. Bancal, Custom Bell inequalities from formal sums of squares, arXiv:2308.08601.
[38] C. Jordan, Essai sur la géométrie à n dimensions, Bull. de la S.M.F. **3**, 103 (1875).
[39] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.132.210802 for proofs of the propositions, which includes Refs. [40–44].
[40] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Device-independent state estimation based on Bell's inequalities, Phys. Rev. A **80**, 062327 (2009).
[41] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Certifying the building blocks of quantum computers from Bell's theorem, Phys. Rev. Lett. **121**, 180505 (2018).
[42] R. Bhavsar, S. Ragy, and R. Colbeck, Improved device-independent randomness expansion rates using two sided randomness, New J. Phys. **25**, 093035 (2023).
[43] L. Masanes, Necessary and sufficient condition for quantum-generated correlations, arXiv:quant-ph/0309137.
[44] L. Masanes, Extremal quantum correlations for n parties with two dichotomic observables per site, arXiv:quant-ph/0512100.
[45] V. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, Cambridge, England, 2003), 10.1017/CBO9780511546631.
[46] There are eight CHSH-type inequalities, equivalent to I_{CHSH} up to relabelings. These are the only facet inequalities separating classical and quantum correlations in this scenario.
[47] Other than the choice of Bell inequality, a key difference in the present work is that the settings used for raw key are among those used for testing; in the protocol of [4] Bob needs an additional setting. We elaborate further on this in the Supplemental Material [39].
[48] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).
[49] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, Commun. Math. Phys. **379**, 867 (2020).
[50] F. Dupuis and O. Fawzi, Entropy accumulation with improved second-order term, IEEE Trans. Inf. Theory **65**, 7596 (2019).
[51] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).
[52] P. Sekatski, J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, and N. Sangouard, Device-independent quantum key distribution from generalized CHSH inequalities, Quantum **5**, 444 (2021).
[53] X. Valcarce, J. Zivy, N. Sangouard, and P. Sekatski, Self-testing two-qubit maximally entangled states from generalized Clauser-Horne-Shimony-Holt tests, Phys. Rev. Res. **4**, 013049 (2022).
[54] Y. Wang, X. Wu, and V. Scarani, All the self-testings of the singlet for two binary measurements, New J. Phys. **18**, 025021 (2016).
[55] K.-S. Chen, G. N. M. Tabia, C. Jebarathinam, S. Mal, J.-Y. Wu, and Y.-C. Liang, Quantum correlations on the no-signaling boundary: Self-testing and more, Quantum **7**, 1054 (2023).
[56] P. J. Brown, S. Ragy, and R. Colbeck, A framework for quantum-secure device-independent randomness expansion, IEEE Trans. Inf. Theory **66**, 2964 (2020).
[57] C. A. Miller and Y. Shi, Randomness in nonlocal games between mistrustful players, Quantum Inf. Comput. **17**, 595 (2017).
[58] H. Fu and C. A. Miller, Local randomness: Examples and application, Phys. Rev. A **97**, 032324 (2018).
[59] T. Metger, O. Fawzi, D. Sutter, and R. Renner, Generalised entropy accumulation, in *Proceedings of the 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), Denver, CO* (IEEE, New York, 2022), pp. 844–850, https://doi.org/10.1109/FOCS54457.2022.00085.
[60] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Robust and versatile black-box certification of quantum devices, Phys. Rev. Lett. **113**, 040401 (2014).
[61] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from nonlocal correlations, Phys. Rev. A **91**, 022115 (2015).
[62] M. Farkas, following Letter, Unbounded device-independent quantum key rates from arbitrarily small nonlocality, Phys. Rev. Lett. **132**, 210803 (2024).