Editors' Suggestion   Featured in Physics

Bell Nonlocality Is Not Sufficient for the Security of Standard Device-Independent Quantum Key Distribution Protocols

Máté Farkas[1,*], Maria Balanzó-Juandó[1], Karol Łukanowski[2,3], Jan Kołodyński[2], and Antonio Acín[1,4]

[1]ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Spain

[2]Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warszawa, Poland

[3]Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warszawa, Poland

[4]ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain

Device-independent quantum key distribution is a secure quantum cryptographic paradigm that allows two honest users to establish a secret key, while putting minimal trust in their devices. Most of the existing protocols have the following structure: first, a bipartite nonlocal quantum state is distributed between the honest users, who perform local projective measurements to establish nonlocal correlations. Then, they announce the implemented measurements and extract a secure key by postprocessing their measurement outcomes. We show that no protocol of this form allows for establishing a secret key when implemented on any correlation obtained by measuring local projective measurements on certain entangled nonlocal states, namely, on a range of entangled two-qubit Werner states. To prove this result, we introduce a technique for upper bounding the asymptotic key rate of device-independent quantum key distribution protocols, based on a simple eavesdropping attack. Our results imply that either different reconciliation techniques are needed for device-independent quantum key distribution in the large-noise regime, or Bell nonlocality is not sufficient for this task.

Introduction.—Device-independent quantum key distribution (DIQKD) is the strongest form of quantum cryptographic protocols [1,2]. DIQKD security proofs are based on the assumption that quantum theory is correct, and on physically observable quantities. Most importantly, the honest users do not need to make any assumptions about the inner workings of their devices and, hence, they do not need to trust the preparation by the manufacturer. These facts make DIQKD a promising paradigm for providing complete security, in that DIQKD protocols are not vulnerable to implementation flaws that may be exploited in hacking attacks [3–5].

In DIQKD protocols, two distant honest parties aim at sharing a cryptographic key, while assuring it to be unknown to any eavesdropper limited by quantum theory. To achieve this, a quantum state is distributed between them in each round of the protocol, and in each of these rounds they measure the part of the state that is available to them. The resulting set of measurement outcomes is the raw data from which they extract the secure key. This data is characterized by the set of measurement outcome probabilities, called the *correlation*. If the observed correlation violates a Bell inequality, the information of any quantum eavesdropper about the outcomes is limited, which opens up the possibility of extracting a secure key.

The first quantitative security proofs were achieved based on the violation of the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [6], using one-way public communication for key extraction [1,2]. The original proofs, valid under collective attacks, were later extended to the most powerful coherent attacks [7–9]. Furthermore, moderate improvements on key rates were recently achieved using the more general *biased* CHSH inequalities [10], and applying noisy preprocessing [11–13]. Similarly, advantage distillation—a protocol for key distillation using two-way public communication—has been shown to be useful under the assumption of collective attacks [14].

While nonlocality of the observed correlations is necessary for DIQKD, it remains an open question whether it is also sufficient. Recently, methods have been proposed for upper bounding secure key rates in DIQKD, even if two-way communication is allowed [15–17]. However, all the bounds constructed thus far remain strictly positive for nonlocal correlations, suggesting that nonlocality may be sufficient for DIQKD.

In this work, we show this not to be the case for DIQKD protocols consisting of the following two steps: (i) nonlocal

correlations are established by applying local measurements on an entangled quantum state; (ii) the implemented measurements are announced and the key is constructed by classically postprocessing the outcomes. Most of the existing DIQKD protocols have this form and, hence, in what follows we refer to such protocols as *standard* protocols. To prove the result, we provide a generic tool for upper bounding key rates in DIQKD. We then apply our tool to standard protocols implemented on a two-qubit Werner state [18] using an arbitrary number of projective measurements. We show that for a range of visibilities for which the Werner state is known to be nonlocal, the upper bound on the key rate is zero, and therefore no standard DIQKD protocol can be secure. This means that there exist nonlocal correlations that cannot be used for standard DIQKD, and, furthermore, that there exist nonlocal quantum states that cannot be used for standard DIQKD with projective measurements. We also show how the provable region of insecurity can be enlarged when fixing the number of measurements in the protocol. In particular, we compute visibilities for which the commonly used protocols based on the (biased) CHSH inequality [1,2,9,11–14] all become insecure despite the correlations still being nonlocal.

Methods.—Formally, in a DIQKD protocol two parties, Alice and Bob, have access to a bipartite quantum state, ρ_{AB}, represented by a positive semidefinite operator with unit trace on the tensor product Hilbert space, $\mathcal{H}_A \otimes \mathcal{H}_B$. The protocol consists of several rounds, in each of which Alice and Bob choose a particular quantum measurement to measure their part of a fresh copy of ρ_{AB}. In particular, Alice chooses a measurement labeled by $x \in \{0, 1, \dots, n_A - 1\} \equiv [n_A]$, and Bob chooses a measurement labeled by $y \in [n_B]$. Without loss of generality, we assume that each of Alice's (Bob's) measurements has k_A (k_B) possible outcomes. According to quantum theory, k_A-(k_B-)outcome measurements correspond to a set of k_A (k_B) positive semidefinite operators on $\mathcal{H}_A$ ($\mathcal{H}_B$), adding up to the identity operator $\mathbb{I}_A$ ($\mathbb{I}_B$). We denote these measurement operators by A_a^x and B_b^y, where $x \in [n_A]$, $a \in [k_A]$, $y \in [n_B]$ and $b \in [k_B]$. Then, the correlation shared by Alice and Bob reads

$$p_{AB}(a, b|x, y) = \text{tr}[\rho_{AB}(A_a^x \otimes B_b^y)], \tag{1}$$

specifying the probabilities of observing the outcomes a and b, given that the measurements x and y were selected.

The raw data in the protocol correspond to the pair of strings held by Alice and Bob containing the measurement outcomes and the implemented measurements, collected over all protocol rounds. Since individually Alice and Bob only have access to their marginal statistics, they publicly reveal the measurement settings and outcomes for a fraction of this data to estimate the joint statistics and detect its nonlocality. This part of the dataset is discarded. The secret key is distilled by classically postprocessing the remaining dataset with the help of public communication, so that they finally hold identical strings that must appear perfectly random to any third party.

As stated earlier, in this work we consider what we call *standard* protocols, in which the measurements implemented by Alice and Bob are announced in the key distillation part. Apart from this constraint, the rest of the protocol is arbitrary. This family is quite broad and covers most DIQKD protocols introduced so far [1,2,9,11–14], with only a few exceptions proposed to date (see, e.g., Ref. [19]).

In order to upper bound the key rate for a given DIQKD protocol, it suffices to consider a particular model of the eavesdropper, Eve. Here, we restrict the analysis to individual attacks that do not require any quantum memory [20]. In device-independent protocols, Alice and Bob have no knowledge of the form of the state ρ_{AB} and the measurements $\{A_a^x\}$, $\{B_b^y\}$, and it is precisely this lack of knowledge that Eve makes use of in her attack. In particular, we assume that she knows the precise form of the measurement operators and that she is the one distributing the quantum state (therefore effectively distributing quantum correlations) to Alice and Bob in each round.

In our *convex combination* (CC) attack—originally considered for eavesdroppers limited only by the no-signalling principle [19,21]—Eve distributes local deterministic correlations with certain probabilities that give rise to a local correlation $p_{AB}^{\mathcal{L}}(a, b|x, y)$ with overall probability $q_{\mathcal{L}}$, and she distributes a nonlocal quantum correlation $p_{AB}^{\mathcal{NL}}(a, b|x, y)$ with probability $1 - q_{\mathcal{L}}$. While presented in this form for the sake of simplicity, Eve can equally implement the attack by fixing the measurements of Alice and Bob and preparing a unique quantum state ρ_{ABE}. Eventually, the observed correlation of Alice and Bob takes the form

$$\begin{aligned} p_{AB}(a, b|x, y) &= q_{\mathcal{L}} p_{AB}^{\mathcal{L}}(a, b|x, y) \\ &\quad + (1 - q_{\mathcal{L}}) p_{AB}^{\mathcal{NL}}(a, b|x, y), \end{aligned} \tag{2}$$

and we call $q_{\mathcal{L}} \in [0, 1]$ the *local weight*. Since nonlocality is necessary for secure DIQKD, in the CC attack Eve maximizes $q_{\mathcal{L}}$ for the given observed correlation $p_{AB}(a, b|x, y)$ and a judiciously chosen nonlocal quantum correlation $p_{AB}^{\mathcal{NL}}(a, b|x, y)$.

We apply the CC attack to the standard DIQKD protocols introduced above. Since Alice and Bob announce their inputs for every round, Eve knows their outcomes in all rounds in which she distributes a local correlation. We represent this knowledge by the classical variable e, and we write $e = (a, b)$ for the local rounds. On the other hand, we assume in what follows that Eve is not correlated to the nonlocal part of the correlation of Alice and Bob, denoted by $e = ?$. Therefore, for any combination of inputs x and y,

Alice, Bob, and Eve share correlated random variables distributed as

$$p_{ABE}(a, b, e|x, y) = q_{\mathcal{L}} p_{AB}^{\mathcal{L}}(a, b|x, y)\delta_{e,(a,b)}$$
$$+ (1 - q_{\mathcal{L}})p_{AB}^{\mathcal{NL}}(a, b|x, y)\delta_{e,?}, \quad (3)$$

where δ is the Kronecker delta.

Well-established results in classical cryptography prove that the asymptotic key rate r extractable from a dataset of strings distributed according to $p_{ABE}(a, b, e)$ is upper bounded by the *intrinsic information* [22,23],

$$I(A, B{\downarrow}E) = \min_{E \to F} I(A:B|F), \quad (4)$$

where $I(A:B|F) = \sum_f p_F(f)I(A:B|F = f)$ is the conditional mutual information of $p_{ABF}(a, b, f)$, and the minimization is taken over all stochastic maps $E \to F$ that map the variable E (with values e) to a new variable F (with values f), such that the alphabet size of F is at most that of E [24]. While this minimization may be hard, any candidate stochastic map provides a valid upper bound.

When applying this bound to the CC attack, the key rate is upper bounded by

$$r \le \sum_{x,y} p_{xy} I_{xy}(A:B{\downarrow}E), \quad (5)$$

where the sum runs over all those settings (x, y) from which the key is distilled, p_{xy} is the probability of Alice and Bob choosing the settings x and y, respectively, and $I_{xy}(A:B{\downarrow}E)$ is the intrinsic information of the distribution in Eq. (3). Note that the bound in Eq. (5) is based only on the observed correlation, without any assumption on the state or the measurements.

Nonlocality is not sufficient for DIQKD.—In what follows, we prove that there exist nonlocal correlations that cannot be used for secure key extraction with standard DIQKD. We do this by applying the CC attack on any correlation obtained by performing arbitrary projective measurements on the two-qubit Werner state [18] with *visibility* $v \in [0, 1]$,

$$\rho_{AB}^v = v|\psi_-\rangle\langle\psi_-| + (1 - v)\frac{\mathbb{I}}{4}, \quad (6)$$

where $|\psi_-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. It is known that for arbitrary (even infinitely many) projective measurements $\{A_a^x\}$ and $\{B_b^y\}$, the correlation $p_{AB}^v(a, b|x, y) :=$ $\mathrm{tr}[\rho_{AB}^v(A_a^x \otimes B_b^y)]$ is local whenever the visibility is at most $v \le v_{\mathcal{L}}^w := 999 \times 689 \times 10^{-6}\cos^4(\pi/50) \approx 0.6829$, see Ref. [25]. On the other hand, it is also known that there exist projective measurements that give rise to nonlocal correlations for $v \ge v_{\mathcal{NL}}^w : \approx 0.6964$, see Ref. [26].

Let us consider all DIQKD protocols that use correlations obtained by implementing arbitrarily many projective measurements on the Werner state. The measurements can be written as $A_a^x = \frac{1}{2}[\mathbb{I} + (-1)^a\vec{\alpha}_x \cdot \vec{\sigma}]$ and $B_b^y = \frac{1}{2}[\mathbb{I} + (-1)^b\vec{\beta}_y \cdot \vec{\sigma}]$, where $a, b \in \{0, 1\}$, $\vec{\alpha}_x$ and $\vec{\beta}_y$ are unit vectors in $\mathbb{R}^3$, and $\vec{\sigma} = (X, Y, Z)$ is a vector containing the Pauli matrices. It is easy to verify that

$$\begin{bmatrix} p_{AB}^v(0, 0|x, y) & p_{AB}^v(0, 1|x, y) \\ p_{AB}^v(1, 0|x, y) & p_{AB}^v(1, 1|x, y) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} s_{xy}^v & 1 - s_{xy}^v \\ 1 - s_{xy}^v & s_{xy}^v \end{bmatrix},$$
$$(7)$$

where $s_{xy}^v = \frac{1}{2}(1 - v\vec{\alpha}_x \cdot \vec{\beta}_y) \in [0, 1]$.

The CC attack we consider is rather intuitive: it uses the nonlocal correlation $p_{AB}^{\mathcal{NL}} = p_{AB}^{v=1}$, and local deterministic correlations that sum up to the correlation for the provable local Werner state, $p_{AB}^{\mathcal{L}} = p_{AB}^{v=v_{\mathcal{L}}^w}$. It is easy to verify that in this case we have that $q_{\mathcal{L}} = q_{\mathcal{L}}^w := (1 - v)/(1 - v_{\mathcal{L}}^w)$. For now, let us assume that $s_{xy}^1 \equiv s_{xy}^{v=1} \ge \frac{1}{2}$. This implies that in the ideal ($v = 1$) case, the outcomes of Alice and Bob are correlated, i.e., they observe $a = b$ more often than $a \ne b$ [see Eq. (7)]. For this reason, in her stochastic relabeling $E \to F$, Eve will attempt to become as correlated to the $a = b$ events as possible, that is, she picks $f = a$ whenever the correlation is local and $a = b$. In order to reduce the conditional mutual information of all the other events, she sets $f = ?$ for all the remaining cases. The resulting distribution reads

$$p_{ABF}(a, b, f|x, y) = q_{\mathcal{L}}^w p_{AB}^{v=v_{\mathcal{L}}^w}(a, b|x, y)$$
$$\times [\delta_{a,b}\delta_{f,a} + (1 - \delta_{a,b})\delta_{f,?}]$$
$$+ (1 - q_{\mathcal{L}}^w)p_{AB}^{v=1}(a, b|x, y)\delta_{f,?}. \quad (8)$$

Note that a similar distribution can be introduced for the case of $s_{xy}^1 < \frac{1}{2}$, in which case Eve becomes correlated with the $a \ne b$ events. For the distribution in Eq. (8) we have that $I_{xy}(A:B|F = a) = 0$ for all a, so the final bound on the key rate is given by

$$r \le \sum_{x,y} p_{xy} p_F(?|x, y)I_{xy}(A:B|F = ?), \quad (9)$$

where $I_{xy}(A:B|F = f)$ is the mutual information of the distribution $p_{AB|F}(a, b|f, x, y) = p_{ABF}(a, b, f|x, y)/p_F(f|x, y)$.

To compute the upper bound, we need to calculate the terms $I_{xy}(A:B|F = ?)$ in Eq. (9), that is, the mutual information of the distribution

$$p_{AB|F}(a,b|?,x,y) = \frac{1}{2(1-q_{\mathcal{L}}^w s_{xy}^w)} \begin{bmatrix} (1-q_{\mathcal{L}}^w)s_{xy}^1 & (1-q_{\mathcal{L}}^w)(1-s_{xy}^1)+q_{\mathcal{L}}^w(1-s_{xy}^w) \\ (1-q_{\mathcal{L}}^w)(1-s_{xy}^1)+q_{\mathcal{L}}^w(1-s_{xy}^w) & (1-q_{\mathcal{L}}^w)s_{xy}^1 \end{bmatrix}, \quad (10)$$

where $s_{xy}^w = s_{xy}^{v=v_{\mathcal{L}}^w}$ and $s_{xy}^1 = s_{xy}^{v=1}$. The mutual information is clearly zero whenever $(1-q_{\mathcal{L}}^w)s_{xy}^w = (1-q_{\mathcal{L}}^w)(1-s_{xy}^1)+q_{\mathcal{L}}^w(1-s_{xy}^w)$, which is equivalent to

$$v = \frac{v_{\mathcal{L}}^w(2s_{xy}^1-1)+1}{v_{\mathcal{L}}^w(1-2s_{xy}^1)+4s_{xy}^1-1} =: v_{xy}. \quad (11)$$

Note that while $I_{xy}(A:B|F=?)$ is in general positive for $v < v_{xy}$, a slight modification of the CC attack leads to $I_{xy}(A:B|F=?) = 0$ for all $v \le v_{xy}$. To see this, note that for $v \le v_{xy}$, the correlation $p_{AB}^v(a,b|x,y)$ is a convex combination of $p_{AB}^{v_{xy}}(a,b|x,y)$ and the uniform correlation $p_{AB}^u(a,b|x,y) = 1/4$. Then, the observed correlation can be obtained by Eve distributing either $p_{AB}^{v_{xy}}$ or p_{AB}^u, both of which having zero intrinsic information. Therefore, Eve can clearly keep $I_{xy}(A:B|F=?) = 0$ for all $v \le v_{xy}$.

Also note that v_{xy} is monotonically decreasing in s_{xy}^1, and hence, it reaches its lowest possible value at $s_{xy}^1 = 1$. This gives rise to the *critical visibility* of the Werner state,

$$v_{\text{crit}}^w = \frac{v_{\mathcal{L}}^w+1}{3-v_{\mathcal{L}}^w} \approx 0.7263 > v_{\mathcal{NL}}^w \approx 0.6964. \quad (12)$$

An analogous derivation yields the same critical visibility for $s_{xy}^1 < \frac{1}{2}$. From the above arguments, it follows that whenever the visibility is $v_{\mathcal{NL}}^w \le v \le v_{\text{crit}}^w$, Alice and Bob cannot extract a secure key from correlations obtained from the Werner state with any (even infinite) number of projective measurements, even though the state is nonlocal (i.e., there exist projective measurements that, measured on the state, give rise to nonlocal correlations) and distillable [27]. This means that the Bell nonlocality of the observed correlation is in general not sufficient for DIQKD whenever Alice and Bob announce their measurement settings, and, moreover, that there exist nonlocal states that cannot be used for standard DIQKD with projective measurements.

CHSH-based protocols.—The most commonly used DIQKD protocols [1,2,9,11–14] are based on the maximal violation of the biased CHSH inequality [10]. In these protocols the shared state is $\rho_{AB} = |\psi_-\rangle\langle\psi_-|$, and Alice's measurements are described by $\vec{\alpha}_0 = (0,0,-1)$ and $\vec{\alpha}_1 = (-1,0,0)$, while Bob's measurements are described by $\vec{\beta}_0^\theta = (\sin\theta,0,\cos\theta)$, $\vec{\beta}_1^\theta = (-\cos\theta,0,\sin\theta)$ and $\vec{\beta}_2^\theta = (0,0,1)$, where $0 < \theta < \pi/2$. The protocol based on the standard CHSH inequality is reproduced by setting $\theta = \pi/4$ [1,2]. The noisy versions of these protocols with visibility v can be described by sharing a Werner state, and our results from the previous section readily apply. In

particular, v_{crit}^w in Eq. (12) is a lower bound on the critical visibility for CHSH-based protocols.

However, for a fixed protocol, the bound on the critical visibility can be improved. This is because in the setting of the CHSH-based protocols, the polytope of local correlations is completely characterized [28]. One can verify that in the CHSH-based protocols, if Alice and Bob observe a correlation that corresponds to the Werner state with visibility v, then this correlation is local if and only if $v \le v_{\mathcal{L}}^\theta := 1/(\cos\theta + \sin\theta)$ [29]. Therefore, an improved bound on the critical visibility for the CHSH-based protocols is given by

$$v_{\text{crit}}^\theta = \frac{v_{\mathcal{L}}^\theta+1}{3-v_{\mathcal{L}}^\theta} > v_{\mathcal{L}}^\theta \quad \forall\ \theta \in (0,\pi/2). \quad (13)$$

That is, for a range of visibilities for which the observed correlation is nonlocal, Alice and Bob cannot extract a secure key. Note that the same critical visibility holds for the recently introduced modification of the standard CHSH-based protocol in Ref. [30], where the authors add a fourth setting for Bob. Indeed, since the local polytope is completely characterized in this case as well [28], one can verify that the correlation becomes local at the same visibility $v_{\mathcal{L}}^\theta$ [29].

Last, we note that in the CHSH-based protocols, Alice and Bob usually extract their key from the setting pair $x = 0$ and $y = 2$, by setting p_{02} in Eq. (5) arbitrarily close
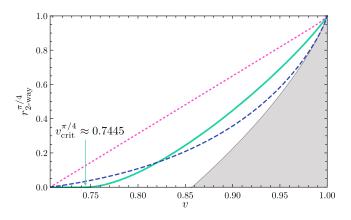

FIG. 1. Upper bounds on the two-way key rate for the standard CHSH protocol in terms of the visibility. The dotted line is the upper bound from [15], the dashed line is the upper bound from [17], and the solid line is the bound in Eq. (14). Note that the visibility can be converted into the CHSH violation S via $S = 2\sqrt{2}v$. The shaded area represents the lower bound from [1].

to 1. In this case, it is possible to compute the upper bound in Eq. (9) for any visibility $v \geq v_{\text{crit}}^{\theta}$, and we get

$$r^{\theta}(v) \leq 2(1 - s^{\theta}q_{\mathcal{L}}^{\theta}) + (1 - q_{\mathcal{L}}^{\theta})\log_2\left[\frac{1 - q_{\mathcal{L}}^{\theta}}{2(1 - s^{\theta}q_{\mathcal{L}}^{\theta})}\right]$$
$$+ q_{\mathcal{L}}^{\theta}(1 - s^{\theta})\log_2\left[\frac{q_{\mathcal{L}}^{\theta}(1 - s^{\theta})}{2(1 - s^{\theta}q_{\mathcal{L}}^{\theta})}\right] \tag{14}$$

where $s^{\theta} = \frac{1}{2}(1 + v_{\mathcal{L}}^{\theta})$ and $q_{\mathcal{L}}^{\theta} = (1 - v)/(1 - v_{\mathcal{L}}^{\theta})$. In Fig. 1 we plot the bound for the standard CHSH protocol ($\theta = \pi/4$), and show that it outperforms the recently derived upper bounds [15,17] near the critical visibility. In the Supplemental Material we also describe a two-dimensional region in the set of quantum correlations corresponding to correlations from the biased CHSH protocol that are nonlocal but cannot be used to extract a key using standard DIQKD [29].

Discussion.—We introduced a generic tool for upper-bounding DIQKD key rates using a simple eavesdropping attack. Using our tool, we showed that Bell nonlocality is not sufficient for secure DIQKD when the honest parties announce their measurement settings. Our results also imply that all the commonly used DIQKD protocols become insecure in the noisy case already in the nonlocal regime, even when assisted by arbitrary two-way communication. Our analysis does not prove that the considered nonlocal correlations are useless for secure key distribution, but it shows that the standard reconciliation—where the settings are announced by both parties—does not work for all nonlocal correlations.

Given the above, one possibility to lower the stringent requirements on noise parameters is to employ protocols such as that of Ref. [19], in which only one party announces their settings. Indeed, for this protocol we were not able to find an upper bound that vanishes in the nonlocal regime. Whether a secure key can be distilled from all nonlocal correlations using these protocols is an open question that deserves further investigation. Another possibility for improving the key rates extractable from a given quantum state is to employ measurements that are not projective. However, we note that no state is known thus far that is local for all arrangements of projective measurements, while exhibiting nonlocality for some arrangement of nonprojective measurements. Hence, the critical visibilities of the Werner state derived in this work also hold for all the hitherto studied arrangements of nonprojective measurements. Another question worth investigating is whether tighter upper bounds can be derived using collective or coherent attacks. Nonetheless, let us note that our (individual) CC attack can be applied to a broad class of DIQKD protocols, and gives rise to bounds on the critical visibility in experimentally relevant scenarios. We elaborate on these findings in [31].

[*]mate.farkas@icfo.eu

[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] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[5] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[7] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[8] R. Arnon-Friedman, Springer Thesis, Institute for Theoretical Physics, ETH Zurich, 2020, https://doi.org/10.1007/978-3-030-60231-4.
[9] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).
[10] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[11] E. Woodhead, A. Acín, and S. Pironio, Quantum **5**, 443 (2021).
[12] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Phys. Rev. Lett. **124**, 230502 (2020).
[13] P. Sekatski, J. D. Bancal, X. Valcarce, E. Y. Z. Tan, R. Renner, and N. Sangouard, Quantum **5**, 444 (2021).
[14] E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner, Phys. Rev. Lett. **124**, 020502 (2020).
[15] E. Kaur, M. M. Wilde, and A. Winter, New J. Phys. **22**, 023039 (2020).
[16] M. Christandl, R. Ferrara, and K. Horodecki, Phys. Rev. Lett. **126**, 160501 (2021).
[17] R. Arnon-Friedman and F. Leditzky, arXiv:2005.12325.
[18] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[19] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[20] S. Pironio, L. Masanes, A. Leverrier, and A. Acín, Phys. Rev. X **3**, 031007 (2013).

[21] A. Acín, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006).

[22] U. Maurer and S. Wolf, in *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, Ulm, 1997), p. 88, https://doi.org/10.1109/ISIT.1997.612915.

[23] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Theory of Cryptography*, edited by S. P. Vadhan (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007), pp. 456–478.

[24] M. Christandl, R. Renner, and S. Wolf, in *Proceedings of the IEEE International Symposium on Information Theory, 2003* (IEEE, Yokohama, 2003), pp. 258–258, https://doi.org/10.1109/ISIT.2003.1228014.

[25] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, Quantum **1**, 3 (2017).

[26] P. Diviánszky, E. Bene, and T. Vértesi, Phys. Rev. A **96**, 012113 (2017).

[27] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).

[28] D. Collins and N. Gisin, J. Phys. A **37**, 1775 (2004).

[29] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.127.050503 for the details of the bounds on CHSH-based protocols.

[30] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y. Z. Tan, R. Wolf, V. Scarani, and C. C. W. Lim, Nat. Commun. **12**, 2880 (2021).

[31] K. Łukanowski, M. Balanzó-Juandó, M. Farkas, A. Acín, and J. Kołodyński (to be published).