PHYSICAL REVIEW A **85**, 010301(R) (2012)

One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering

Cyril Branciard,[1] Eric G. Cavalcanti,[2] Stephen P. Walborn,[3] Valerio Scarani,[4,5] and Howard M. Wiseman[2,5]
[1]*School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia*
[2]*Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia*
[3]*Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil*
[4]*Centre for Quantum Technologies and Department of Physics, National University of Singapore, Singapore 117543*
[5]*ARC Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane QLD 4111, Australia*

(Received 27 September 2011; published 3 January 2012)

We analyze the security and feasibility of a protocol for quantum key distribution (QKD) in a context where only one of the two parties trusts his measurement apparatus. This scenario lies naturally between standard QKD, where both parties trust their measurement apparatuses, and device-independent QKD (DI-QKD), where neither do, and can be a natural assumption in some practical situations. We show that the requirements for obtaining secure keys are much easier to meet than for DI-QKD, which opens promising experimental opportunities. We clarify the link between the security of this one-sided DI-QKD scenario and the demonstration of quantum steering, in analogy to the link between DI-QKD and the violation of Bell inequalities.

DOI: 10.1103/PhysRevA.85.010301 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Mn

Quantum key distribution (QKD) allows two parties (Alice and Bob) to establish secret keys at a distance, with security guaranteed by the laws of quantum mechanics [1]. In standard QKD (S-QKD), the security is typically proven under the assumption that Alice and Bob can trust the physical functioning of their preparation and measurement apparatuses. For instance, standard security proofs for the Bennett-Brassard 1984 (BB84) protocol [2] assume that Alice sends qubits to Bob, prepared in some eigenstates of the σ_z or σ_x Pauli operators, and that Bob measures them in one of those two bases. Recent demonstrations of hacking of the devices has shown the importance and weakness of this assumption [3]. Moreover, since QKD is becoming commercially available, Alice and Bob may end up buying their devices from untrusted providers.

Remarkably, there are ways to guarantee security with fewer assumptions. The minimal set of assumptions is the one used in device-independent QKD (DI-QKD) [4,5]. There, Alice and Bob can certify the security of QKD based only on the observed violation of Bell inequalities [6]: the measurement apparatuses are untrusted black boxes, with a knob supposedly related to the measurement settings. Alice and Bob have only to trust the random number generator with which they vary the positions of the knob and, of course, the integrity of their locations. While the qualitative understanding "Bell violation implies security" is certainly true, the derivation of quantitative security bounds is challenging. The most recent results report on security against the most general attacks ("coherent attacks") under the assumption that previous measurements do not feed any information forward to subsequent ones [7,8] (or, to put it simply, that the devices are memoryless). In addition to these (hopefully temporary) limitations of the theoretical studies, DI-QKD imposes very demanding requirements on practical demonstrations. In particular, the Bell test would need to close the detection loophole [9], which requires very high detection efficiencies [10].

Intermediate scenarios between S-QKD and DI-QKD require less trust than the former and will be easier to implement than the latter [11]. Imagine for instance that a bank wants to establish secret keys with its clients; the bank could invest a lot of money to establish one trustworthy measurement device, but the clients at the other end of the channel would certainly get cheap (and insecure) detection terminals. This leads us to study *one-sided* DI-QKD (1SDI-QKD): we consider an entanglement-based scenario in which Bob's measurement apparatus is trusted, while Alice's is not. In the entanglement-based setup the source is also untrusted, although we will also discuss prepare-and-measure (P&M) implementations where the source is trusted. We present a security bound against coherent attacks with similar assumptions as in Refs. [7,8], in particular that the devices are memoryless, as this enables the strongest security analysis presently available. Focusing on practical implementations, we show that the detector efficiencies required for a practical implementation of 1SDI-QKD are much lower than for DI-QKD, making it feasible with existing devices. Before that, let us start by stressing a link with a hierarchy of tests of quantum nonlocality [12].

QKD and quantum nonlocality. It is known that no secret key can be extracted in a QKD experiment if the channel between Alice and Bob is entanglement-breaking [13]. Hence, in order to demonstrate security, one must show that the channel preserves entanglement. The three different assumptions on Alice's and Bob's devices mentioned above correspond naturally to three different criteria for quantum nonlocality [12] (see Fig. 1): S-QKD or DI-QKD require the observed correlations to violate a separability criterion or a Bell inequality respectively; 1SDI-QKD requires the correlations to violate an *EPR-steering inequality* as defined in Ref. [14]. That is, if one imagines that Bob's system has a definite (albeit unknown to him) quantum state, the protocol must prove that Alice, by her choice of measurement, can affect this state. This sort of nonlocality, first discussed by Einstein, Podolsky, and Rosen [15], was called "steering" by Schrödinger [16]. In Ref. [12] these concepts of nonlocality arose from considering entanglement verification with untrusted *parties*. However, even if Alice and Bob trust each other, as in QKD, they may

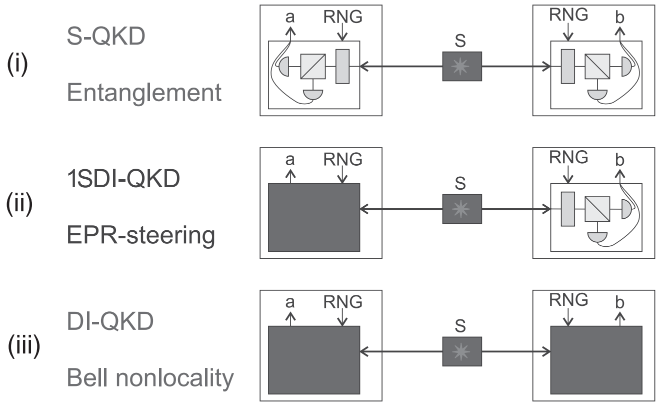

FIG. 1. Link between the three concepts of quantum nonlocality as classified in Ref. [12] and the three scenarios of S-QKD, 1SDI-QKD (this paper), and DI-QKD. In order to obtain a secret key, (i) if Alice and Bob trust their measurement devices (transparent boxes), then they must necessarily demonstrate *entanglement*; (ii) if Alice's measurement device is untrusted (black box), while Bob's is trusted, then Alice must demonstrate *steering* of Bob's state; (iii) if both Alice's and Bob's measurement devices are untrusted, then they must demonstrate *Bell nonlocality*. In all cases, Alice and Bob must trust their random number generator (RNG), and the integrity of their location.

not trust their devices, which is an analogous situation. From this perspective, our scenario of 1SDI-QKD can thus be seen as a practical application of the concept of *quantum steering*.

A 1SDI-QKD protocol. We consider the following 1SDI version of the Bennett-Brassard-Mermin 1992 (BBM92) entanglement-based protocol [17]: Alice and Bob receive some (typically photonic) quantum systems from an external source. Alice can choose between two binary measurements, A_1 and A_2; since she does not trust her measurement device, she treats it as a black box with two possible settings, yielding each time one of two possible outputs. Bob, on the other hand, trusts his device to make projective measurements B_1 or B_2 in some qubit subspace, typically corresponding to the operators σ_z and σ_x, respectively. After publicly announcing which measurements they chose for each system, Alice and Bob will try to extract a secret key from the conclusive results of the measurements A_1 and B_1; as explained below, the results of measurements A_2 and B_2 will allow them to estimate Eve's information.

Alice and Bob might not always detect the photons sent by the source, because of losses or inefficient detectors. Since Bob trusts his detectors, he trusts that Eve cannot control his detections. Also, Eve cannot get any useful information from Bob's (null) result if the photons going to him are lost or if she keeps them. Cases where Bob gets ambiguous results (e.g., double clicks) can be dealt with using the techniques of Ref. [18]—see the supplementary material [19] for details. Hence, we can safely consider only the cases where Bob gets detections. On the other hand, since Alice's measurement device is untrusted, Eve could control whether her detectors click depending on the state she receives and on her choice of measurement setting. We can therefore not simply discard Alice's no-detection events. In case her detectors do not click, she records a bit value of her choice as the result of her measurement, keeps track of the fact that her detectors did not click, and tells Bob (so that they can later postselect the raw key on Alice's detections); Eve has access to that information.

We denote by $\boldsymbol{A}_i$ and $\boldsymbol{B}_i$ the strings of classical bits Alice and Bob get from measurements A_i and B_i (and where Bob got a detection, as discussed above). Among the bits of $\boldsymbol{A}_1$, some correspond to actual detections by Alice, and some, corresponding to nondetections, were simply chosen by Alice herself. Everyone knows which ones are which. The detected bits form a string $\boldsymbol{A}_1^{\mathrm{ps}}$ (they will be *postselected* by Alice and Bob), while those that were not actually detected form a string $\boldsymbol{A}_1^{\mathrm{dis}}$ (they will be *discarded* for the key extraction), so that $\boldsymbol{A}_1 = (\boldsymbol{A}_1^{\mathrm{ps}},\boldsymbol{A}_1^{\mathrm{dis}})$. Bob's corresponding bit strings are $\boldsymbol{B}_1^{\mathrm{ps}}$ and $\boldsymbol{B}_1^{\mathrm{dis}}$, respectively, so that $\boldsymbol{B}_1 = (\boldsymbol{B}_1^{\mathrm{ps}},\boldsymbol{B}_1^{\mathrm{dis}})$. We denote by N the length of the strings $\boldsymbol{A}_1$ and $\boldsymbol{B}_1$ and by n the length of the strings $\boldsymbol{A}_1^{\mathrm{ps}}$ and $\boldsymbol{B}_1^{\mathrm{ps}}$.

Security proof and key rate. Recently,Tomamichel and Renner [20], together also with Lim and Gisin [21], have developed an approach to QKD based on an uncertainty relation for smooth entropies, which enables one to prove security against coherent attacks in precisely this 1SDI-QKD scenario; note however that one also needs (as in Refs. [7,8]) the assumption that the devices are memoryless [22]. To prove the security of our protocol in realistic implementations, we extend their analysis by considering imperfect detection efficiencies [23].

From the n-bit strings $\boldsymbol{A}_1^{\mathrm{ps}}$ and $\boldsymbol{B}_1^{\mathrm{ps}}$, on which Eve may have some (possibly quantum) information E, Alice and Bob can extract, through classical error correction and privacy amplification (from Bob to Alice), a secret key of length [24]

$$\ell \approx H_{\min}^{\epsilon}\big(\boldsymbol{B}_1^{\mathrm{ps}}\big|E\big) - nh\big(Q_1^{\mathrm{ps}}\big). \tag{1}$$

Here $H_{\min}^{\epsilon}(\boldsymbol{B}_1^{\mathrm{ps}}|E)$ denotes the *smooth min entropy* [25] of $\boldsymbol{B}_1^{\mathrm{ps}}$, conditioned on quantum side information E; h is the binary entropy function: $h(Q) \equiv -Q\log_2 Q - (1-Q)\log_2(1-Q)$; and Q_1^{ps} is the bit error rate between $\boldsymbol{A}_1^{\mathrm{ps}}$ and $\boldsymbol{B}_1^{\mathrm{ps}}$.

To bound $H_{\min}^{\epsilon}(\boldsymbol{B}_1^{\mathrm{ps}}|E)$, we will use the uncertainty relation introduced in Ref. [20], which bounds Eve's information on B_1 given Alice's information on the incompatible observable B_2. However, we need to use the full strings $\boldsymbol{B}_1,\boldsymbol{B}_2$, as postselection may lead to an apparent violation of the uncertainty relation. Using the chain rule [24] and the data-processing inequality [26] for smooth min-entropies, we first bound Eve's information on $\boldsymbol{B}_1^{\mathrm{ps}}$ relative to her information on $\boldsymbol{B}_1$:

$$\begin{aligned} H_{\min}^{\epsilon}(\boldsymbol{B}_1|E) &= H_{\min}^{\epsilon}\big(\boldsymbol{B}_1^{\mathrm{ps}},\boldsymbol{B}_1^{\mathrm{dis}}\big|E\big) && (2)\\ &\leqslant H_{\min}^{\epsilon}\big(\boldsymbol{B}_1^{\mathrm{ps}}\big|\boldsymbol{B}_1^{\mathrm{dis}}E\big) + \log_2\big|\boldsymbol{B}_1^{\mathrm{dis}}\big| && (3)\\ &\leqslant H_{\min}^{\epsilon}\big(\boldsymbol{B}_1^{\mathrm{ps}}\big|E\big) + N - n. && (4) \end{aligned}$$

Now, consider a hypothetical run of the protocol where the bits of $\boldsymbol{A}_1$ and $\boldsymbol{B}_1$ would be measured in the second basis; we denote by $\boldsymbol{A}_2$ and $\boldsymbol{B}_2$ the corresponding hypothetical strings. From the generalized uncertainty relation of [20], one has

$$H_{\min}^{\epsilon}(\boldsymbol{B}_1|E) \geqslant qN - H_{\max}^{\epsilon}(\boldsymbol{B}_2|\boldsymbol{A}_2), \tag{5}$$

where q is a measure of how distinct Bob's two measurements are; for orthogonal qubit measurements, $q = 1$.

Here, $H^{\epsilon}_{\max}(\boldsymbol{B}_2|\boldsymbol{A}_2)$ is the *smooth max entropy* [25] of $\boldsymbol{B}_2$, conditioned on $\boldsymbol{A}_2$. It satisfies the following [21]:

$$H^{\epsilon}_{\max}(\boldsymbol{B}_2|\boldsymbol{A}_2) \lesssim Nh(Q_2), \tag{6}$$

where Q_2 is the bit error rate between $\boldsymbol{A}_2$ and $\boldsymbol{B}_2$. Now, since the choice of basis was made randomly, Q_2 is the same as the bit error rate observed—without postselection—when the second basis was actually chosen (no matter how rarely) by both Alice and Bob.

Substituting (4)–(6) in Eq. (1), we obtain

$$\ell \gtrsim n\big[1 - h\big(Q_1^{\text{ps}}\big)\big] - N[h(Q_2) + 1 - q]. \tag{7}$$

In the asymptotic limit of infinite key lengths, the above approximate inequality becomes exact [21,27]. The fraction n/N of photons which Alice detects, given that Bob detected one, will be denoted η_A. This allows us to write the *secret key rate* $r \equiv \ell/N$ (the number of secret bits obtained per photon detected by Bob, measured in the first basis), as

$$r \geqslant \eta_A\big[1 - h\big(Q_1^{\text{ps}}\big)\big] - h(Q_2) - (1 - q). \tag{8}$$

Relation to EPR steering. As we recalled before, the secret key rate above can only be positive if Alice and Bob can check that they share entanglement. In our 1SDI scenario, this amounts to demonstrating quantum steering. Hence, the inequality $\eta_A[1 - h(Q_1^{\text{ps}})] - h(Q_2) - (1 - q) \leqslant 0$ can be understood as an EPR-steering inequality [14]. In the supplementary material [19], we give a more direct proof of this claim, starting from the so-called *local hidden state model* [12].

Experimental prospects. We now turn to the feasibility analysis. Consider a typical experimental setup, where a source sends maximally entangled two-qubit states to Alice and Bob, through a depolarizing channel with visibility V, and where, as in the BBM92 protocol, $A_1 = B_1 = \sigma_z$ and $A_2 = B_2 = \sigma_x$, with Alice's detection efficiency being η_A as above. (We emphasize that this is simply a model for Alice's measurements, which are implemented in a black box.)

The secret key rate that Alice and Bob can extract is then bounded by (8), with $q = 1$ and

$$Q_1^{\text{ps}} = (1 - V)/2, \quad Q_2 = (1 - \eta_A V)/2.$$

Figure 2 shows the values of the bound (8) as a function of η_A and for different values of V. For a perfect visibility $V = 1$, one gets a positive secret key rate for all $\eta_A > 65.9\%$.

This detection probability threshold is much lower than those required for DI-QKD. For instance, if Alice and Bob have the same detection efficiency η, then they require $\eta > 94.6\%$ for the protocol studied in Ref. [7], when they extract their key from the nonpostselected data. If the key is extracted from the postselected data (as we considered here for 1SDI-QKD), the threshold remains quite high, $\eta > 91.1\%$ (see Fig. 2 and supplementary material [19]). The much lower efficiency threshold for 1SDI-QKD compared with DI-QKD is related to the fact that it is much easier to close the detection loophole in a steering experiment [28–30] than in a Bell test, for which there are no photonic detection-loophole-free demonstrations to date. Heralding efficiencies of ~62% have recently been reported [30] in an experiment demonstrating detection-loophole-free quantum steering; our 1SDI-QKD protocol could be demonstrated with a very similar (but slightly improved) experimental setup.

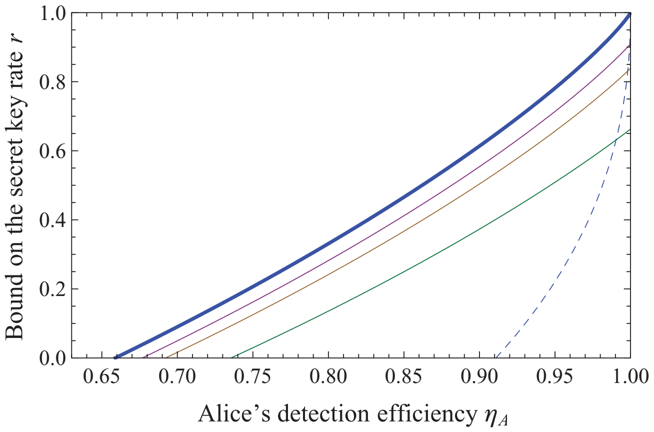

FIG. 2. (Color online) Solid curves: bounds (8) on the secret key rate r in a typical implementation of 1SDI-QKD, as a function of Alice's detection efficiency η_A, for visibilities $V = 1, 0.99, 0.98, 0.95$ (from top to bottom) and $q = 1$. Dashed curve: for comparison, bounds (for $V = 1$) for DI-QKD, obtained by adapting the security analysis of Ref. [7], when Bob has the same detection efficiency $\eta_B = \eta_A$ as Alice (see supplementary material [19]).

Note also that, in the 1SDI-QKD case, the losses between the source and Bob's laboratory do not affect the security of the protocol; they only decrease the key rate proportionally to the decrease of Bob's detection rate (as long as the noise in Bob's detectors does not become prominent). Hence, long distances can in principle be reached if the source stays close to Alice; this is in contrast to the fully DI-QKD case, where the limit on the detection efficiencies imposes a limit on the allowed distance between Alice and Bob (although some proposals have been suggested to overcome this problem [31–33]).

Comparison of different scenarios. Key rate bounds for entanglement-based QKD also apply to P&M schemes, as long as the preparation device can be trusted to produce a certain *average* state independent of Alice's (or Bob's, as the case may be) choice of preparation basis (e.g., the completely mixed state, regardless of whether σ_x or σ_z is the chosen basis). A preparation device with this property can be envisaged as a trusted entanglement source situated in Alice's (or Bob's) laboratory, with a trusted channel between it and the local detector. In this picture it still makes sense to consider the case where the local "hypothetical" detector is untrusted, as this is equivalent to saying that we cannot trust the preparation device to prepare the desired state. Here the efficiency (which we will denote as η^*) of the hypothetical detector models the probability that the preparation device registers to the sender which of the two states (in the chosen basis) was sent. For a well-functioning device this can be close to unity; even if the preparation does use a probabilistic photon-pair source and a detector, the sender can generate many pairs within the time window for each system and switch out the system (one photon, ideally) only when its preparation is heralded by the detection of the other. A greater experimental challenge is the loss of the heralded photon (within the sender's laboratory or *en route*), which must be factored into the receiver's efficiency.

TABLE I. Best known bounds on secret key rates for QKD (secure against coherent attacks) with privacy amplification from Bob to Alice and memoryless devices—both P&M and entanglement-based. The second column tells which of the components—Alice's detectors (AD), the source (S), Bob's detector (BD), and each of the channels (C) between the source and the detectors—are trusted (T) or untrusted (U). Thick vertical lines in each row separate Alice's laboratory, the channel open to Eve, and Bob's laboratory. In the P&M cases, the detector plus source in a laboratory is a formal model for a preparation device; the efficiency η^* in these cases models the probability that the preparation device registers which state is prepared, and would typically be close to unity (for details see text). In column three, the bounds on key rates (here, per *photon pair* produced by the source; that is, per *preparation event* in the P&M cases) are given in terms of the functions $r_0(Q_1^{\rm ps},Q_2^{\rm ps}) \equiv \eta_B\eta_A[1-h(Q_1^{\rm ps})-h(Q_2^{\rm ps})]$ from S-QKD, $r_1(Q_1^{\rm ps},Q_2) \equiv \eta_B\{\eta_A[1-h(Q_1^{\rm ps})]-h(Q_2)\}$ from Eq. (8), and $r_2(Q_1^{\rm ps},S) \equiv \eta_A\eta_B[1-h(Q_1^{\rm ps})]-\log_2[1+\sqrt{2-(S/2)^2}]$ (see supplemental material [19]). Here S is the value of the CHSH polynomial [34], while Q_1 and Q_2 are bit error rates. The superscript ps means postselection on coincident detections; Q_2 in $r_1(Q_1^{\rm ps},Q_2)$ is postselected on Bob's detections, but not on Alice's; S must be estimated from the whole nonpostselected data. The efficiency thresholds (column four) are calculated with everything else perfect. In row four, we assumed $\eta_B^* \to 1$ (the threshold we quote is therefore a lower bound on the thresholds for $\eta_B^* < 1$), while in row seven, $\eta_A = \eta_B = \eta$.

Based on	AD	C	S	C	BD	Key rate bound	Eff. thresh.
P&M	T	T	T	U	T	$r_0(Q_1^{\rm ps},Q_2^{\rm ps})$	none
P&M	U	T	T	U	T	$r_1(Q_1^{\rm ps},Q_2)$	$\eta_A^* > 65.9\%$
P&M	U	U	T	T	T	$r_1(Q_1^{\rm ps},Q_2)$	$\eta_A > 65.9\%$
P&M	U	U	T	T	U	$r_2(Q_1^{\rm ps},S)$	$\eta_A > 83.3\%$
Entang.	T	U	U	U	T	$r_0(Q_1^{\rm ps},Q_2^{\rm ps})$	none
Steering	U	U	U	U	T	$r_1(Q_1^{\rm ps},Q_2)$	$\eta_A > 65.9\%$
Bell	U	U	U	U	U	$r_2(Q_1^{\rm ps},S)$	$\eta > 91.1\%$

Considering all nontrivial permutations of device trustworthiness, there are eight P&M scenarios and four genuine entanglement-based scenarios whose security can be analyzed using the methods of Refs. [7,20]. We remove mirror-image scenarios by keeping only the version which is better (or equally good) under the assumption of the privacy amplification being from Bob to Alice, as shown in Table I. Note that P&M by Bob with a fully trusted preparation device (row 3) does not improve the threshold efficiency required for Alice's untrusted detector, as compared to steering-based 1SDI-QKD with an untrusted entanglement source (row 6).

Conclusion. We have introduced the scenario of 1SDI-QKD and analyzed its security against coherent attacks in a practical situation where losses are taken into account. Our analysis shows that the assumptions of 1SDI-QKD allow one to significantly lower the necessary detection efficiencies compared to fully DI-QKD, and that the requirements for obtaining secure key rates in an experiment are within the range of current technology.

We have also stressed that 1SDI-QKD requires the violation of an EPR-steering inequality, in analogy with the requirement of violation of a Bell inequality for security of DI-QKD. The relation between the QKD hierarchy and the nonlocality hierarchy introduces some open questions: (i) It has recently been shown that steering can be demonstrated with arbitrarily low efficiencies [28]. Can one find (and prove the security of) 1SDI-QKD protocols that would also tolerate arbitrarily low efficiencies? (ii) With two measurement settings per party, steering can be demonstrated for efficiencies $\eta_A >$ 50% [28,30]. There is a large gap between this and the threshold of ~66% for our 1SDI-QKD protocol. The same situation occurs for fully DI-QKD, where there is also a gap between the threshold of $\eta > 82.8\%$ for a violation of the CHSH inequality [34] and that for the security of DI-QKD. How small can these be made in general? Another topic for further research is to extend our results to finite keys; for instance, along the lines of Ref. [21].

Note added. Recently, we became aware of a related work [35] where similar bounds on the detection efficiency thresholds are derived.

Acknowledgments. This work was supported by the Australian Research Council Programs CE110001027 and DP0984863, the National Research Foundation and the Ministry of Education, Singapore, the Brazilian agencies CNPq, FAPERJ, and the INCT-Informação Quântica.

[1] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[2] C. H. Bennett and G. Brassard, *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[3] L. Lydersen *et al.*, Nat. Photon. **4**, 686 (2010); I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011).
[4] D. Mayers and A. Yao, *Proc. of the 39th IEEE Conf. on Foundations of Computer Science* (IEEE, Los Alamitos, 1998), p. 503.
[5] A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
[6] J. S. Bell, Physics (NY) **1**, 195 (1964).
[7] L. Masanes, S. Pironio, and A. Acin, Nat. Comm. **2**, 238 (2011).
[8] E. Hänggi and R. Renner, e-print arXiv:1009.1833 (to be published).
[9] P. M. Pearle, Phys. Rev. D **2**, 1418 (1970).
[10] S. Pironio *et al.*, New J. Phys. **11**, 045021 (2009).
[11] M. Pawlowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).
[12] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[13] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[14] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

[15] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[16] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935).

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[18] T. Moroder, O. Guhne, N. Beaudry, M. Piani, and N. Lutkenhaus, Phys. Rev. A **81**, 052342 (2010).

[19] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.85.010301 for more details on practical detectors and multiple counts, a direct proof of the steering inequality, and a more detailed comparison of our results with those for DI-QKD.

[20] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[21] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, e-print arXiv:1103.4130 (to be published).

[22] S. Fehr and R. Renner (private communication).

[23] To avoid any confusion, we note that here we have reversed the roles of Alice and Bob compared to that in Refs. [20,21] in order to be consistent with earlier work on steering [12,14], in which Alice's detectors are not trusted, while Bob's are.

[24] J. M. Renes and R. Renner, e-print arXiv:1008.0452 (to be published).

[25] R. Renner and S. Wolf, in *Advances in Cryptology - ASIACRYPT*, Vol. 3788 of LNCS (Springer, Berlin, 2005), p. 199; R. Renner, Int. J. Quantum. Inform. **6**, 1 (2008).

[26] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).

[27] The approximate (in)equalities in the derivation of Eq. (7) account for additional correcting terms that appear in the equations in the case of finite key lengths. One typically finds that for raw key lengths longer than 10^4 to 10^5 bits, significant fractions of the asymptotic secret key rates are obtained [21].

[28] A. J. Bennet *et al.*, e-print arXiv:1111.0739 (to be published).

[29] B. Wittmann *et al.*, e-print arXiv:1111.0760 (to be published).

[30] D. H. Smith *et al.*, e-print arXiv:1111.0829, Nat. Commun. (to be published).

[31] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

[32] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304 (2011).

[33] D. Pitkänen *et al.*, Phys. Rev. A **84**, 022325 (2011).

[34] J. F. Clauser, M. A. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[35] X. Ma and N. Lütkenhaus, e-print arXiv:1109.1203 (to be published).