Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier

Nicolas Gisin,[1] Stefano Pironio,[1,2] and Nicolas Sangouard[1]

[1]*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland*

[2]*Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium*

(Received 22 March 2010; revised manuscript received 13 July 2010; published 12 August 2010)

In device-independent quantum key distribution (DIQKD), the violation of a Bell inequality is exploited to establish a shared key that is secure independently of the internal workings of the QKD devices. An experimental implementation of DIQKD, however, is still awaited, since hitherto all optical Bell tests are subject to the detection loophole, making the protocol unsecured. In particular, photon losses in the quantum channel represent a fundamental limitation for DIQKD. Here we introduce a heralded qubit amplifier based on single-photon sources and linear optics that provides a realistic solution to overcome the problem of channel losses in Bell tests.

DOI: 10.1103/PhysRevLett.105.070501 PACS numbers: 03.67.Dd, 03.65.Ud, 42.50.−p

Bell inequalities had an enormous impact on the foundations of quantum physics [1]. Interestingly, they also find application in device-independent quantum key distribution (DIQKD) [2–8]; as their violation guarantees the presence of entanglement independently of what precisely is measured, they can be exploited to establish a secret key between two black boxes without the necessity to know anything about how the boxes operate (see Fig. 1).

An experimental demonstration of DIQKD, however, is still awaited. Indeed, all optical tests of Bell's inequality suffer from the *detection loophole* [9]: Not all entangled photons are detected, because of unavoidable losses in the quantum channel, losses in the coupling between the photon-pair source and the optical fibers, and because of finite detector efficiency. The usual way out in Bell tests consists in assuming that the set of detected photon pairs is a fair set (the fair sampling assumption). It is indeed reasonable to assume that nature is not malicious and does not trick us. But the situation is completely different in DIQKD. Here one does not test nature but fights against a possible active adversary [10,11]; it would make no sense to assume that the eavesdropper is not malicious. Missed events could be used to perform simple and powerful attacks; e.g., the eavesdropper could force the black boxes to produce results only if the settings of the measuring devices are in agreement with a predeterminate scheme. Closing the detection loophole in an optical experiment is therefore a requirement for a demonstration of DIQKD.

The detection efficiency, the product of the transmission efficiency (including the coupling into the fiber) and the photon-detector efficiency, required to rule out attacks based on the detection loophole is very high, typically larger than 82.8% for the Clauser-Horne-Shimony-Holt (CHSH) inequality [12] in the absence of other limitations. However, even assuming perfect photodetection and lossless components, the transmission efficiency of a 5-km-long optical fiber at telecom wavelength is roughly 80%. Transmission losses thus represent a fundamental limitation for the realization of a detection-loophole-free Bell test on any distance relevant for QKD.

The problem of transmission losses might be circumvented by performing quantum-nondemolition measurements of the incoming photon or by using quantum repeaters to distribute entanglement over large distances [13] in a heralded way [14]. Here we propose a much simpler scheme based on heralded qubit amplification that combines single-photon sources and linear optical elements only. Our proposal could be implemented with

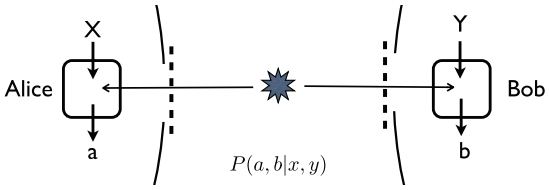

FIG. 1 (color online). Principle of DIQKD. Alice and Bob repeatedly choose for their QKD devices inputs x and y (the measurements on entangled particles) and obtain outputs a and b (the measurement outcomes). They then use an authenticated public channel to compare a sample of their data in order to estimate the conditional probability distribution $P(a, b \mid x, y)$. If $P(a, b \mid x, y)$ violates the CHSH inequality by a sufficient amount, then Alice and Bob can use standard error correction and privacy amplification to distill a secret key out of the remaining data. To establish security, nothing has to be known or assumed about Alice's and Bob's black boxes, except that they can be described by quantum physics. Note, however, that it is assumed that Alice and Bob are each located in a secure place and control the information going in and out of their locations (dotted lines). In particular, the value of the inputs x and y and of the outputs a and b should not leak out unwillingly of Alice's and Bob's secure place. This is the only part of the protocol that cannot be untrusted: Alice and Bob should either enforce these conditions (e.g., by closing a ''door'') or test it (e.g., by monitoring the output signals of the boxes).

present-day technology. It provides a realistic avenue towards device-independent quantum cryptography.

Heralded qubit amplifier.—Recently, Ralph and Lund proposed a clever use of quantum teleportation to realize a heralded single-photon amplifier [16]. Their scheme, presented in Fig. 2(a), has already motivated several experiments [17,18]. We show how it can be extended for polarization-qubit amplification, and we describe how this can be used in long-distance Bell experiments.

We consider a (normalized) coherent superposition

$$\psi_{\text{in}} = \alpha|0\rangle + (\beta_h \text{in}_h^\dagger + \beta_v \text{in}_v^\dagger)|0\rangle$$

of a vacuum component and of a qubit corresponding to a single photon either horizontally (corresponding to the creation operator $\text{in}_h^\dagger$) or vertically polarized (associated to $\text{in}_v^\dagger$). This state enters the device presented in Fig. 2(b). Two auxiliary photons, one horizontally $|1_h\rangle$ polarized and the other one vertically $|1_v\rangle$ polarized, are sent through a beam splitter with transmission t. This leads to the entanglement $(\sqrt{1-t}c_h^\dagger + \sqrt{t}\text{out}_h^\dagger) \otimes (\sqrt{1-t}c_v^\dagger + \sqrt{t}\text{out}_v^\dagger)|0\rangle$ of modes c and out. The modes $c_{h,v}$ and $\text{in}_{h,v}$ are then combined on a 50/50 beam splitter. The modes after this beam splitter are $d_h = (c_h + \text{in}_h)/\sqrt{2}$, $\tilde{d}_h = (c_h - \text{in}_h)/\sqrt{2}$, $d_v = (c_v + \text{in}_v)/\sqrt{2}$, and $\tilde{d}_v = (c_v - \text{in}_v)/\sqrt{2}$. The detection of two photons with orthogonal polarization,

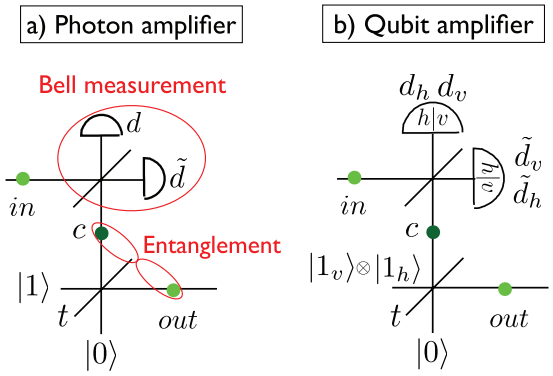

FIG. 2 (color online). (a) Heralded amplifier for single photons as proposed in Ref. [16]. A beam splitter with transmission coefficient t turns an incoming photon into the entanglement of modes c and out which can be used to teleport an arbitrary state $\alpha|0\rangle + \beta\text{in}^\dagger|0\rangle$ with the help of a partial Bell state analyzer. If $t = \frac{1}{2}$, this is standard quantum teleportation; i.e., the outcoming state $\alpha|0\rangle \pm \beta\text{out}^\dagger|0\rangle$ is similar to the incoming one, up to a possible unitary transformation depending on which detector clicked. But if $t > \frac{1}{2}$, a successful Bell state measurement projects the outcoming state in the incoming one but shifted towards the single-photon state $|1\rangle$: $\sqrt{1-t}\alpha|0\rangle \pm \sqrt{t}\beta\text{in}^\dagger|0\rangle$. (b) Setup for amplifying polarization qubits in a heralded way. This scheme is similar to the single-photon amplifier except that a product state of two photons with orthogonal polarization are sent through the partial beam splitter. The probabilistic Bell measurement is based on a 50–50 beam splitter followed by polarization measurements in the h/v basis (which require a polarization beam splitter and two photodetectors).

for example, one in mode d_h and the other one in mode d_v, projects the output mode into

$$\psi_{\text{out}} = \frac{\sqrt{1-t}}{2}[\sqrt{1-t}\alpha|0\rangle + \sqrt{t}(\beta_h \text{in}_h^\dagger + \beta_v \text{in}_v^\dagger)|0\rangle].$$

For $t = 1/2$, the output state is equal to the input state and the scheme reduces to a teleportation protocol for qutrits with a partial Bell state analyzer. But for $t > 1/2$, the relative weight of the vacuum component decreases, leading to the amplification of the polarization qubit. This qubit amplification is probabilistic, since it depends on the accomplishment of the Bell measurement, but it is heralded by two detector clicks. The success probability is given by $|\psi_{\text{out}}|^2$. Since the detection of two photons in modes $(d_h, \tilde{d}_v)$, $(\tilde{d}_h, d_v)$, or $(\tilde{d}_h, \tilde{d}_h)$ combined with the appropriate one-qubit rotation also collapses the outcoming state into ψ_{out}, the overall success probability of the heralding amplifier is given by $4|\psi_{\text{out}}|^2$.

Application to DIQKD.—As all teleportation protocols, the qubit amplifier also applies to mixed states. This provides a powerful tool to overcome the problem of losses in DIQKD. Suppose that a photon-pair source located on Alice's side is excited and emits entangled photons with a small probability $p \ll 1$, leading to the state

$$|0\rangle\langle 0| + p\left|\frac{a_h^\dagger b_h^\dagger + a_v^\dagger b_v^\dagger}{\sqrt{2}}\right\rangle\left\langle\frac{a_h^\dagger b_h^\dagger + a_v^\dagger b_v^\dagger}{\sqrt{2}}\right| + O(p^2).$$

The term $O(p^2)$ introduces errors in the protocol, leading to the requirement that p has to be kept small. The mode b is sent to Bob through a quantum channel, and, because of losses, Alice and Bob share the state

$$|0\rangle\langle 0| + \frac{1}{2}p(1-\eta_t)(|a_h^\dagger\rangle\langle a_h^\dagger| + |a_v^\dagger\rangle\langle a_v^\dagger|) + p\eta_t\left|\frac{a_h^\dagger b_h^\dagger + a_v^\dagger b_v^\dagger}{\sqrt{2}}\right\rangle\left\langle\frac{a_h^\dagger b_h^\dagger + a_v^\dagger b_v^\dagger}{\sqrt{2}}\right|, \quad (1)$$

where η_t denotes the transmission efficiency of the quantum channel. Before Bob performs measurements, he amplifies the modes b_h and b_v by using the setup described in Fig. 3. The state resulting from the successful amplification of both polarization modes is given by

$$\frac{(1-t)^2}{4}|0\rangle\langle 0| + \frac{(1-t)^2 p(1-\eta_t)}{8}(|a_h^\dagger\rangle\langle a_h^\dagger| + |a_v^\dagger\rangle\langle a_v^\dagger|) + \frac{t(1-t)p\eta_t}{4}\left|\frac{a_h^\dagger b_h^\dagger + a_v^\dagger b_v^\dagger}{\sqrt{2}}\right\rangle\left\langle\frac{a_h^\dagger b_h^\dagger + a_v^\dagger b_v^\dagger}{\sqrt{2}}\right|. \quad (2)$$

For large enough t, the entangled component is amplified in a heralded way, offering the possibility for Alice and Bob to share a maximally entangled state despite losses. This promises a considerable advance towards the implementation of DIQKD on meaningful distances. The heralding signal from the amplifier allows Bob to introduce an input y in his black box only when he shares an entangled state with Alice. Hence, the overall detection efficiency required to close the detection loophole does not depend

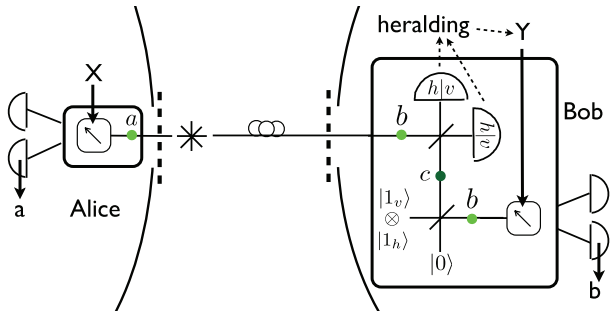

FIG. 3 (color online). Proposed setup for the implementation of DIQKD based on a heralded qubit amplifier. The entangled-photon source is located close to Alice's location. Each of Alice's and Bob's black boxes includes a measurement apparatus. Furthermore, Bob's box contains the qubit amplifier which gives an heralding signal each time an entangled pair has been successfully distributed. Since Bob performs a measurement or, in other words, inputs a y, only when he gets the heralding signal, Alice and Bob can safely discard all events where a photon got lost in the quantum channel. Note that the detectors can be either out or in the boxes depending on whether they can be trusted or not. In the figure, they are outside the black boxes.

anymore on the transmission efficiency but reduces to the intrinsic detection efficiency of Alice's and Bob's boxes.

The probability to obtain a heralded signal is

$$P_H = (1-t)^2 + p(1-t)^2(1-\eta_t) + t(1-t)p\eta_t, \quad (3)$$

which roughly reduces to $(1-t)^2$ for small transmission efficiency. As can be seen from Eqs. (2) and (3), there is a trade-off on the transmission coefficient t of the partial beam splitter. The amplification of the entangled component favors $t \approx 1$, whereas a high success probability favors $t \approx 0$. In order to rule out attacks based on the detection loophole, it is essential to choose a large transmission coefficient $t \approx 1$ to guarantee the distribution of highly entangled states. The price to pay is a reduction in the key rate because of the limited success probability of the qubit amplifier.

Implementation and performance analysis.—In practice, photons get lost not only because of the transmission losses in the quantum channel but also because of the imperfect coupling of photons into the optical fibers, which is characterized by an efficiency η_c. On Bob's side, the coupling loss can be counterbalanced by the amplifier, as the transmission losses. However, the amplifier itself contributes a factor η_c back to the detection efficiency of Bob's box since the single-photon sources used in the amplifier must themselves be coupled into fibers. Hence, the overall detection efficiency required to close the detection loophole reduces to the product of the coupling efficiency η_c by the detector efficiency η_d but does not depend anymore on the transmission efficiency η_t.

We now perform a detailed analysis to assess the performance of our scheme where we consider two possibilities for the single-photon sources: either on-demand or heralded sources. The latter can be realized from a pair source where the emission of an individual photon is heralded by the detection of the twin photon, as implemented in Ref. [19] from the parametric down-conversion process. A single-photon source on-demand could then be obtained by adding a quantum memory. In the long run, on-demand sources based on quantum dots embedded in microcavities [20] or single atoms inside high-finesse cavities [21] are also potential candidates.

We consider the DIQKD protocol based on the CHSH inequality analyzed in Ref. [4]. Existing security proofs valid against collective attacks assume perfect detectors [5,6]. We show in the supplementary material [15] how to apply them to the case of imperfect devices and how to compute the corresponding key rate. Moving slightly away from a full device-independent scenario, we also consider the case where the end detectors are trusted and can be moved out of the black boxes. This means that the detectors are well characterized, that they have a known efficiency, and that the eavesdropper cannot tamper with them. In this case, a Bell violation can be observed independently of the detector efficiency η_d, and any local description is ruled out provided that the coupling η_c of single photons into optical fibers is high enough.

To compute the key rate, we consider a fiber attenuation of 0.2 dB/km, corresponding to telecom-wavelength photons, and a coupling efficiency of $\eta_c = 0.9$. The coupling efficiency of single photons within optical fibers is being maximized in many laboratories, and a coupling of 83% was reported in Ref. [19]. We assume that the photon sources are excited with a repetition rate of 10 GHz [22]. We take all detectors to be photon-number-resolving detectors with efficiency η_d, and we neglect dark counts. Note that superconducting transition-edge sensor detectors can already resolve telecom-wavelength photons and have 95% efficiency with negligible noise [23]. Since we consider realistic sources, e.g., based on parametric down-conversion to provide high repetition rates, the dominant errors come from the multipair emissions which have to be made small by controlling the intensity of pumping lasers, i.e., the parameter p for the entangled-pair source and p' for the pair source used to produce heralded single photons. For a given distance, we optimized the transmission coefficient t and the pump dependent parameters p and p' to maximize the key rate; see supplementary material [15]. The results of our calculations are presented in Fig. 4 for untrusted detectors of efficiency $\eta_d = 0.95$ and for trusted detectors of efficiency $\eta_d = 0.8$.

Without an amplifier, no secret key can be established beyond 1.4 km for untrusted detectors and beyond 3.6 km for trusted detectors. On the other hand, an implementation based on a qubit amplifier with heralded single-photon sources achieves rates of about 1 bit/min on distances of 10–20 km and of about 1 bit/s on distances of 80–90 km with on-demand single-photon sources. Note that, contrarily to the situation without the amplifier, there are in principle no limitations other than technical ones on these

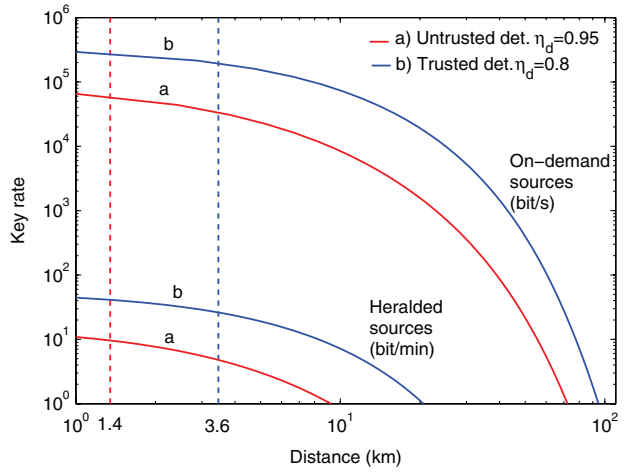

FIG. 4 (color online). Key rate vs distance for DIQKD with imperfect devices (log-log scale). (Red) curves labeled (a) correspond to untrusted detectors of efficiency $\eta_d = 0.95$ (seen as part of the QKD black boxes); (blue) curves labeled (b) correspond to trusted detectors of efficiency $\eta_d = 0.8$ (moved out of the QKD black boxes). The dotted vertical line represents the maximal distance above which no secret key can be extracted in the absence of an amplification process that counterbalances transmission losses. The two lower curves give the key rate (in bit/ min) as a function of the distance for an amplifier based on heralded single-photon sources; the two upper curves represent the key rate (in bit/s) for an amplifier with on-demand single-photon sources.

distances and they can be further extended, provided that one is willing to lower the key rate.

Finally, note that the physics behind the qubit amplification is based on the bosonic character of indistinguishable photons. The temporal, spectral, spatial, and polarization properties of modes produced by the entangled-pair source and by the single-photon sources (the modes b and c involved in the Bell measurement; see Fig. 3) thus have to overlap. However, when the input state is a mixture between a qubit state and an empty component, as caused by losses, the optical path length does not require an interferometric control. The degree of indistinguishability of two photons is measured through the visibility V of the "Hong-Ou-Mandel" dip [24]. Reference [25] has reported a visibility $V = 0.994$, largely sufficient for the successful implementation of our scheme (see analysis in supplementary material [15]).

Conclusion.—We have presented a simple qubit-amplification scheme suited to the distribution of entanglement over large distances in a heralded way. This scheme could find applications, e.g., in traditional QKD [26] or in quantum repeaters [13]. Here we show how to use it in DIQKD to overcome transmission losses. An implementation of our proposal with heralded single-photon sources represents an experiment feasible with today's best technology that demonstrates DIQKD over 10–20 km of telecom fibers. The experiment promises to be difficult, though every single step of the proposed experiment has already been demonstrated. We see our proposal as a great challenge for the quantum communication community.

We thank H. Zbinden and one of the referees for pointing out simplifications in the implementation of the qubit amplifier. We also thank M. Afzelius, J. D. Bancal, N. Brunner, S. Massar, J. Minář, H. de Riedmatten, P. Sekatski, C. Simon, and R. Thew for valuable discussions. This work was supported by the ERC-AG QORE, the EU project Qessence, the Swiss NCCR Quantum Photonics, and the Brussels-Capital region through a BB2B grant.

[1] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, England, 1987).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] D. Mayers and A. C. Yao, in *FOCS 98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1998), p. 503.
[4] A. Acin *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
[5] S. Pironio *et al.*, New J. Phys. **11**, 045021 (2009).
[6] M. McKague, New J. Phys. **11**, 103037 (2009); arXiv:1006.2352.
[7] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[8] L. Masanes, Phys. Rev. Lett. **102**, 140501 (2009).
[9] P. Pearle, Phys. Rev. D **2**, 1418 (1970).
[10] Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008).
[11] V. Makarov, New J. Phys. **11**, 065003 (2009).
[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[13] N. Sangouard *et al.*, arXiv:0906.2699.
[14] Note that the problem of transmission losses cannot be overcome by using a standard quantum relay [15].
[15] See supplementary material at http://link.aps.org/supplemental/10.1103/PhysRevLett.105.070501 for how to apply existing security proofs for DIQKD which assume perfect detectors to the case of imperfect devices and details of the calculation of the achievable key rate when DIQKD is implemented with a heralded qubit amplifier.
[16] T. C. Ralph and A. P. Lund, in *Proceedings of 9th International Conference on Quantum Measurement and Computing*, edited by A. Lvovsky (AIP, New York, 2009), p. 155.
[17] G. Y. Xiang *et al.*, Nat. Photon. **4**, 316 (2010).
[18] F. Ferreyrol *et al.*, Phys. Rev. Lett. **104**, 123603 (2010).
[19] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Opt. Commun. **246**, 545 (2005).
[20] E. Moreau *et al.*, Appl. Phys. Lett. **79**, 2865 (2001); M. Pelton *et al.*, Phys. Rev. Lett. **89**, 233602 (2002).
[21] J. C. McKeever *et al.*, Science **303**, 1992 (2004); M. Hijlkema *et al.*, Nature Phys. **3**, 253 (2007).
[22] Q. Zhang *et al.*, Opt. Express **15**, 10 288 (2007).
[23] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).
[24] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[25] T. B. Pittman and J. D. Franson, Phys. Rev. Lett. **90**, 240401 (2003).
[26] X. Ma, T. Moroder, and N. Lütkenhaus, arXiv:0812.4301.