Measurement-Device-Independent Quantum Key Distribution

Hoi-Kwong Lo,[1] Marcos Curty,[2] and Bing Qi[1]

[1]*Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

[2]*Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo, Pontevedra, 36310, Spain*

(Received 13 October 2011; published 30 March 2012)

How to remove detector side channel attacks has been a notoriously hard problem in quantum cryptography. Here, we propose a simple solution to this problem—*measurement*-device-independent quantum key distribution (QKD). It not only removes all detector side channels, but also doubles the secure distance with conventional lasers. Our proposal can be implemented with standard optical components with low detection efficiency and highly lossy channels. In contrast to the previous solution of full device independent QKD, the realization of our idea does not require detectors of near unity detection efficiency in combination with a qubit amplifier (based on teleportation) or a quantum nondemolition measurement of the number of photons in a pulse. Furthermore, its key generation rate is many orders of magnitude higher than that based on full device independent QKD. The results show that long-distance quantum cryptography over say 200 km will remain secure even with seriously flawed detectors.

DOI: 10.1103/PhysRevLett.108.130503 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) allows two parties (typically called Alice and Bob) to generate a common string of secret bits, called a secret key, in the presence of an eavesdropper, Eve [1]. This key can be used for tasks such as secure communication and authentication. Unfortunately, there is a big gap between the theory and practice of QKD. In principle, QKD offers unconditional security guaranteed by the laws of physics [2,3]. However, real-life implementations of QKD rarely conform to the assumptions in idealized models used in security proofs. Indeed, by exploiting security loopholes in practical realizations, especially imperfections in the detectors, different attacks have been successfully launched against commercial QKD systems [4,5], thus highlighting their practical vulnerabilities.

To connect theory with practice again, several approaches have been proposed. The first one is the presumably hard-verifiable problem of trying to characterize real devices fully and account for all side channels. The second approach is a teleportation trick [2,6]. The third solution is (full) device independent QKD (DI-QKD) [8]. This last technique does not require detailed knowledge of how QKD devices work and can prove security based on the violation of a Bell inequality. Unfortunately, DI-QKD is highly impractical because it needs near unity detection efficiency together with a qubit amplifier or a quantum nondemolition (QND) measurement of the number of photons in a pulse, and even then generates an extremely low key rate (of order 10^{-10} bits per pulse) at practical distances [9].

In this Letter we present the idea of measurement-device-independent QKD (MDI-QKD) as a simple solution to remove all (existing and yet to be discovered) detector side channels [5], arguably the most critical part of the implementation, and show that it has both excellent security and performance. Therefore, it offers an immense security advantage over standard security proofs such as Inamori-Lütkenhaus-Mayers (ILM) [10] and Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [11]. Furthermore, it has the power to double the transmission distance that can be covered by those QKD schemes that use conventional laser diodes, and its key generation rate is comparable to that of standard security proofs with entangled pairs. In contrast to DI-QKD, in its simplest formulation MDI-QKD requires the additional assumption that Alice and Bob have almost perfect state preparation. However, we believe that this is only a minor drawback because Alice's and Bob's signal sources can be attenuated laser pulses prepared by themselves. Their states can thus be experimentally verified in a fully protected laboratory environment outside Eve's interference through random sampling. Moreover, as will be discussed later, imperfections in Alice's and Bob's preparation process can, in fact, be readily taken care of in a more refined formulation of the protocol.

A simple example of our method is as follows. Both Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in the four possible BB84 polarization states (i.e., vertical, horizontal, 45°, and 135° polarized states) [12] and send them to an *untrusted* relay Charlie (or Eve) located in the middle, who performs a Bell state measurement that projects the incoming signals into a Bell state [13]. Such measurement can be realized, for instance, using only linear optical elements with say the setup given in Fig. 1. (Actually, such setup only identifies two of the four Bell states. But, this is fine as any Bell state will allow a security proof to go through.) Furthermore,

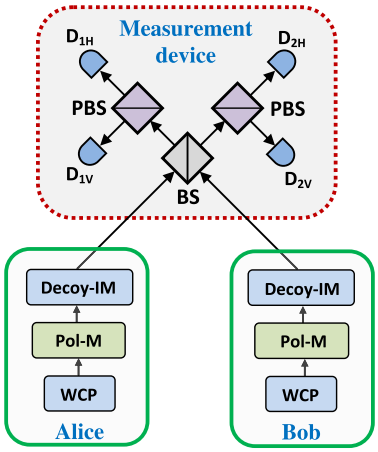

FIG. 1 (color online). Basic setup of a MDI-QKD protocol. Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in a different BB84 polarization state which is selected, independently and at random for each signal, by means of a polarization modulator (Pol-M). Decoy states are generated using an intensity modulator (Decoy-IM). Inside the measurement device, signals from Alice and Bob interfere at a 50:50 beam splitter (BS) that has on each end a polarizing beam splitter (PBS) projecting the input photons into either horizontal (H) or vertical (V) polarization states. Four single-photon detectors are employed to detect the photons and the detection results are publicly announced. A successful Bell state measurement corresponds to the observation of precisely two detectors (associated to orthogonal polarizations) being triggered. A click in D_{1H} and D_{2V}, or in D_{1V} and D_{2H}, indicates a projection into the Bell state $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$, while a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}, reveals a projection into the Bell state $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$. Alice's and Bob's laboratories are well shielded from the eavesdropper, while the measurement device can be untrusted.

Alice and Bob apply decoy-state techniques [14] to estimate the gain (i.e., the probability that the relay outputs a successful result) and quantum bit error rate (QBER) for various input photon numbers.

Once the quantum communication phase is completed, Charles uses a public channel to announce the events where he has obtained a successful outcome in the relay, including as well his measurement result. Alice and Bob keep the data that correspond to these instances and discard the rest. Moreover, as in BB84, they post-select the events where they use the same basis in their transmission by means of an authenticated public channel. Finally, to guarantee that their bit strings are correctly correlated, either Alice or Bob has to apply a bit flip to her or his data, except for the cases where both of them select the diagonal basis and Charles obtains a successful measurement outcome corresponding to a triplet state. This is illustrated in Table I.

Let us now evaluate the performance of the protocol above in detail. The proof of its unconditional security is shown in the supplemental material [15]. For simplicity, we consider a refined data analysis where Alice and Bob

TABLE I. Alice and Bob post-select the events where the relay outputs a successful result and they use the same basis in their transmission. Moreover, either Alice or Bob flips her or his bits except for the cases where both of them select the diagonal basis and the relay outputs a triplet.

Alice & Bob	Relay output $\|\psi^-\rangle$	Relay output $\|\psi^+\rangle$
Rectilinear basis	Bit flip	Bit flip
Diagonal basis	Bit flip	No bit flip

evaluate the data sent in two bases *separately* [16]. In particular, we use the rectilinear basis as the key generation basis, while the diagonal basis is used for testing only. A piece of notation: Let us denote by $Q^{n,m}_{\text{rect}}$, $Q^{n,m}_{\text{diag}}$, $e^{n,m}_{\text{rect}}$, and $e^{n,m}_{\text{diag}}$, the gain and QBER, respectively, of the signal states sent by Alice and Bob, where n and m denote the number of photons sent by the legitimate users, and rect or diag represents their basis choice.

(A) Rectilinear basis.—An error corresponds to a successful relay output when both Alice and Bob prepare the same polarization state (i.e., their results should be anticorrelated before they apply a bit flip). Assuming for the moment ideal optical elements and detectors, and no misalignment, we have that whenever Alice and Bob send, respectively, n and m photons prepared in the same polarization state the relay will never output a successful result. We obtain then that $e^{n,m}_{\text{rect}}$ is zero for all n, m. This means that no error correction is needed for the sifted key. This is remarkable because it implies that the usage of WCP sources (rather than single-photon sources) does not substantially lower the key generation rate of the QKD protocol (in the error correction part).

(B) Diagonal basis.—To work out the amount of privacy amplification needed we examine the diagonal basis. An error corresponds to a projection into the singlet state given that Alice and Bob prepared the same polarization state, or into the triplet state when they prepare orthogonal polarizations. Assuming again the ideal scenario discussed in the previous paragraph, we find that $e^{1,1}_{\text{diag}} = 0$. (This is because when two identical single-photons enter a 50:50 BS the Hong-Ou-Mandel (HOM) effect [17] ensures that both photons will always exit the BS *together* in the same output mode. Also, if the two photons are prepared in orthogonal polarizations and they exit the 50:50 BS in the same output arm, both photons will always reach the same detector within the relay.) The fact that $e^{1,1}_{\text{diag}}$ is zero is again remarkable as it means that the usage of WCP sources does not substantially lower the key generation rate (in also the privacy amplification part).

(C) Key generation rate.—In the ideal scenario described above the key generation rate will be simply given by $R = Q^{1,1}_{\text{rect}}$ in the asymptotic limit of an infinitely long key. On the other hand, if we take imperfections such as basis misalignment and dark counts into account, the key

generation rate in a realistic setup will be given by [11,16,18]

$$R = Q_{\mathrm{rect}}^{1,1}[1 - H(e_{\mathrm{diag}}^{1,1})] - Q_{\mathrm{rect}} f(E_{\mathrm{rect}}) H(E_{\mathrm{rect}}), \quad (1)$$

where Q_{rect} and E_{rect} denote, respectively, the gain and QBER in the rectilinear basis (i.e., $Q_{\mathrm{rect}} = \sum_{n,m} Q_{\mathrm{rect}}^{n,m}$, and $E_{\mathrm{rect}} = \sum_{n,m} Q_{\mathrm{rect}}^{n,m} e_{\mathrm{rect}}^{n,m} / Q_{\mathrm{rect}}$), $f(E_{\mathrm{rect}}) > 1$ is an inefficiency function for the error correction process, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

There are few loose ends that need to be tightened up. First, we have implicitly assumed that the decoy-state method can be used to estimate the gain $Q_{\mathrm{rect}}^{1,1}$ and the QBER $e_{\mathrm{diag}}^{1,1}$. Second, we need to evaluate the secret key rate given by Eq. (1) for a realistic setup. Let us tighten up these loose ends here. Indeed, it can be shown that the technique to estimate the relevant parameters in the key rate formula is equivalent to that used in standard decoy-state QKD systems (see supplemental material for details [15]). For simulation purposes, we consider inefficient and noisy threshold detectors and employ experimental parameters from [19] with the exception that [19] considered a free-space channel whereas here we consider a fiber-based channel with a loss of 0.2 dB/km. Moreover, for simplicity, we assume that all detectors are identical (i.e., they have the same dark count rate and detection efficiency), and their dark counts are, to a good approximation, independent of the incoming signals. Furthermore, we use an error correction protocol with inefficiency function $f(E_{\mathrm{rect}}) = 1.16$ [20]. The resulting lower bound on the secret key rate is illustrated in Fig. 2. Our calculations and simulation results demonstrate that the key rate is highly comparable to a security proof [21] for entanglement-based QKD protocols. Our scheme can tolerate a high optical loss of more than 40 dB (i.e., 200 km of optical fibers) when a relay is placed in the middle of Alice and Bob. That is, one can essentially double the transmission distance over a setup where the Bell measurement apparatus is on Alice's side or a setup using a standard decoy-state BB84 protocol [22].

To experimentally implement the MDI-QKD protocol proposed, there are a few practical issues that have to be addressed. Among them, the most important one is probably how to generate indistinguishable photons from two independent laser sources and observe stable HOM interference [17]. Note that the physics behind this protocol is based on the photon bunching effect of two indistinguishable photons at a 50:50 BS. We performed a simple proof of principle experiment to show that a high-visibility HOM interference between two independent off-the-shelf lasers is actually feasible (see details in supplemental material [15]). The results are shown in Fig. 3. The consistency between experimental and theoretical results confirms that a high-visibility HOM dip can be obtained even with two independent lasers.

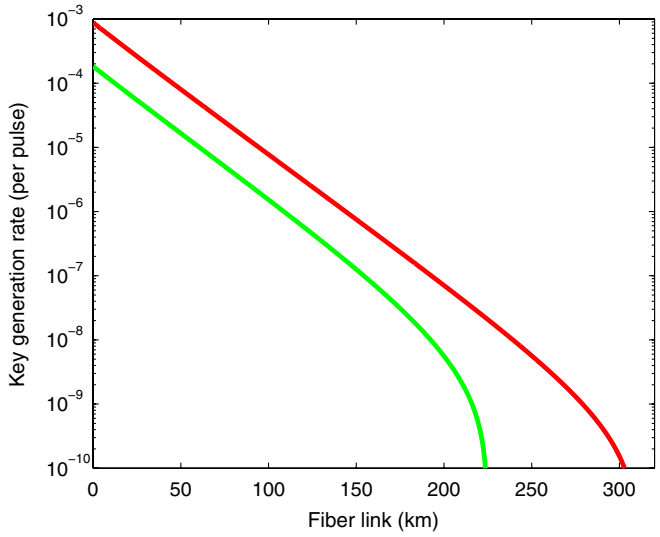

FIG. 2 (color online). Lower bound on the secret key rate R given by Eq. (1) in logarithmic scale for the MDI-QKD setup with WCPs illustrated in Fig. 1 (green curve). For simulation purposes, we consider the following experimental parameters [19]: the loss coefficient of the channel is 0.2 dB/km, the intrinsic error rate due to misalignment and instability of the optical system is 1.5%, the detection efficiency of the relay (i.e., the transmittance of its optical components together with the efficiency of its detectors) is 14.5%, and the background count rate is 6.02×10^{-6}. (For simplicity, we consider a simplified model of misalignment by putting a unitary rotation in one of the input arms of the 50:50 BS and also a unitary rotation in one of its output arms. The total misalignment value is 1.5%. That is, we assume a misalignment of 0.75% in each rotation.) In comparison, the red curve represents a lower bound on R for an entanglement-based QKD protocol with a parametric down conversion (PDC) source situated in the middle between Alice and Bob [21]. In the red curve, we have assumed that an optimal brightness of a PDC source is employed. However, in practice, the brightness of a PDC source is limited by technology. Therefore, the key rate of an entanglement-based QKD protocol will be much lower than what is shown in the red curve. This makes our new proposal even more favorable than the comparison that is presented in the current Figure.

The idea of MDI-QKD can be generalized much further. First of all, it also applies to the case where Alice and Bob use entangled photon pairs as sources. Second, it works even when Alice and Bob's preparation processes are imperfect. Indeed, basis dependence that originates from the imperfection in Alice and Bob's preparation processes can be readily taken care of by using a quantum coin idea [11,18] to quantify the amount of basis-dependent flaw [24]. Third, notice that in practical applications only a finite number of decoy states will be needed. This is similar to standard finite decoy state QKD protocols [25] that have been widely employed in experiments [26]. Fourth, MDI-QKD works even without a refined data analysis. Fifth, it works also for other QKD protocols including the six-state

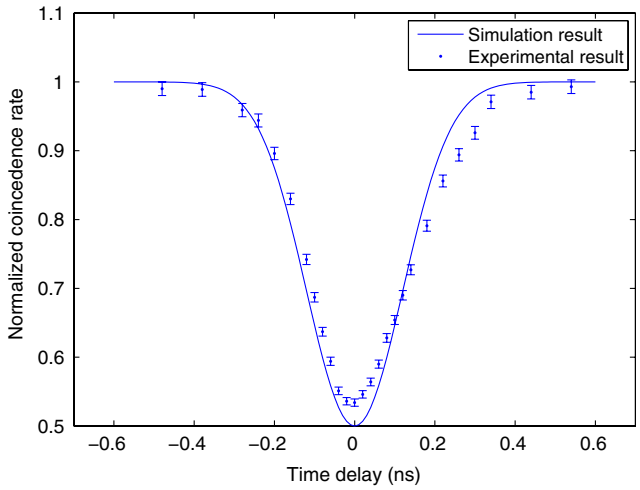

FIG. 3 (color online). Hong-Ou-Mandel interference between two phase randomized WCPs. The average photon number is 0.1 per pulse. The coincidence rate is recorded at different time delays. The error bars show the statistical fluctuation (± 1 standard deviation) due to finite data size.

protocol [27]. These subjects, together with the consideration of finite size effects that arise because Alice and Bob only send a finite number of signals in each run of a QKD protocol, will be discussed further in future publications; see, e.g., [24].

In summary, we have proposed the idea of measurement-device-independent QKD (MDI-QKD). Compared to standard security proofs, it has a key advantage of removing all detector side channels, and it can double the transmission distance covered with conventional QKD schemes using WCPs. Moreover, it has a rather high key generation rate which is comparable to that of standard security proofs. Indeed, its key generation rate is orders of magnitude higher than the previous approach of full device independent QKD. Our idea can be implemented with standard threshold detectors with low detection efficiency and highly lossy channels. In view of its excellent security, performance and simple implementation, we believe MDI-QKD is a big step forward in bridging the gap between the theory and practice of QKD, and we expect it to be widely employed in practical QKD systems in the future.

Useful conversations with C. H. Bennett, H. F. Chau, C.-H. F. Fung, P. Kwiat, X. Ma, K. Tamaki and Y. Zhao are gratefully acknowledged. We thank N. Lütkenhaus for discussions about Inamori's security proof, C. Weedbrook for comments on the presentation of the paper, and Z. Liao and Z. Tang for helping us in some parts of the experiment. We thank NSERC, the Canada Research Chair Program, QuantumWorks, CIFAR and Xunta de Galicia for financial support.

Note added.—After the posting of our paper on public preprint servers, another paper by Braunstein and Pirandola [28] was posted on the preprint servers [29].

[1] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); D. Mayers, J. ACM **48**, 351 (2001).
[4] C.-H. F. Fung *et al.*, Phys. Rev. A **75**, 032314 (2007); F. Xu, B. Qi and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[5] B. Qi *et al.*, Quantum Inf. Comput. **7**, 73 (2007); Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008); L. Lydersen *et al.*, Nature Photon. **4**, 686 (2010); I. Gerhardt *et al.*, Nature Commun. **2**, 349 (2011).
[6] Instead of receiving quantum signals from Alice through a quantum channel directly, Bob teleports any incoming signal from outside to himself. Provided that Bob has perfect control on the state preparation, he can remove all side-channels through teleportation. See Note 21 of [2] for details. While this proposal is technologically feasible, a high-performance implementation of teleportation is not without its own challenges [7].
[7] D. Bouwmeester *et al.*, Nature (London) **390**, 575 (1997).
[8] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (IEEE Computer Society, Washington, DC, 1998), p. 503; A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
[9] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010); M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).
[10] H. Inamori, N. Lütkenhaus and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[11] D. Gottesman *et al.*, Quantum Inf. Comput. **5**, 325 (2004).
[12] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, Bangalore, India New York, 1984), p. 175.
[13] Note that a key advantage of our work is that Charles' detection system can be arbitrarily flawed without compromising security.
[14] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[15] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.108.130503 for details.
[16] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
[17] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[18] M. Koashi, arXiv:quant-ph/0505108.
[19] R. Ursin *et al.*, Nature Phys. **3**, 481 (2007).
[20] In practice, the effect of the inefficiency function $f(E_{\mathrm{rect}})$ on the key rate is very small. Notice that the value $f(E_{\mathrm{rect}}) = 1.16$ that we use here is rather conservative. One can achieve better results with, for instance, good error correcting codes. For a given distance, we optimize the intensity of Alice's and Bob's lasers numerically to maximize the key rate. As expected, such intensities are on the order of 1.
[21] X. Ma, C.-H. F. Fung and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
[22] The dark count rate affects in a significant way the cutoff point. For instance, if we assume detectors with

slightly lower dark count rate like the ones by Gobby *et al.* [23] [with dark count rate equal to 3.2×10^{-7} and a detection efficiency of 12% (lower than before)], we find that the cutoff point is more than 300 km. Our work shows clearly that it is feasible for QKD with WCPs to achieve similar long-distance transmission to what was previously thought [21] to be possible with only entangled states. Furthermore, in contrast to both the protocol of [21] and a standard decoy-state BB84 protocol [14], our new scheme has a tremendous advantage of being immune to all detector side channel attacks.

[23] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[24] K. Tamaki *et al.*, arXiv:1111.3413.

[25] X. Ma *et al.*, Phys. Rev. A **72**, 012326 (2005); X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[26] D. Rosenberg *et al.*, New J. Phys. **11**, 045009 (2009).

[27] C. H. Bennett *et al.*, IBM Technical Disclosure Bulletin **26**, 4363 (1984); D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[28] S. L. Braunstein and S. Pirandola, preceding article, Phys. Rev. Lett. **108**, 130502 (2012).

[29] Unlike our Letter, [28] does not consider decoy state or weak coherent pulses. So, it is unclear what key rate it will give. Moreover, the relationship between [28] and previous works by Biham [30] and by Inamori [31] remains to be carefully discussed.

[30] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[31] H. Inamori, Algorithmica **34**, 340 (2002).