Quantum key distribution with untrusted detectors

P. González,[1,2,3] L. Rebón,[4,5] T. Ferreira da Silva,[6] M. Figueroa,[2,7] C. Saavedra,[1,2] M. Curty,[8] G. Lima,[1,2,3]
G. B. Xavier,[2,3,7] and W. A. T. Nogueira[2,3,9]

[1]*Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile*
[2]*Center for Optics and Photonics, Universidad de Concepción, Casilla 4016, Concepción, Chile*
[3]*MSI-Nucleus for Advanced Optics, Universidad de Concepción, Concepción, Chile*
[4]*Instituto de Física de La Plata, Universidad Nacional de La Plata, La Plata, Argentina*
[5]*Laboratorio de Procesado de Imágenes, Departamento de Física, Universidad de Buenos Aires, Buenos Aires, Argentina*
[6]*Optical Metrology Division, National Institute of Metrology, Quality and Technology, 25250-020 Duque de Caxias, RJ, Brazil*
[7]*Departamento de Ingeniería Eléctrica, Universidad de Concepción, 160-C Concepción, Chile*
[8]*EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain*
[9]*Departamento de Física, ICE, Universidade Federal de Juiz de Fora, Juiz de Fora, CEP 36036-330, Brazil*

(Received 16 May 2013; revised manuscript received 14 October 2014; published 18 August 2015)

Side-channel attacks currently constitute the main challenge for quantum key distribution (QKD) to bridge theory with practice. So far two main approaches have been introduced to address this problem, (full) device-independent QKD and measurement-device-independent QKD. Here we present a third solution that might exceed the performance and practicality of the previous two in circumventing detector side-channel attacks, which arguably is the most hazardous part of QKD implementations. Our proposal has, however, one main requirement: the legitimate users of the system need to ensure that their labs do not leak any unwanted information to the outside. The security in the low-loss regime is guaranteed, while in the high-loss regime we already prove its robustness against some eavesdropping strategies.

DOI: 10.1103/PhysRevA.92.022337 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Today quantum key distribution (QKD) [1–3] faces the challenge of bridging the large gap between theory and practice. Theoretically, QKD offers perfectly secure communications based on the laws of physics. In practice, however, it does not because most physical devices do not operate as it is presumed in the security proofs. As a result, current QKD implementations suffer from security loopholes that allow for side-channel attacks [4–14].

To avoid these loopholes and recover the security of QKD realizations there are currently two main approaches where assumptions on the internal functioning of the measurement devices are avoided. The first one is called (full) device-independent QKD (diQKD) [15–19]. Here, the legitimate users of the system (Alice and Bob) treat their apparatuses as two black boxes. Given that certain conditions are satisfied, it is possible to prove the security of diQKD based solely on the violation of a Bell inequality. Importantly, this solution can remove all side channels from the quantum part of a QKD implementation. Its main drawback, however, is that it requires a loophole-free Bell test [20–25] with distant communicating parties, which is yet to be achieved. Also, its expected secret key rate with current technology is very low at practical distances [26,27].

The second approach is called measurement-device-independent QKD (mdiQKD) [28]. In contrast to diQKD, Alice and Bob need to know their state preparation processes but they can treat the measurement device as a black box fully controlled by the eavesdropper (Eve). This solution eliminates all side channels from the measurement unit, which can be regarded as the weakest part of a QKD implementation [4–10], and guarantees a very high performance. Indeed, mdiQKD tolerates a high optical loss of more than 40 dB and it can give a secret key rate similar to that of standard entanglement-based QKD protocols [29]. Moreover, its feasibility has already been proven both in laboratories and via field tests [30–35]. This suggests the viability of mdiQKD to connect theory and practice in QKD. This approach has, however, two slight drawbacks. First, mdiQKD requires high-visibility two-photon interference using two different light sources, which makes its experimental implementation more demanding than that of conventional QKD systems. Second, the current finite-key security bounds [36] require relatively large postprocessing data block sizes to achieve good performance.

Here we propose an alternative solution to remove detector side channels in QKD realizations. It follows a similar spirit to that of mdiQKD. That is, Alice and Bob need to characterize their state preparation processes but do not have to trust the measurement device, which is treated as a black box. Note, however, that the concept of a black box is now different from that of mdiQKD. In particular, we require that Alice and Bob know the optical elements contained in the box, but no knowledge is required on the way they work or on which quantum system they operate [39]. This is to prevent attacks that exploit the fact that Eve can build the measurement unit herself and she includes additional elements that leak key information to the channel [37,38]. Indeed, our proposal requires that Alice and Bob guarantee that the measurement system does not leak any unwanted information to the outside (just like in diQKD). This could be achieved, in principle, by placing the measurement apparatus within Bob's laboratory, and with a measurement device built by them, albeit not necessarily characterized [37]. This condition can be checked or fulfilled in most practical scenarios. In this case, the only

relevant information to prove security is the statistics of the input and output data from the box.

In doing so, as will be explained below, it is possible to avoid the problem of interfering photons from independent sources, which considerably simplifies its experimental implementation when compared to mdiQKD. In the low-loss regime, the security of our approach is guaranteed by the results in Ref. [40]. Here we also conjectured its security in the high-loss regime by analyzing a particular class of attacks. In parallel to this work, further developments towards more general security proofs of single-photon two-qubit device-independent QKD [37,41] have been carried out, together with other experimental implementations [42–44].

II. DESCRIPTION OF THE PROTOCOL

The key idea of our protocol is illustrated in Fig. 1. For comparison, this figure also includes a schematic diagram of mdiQKD [28]. Alice uses a transmitter to prepare different quantum states that she sends to Bob. On the receiving side, Bob uses a linear optics network (LON) to manipulate the state of the incoming signals. Alice's transmitter and Bob's LON are both trusted and characterized. When compared to mdiQKD, this LON can be regarded as Bob's trusted transmitter, although it does not include any light source. Afterwards, Bob is supposed to implement a Bell state measurement (BSM), which is considered to be a black box.

One requirement for the measurement device, as mentioned above, is that no unwanted information leaks from the BSM. In practice, a simple way to achieve this is to place the measurement device within Bob's shielded laboratory, and that Bob builds the BSM himself, such that he can assure

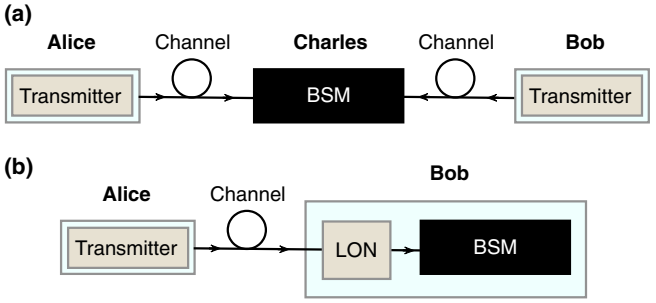

FIG. 1. (Color online) (a) Schematic diagram of measurement-device-independent QKD (mdiQKD) [28]. Alice and Bob prepare different quantum states and send them to an untrusted relay Charles, which can be treated as a black box fully controlled by Eve. Charles is supposed to implement a Bell state measurement (BSM) that projects the incoming signals into a Bell state. (b) Schematic diagram of our proposal. Alice generates different quantum states and sends them to Bob. On receiving the signals, Bob encodes his information by means of a trusted linear optics network (LON), which can be regarded as Bob's transmitter (when compared to mdiQKD). This LON does not include any light source but it simply manipulates the state of the incoming signals. Afterwards, Bob implements a BSM, which is treated as a black box. In the figure: (brown box) characterized device; (black box) uncharacterized device; and (light turquoise box) secure laboratory, i.e., the laboratory does not leak any unwanted information to the outside.

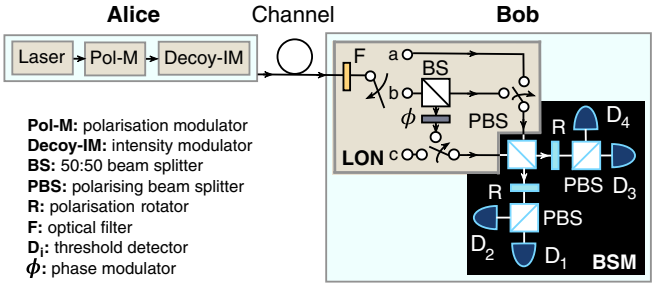

FIG. 2. (Color online) Schematic diagram of an example of a possible implementation of our method. Alice generates phase-randomized weak coherent pulses (WCPs) in different BB84 polarization states [48], and sends them to Bob. In addition, she prepares decoy-states [45–47] using an intensity modulator (Decoy-IM). Bob employs a trusted LON to encode his information on the incoming signals by using their path degree of freedom. For this, he uses an optical switch that sends the arriving states through one out of three possible optical paths of the same length (paths a, b, and c in the figure). Two additional optical switches are used to guarantee that the selected path is actually connected to the polarizing beam splitter (PBS). The switches are represented in the figure with the standard drawing of arrows and white connectors. The phase modulator ϕ shifts the phase of each pulse by 0 or π. Bob measures the outcoming pulses from the LON with a linear-optics single-photon BSM [50]. A successful BSM result is obtained when only one detector D_i clicks. The polarization rotator R changes the horizontal (vertical) polarization to a 45° (−45°) linear polarization. As in Fig. 1: (brown box) characterized device; (black box) uncharacterized device; and (light turquoise box) secure laboratory.

that it does not contain any eavesdropping device prepared by Eve [37]. This is indeed the expected situation in most realistic scenarios. Even though Bob builds the BSM, he does not need to characterize the exact functioning of the optical elements within the BSM (e.g., polarization rotators, beam splitters, single-photon detectors, etc.). That is, in the security analysis one can treat the whole BSM as a black box, where the only relevant information is the input and output data of the box.

Let us describe our quantum key distribution protocol by using a particular example of a possible implementation. This setup is schematically shown in Fig. 2. The protocol can be summarized with the following three steps.

Step 1. Alice sends Bob phase-randomized weak coherent pulses (WCPs), together with decoy signals [45–47], prepared in different BB84 polarization states [48]. For each signal, these states are selected independently and at random from two mutually unbiased bases, e.g., either a rectilinear (H [horizontal] or V [vertical]) or a diagonal (45° or −45°) polarization basis.

Step 2. On receiving the transmission, Bob employs a LON to encode his information on the incoming pulses using their path degree of freedom. For this, he utilizes an optical switch that distributes the arriving signals into one out of three possible optical paths (a, b, and c in Fig. 2), which he selects independently and at random for each pulse. In analogy to Alice, we shall denote the paths a and c in Fig. 2 as Bob's rectilinear bases, and the path b (with $\phi = 0$ or $\phi = \pi$) as Bob's diagonal bases. Moreover, we will consider that Bob's bit value associated to selecting the path a (c) is equal to

TABLE I. To guarantee that their bit strings are correctly correlated, either Alice or Bob applies a bit flip to part of her or his data, depending on which detector D_i clicked (which identifies the Bell state obtained by the BSM) and the basis setting selected. Detections at D_1, D_2, D_3, and D_4 correspond to the Bell state projections $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, and $|\psi^-\rangle$, where the Bell states are written in terms of the hybrid polarization-path encoding [49,50].

	Clicking detector			
Alice & Bob	D_1	D_2	D_3	D_4
Rectilinear basis	-	-	Bit flip	Bit flip
Diagonal basis	-	Bit flip	-	Bit flip

that of Alice when she chooses H (V) polarization, and that Bob's bit value associated to selecting the path b with $\phi = 0$ ($\phi = \pi$) is equal to that of Alice when she employs 45° (-45°) polarization. If we compare this procedure to that of mdiQKD, one could say that to select path a (c) in our proposal is somehow equivalent to Bob preparing a H (V) polarization signal in mdiQKD, and similarly for the diagonal basis. Once Bob has encoded his information, the signals are recombined at a polarizing beam splitter (PBS) and then measured with a linear-optics single-photon BSM [49,50]. A successful BSM result corresponds to observing a click in only one detector D_i, with $i \in \{1, \ldots, 4\}$. If two or more detectors click simultaneously, the event is considered unsuccessful.

Step 3. Alice and Bob employ an authenticated classical channel to announce their results. In particular, Bob declares which pulses produced a successful BSM result together with the Bell state obtained. Also, Alice and Bob broadcast the polarization and path basis that they have used to generate and measure each successful signal respectively. They keep the data associated with those successful events where they used the same basis and discard the rest. In addition, they use the decoy-state method [45–47] to estimate the yield (i.e., the probability that Bob obtains a successful BSM result) and the quantum bit error rate (QBER) for various n-photon states. Like in mdiQKD, the key point is that with this information Alice and Bob can determine whether or not the BSM is working well enough to be able to distill a secret key. If this is the case, either Alice or Bob applies a bit flip to part of her or his data to assure that their bit strings are correctly correlated (see Table I). They then finally perform error-correction and privacy amplification procedures to obtain a final secret key.

Let us emphasise that the method described above could be applied as well to other QKD protocols like, for instance, the three-state scheme [51,52]. Also, it could be adapted to other encoding strategies (e.g., phase encoding or time-bin encoding). In addition, let us point out that the use of optical switches (within Bob's LON) is not essential; indeed, it is possible to design alternative receivers without these elements.

III. SECURITY ASSUMPTIONS

Before we analyze the security of the protocol, let us begin by stating the security assumptions. In particular, we assume that Alice and Bob have access to (i) true random number generators, (ii) trusted classical postprocessing techniques, (iii) an authenticated classical channel, (iv) Alice's source and Bob's LON are fully characterized and cannot be influenced by Eve, and (v) Alice's and Bob's labs do not leak any unwanted information to the outside.

The first three assumptions are also required in conventional QKD systems. The fourth one needs special attention. In principle, it is reasonable to expect that Alice can verify the states she sends to Bob in a fully protected environment outside Eve's control. For this, she could protect herself with different optical elements such as, for instance, optical isolators, optical filters, and a monitoring detector; also, she could use random sampling techniques. This is precisely the scenario we face in mdiQKD. The case of Bob, however, is more delicate. This is so because he actually receives signals from the quantum channel. Eve may try to perform, for example, a so-called Trojan horse attack [53,54]. That is, she could launch bright light pulses into Bob's LON and then analyze the back-reflected light. In doing so, Eve could try to determine Bob's bit value (i.e., the position of his optical switch in the example above) for each arriving signal. In practice, however, these types of attacks (or similar ones) might be avoided as well by including additional components on Bob's side, just like in the case of Alice. For example, Bob could insert several optical circulators to attenuate the back-reflected light together with optical filters to remove undesired modes and a monitoring detector to test the incoming and/or reflected light. Further details on possible countermeasures against Trojan horse attacks can be found in Refs. [53,54].

Alternatively, Eve could also try to manipulate the correct operation of Bob's LON by shifting, for instance, the frequency or the arrival time of the incoming pulses. This way she might influence the functioning of both the beam splitter and the phase modulator within the LON. Again, however, in practice one expects that Bob could avoid such types of attacks by using, for example, optical filters together with a time-dependent attenuator. This attenuator could restrict the arrival time of the signals to only a certain time window where the devices work as predicted by the mathematical models used to prove security. In the example given by Fig. 2 the role of such attenuator is performed by the optical switch. Furthermore, note that Bob could even remove the phase modulator within his LON. If Alice sends him only three different states, it can be shown that this scenario (i.e., without phase modulator on Bob's side) would be completely equivalent to that of the three-state protocol [51,52]. According to the results in Ref. [52] the expected performance in this case would be basically the same as that of the original situation where Alice and Bob use four different states.

To conclude this part, let us discuss the fifth assumption considered. Note that this assumption is also required both in diQKD [38] and mdiQKD. The only difference is that in mdiQKD this condition does not affect the measurement unit, which can be located outside Alice's and Bob's secure labs. In our proposal, however, Bob's state preparation process is performed by his LON, which is situated between the channel and the BSM. Therefore, if we treat the BSM as a black box under Eve's control and, moreover, this box can send any information that Eve wishes to the outside, Eve might try to learn the whole key without introducing any errors, as discussed in Ref. [37]. For this reason, it is essential that Bob

can guarantee the requirement that the BSM does not leak unwanted information to the outside.

IV. SECURITY ANALYSIS

We now evaluate the security of the protocol. From the results in Ref. [40] we have that our scheme is secure against general attacks in the low-loss regime (i.e., when the overall transmittance of the single-photon pulses sent by Alice is greater or equal to 65.9%) given that Bob's measurement device is memoryless. This is so because the work in Ref. [40] contains our proposal as a special case; more precisely, its security analysis considers the worst-case scenario where Bob's device is untrusted. For this reason, such result, although it guarantees security when the loss is low, might be overly pessimistic since here we assume that part of Bob's apparatus (i.e., his LON) can be actually trusted.

Below we conjecture the security of our scheme also in the practical and relevant scenario of high losses. For this, we prove its security against a certain class of attacks. In particular, we assume that Eve can block or correlate the single-photon pulses sent by Alice with an ancilla system in her hands, but she cannot add additional photons to these pulses. That is, whenever Alice emits a single-photon signal Bob receives either vacuum or a single-photon. In addition, we permit that Eve can decide the output of the BSM for each pulse sent by Alice. A full security proof against general attacks in the high-loss regime is left for future analysis. Note that recently a similar mathematical proof to the one presented here, with an equivalent level of security, was given in Ref. [42].

We use similar arguments to those employed in mdiQKD [28], which relies on the security of a time-reversed EPR-based QKD protocol [19,55,56]. Indeed, it can be shown that the protocol illustrated in Fig. 2, when viewed in the reverse order, is equivalent to a counterfactual entanglement-based BB84 protocol [57]. That is, whenever Bob observes a single click in a detector D_i in our protocol, this corresponds to the situation where Eve distributes a certain Bell state $|\phi_i\rangle$ in the counterfactual protocol.

To see this, we focus on the single-photon states sent by Alice. In an equivalent virtual protocol, her signal state preparation can be thought of as follows. Alice prepares an entangled bipartite state of the form $|\Psi\rangle_{AA'} = \sum_i \sqrt{p_i}|a_i\rangle_A|\psi_i\rangle_{A'}$. If she measures the virtual system A in the orthonormal basis $|a_i\rangle_A$, she effectively prepares the BB84 states $|\psi_i\rangle_{A'}$ with probability p_i. Moreover, she can also incorporate in her virtual measurement the information about the reduced density matrix of system A, i.e., $\rho_A = \mathrm{Tr}_{A'}(|\Psi\rangle_{AA'}\langle\Psi|)$, which is known and fixed by the state preparation process [58,59].

The case of Bob is more subtle. In a virtual protocol, he first prepares the virtual state $|\Phi\rangle_B = \sum_i \sqrt{p_i}|b_i\rangle_B$, with $|b_i\rangle_B$ being an orthonormal basis for system B. Then, whenever he receives a single-photon signal $\sigma_{A'}$ from the channel, which might have been manipulated by Eve, he applies a controlled unitary operation $U_{BA'} = \sum_i |b_i\rangle\langle b_i|_B \otimes U_{i,A'}$ on systems B and A', where the unitary operators $U_{i,A'}$ are fixed by his state preparation process (i.e., by the action of his LON). That is, each operator $U_{i,A'}$ corresponds to one particular setting of his optical switch and phase modulator. Now, the key point is that it can be shown (see the Appendix) that after applying $U_{BA'}$ the reduced density matrix of system B, that we denote as ρ_B, is fixed and equal to ρ_A independently of the incoming single-photon state $\sigma_{A'}$. That is, Bob's virtual system B is in the same state as if he would have followed the same state preparation process as Alice to generate BB84 signals. Now, the scenario is precisely the same as that of mdiQKD. That is, in the virtual picture Alice and Bob could in principle keep their systems A and B in a quantum memory and delay their measurements on them until the BSM is completed. In such virtual scenario the protocol is then directly equivalent to an entanglement-based BB84 scheme [29,57].

As a result, we have that the asymptotic secret key rate formula has the form $R \geqslant \sum_i \max\{R_i,0\}$, with R_i denoting the key rate associated with those events where Bob observes a click only in detector D_i. This parameter is given by [60–62]

$$R_i \geqslant q\{p_0 Y_{i,0} + p_1 Y_{i,1}[1 - h(e_{i,1})] - Q_i f(E_i) h(E_i)\}. \quad (1)$$

Here, the coefficient q denotes the efficiency of the protocol (i.e., $q = 1/2$ for the standard BB84 protocol [48] and $q \approx 1$ for its efficient version [63]); $p_n = \exp(-\mu)\mu^n/n!$ is the probability that Alice sends Bob a signal, which contains n photons, with μ being the average photon number of the signals; $Y_{i,n}$ denotes the conditional probability that Bob only observes a click in detector D_i given that Alice sent him an n-photon state; the parameter $e_{i,n}$ represents the QBER of those n-photon signals which only produce a click in detector D_i; $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denotes the binary Shannon entropy function; the term Q_i represents the probability that Bob only obtains a click in detector D_i when Alice sends him a signal state, i.e., $Q_i = \sum_n p_n Y_{i,n}$; the parameter E_i is the overall QBER associated with a detection in D_i, i.e., $E_i = \sum_n p_n Y_{i,n} e_{i,n}/Q_i$; and $f(x)$ is an inefficiency function for the error correction process in the protocol [typically $f(E_i) \geqslant 1$; with the Shannon limit $f(E_i) = 1$].

Equation (1) contains three parameters, which are not directly observed in the experiment: $Y_{i,0}$, $Y_{i,1}$, and $e_{i,1}$. To estimate these quantities we use the decoy-state method [45–47]. Here, for simplicity, we consider that Alice employs an infinite number of decoy settings and, therefore, Alice and Bob are able to obtain the precise values of these parameters. In the practical scenario where Alice and Bob only use a finite number of decoy settings one can solve such estimation problem either by using linear programming tools, or by employing, for instance, the analytical procedure reported in Ref. [64].

As a final remark, let us emphasize once again that in the scenario where Eve can replace the single photons with multiphoton or strong pulses, the security of our scheme is not yet clear. However, one possible solution might be to ensure that the overall detection efficiency of all outputs of the measurement device are the same [37,65]. This could be verified through the input/output statistics, and finely tuned by Bob through optical attenuators in each output. Another alternative solution might be to follow the ideas introduced in Ref. [42] and assume that the linear optical elements within the BSM are also trusted (i.e., to consider that the only untrusted components within Bob are the detectors). Both approaches, nevertheless, require further investigations.

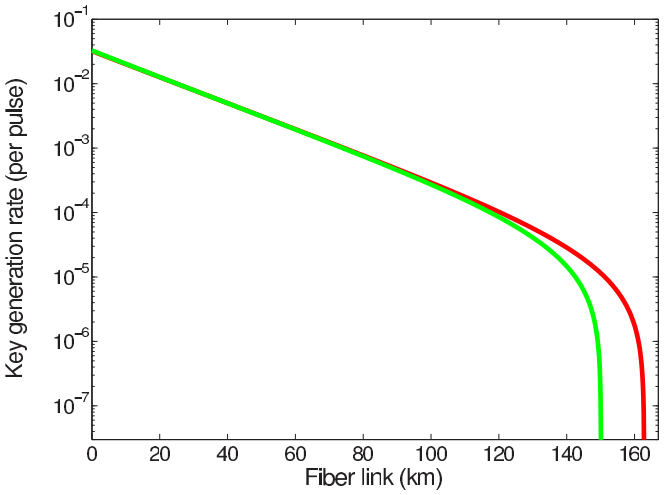

FIG. 3. (Color online) Lower bound on the secret key rate R given by Eq. (1) in logarithmic scale for the setup illustrated in Fig. 2 with WCPs (green curve). For simulation purposes, we use experimental parameters from Ref. [66]: the loss coefficient of the quantum channel is 0.2 dB/km, the intrinsic error rate due to misalignment and instability of the optical system is 1.5%, the overall detection efficiency of the detectors D_i is 14.5%, and the background count rate is 6.02×10^{-6}. Furthermore, we consider that the parameter $q \approx 1$ [63] and the efficiency of the error correction protocol satisfies $f(E_i) = 1.16$. For comparison, this figure also includes a lower bound on the secret key rate for a standard decoy-state BB84 system with an infinite number of decoy settings and an active measurement setup (red curve) [45–47].

V. SIMULATION

For simulation purposes we consider inefficient and noisy threshold detectors D_i, and we use experimental parameters from Ref. [66]. In addition, for simplicity, we assume that all detectors are identical and their dark counts are, to a good approximation, independent of the incoming signals. Moreover, we use a channel model that includes an intrinsic error rate of 1.5%, simulating the misalignment and instability of the optical system.

The resulting lower bound on the secret key rate R given by Eq. (1) is illustrated in Fig. 3. For a given total system loss, i.e., including the losses in the channel and in Bob's detection apparatus, we optimize the lower bound on R over the average photon number μ of Alice's signal states, which is around 0.7 for most of the distances. For comparison, this figure also includes a lower bound on the secret key rate for an asymptotic decoy-state BB84 system with an infinite number of decoy settings and an active receiver with two detectors [45–47]. We consider the BB84 scheme with two detectors as a comparison because this is a standard configuration for this protocol, whereas in our new proposal four detectors are required to maximise its key rate. As a result, we find that both secret key rates are very similar. Only the cut-off point of the standard decoy-state BB84 scheme (163 km) is slightly larger than that of the protocol illustrated in Fig. 2 (150 km). This is because in the case of the standard decoy-state BB84 system Bob's measurement device has a lower overall dark count rate than that of our proposal, since it only contains two detectors instead of four. Most importantly, our scheme illustrated in Fig. 2 delivers a secret key rate, which is approximately two orders of magnitude higher than that of mdiQKD (please see

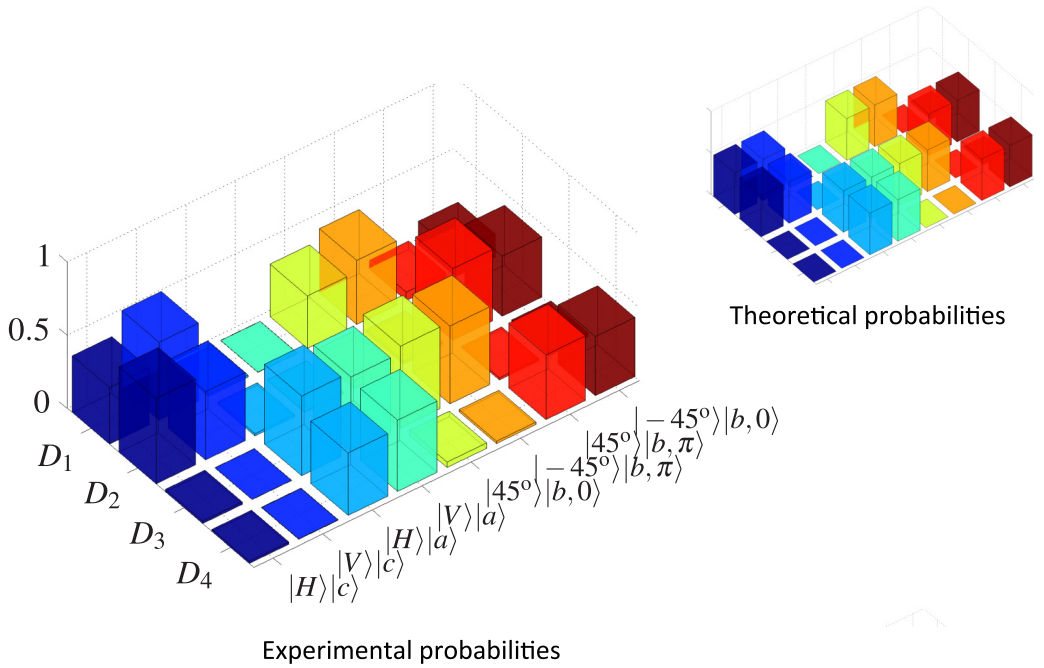

FIG. 4. (Color online) Experimental and theoretical (inset) probabilities to obtain a click in detector D_i for all possible combinations of states when both Alice and Bob use compatible bases. See Table II for further details. The states $|a\rangle$ and $|c\rangle$ in the figure denote the paths a and c, respectively, while $|b,0\rangle$ and $|b,\pi\rangle$ represent path b with $\phi = 0$ and $\phi = \pi$, respectively.

TABLE II. Detection probabilities for the eight possibilities when Alice and Bob use compatible bases.

	Detection probabilities			
State	D_1	D_2	D_3	D_4
$\|H\rangle\|c\rangle$	0.3863 ± 0.0007	0.5823 ± 0.0010	0.0168 ± 0.0001	0.0146 ± 0.0001
$\|V\rangle\|c\rangle$	0.5316 ± 0.0008	0.4652 ± 0.0007	0.0010 ± 0.000 02	0.0022 ± 0.000 03
$\|H\rangle\|a\rangle$	0.0152 ± 0.0001	0.0153 ± 0.0001	0.5432 ± 0.0009	0.4263 ± 0.0007
$\|V\rangle\|a\rangle$	0.0010 ± 0.000 02	0.0020 ± 0.000 04	0.5101 ± 0.0008	0.4862 ± 0.0008
$\|45°\rangle\|b,0\rangle$	0.3574 ± 0.0005	0.0488 ± 0.0001	0.5569 ± 0.0007	0.0369 ± 0.0001
$\|-45°\rangle\|b,\pi\rangle$	0.4357 ± 0.0005	0.0175 ± 0.000 08	0.5309 ± 0.0007	0.0158 ± 0.000 07
$\|45°\rangle\|b,\pi\rangle$	0.0569 ± 0.0001	0.4871 ± 0.0006	0.0144 ± 0.000 06	0.4417 ± 0.000 01
$\|-45°\rangle\|b,0\rangle$	0.1591 ± 0.0002	0.4091 ± 0.0005	0.0285 ± 0.000 009	0.4033 ± 0.000 05

Fig. 2 in Ref. [28]) for the experimental parameters considered, although now the covered distance is shorter.

VI. PROOF-OF-PRINCIPLE EXPERIMENT

For the sake of completeness, we performed a proof-of-principle experiment to simply demonstrate that all the required states by the protocol can be successfully generated and detected. More specifically, a complete key exchange session with realistic security requirements (that is, random generation and measurement by Alice and Bob, decoy states, error correction, and privacy amplification) is outside the scope of the current work. Also, for simplicity, instead of using phase-randomized WCPs, the signal states emitted by Alice are generated with a continuous wave laser at 690 nm attenuated to the single photon level, calibrated to a detection window of 4 ns. Alice controls the polarization of these signals with a half-wave plate (HWP), and sends them to Bob through a free-space channel. Bob's measurement device is a slightly modified version of that illustrated in Fig. 2. In particular, the rectilinear path basis is defined by blocking one of the two possible paths of the interferometer, while the diagonal path basis follows the description of Fig. 2. This simpler configuration is equivalent to the one depicted in Fig. 2, but now the rectilinear basis suffers an additional 3 dB loss. Note, however, that one could remove this extra loss (introduced by the rectilinear path basis) if Alice and Bob resort to the diagonal and circular bases. In this case, Bob would always have the interferometer with both arms unblocked, and use four different phase settings, two for each basis.

As a phase modulator, we use a mirror mounted over a piezoelectric actuator in one of the paths of the interferometer. No active stabilization of the interferometer was needed for the timescale involved in the experimental measurements, which were taken with an integration time of 1 s per data point. In order to implement the BSM we employ two HWPs set to 22.5° as rotators R. The detectors D_i are commercial pigtailed single-photon detectors based on Si avalanche photodiodes, operating in free-running mode. The overall raw visibility of the interference curves was $88.4 \pm 0.2\%$.

We experimentally measured all possible combinations of states used for the BB84 protocol when both Alice and Bob simultaneously choose the rectilinear or diagonal bases. The single counts are recorded simultaneously on all four detectors using independent counting circuits programmed on FPGA-based electronics. The results are shown in Fig. 4 (see also Table II). They are in good agreement with the theoretical predictions. From the measured visibility, the average projected QBER over all different states is $5.8 \pm 0.1\%$.

VII. CONCLUSIONS

We have presented an approach to the problem of detector side channels in practical QKD, which arguably constitutes the Achilles' heel of current experimental realizations. It builds on the approach known as measurement-device-independent QKD (mdiQKD) [28]. However, when compared to mdiQKD, it has two main potential advantages. First, it is simpler to implement experimentally since it does not require interference of independent laser sources, just like conventional QKD systems. This means, in particular, that no active tracking of the arrival times of independent photons nor frequency control of their sources are necessary. Also, it does not need coincidence detections, which is particularly important for setups with low overall detection efficiency. Second, although in this paper we have assumed for simplicity the asymptotic scenario where Alice sends Bob an infinite number of signals, one expects that the finite secret key rate of our approach will be much higher than that of mdiQKD as now only Alice needs to send decoy states. For the same reason, one also expects that the size of the postprocessing data blocks will be significantly smaller than those required in mdiQKD, which is essential in practice [67].

In this work, we already prove the security of our scheme against general attacks in the low-loss regime and against a particular class of attacks in the high-loss regime. Nevertheless, in order for it to be a plausible alternative to mdiQKD, it is crucial to demonstrate its security against general attacks also in the high-loss regime. This important open question is left for further studies.

ACKNOWLEDGMENTS

We would like to thank Koji Azuma, Hoi-Kwong Lo, Kiyoshi Tamaki, Bing Qi, and Zhen-Qiang Yin for very useful discussions. L.R. thanks the Center for Optics and Photonics (Universidad de Concepción) for hospitality and CONICET for financial support. This work was supported by the grants FONDEF Idea IT13I10017 CONICYT PFB08-024, Milenio P10-030-F, FONDECYT (Grants No. 11110115, No. 1150101, No. 1120067, and No. 1151278), and by the Galician

Regional Government (program "Ayudas para proyectos de investigación desarrollados por investigadores emergentes", and consolidation of Research Units: AtlantTIC), and the Spanish Government (project TEC2014-54898-R). In addition W.A.T.N. and P.G. thank CNPq (Brazil) and Conicyt (Chile), respectively, for financial support.

APPENDIX

Reduced density matrix ρ_B. Here we briefly show that after applying the controlled unitary operation $U_{BA'}$ the reduced density matrix ρ_B of Bob's virtual system is equal to that of Alice's virtual system.

For this, we first obtain an expression for the unitary operators $U_{i,A'}$, with $i \in \{1,\ldots,4\}$. As explained in the main text, here we will assume that system A' is a qubit. In particular, when Bob selects path a we have that

$$\begin{aligned} U_{1,A'}|1,0\rangle_{A'}|0,0\rangle_{\text{aux}} &= |1,0\rangle_{\text{inp}_1}|0,0\rangle_{\text{inp}_2}, \\ U_{1,A'}|0,1\rangle_{A'}|0,0\rangle_{\text{aux}} &= |0,1\rangle_{\text{inp}_1}|0,0\rangle_{\text{inp}_2}, \end{aligned} \tag{A1}$$

where the state $|1,0\rangle$ denotes one photon in horizontal polarization and $|0,1\rangle$ is one photon in vertical polarization. System aux represents the signal in the orthogonal path (i.e., in path c). The labels inp_1 and inp_2 denote, respectively, the signals in the two input ports of the BSM. That is, Eq. (A1) tells us that when the single-photon A' is prepared in horizontal (vertical) polarization, and Bob selects path a, then we have one photon in horizontal (vertical) polarization in the input port inp_1 of the BSM.

When Bob chooses path c we have that

$$\begin{aligned} U_{2,A'}|1,0\rangle_{A'}|0,0\rangle_{\text{aux}} &= |0,0\rangle_{\text{inp}_1}|1,0\rangle_{\text{inp}_2}, \\ U_{2,A'}|0,1\rangle_{A'}|0,0\rangle_{\text{aux}} &= |0,0\rangle_{\text{inp}_1}|0,1\rangle_{\text{inp}_2}, \end{aligned} \tag{A2}$$

where system aux denotes again the signal in the orthogonal path (i.e., in path a in this case). That is, when the single-photon A' is prepared in horizontal (vertical) polarization, and Bob selects path c, then we have one photon in horizontal (vertical) polarization in the input port inp_2.

Using the same procedure we obtain that $U_{3,A'}$, which corresponds to selecting path b and $\phi = 0$, and $U_{4,A'}$ (for path b and $\phi = \pi$) have the form

$$\begin{aligned} U_{3,A'}|1,0\rangle_{A'}|0,0\rangle_{\text{aux}} &= 1/\sqrt{2}[|1,0\rangle_{\text{inp}_1}|0,0\rangle_{\text{inp}_2} \\ &\quad +|0,0\rangle_{\text{inp}_1}|1,0\rangle_{\text{inp}_2}], \\ U_{3,A'}|0,1\rangle_{A'}|0,0\rangle_{\text{aux}} &= 1/\sqrt{2}[|0,1\rangle_{\text{inp}_1}|0,0\rangle_{\text{inp}_2} \\ &\quad +|0,0\rangle_{\text{inp}_1}|0,1\rangle_{\text{inp}_2}], \\ U_{4,A'}|1,0\rangle_{A'}|0,0\rangle_{\text{aux}} &= 1/\sqrt{2}[|1,0\rangle_{\text{inp}_1}|0,0\rangle_{\text{inp}_2} \\ &\quad -|0,0\rangle_{\text{inp}_1}|1,0\rangle_{\text{inp}_2}], \\ U_{4,A'}|0,1\rangle_{A'}|0,0\rangle_{\text{aux}} &= 1/\sqrt{2}[|0,1\rangle_{\text{inp}_1}|0,0\rangle_{\text{inp}_2} \\ &\quad -|0,0\rangle_{\text{inp}_1}|0,1\rangle_{\text{inp}_2}]. \end{aligned} \tag{A3}$$

System $\sigma_{A'}$ can always be written as $\sigma_{A'} = \sum_i q_i|\phi_i\rangle_{A'}\langle\phi_i|$ for certain pure states $|\phi_i\rangle_{A'}$. This means, in particular, that in order to prove that $\rho_B = \rho_A$ for any input state $\sigma_{A'}$ it is enough to show that this condition is satisfied for any signal $|\phi_i\rangle_{A'} = \alpha|1,0\rangle_{A'} + \beta|0,1\rangle_{A'}$. Let

$$\begin{aligned} |\phi\rangle_{B,\text{inp}_1,\text{inp}_2} &= U_{BA'}\sum_i \sqrt{p_i}|b_i\rangle_B|\phi_i\rangle_{A'}|0,0\rangle_{\text{aux}} \\ &= \sum_i \sqrt{p_i}|b_i\rangle_B U_{i,A'}|\phi_i\rangle_{A'}|0,0\rangle_{\text{aux}}. \end{aligned} \tag{A4}$$

Then, we have that $\rho_B = \text{Tr}_{\text{inp}_1,\text{inp}_2}(|\phi\rangle_{B,\text{inp}_1,\text{inp}_2}\langle\phi|)$. Finally, by combining the equations above now it is straightforward to show that, independently of the state $|\phi_i\rangle_{A'}$, indeed ρ_B is a density matrix of rank two equal to $\rho_A = \text{Tr}_{A'}(|\Psi\rangle_{AA'}\langle\Psi|)$ with $|\Psi\rangle_{AA'} = \sum_i \sqrt{p_i}|a_i\rangle_A|\psi_i\rangle_{A'}$ and where $|a_i\rangle_A$ in an orthonormal basis and $|\psi_i\rangle_{A'}$ denotes de BB84 single-photon states. We omit this step here for simplicity, but the calculations are direct. Using the same type of calculations it can also be shown that ρ_B is basis independent.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[3] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photon. **8**, 595 (2014).
[4] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).
[5] Y. Zhao, C.-Hang Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[6] H. Weier *et al.*, New J. Phys. **13**, 073024 (2011).
[7] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[8] M.-S. Jiang, S.-H. Sun, G.-Z. Tang, X.-C. Ma, C.-Y. Li, and L.-M. Liang, Phys. Rev. A **88**, 062335 (2013).
[9] L. Lydersen *et al.*, Nature Photon. **4**, 686 (2010).
[10] I. Gerhardt *et al.*, Nature Commun. **2**, 349 (2011).
[11] C.-Hang Fred Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[12] S. Nauerth *et al.*, New J. Phys. **11**, 065001 (2009).
[13] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[14] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).
[15] 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), pp. 503–509.
[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[17] B. W. Reichardt, F. Unger, and U. Vazirani, Nature (London) **496**, 456 (2013).
[18] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[19] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[20] J. S. Bell, Physics **1**, 195 (1964).
[21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[22] P. Pearle, Phys. Rev. D **2**, 1418 (1970).

[23] M. Giustina *et al.*, Nature (London) **497**, 227 (2013).
[24] B. G. Christensen *et al.*, Phys. Rev. Lett. **111**, 130406 (2013).
[25] A. Cuevas *et al.*, Nature Commun. **4**, 2871 (2013).
[26] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[27] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).
[28] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[29] X. Ma, C.-Hang Fred Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
[30] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[31] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).
[32] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
[33] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[34] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).
[35] Y.-L. Tang *et al.*, IEEE J. Sel. Topics Quantum Elect. **21**, 6600407 (2015).
[36] M. Curty *et al.*, Nature Commun. **5**, 4732 (2014).
[37] B. Qi, Phys. Rev. A **91**, 020303(R) (2015).
[38] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).
[39] Note, however, that this condition is not needed in mdiQKD where the measurement device can be even manufactured by Eve.
[40] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
[41] X. Ma, arXiv:1410.5260.
[42] C. C. W. Lim, B. Korzh, A. Martin, F. Bussiéres, R. Thew, and H. Zbinden, Appl. Phys. Lett. **105**, 221112 (2014).
[43] W.-F. Cao, Y.-Z. Zhen, Y.-L. Zheng, Z.-B. Chen, N.- L. Liu, K. Chen, and J.-W. Pan, arXiv:1410.2928.
[44] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **92**, 012319 (2015).
[45] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[46] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[47] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[48] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, Bangalore, India, 1984), p. 175.
[49] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).
[50] Y.-H. Kim, Phys. Rev. A **67**, 040301(R) (2003).
[51] Chi-Hang Fred Fung and H.-K. Lo, Phys. Rev. A **74**, 042342 (2006).
[52] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[53] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[54] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, IEEE J. Sel. Topics Quantum Elect. **21**, 6600710 (2015).
[55] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[56] H. Inamori, Algorithmica **34**, 340 (2002).
[57] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[58] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[59] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).
[60] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[61] M. Koashi, arXiv:quant-ph/0505108.
[62] H.-K. Lo, Quantum Inf. Comput. **5**, 413 (2005).
[63] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[64] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[65] T. Ferreira da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, IEEE J. Selected Topics Quant. Electron. **21**, 6600309 (2015).
[66] R. Ursin *et al.*, Nature Phys. **3**, 481 (2007).
[67] Charles Ci Wen Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).