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. We prove its security in the high-loss regime against a particular class of attacks, and we present a proof-of-principle experiment that demonstrates the feasibility of the protocol.

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 realisations there are currently two main approaches. The first one is called (full) device-independent QKD (diQKD) [15–18]. 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 [19–24] 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 [25, 26].

The second approach is called measurement-device-independent QKD (mdiQKD) [27]. 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 [28]. Moreover, its feasibility has already been proven both in laboratories and via field-tests [29–34]. 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 [35] require relatively large post-processing data block sizes (of the order of $10^{13}$ bits) to achieve good performance.

Here we propose an alternative solution to remove all detector side-channels in practical QKD realisations. It follows a similar spirit to that of mdiQKD. That is, Alice and Bob need to characterise their state preparation processes but do not have to trust the measurement device, which is treated as a “black box”. Our proposal includes, however, one additional assumption that is not required in mdiQKD. In particular, Alice and Bob need to 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 lab. 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. Also, since now only Alice sends decoy states to Bob, one expects that the post-processing data block sizes will be significantly smaller.
than those required in mdiQKD [36]. In the low-loss regime, the security of our approach is guaranteed by the results in [37]. Here we conjectured as well its security in the high-loss regime by analysing a particular class of attacks. However, a full security proof for this last scenario is left for further studies.

II. DESCRIPTION OF THE PROTOCOL

The key idea is illustrated in Fig. 1. For comparison, this figure includes as well a schematic diagram of mdiQKD [27]. The working-principle of our proposal is as follows. Alice uses a trusted transmitter to 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. Importantly, Alice and Bob can determine whether or not Charles is honest by comparing a randomly chosen portion of their data. (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 is supposed to implement a BSM, which is treated as a “black box”. Like in mdiQKD, Alice and Bob can determine whether or not the BSM is working correctly by comparing a randomly chosen subset of their data. In the figure: (brown box) characterised device; (black box) uncharacterised device; and (light turquoise box) secure lab, i.e., the lab does not leak any unwanted information to the outside.

FIG. 1: (a) Schematic diagram of measurement-device-independent QKD (mdiQKD) [27]. 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. Importantly, Alice and Bob can determine whether or not Charles is honest by comparing a randomly chosen portion of their data. (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 is supposed to implement a BSM, which is treated as a “black box”. Like in mdiQKD, Alice and Bob can determine whether or not the BSM is working correctly by comparing a randomly chosen subset of their data. In the figure: (brown box) characterised device; (black box) uncharacterised device; and (light turquoise box) secure lab.

II. DESCRIPTION OF THE PROTOCOL

The key idea is illustrated in Fig. 1. For comparison, this figure includes as well a schematic diagram of mdiQKD [27]. The working-principle of our proposal is as follows. Alice uses a trusted transmitter to prepare different quantum states and send them to Bob. On the receiving side, Bob uses a trusted linear optics network (LON) to manipulate the state of the incoming signals. 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 can be treated as a “black box”. That is, Alice and Bob do not need to know how the BSM functions, but they can determine whether or not it is working correctly by comparing a randomly chosen subset of their data.

Let us now illustrate this general idea by using a particular example of a possible implementation. It is shown in Fig. 2. The protocol can be summarised with the following three steps:

Step 1: Alice sends Bob phase-randomised weak coherent pulses (WCPs), together with decoy signals [38–40], prepared in different BB84 polarisation states [41], and sends them to Bob. In addition, she prepares decoy-states [38–40] 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 polarising beamsplitter (PBS).

The phase modulator $\phi$ shifts the phase of each pulse by 0 or $\pi$. Bob measures the outcoming pulses from the LON with a linear-optics single-photon BSM [42]. A successful BSM result is obtained when only one detector $D_i$ “clicks”. The polarisation rotator $R$ changes the horizontal (vertical) polarisation to a $45^\circ$ ($-45^\circ$) linear polarisation. As in Fig. 1: (brown box) characterised device; (black box) uncharacterised device; and (light turquoise box) secure lab.

FIG. 2: Schematic diagram of an example of a possible implementation of our method. Alice generates phase-randomised weak coherent pulses (WCPs) in different BB84 polarisation states [41], and sends them to Bob. In addition, she prepares decoy-states [38–40] 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 polarising beamsplitter (PBS).

The phase modulator $\phi$ shifts the phase of each pulse by 0 or $\pi$. Bob measures the outcoming pulses from the LON with a linear-optics single-photon BSM [42]. A successful BSM result is obtained when only one detector $D_i$ “clicks”. The polarisation rotator $R$ changes the horizontal (vertical) polarisation to a $45^\circ$ ($-45^\circ$) linear polarisation. As in Fig. 1: (brown box) characterised device; (black box) uncharacterised device; and (light turquoise box) secure lab.

Let us now illustrate this general idea by using a particular example of a possible implementation. It is shown in Fig. 2. The protocol can be summarised with the following three steps:

Step 1: Alice sends Bob phase-randomised weak coherent pulses (WCPs), together with decoy signals [38–40], prepared in different BB84 polarisation states [41], and sends them to Bob. In addition, she prepares decoy-states [38–40] 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 polarising beamsplitter (PBS).

The phase modulator $\phi$ shifts the phase of each pulse by 0 or $\pi$. Bob measures the outcoming pulses from the LON with a linear-optics single-photon BSM [42]. A successful BSM result is obtained when only one detector $D_i$ “clicks”. The polarisation rotator $R$ changes the horizontal (vertical) polarisation to a $45^\circ$ ($-45^\circ$) linear polarisation. As in Fig. 1: (brown box) characterised device; (black box) uncharacterised device; and (light turquoise box) secure lab.

Let us now illustrate this general idea by using a particular example of a possible implementation. It is shown in Fig. 2. The protocol can be summarised with the following three steps:

Step 1: Alice sends Bob phase-randomised weak coherent pulses (WCPs), together with decoy signals [38–40], prepared in different BB84 polarisation states [41], and sends them to Bob. In addition, she prepares decoy-states [38–40] 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 polarising beamsplitter (PBS).

The phase modulator $\phi$ shifts the phase of each pulse by 0 or $\pi$. Bob measures the outcoming pulses from the LON with a linear-optics single-photon BSM [42]. A successful BSM result is obtained when only one detector $D_i$ “clicks”. The polarisation rotator $R$ changes the horizontal (vertical) polarisation to a $45^\circ$ ($-45^\circ$) linear polarisation. As in Fig. 1: (brown box) characterised device; (black box) uncharacterised device; and (light turquoise box) secure lab.
for the diagonal basis. Once Bob has encoded his information, the signals are recombined at a polarising beamsplitter (PBS) and then measured with a linear-optics single-photon BSM [42]. A successful BSM result corresponds to observing a “click” in only one detector $D_i$, with $i \in \{1, \ldots, 4\}$.

**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 polarisation 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 [38–40] 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.

To conclude, either Alice or Bob applies a bit flip to part of her/his data to assure that their bit strings are correctly correlated (see Table I).

| “Clicking” detector | Alice & Bob | Rectilinear basis | Diagonal basis |
|----------------------|-------------|-------------------|----------------|
|                      | $D_1$       | $D_2$             | $D_3$          |
|                      | -           | Bit flip          | Bit flip       |
|                      | -           | Bit flip          | -              |

**TABLE I:** To guarantee that their bit strings are correctly correlated, either Alice or Bob applies a bit flip to part of her/his data, depending on which detector $D_i$ “clicked” (which identifies the Bell state obtained by the BSM) and the basis setting selected.

Let us emphasise that the method described above could be applied as well to other QKD protocols like, for instance, the three-state scheme [43–45]. 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. Moreover, note that the protocol above also works with just one single-photon detector at Bob’s side. This is so because it is sufficient to project the incoming signals into only one Bell state at the cost, of course, of reducing the final secret key rate by a factor of four.

### III. SECURITY ASSUMPTIONS

Before we analyse 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 post-processing techniques and (iii) an authenticated classical channel. In addition, we consider that (iv) Alice’s source and Bob’s LON are fully characterised 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 like, 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 [46, 47]. That is, she could launch bright light pulses into Bob’s LON and then analyse 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, this type 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 [46, 47].

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. In doing so, she might influence the functioning of both the beamsplitter and the phase modulator within the LON. Again, however, in practice one expects that Bob could avoid such type 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 [43–45]. According to the results in [45] 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 [48] 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 error. For instance, she could use quantum process tomography techniques to learn the position of Bob’s optical switch for each incoming signal and therefore obtain all his bit values. That is, she could occupy part of the quantum channel with signals prepared by herself. Then, she could measure these signals with a suitable device located within the “black box” (while, in parallel, she also measures Alice’s signals following the prescriptions of the protocol) and then she broadcasts the results obtained (i.e., Bob’s bit values) to herself. In order to do this, she could use, for example, the method described in [48] if the classical post-processing techniques of the protocol cannot be trusted (which, however, would violate our second security assumption). Alternatively, she could employ as transmitter the timing information about which detector $D_i$ “clicked” each given time [49]. That is, Eve could first use high efficiency detectors to measure Alice’s signals and then encode her information about Bob’s bit values by post-selecting which particular “clicks” actually output the BSM. For instance, in order to broadcast a bit value 0 (1) Eve could make the BSM to output a “click” that happened in an even (odd) time slot, while she discards other “clicks” [49].

For this reason, it is essential that Bob can guarantee that the BSM does not leak unwanted information to the outside. In practice, a simple way to achieve this would be that Bob builds the BSM himself, such that he can assure that it does not contain any transmitter prepared by Eve. This is indeed the expected situation in most realistic scenarios. Note, for instance, that the second attack described above [49] would require that Eve could substantially modify the BSM by including additional devices to separate and measure her own signals together with the ability to post-select the output information of the BSM. Importantly, if Bob builds the BSM themselves the presence of unwanted devices prepared by Eve could be discarded, and, in this situation, Bob does not need anymore to characterise the exact functioning of the optical elements within the BSM (i.e., the PBS, the polarisation rotators or the single-photon detectors $D_i$). That is, in the security analysis he could treat the whole BSM as a “black box”, where the only relevant information is the input and output data of the box. This is the key idea of our proposal. Most importantly, in this scenario our protocol can provide security against any detector side-channel attack.

IV. SECURITY ANALYSIS

We now evaluate the security of the protocol. From the results in [37] 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 [37] 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 over 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 restricted 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. Of course, this is a very particular eavesdropping strategy, and it does not include, for instance, detector blinding attacks [9, 10]. However, it will help us to illustrate the main security principles of the protocol. A full security proof against general attacks in the high-loss regime is left for future analysis.

Next we present a sketch of the security proof against the class of attacks described above. For this, we use similar arguments to those employed in mdiQKD [27], which rely on the security of a time reversed EPR-based QKD protocol [50–52]. Indeed, it can be shown that the protocol illustrated in Fig. 2, when viewed in the reverse order, is equivalent to a counter-factual entanglement based BB84 protocol [53]. That is, whenever Bob observes a single “click” in a detector $D_i$ in the actual protocol, in the counter-factual protocol this corresponds to the situation where Eve distributes a certain Bell state $|\phi_i\rangle$.

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., $\rho_A = \text{Tr}_{A'}(|\Psi\rangle_{AA'}\langle\Psi|)$, which is known and fixed by the state preparation process [54, 55].

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 $U_{BA} = \sum_i |b_i\rangle\langle b_i| \otimes U_{iA'}$ on systems $B$ and $A'$, where the unitary operators $U_{iA'}$ are fixed by his state preparation process (i.e., by the action of his LON). That is, each operator $U_{iA'}$ corresponds to one particular setting of his optical switch and phase modulator. Now, the key
point is that it can be shown (see the Methods section) that after applying $U_{BA'}$, the reduced density matrix of system $B$, that we denote as $\rho_B$, is fixed and equal to $\rho_A$ 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 [28, 53].

As a result, we have that the asymptotic secret key rate formula has the form $R \geq \sum_i \max\{R_i, 0\}$, 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 [56–58]

$$R_i \geq q\{p_0Y_{i,0} + p_1Y_{i,1}[1 - h(e_{i,1})]\} - Q_i f(E_i)h(E_i). \tag{1}$$

Here, the coefficient $q$ denotes the efficiency of the protocol (i.e., $q = 1/2$ for the standard BB84 protocol [41] and $q \approx 1$ for its efficient version [59]); $p_n = \exp(-\mu)\mu^n/n!$ is the probability that Alice sends Bob a signal which contains $n$ photons, with $\mu$ 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 efficiency function for the error correction process in the protocol (typically $f(E_i) \geq 1$; 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 [38–40]. 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. [60]. In both cases, it can be shown that the use of two weak decoy-states is already sufficient to obtain a tight estimation for these quantities.

![FIG. 3: 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. [61]: 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 $6.02 \times 10^{-6}$. Furthermore, we consider that the parameter $q \approx 1$ [59] 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) [38–40]. Note, however, that our proposal has the potential advantage of being immune against detector side-channel attacks.](image-url)
of our proposal, since it only contains two detectors instead of four. Most importantly, Fig. 3 shows that the scheme illustrated in Fig. 2 could deliver a secret key rate which is approximately two orders of magnitude higher than that of mdiQKD, although now the covered distance may be shorter.

VI. PROOF-OF-PRINCIPLE EXPERIMENT

We performed an experiment that demonstrates the feasibility of some relevant parts of the protocol. For simplicity, however, instead of using phase-randomised WCPs, the signal states emitted by Alice are generated with a continuous wave laser at 690 nm attenuated to the single photon level. Alice controls the polarisation 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 [62]. As a phase modulator, we use a mirror mounted over a piezoelectric actuator. No active stabilisation of the interferometer was needed for the time-scale involved in the experimental measurements, which were taken with an integration time of a few seconds. 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 93%.

We experimentally demonstrated the protocol for all possible combinations of states when both Alice and Bob use compatible or incompatible bases. That is, in our proof-of-principle experiment Alice and Bob use the same quantum states repeatedly without random selection of the encoding states or bases. Therefore, no secret key is actually distributed between them. 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. They are in good agreement with the theoretical predictions. When Alice and Bob use compatible bases [see Fig. 4(a)], we find that the average measured QBER over all different states is 5.8 ± 0.1%.

VII. CONCLUSIONS

We have proposed a novel solution to the problem of detector side-channels in practical QKD, which arguably constitutes the Achilles heel of current experimental realisations. It builds on the approach known as measurement-device-independent QKD (mdiQKD) [27]. However, when compared to mdiQKD, it has two main potential advantages. First, it is simpler to implement experimentally since it does not require to interfere 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 post-processing data blocks will be significantly smaller than those required in mdiQKD, which is essential in practice. Also, due to the hybrid encoding, our scheme employs a deterministic Bell-state analyser [42], yielding a factor two in the key generation rate when compared to mdiQKD.

So far, however, the security of our scheme has only been proven against a particular class of attacks, or against general attacks but in the low-loss regime. Therefore, in order for it to be a plausible alternative tomdiQKD 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.

Note added.—Based on the same conceptual idea, an
experimental demonstration with an alternative receiver and all-fiber components at telecom wavelengths was recently performed in [63].

Acknowledgements.—We would like to thank Koji Azuma, Hoi-Kwong Lo, Kiyoshi Tamaki and Bing Qi for very useful discussions. L. Rebón thanks the Center for Optics and Photonics (Universidad de Concepción) for hospitality and CONICYT for financial support. This work was supported by the grants CONICYT PFB08-024, Milenio P10-030-F, FONDECYT (grants No. 11110115, 1120067 and 1121010), and by the Galician Regional Government (program “Ayudas para proyectos de investigación desarrollados por investigadores emergentes”, and consolidation of Research Units: AtlantTIC). In addition W. A. T. Nogueira thanks CNPq (Brazil) for financial support.

Appendix

Reduced density matrix $\rho_B$. Here we briefly show that after applying the controlled unitary operation $U_{BA'}$ the reduced density matrix $\rho_B$ 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

$$U_{1,A'}|1,0\rangle_A|0,0\rangle_{aux} = |1,0\rangle_{inp_1}|0,0\rangle_{inp_2},$$

$$U_{1,A'}|0,1\rangle_A|0,0\rangle_{aux} = |0,1\rangle_{inp_1}|0,0\rangle_{inp_2},$$

where the state $|1,0\rangle$ denotes one photon in horizontal polarisation and $|0,1\rangle$ is one photon in vertical polarisation. System aux represent 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. (2) tells us that when the single-photon $A'$ is prepared in horizontal (vertical) polarisation, and Bob selects path $a$, then we have one photon in horizontal (vertical) polarisation in the input port inp$_1$ of the BSM.

When Bob chooses path $c$ we have that

$$U_{2,A'}|1,0\rangle_A|0,0\rangle_{aux} = |0,0\rangle_{inp_1}|1,0\rangle_{inp_2},$$

$$U_{2,A'}|0,1\rangle_A|0,0\rangle_{aux} = |0,0\rangle_{inp_1}|0,1\rangle_{inp_2},$$

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) polarisation, and Bob selects path $c$, then we have one photon in horizontal (vertical) polarisation 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

$$U_{3,A'}|1,0\rangle_A|0,0\rangle_{aux} = 1/\sqrt{2}|1,0\rangle_{inp_1}|0,0\rangle_{inp_2} + |0,0\rangle_{inp_1}|1,0\rangle_{inp_2},$$

$$U_{3,A'}|0,1\rangle_A|0,0\rangle_{aux} = 1/\sqrt{2}|0,1\rangle_{inp_1}|0,0\rangle_{inp_2} + |0,0\rangle_{inp_1}|0,1\rangle_{inp_2},$$

$$U_{4,A'}|1,0\rangle_A|0,0\rangle_{aux} = 1/\sqrt{2}|1,0\rangle_{inp_1}|0,0\rangle_{inp_2} - |0,0\rangle_{inp_1}|1,0\rangle_{inp_2},$$

$$U_{4,A'}|0,1\rangle_A|0,0\rangle_{aux} = 1/\sqrt{2}|0,1\rangle_{inp_1}|0,0\rangle_{inp_2} - |0,0\rangle_{inp_1}|0,1\rangle_{inp_2}.\ (4)$$

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 $|\phi_i\rangle_{B,inp_1,inp_2} = U_{BA}\sum_i \sqrt{p_i}|b_i\rangle_B|\phi_i\rangle_{A'}|0,0\rangle_{aux}$.

Then, we have that $\rho_B = Tr_{inp_1,inp_2}(|\phi_i\rangle_{B,inp_1,inp_2}\langle \phi_i|)$. Finally, by combining the equations above now it is straightforward to show that, independently of the state $|\phi_i\rangle_{A'}$, indeed $\rho_B$ is a density matrix of rank two equal to $\rho_A = Tr_{A'}(|\Psi\rangle_{A'}\langle \Psi|)$ 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 $\rho_B$ 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 Photonics 8, 595-604 (2014).
[4] B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, Quantum Inf. Comput. 7, 73 (2007).
[5] Y. Zhao, C.-H. F. 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 et al., Phys. Rev. A 88, 062335 (2013).
[9] L. Lydersen et al., Nature Photon. 4, 686 (2010).
[10] I. Gerhardt et al., Nat. Commun. 2, 349 (2011).
[11] C.-H. F. 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).
A. Lamas-Linares and C. Kurtsiefer, Opt. Express 15, 9388 (2007).

D. Mayers and A. C.-C. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98) 503–509 (IEEE Computer Society, Washington, DC, USA, 1998).

A. Acín et al., Phys. Rev. Lett. 98, 230501 (2007).

D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. 5, 325 (2004).

M. Koashi, preprint arXiv:quant-ph/0505108 (2005).

H.-K. Lo, Quantum Inf. Comput. 5, 413 (2005).

H.-K. Lo, H. F. C. Chau and M. Ardehali, J. Cryptology 18, 133 (2005).

R. Ursin et al., Nature Phys. 3, 481 (2007).

This simpler configuration is equivalent to that illustrated in Fig. 2, but now the rectilinear basis suffers an additional 3dB 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.