SCIENTIFIC REPORTS
nature research

OPEN

Long-distance device-independent quantum key distribution

Víctor Zapatero* & Marcos Curty

Besides being a beautiful idea, device-independent quantum key distribution (DIQKD) is probably the ultimate solution to defeat quantum hacking. Its security is based on a loophole-free violation of a Bell inequality, which results in a very limited maximum achievable distance. To overcome this limitation, DIQKD must be furnished with heralding devices like, for instance, qubit amplifiers, which can signal the arrival of a photon before the measurement settings are actually selected. In this way, one can decouple channel loss from the selection of the measurement settings and, consequently, it is possible to safely post-select the heralded events and discard the rest, which results in a significant enhancement of the achievable distance. In this work, we investigate photonic-based DIQKD assisted by two main types of qubit amplifiers in the finite data block size scenario, and study the resources—particularly, the detection efficiency of the photodetectors and the quality of the entanglement sources—that would be necessary to achieve long-distance DIQKD within a reasonable time frame of signal transmission.

The use of quantum mechanics for cryptographic means was first proposed in the early 70's by Stephen Wiesner, aiming to create unfalsifiable banknotes[1]. Inspired by this seminal work, Charles Bennett and Gilles Brassard introduced a protocol to securely distribute cryptographic keys[2]. Nowadays, intense theoretical and experimental research[3–5] has turned this latter task—called quantum key distribution (QKD)—into a feasible commercial solution[6].

Despite such tremendous progress, a major flaw of QKD today is the existing big gap between the theory and the practice. This is so because security proofs of QKD typically rely on simple mathematical models to describe the behaviour of the different physical devices. As a result, any departure from these models might render real-life QKD implementations vulnerable to quantum hacking attacks[7–13].

To overcome this problem, the ultimate solution probably is device-independent QKD (DIQKD)[14–19]. Given that the users' devices are honest[20,21], DIQKD can guarantee security without characterizing the internal functioning of the apparatuses, thereby ruling out all hacking attacks against the physical implementation. It is based on a feature of some entangled states known as nonlocality[22], which guarantees that two distant parties (say, Alice and Bob) sharing an ideal nonlocal quantum state observe perfectly correlated outcomes when performing adequate quantum measurements on their shares. Moreover, these correlations are monogamous, *i.e.*, the measurement outcomes are statistically independent of any pre-existing information held by a third party. This property can be verified with a two-party Bell test[22–27] known as the Clauser-Horne-Shimony-Holt (CHSH) test, which basically consists of repeatedly playing a two-party nonlocal game[19,28]. The winning rate of the game indicates the amount of monogamous correlations shared between Alice and Bob.

The security of DIQKD has been rigorously established in different works, first against collective attacks[15] in the asymptotic regime, then against coherent attacks[17] also in the asymptotic regime, and only recently in the practical scenario of finite data block sizes[28] (see also[29]). The security proof in[28] relies on the so-called entropy accumulation theorem[30,31], which effectively allows to prove the security of the full protocol from the security of a single round of the protocol by using a worst-case scenario.

Security proofs require, however, that two fundamental loopholes are closed: the *locality loophole*[22] and the *detection loophole*[22,32,33]. The former is closed by enforcing a proper isolation of Alice's and Bob's devices. Closing the detection loophole is more tricky, especially if Alice and Bob wish to cover long distances. Indeed, if an adversary were able to correlate channel loss to Alice's or Bob's measurement settings, such an adversary could easily fake nonlocal correlations, and thus compromise the security of the distilled key. A simple solution is to assign a pre-established outcome value to each lost signal while running the CHSH test. The main drawback of this technique is however the limited achievable distance, because such mapping translates loss into errors. Indeed, with such an approach, even if the entanglement source could generate perfect Bell pairs and Alice and Bob could

Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo, E-36310, Spain. *email: vzapatero@com.uvigo.es

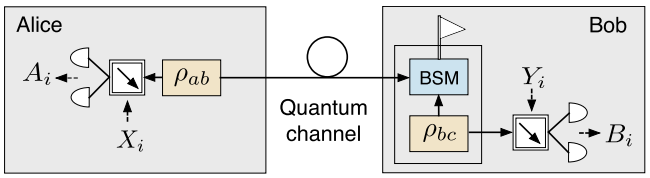

Figure 1. Schematic of the considered DIQKD protocol. While Alice holds an entanglement source, ρ_{ab}, in her lab, Bob holds a qubit amplifier, which consists of an entanglement source, ρ_{bc}, and a Bell state measurement (BSM) used for teleportation. The role of the qubit amplifier is to mitigate the effect of channel loss. In every round of the protocol in which a successful heralding takes place at the qubit amplifier, Bob randomly chooses a bit value $T_i \in \{0, 1\}$. If $T_i = 0$, Alice (Bob) chooses as measurement setting $X_i = \sigma_z$ ($Y_i = \sigma_z$). If $T_i = 1$, Alice chooses at random her measurement setting $X_i \in \{\sigma_z, \sigma_x\}$, with σ_z and σ_x being the Pauli matrices given by Eq. (1). Similarly, in this latter case, Bob chooses at random his measurement setting $Y_i \in \{\sigma_+, \sigma_-\}$, where $\sigma_\pm = (\sigma_z \pm \sigma_x)/\sqrt{2}$. Their respective outcomes are recorded as A_i, $B_i \in \{0, 1\}$, where A_i (B_i) indicates which of Alice's (Bob's) two photodetectors registered a single-photon pulse. If, say, Alice obtains an inconclusive result (*i.e.*, no photons or multiple photons are observed, she deterministically selects $A_i = 1$, and similarly for Bob. The reader is referred to the main text for further details.

measure them with unit efficiency detectors, channel loss would limit the maximum DIQKD transmission distance to about only 3.5 km for a typical optical fiber in the telecom wavelength with an attenuation coefficient equal to $\alpha = 0.2$ dB/km.

To enhance the distance, Alice and Bob need to use heralding devices. These are devices that herald the arrival of a signal to the receiver, allowing a fair post-selection of the heralded events. Then, if Alice and Bob choose their measurement settings *a posteriori*, *i.e.*, once their heralding devices have declared the reception of a signal, they actually decouple channel loss from their measurement settings selection, thus paving the way for DIQKD over long distances.

A heralding device particularly suited for DIQKD is a qubit amplifier[34–36], which basically consists of a teleportation gate. That is, a successful heralding corresponds to the teleportation of the state of the arriving signal to a signal at the output port of the qubit amplifier. DIQKD supported by qubit amplifiers has been analysed in[34–38] in the asymptotic regime, *i.e.*, by considering an infinite number of signals. In this work, we focus on the practical finite data block size scenario. More precisely, we study finite-key DIQKD with the two different types of qubit amplifier architectures introduced in[35] and[36]. We pay particular attention to the effect that typical device imperfections (especially, the finite detection efficiency of the photodetectors and the multi-photon pulses emitted by practical entanglement light sources) have on the performance of the system. In doing so, we determine the resources needed to achieve long-distance implementations of DIQKD within a reasonable time frame of signal transmission.

Results

DIQKD protocol. We consider the DIQKD protocol introduced in[28]. It is based on a CHSH test[24], and it is equivalent to a certain two-party nonlocal game known as the CHSH game.

Before presenting the steps of the protocol in detail, let us introduce some notation first. Alice's measurement setting in the i-th successfully heralded round of the protocol is denoted by $X_i \in \{0, 1\}$, where $X_i = 0$ and $X_i = 1$ tag the measurements described by the two following Pauli operators

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1}$$

respectively. On the other hand, Bob's measurement setting in the i-th successfully heralded round of the protocol is denoted by $Y_i \in \{0, 1, 2\}$, where $Y_i = 0$ tags the measurement $\sigma_+ = (\sigma_z + \sigma_x)/\sqrt{2}$, $Y_i = 1$ indicates the measurement $\sigma_- = (\sigma_z - \sigma_x)/\sqrt{2}$ and $Y_i = 2$ refers to the measurement σ_z, with σ_z and σ_x again given by Eq. (1). Similarly, Alice's (Bob's) outcome in the i-th successfully heralded round is denoted by $A_i \in \{0, 1\}$ ($B_i \in \{0, 1\}$).

Next, we present the different steps of the protocol. A schematic is shown in Fig. 1. For simplicity, we shall assume here that only Bob holds a qubit amplifier to compensate channel loss (see the Methods section for a description of the qubit amplifiers we consider), while Alice has the entanglement source, ρ_{ab}, in her lab. The case where both Alice and Bob hold a qubit amplifier and the entanglement source is located in the middle of the channel between them is analyzed in the Supplementary Information.

Protocol steps

1. *Initialization*. Bob sets the counter i of successfully heralded rounds to 0. While $i < n_{SH}$ for a certain prefixed value n_{SH}, steps 2 and 3 below are repeated.
2. *Distribution*. Alice prepares a bipartite entangled state, ρ_{ab}, and sends system B to Bob through the quantum channel. If no successful heralding takes place at Bob's qubit amplifier, the signal is discarded and step 2 is repeated. Otherwise, Bob updates the counter i to $i + 1$. Then, he randomly chooses a bit value $T_i \in \{0, 1\}$ with probabilities $P(T_i = 0) = 1 - \gamma$ and $P(T_i = 1) = \gamma$, respectively, and sends it to Alice through an authenticated classical channel. We denote by $T = (T_1, T_2, \ldots, T_{n_{SH}})$ the string of all bit values T_i.

	Protocol arguments
n_{SH}	Post-processing block size
γ	Probability of a test round
δ_{est}	Confidence interval for the CHSH game winning rate
ϵ_{IR}	Error probability of information reconciliation
ϵ_{PA}	Error probability of privacy amplification
l	Length of the final keys K_A and K_B

Table 1. List containing the main protocol arguments.

3. *Measurement*. If $T_i = 0$, the i-th successfully heralded round is considered to be a key generation round, and Alice and Bob choose the settings $(X_i, Y_i) = (0, 2)$. If $T_i = 1$, such round is considered to be a test round (*i.e.*, a CHSH game round), and they independently select $X_i, Y_i \in \{0, 1\}$ uniformly at random. Alice and Bob record their measurement outcomes as $A_i, B_i \in \{0, 1\}$, respectively. If, say, Alice (Bob) obtains an inconclusive result (*i.e.*, no photon or multiple photons are observed in the detectors) she (he) deterministically assigns $A_i = 1$ ($B_i = 1$) to keep the detection loophole closed. Finally, Alice (Bob) publicly announces the measurement settings X_i (Y_i). In what follows, we will denote by X (Y) the bit string $X_1, X_2, \ldots, X_{n_{SH}}$ ($Y_1, Y_2, \ldots, Y_{n_{SH}}$) of Alice's (Bob's) measurement settings for the successfully heralded rounds. Similarly, a (B) will denote the string of measurement outcomes $A_1, A_2, \ldots, A_{n_{SH}}$ ($B_1, B_2, \ldots, B_{n_{SH}}$).
4. *Information reconciliation*. Alice and Bob use an error correction protocol to obtain two identical bit strings, Z_A and Z_B, from A and B, respectively. For this, Alice sends Bob $leak_{IR}$ bits of syndrome information and Bob obtains an estimate, Z_B, of A. Next, they perform an error verification step (using two-universal hash functions) that leaks at most $\lceil \log_2(1/\epsilon_{IR}) \rceil$ bits of information to Eve, for a certain prefixed parameter ϵ_{IR}. If this last step is successful, it is guaranteed that Alice's and Bob's bit strings $Z_A = A$ and Z_B satisfy $P(Z_A \neq Z_B) \leq \epsilon_{IR}$. Otherwise, the protocol aborts.
5. *Parameter estimation*. Bob sets the parameter $C_i = \perp$ for the key generation rounds (*i.e.*, when $T_i = 0$) and $C_i = \omega_{CHSH}(Z_{B_i}, B_i, X_i, Y_i)$ for the test rounds (*i.e.*, when $T_i = 1$), with $i = 1, 2, \ldots, n_{SH}$, and where Z_{B_i} denotes the i-th bit of the string Z_B and the function ω_{CHSH} is defined as

$$\omega_{CHSH}(a, b, x, y) = \begin{cases} 1 & \text{if } a \oplus b = x \cdot y, \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

with $\oplus$ denoting bit addition modulo 2 and $\cdot$ denoting bit multiplication. The overall number of test rounds in which $C_i = 1$ (and thus the parties win the CHSH game) is denoted by $C_{SH} = \sum_{\{i:T_i=1\}} C_i$. This quantity allows to compute a lower bound on the number of secret bits that can be extracted from Z_A and Z_B using privacy amplification[28]. Bob aborts the protocol if the fraction of wins lies below a certain prefixed threshold value, *i.e.*, when $C_{SH}/n_{SH} < \omega|_{SH}\gamma - \delta_{est}$, where $\omega|_{SH} \in (3/4, (2 + \sqrt{2})/4)$ is the expected winning rate of the CHSH game in the test rounds (which requires an experimental characterization of the setup), γ is again the probability that Bob uses a successfully heralded round as a test round, and δ_{est} is the confidence interval that defines the abortion threshold. That is, δ_{est} is the maximum difference between the expected and the actual winning rates of the CHSH game that Bob accepts without aborting.
6. *Privacy amplification*. Alice and Bob apply a privacy amplification protocol to their bit strings Z_A and Z_B to obtain the final keys, K_A and K_B, of length l. This protocol uses a randomness extractor that succeeds except with error probability ϵ_{PA}.

The main protocol arguments are summarised in Table 1.

We remark that in the distribution step of the protocol, Alice and Bob need to store their signals until they choose their measurement settings and measure the signals in the third step of the protocol. For simplicity, below we will optimistically assume that, for this purpose, both of them hold noiseless and lossless quantum memories in their labs. Alternatively, they could also decide which rounds are key generation rounds and which ones are test rounds *a posteriori* by using the typical sifting step in QKD, though this approach results in a slightly less efficient solution. This is so because the data associated to Alice measuring σ_x and Bob measuring σ_z is not used in the protocol.

Also, we note that in a photonic implementation of the DIQKD scheme, the measurements X_i and Y_i can be realised by means of a polarization modulator that rotates the polarization state of the incoming signals, together with a PBS that separates vertical and horizontal polarization modes, followed by two photodetectors. For example, the rotation angles of the polarization modulator associated to the measurements σ_z, σ_x, σ_+ and σ_- are 0, $\pi/4$, $\pi/8$ and $-\pi/8$ radians, respectively. The observation of one single-photon in, say, horizontal (vertical) polarization is recorded by Alice as $A_i = 0$ ($A_i = 1$), and the same applies to Bob.

Evaluation. A major goal of this work is to determine the resources needed to implement DIQKD over long distances, with a particular emphasis on the detection efficiency and the quality of the entanglement sources. In this section, we use the device models and the secret key rate formula presented in the Methods section to

evaluate the performance of the DIQKD protocol described above. All the relevant calculations required to reproduce the results presented here are included in the Supplementary Information.

To start up with, let us introduce some concepts and notation that shall be used in what follows. First of all, we will refer to two different DIQKD setups: the entanglement swapping relay (ESR) based setup and the polarizing qubit amplifier (PQA) based setup. The only difference between them lies in the qubit amplifier[34–36], particularly, in the internal mechanism it uses to generate entangled photons for teleportation. To be precise, the ESR utilizes a source of entangled pairs directly[36] (for instance, a PDC source), while the PQA[34,35] generates entanglement by interfering single photon pulses in a linear optics network (see the Methods section). In both cases, we suppose that the teleportation is performed using a standard linear optics Bell state measurement (BSM). Regarding the photodetectors, we assume that all of them are photon-number-resolving (PNR) with the same detection efficiency, η_{d}, and the same dark count probability, p_{d}. Similarly, all the optical couplers used to link the light sources to the optical fiber are assumed to have the same coupling efficiency, η_{c}. See the Methods section for further details about the device models, as well as for a detailed description of the qubit amplifiers we consider.

For simplicity, in the simulations below we assume that the coupling efficiency of the light sources is equal to the detection efficiency of the photodetectors, *i.e.*, we set $\eta_{\mathrm{c}} = \eta_{\mathrm{d}} = \eta_{\mathrm{c,d}}$. This decision is motivated because DIQKD requires very high values of $\eta_{\mathrm{c,d}}$, so the effect of this simplification is negligible, and it reduces the number of experimental parameters to consider. Also, unless otherwise stated, we fix the dark count rate of the photodetectors to $p_{\mathrm{d}} = 10^{-7}$. Although this is a quite low value, it is achievable with current technology, for instance, by using superconducting nanowire single-photon detectors[39,40] or even avalanche photodiodes[41].

Regarding the security of the protocol, Alice and Bob should agree on the value of the secrecy parameter, ϵ_{sec}, the correctness parameter, ϵ_{cor}, and the robustness parameter, ϵ_{rob} in advance. Of course, these and other parameters, together with the secret key length of the protocol, are properly presented in the Methods section. For illustration purposes, in the simulations we consider two examples of security parameter sets (ϵ_{sec}, ϵ_{cor}, ϵ_{rob}), which we denote by S_1 and S_2. These sets are given in Table 2. In addition, we further simplify the numerics by fixing the value of the failure probability of the entropy accumulation theorem, ϵ_{EA}, which is another parameter entering the security analysis. Precisely, we take $\epsilon_{\mathrm{EA}} = 10^{-6}$ ($\epsilon_{\mathrm{EA}} = 10^{-10}$) for the set S_1 (S_2). We remark, however, that according to our simulations the loss of generality that results from fixing the value of ϵ_{EA} in advance is very small. The secret key rate is then maximised over the remaining parameters. These include some security error terms affecting the secret key length, together with some experimental parameters that depend on the photon sources and on the qubit amplifier under consideration.

Importantly, the number of signals transmitted in an execution of the protocol, which we shall denote by N, is not determined a priori. Indeed, as described in the previous section, it is the target number of successful heralding events that we fix, n_{SH}. Therefore, in the absence of real experimental data, we set N to its expected value $\langle N\rangle$ for the simulations. In this way, what we shall refer to as the secret key rate in this section is the ratio

$$K = \frac{l}{\langle N\rangle}, \tag{3}$$

l being the secret key length of the protocol. Similarly, the *conditional* secret key rate (*i.e.*, the number of secret key bits per successful heralding event) reads $K|_{\mathrm{SH}} = l/n_{\mathrm{SH}}$, and it is related to k via $K = P_{\mathrm{SH}}K|_{\mathrm{SH}}$, where P_{SH} is the successful heralding probability of the qubit amplifier. Note that we are assuming here that P_{SH} is the same for all the rounds of the protocol, in such a way that

$$\langle N\rangle = \frac{n_{\mathrm{SH}}}{P_{\mathrm{SH}}} \tag{4}$$

Finally, in all the plots below we assume a threshold value for the secret key rate K as low as 10^{-10}. That is, whenever the resulting secret key rate is smaller than this threshold value, it is considered to be impractical and we neglect it. Although this choice is arbitrary, 10^{-10} seems to be a reasonable value: even with an ideal entanglement source with a high repetition-rate of 10 GHz, one could only extract 1 secret bit/s at most, which is probably too low for most applications.

Ideal sources. We start by analyzing the ideal scenario where Alice and Bob hold perfect photon sources. Obviously, this case provides the best possible performance, and thus it can be used as a reference about the minimum resources (say, *e.g.*, the minimum value of the detection and coupling efficiency, $\eta_{\mathrm{c,d}}$, and the minimum block size, n_{SH}) that are required to achieve a certain secret key rate.

More precisely, we consider here that the entanglement source ρ_{ab} at Alice's lab generates perfect polarization Bell pairs. On the other side, the entangled states ρ_{bc} used for teleportation are different for each qubit amplifier architecture. In the case of a PQA, ρ_{bc} is generated via the interference of two single photon signals, $\rho^{h}_{\mathrm{single}}$ and $\rho^{v}_{\mathrm{single}}$, on a beamsplitter of tunable transmittance t (see the Methods section for more details). Here, we set $\rho^{h}_{\mathrm{single}}$ ($\rho^{v}_{\mathrm{single}}$) to be a perfect single-photon source generating horizontally (vertically) polarised single photons. Similarly, in the case of an ESR, we directly set ρ_{bc} to be a perfect source of polarization Bell pairs, as ρ_{ab}.

No channel loss. To begin with, we compare the achievable performance when using PQAs and ESRs in the absence of channel loss, *i.e.*, we set the transmission distance L to zero. This scenario allows us to determine the minimum value of n_{SH} as a function of $\eta_{\mathrm{c,d}}$.

	ϵ_{sec}	ϵ_{cor}	ϵ_{rob}
S_1	10^{-5}	10^{-10}	10^{-2}
S_2	10^{-9}	10^{-15}	10^{-3}

Table 2. Sets of security parameters ϵ_{sec}, ϵ_{cor} and ϵ_{rob} considered in the performance evaluation of DIQKD. The set S_1 provides a lower level of security than the set S_2.

As we will show below, it turns out that $\eta_{\text{c,d}}$ is quite high even in this ideal scenario. This means that the probability that any of these two amplifiers provides a spurious success at Bob's side due to the dark counts of the PNR detectors within the BSM is negligible compared to that of a genuine success triggered by a single photon from Alice. Therefore, for simplicity, in this subsection we set the dark count rate p_{d} equal to zero. With this approximation and on the basis of the ideal form of ρ_{ab} and ρ_{bc} just presented, one can readily use the models for the detectors and the optical couplers to derive analytical expressions for the three experimental parameters that enter the secret key rate formula: the successful heralding probability of the qubit amplifier, P_{SH} (entering K via $\langle N\rangle$), the expected conditional winning rate at the CHSH game, $\omega|_{\text{SH}}$, and the expected conditional quantum bit error rate, $Q|_{\text{SH}}$ (the latter two entering K via l). In the ESR-based setup, one obtains

$$\begin{aligned} P_{\text{SH}}^{\text{ESR}} &= \frac{\xi^2}{2}, \\ \omega|_{\text{SH}}^{\text{ESR}} &= \frac{2+\sqrt{2}}{4}\xi^2 + \frac{3}{4}(1-\xi)^2 + \xi(1-\xi), \\ Q|_{\text{SH}}^{\text{ESR}} &= \xi(1-\xi), \end{aligned} \tag{5}$$

where the parameter $\xi = \eta_{\text{c,d}}^2$. We remark that the successful heralding probability scales with ξ^2, *i.e.*, with $\eta_{\text{c,d}}^4$, because it requires the successful detection of two photons in the BSM. Note that the detection probability of each photon scales with ξ, as this quantity includes both the detection and the coupling factors, *i.e.*, $\xi = \eta_{\text{c}}\eta_{\text{d}} = \eta_{\text{c,d}}^2$. Similarly, in the PQA-based setup, one finds

$$\begin{aligned} P_{\text{SH}}^{\text{PQA}} &= (1-t)\xi^2[1-\xi(1-t)], \\ \omega|_{\text{SH}}^{\text{PQA}} &= \frac{1}{1-\xi(1-t)}\left[\frac{2+\sqrt{2}}{4}t\xi^2 + \frac{3}{4}(1-\xi)^2 \right. \\ &\quad \left. + \frac{(1+t)}{2}\xi(1-\xi)\right], \\ Q|_{\text{SH}}^{\text{PQA}} &= \frac{(1+t)\xi(1-\xi)}{2[1-\xi(1-t)]}, \end{aligned} \tag{6}$$

where the parameter t corresponds to the transmittance of the BS within the amplifier. The reader is referred to the Supplementary Information for the detailed calculation of P_{SH}, $\omega|_{\text{SH}}$ and $Q|_{\text{SH}}$ in more general settings that reduce to Eqs. (5) and (6) when ideal sources are considered.

From Eq. (6), it is evident that there is a trade-off on the coefficient t. The terms $\omega|_{\text{SH}}^{\text{PQA}}$ and $Q|_{\text{SH}}^{\text{PQA}}$ favor $t \approx 1$, and thus the conditional secret key rate $K|_{\text{SH}}$, which depends on these parameters but not on $P_{\text{SH}}^{\text{PQA}}$, also favors $t \approx 1$. Indeed, in the limit $t \to 1$ we have that $\omega|_{\text{SH}}^{\text{PQA}} = \omega|_{\text{SH}}^{\text{ESR}}$ and $Q|_{\text{SH}}^{\text{PQA}} = Q|_{\text{SH}}^{\text{ESR}}$. On the other hand, $P_{\text{SH}}^{\text{PQA}}$ is maximised when $t = 1 - (2\xi)^{-1}$, and it actually vanishes when $t = 1$. This behaviour can be easily understood by examining the states $\rho_{bc} = |\varphi\rangle_{bc}\langle\varphi|$ generated with the single-photon interference inside the PQA, whose expression with ideal single photon sources is of the form $|\varphi\rangle_{bc} = (1-t)|\psi\rangle_{bb} + t\,|\phi\rangle_{cc} - \sqrt{2t(1-t)}\,|\chi\rangle_{bc}$ and the states $|\psi\rangle_{bb}$, $|\phi\rangle_{cc}$ and $|\chi\rangle_{bc}$ are given in Eq. (17) of the Methods section. In short, by setting t close to 1 we have that whenever a successful heralding takes place at the qubit amplifier, this event is due to the entangled pair $|\chi\rangle_{bc}$ with a high probability, and thus $K|_{\text{SH}}$ is maximised. On the contrary, the lower the transmittance t is, the more likely it is that a success comes from the spurious term $|\psi\rangle_{bb}$ and, consequently, $K|_{\text{SH}}$ is minimised. In our simulations, we numerically optimise the value of t so that the overall secret key rate K is maximised.

Also, we remark that by substituting the parameters from Eqs. (5) and (6) in Eq. (31), equating the resulting expression to zero and numerically solving for ξ, one obtains the minimum value of ξ required for a positive key rate. This minimum value happens to be very large, $\xi \gtrapprox 92.3\%$ (or, equivalently, $\eta_{\text{c,d}} = \sqrt{\xi} \gtrapprox 96.1\%$) for both types of qubit amplifiers. Similarly, from Eqs. (5) and (6), it can be shown that, irrespectively of the value of t, whenever $\xi \geq 50\%$ we have that $P_{\text{SH}}^{\text{ESR}} > P_{\text{SH}}^{\text{PQA}}$, $\omega|_{\text{SH}}^{\text{ESR}} \geq \omega|_{\text{SH}}^{\text{PQA}}$ and $Q|_{\text{SH}}^{\text{ESR}} \leq Q|_{\text{SH}}^{\text{PQA}}$. That is, an ESR-based qubit amplifier always outperforms a PQA in the absence of channel loss, if perfect sources are assumed. In Fig. 2(a) we plot the minimum block size, n_{SH}, and the minimum detection efficiency, $\eta_{\text{c,d}}$, that are needed to obtain a secret key rate above the threshold value of 10^{-10} at $L = 0$ km. We denote this secret key rate by $K|_{L=0}$ and the minimum block size by $n_{\text{SH}}^*|_{L=0}$. The value of $n_{\text{SH}}^*|_{L=0}$ is obtained for each $\eta_{\text{c,d}}$ via exhaustive numerical search over all the free parameters contained in the finite-key rate formula. The solid (dashed) bluish (reddish) lines correspond to the ESR (PQA) architecture, and in each case the lower (upper) line uses the set of security requirements S_1 (S_2) of

Table 2. Remarkably, despite the security parameters of S_2 being significantly more demanding than those of S_1, it turns out that the set S_2 does not require much larger block sizes than S_1.

Also, Fig. 2(a) indicates that both qubit amplifiers require a similar minimum block size, $n^*_{\mathrm{SH}}|_{L=0}$, to deliver a secret key rate above the threshold value. Indeed, it is easy to show that if the threshold value for the secret key rate were zero (instead of 10^{-10}) then the value of $n^*_{\mathrm{SH}}|_{L=0}$ would be equal for both qubit amplifiers. However, the fact that we use a threshold value greater than zero implies that $n^*_{\mathrm{SH}}|_{L=0}$ is always slightly lower for the ESR than for the PQA. This is so because, even though the latter can mimic the conditional secret key rate of the former for any efficiency $\eta_{\mathrm{c,d}}$, the ESR has a higher success probability $P^{\mathrm{ESR}}_{\mathrm{SH}}$, thus leading to a higher overall secret key rate. Nevertheless, this effect cannot be fully appreciated with the resolution of Fig. 2(a).

Finally, the dotted black vertical line illustrated in Fig. 2(a) corresponds to the (asymptotic) minimum efficiency, $\eta_{\mathrm{c,d}} \approx 96.1\%$, required to obtain $K_\infty|_{L=0} \geq 10^{-10}$. That is, no secret key rate above such threshold value is possible when $\eta_{\mathrm{c,d}} \lessapprox 96.1\%$, no matter how much we increase the block size.

In what follows, we will refer to the lines in Fig. 2(a) as the *critical lines*, since every pair $(\eta_{\mathrm{c,d}}, n_{\mathrm{SH}})$ lying below these lines delivers a negligible secret key rate with the corresponding security requirements.

Figure 2(b) shows the zero-distance secret key rate, $K|_{L=0}$, as a function of the detection and coupling efficiency, $\eta_{\mathrm{c,d}}$, for different values of the block size, n_{SH}. As already discussed above, the ESR architecture always leads to larger secret key rates for all values of $\eta_{\mathrm{c,d}}$, while the minimum efficiencies required to have a secret key rate larger than the threshold value are roughly equal for both qubit amplifiers. Again, the small mismatch between the minimum efficiencies required by both amplifiers occurs because the selected threshold is greater than zero. Otherwise, the minimum efficiencies would match. For illustrative purposes, Fig. 2(b) considers four different block sizes: $n_{\mathrm{SH}} \to \infty$, $n_{\mathrm{SH}} = 10^{11}$, $n_{\mathrm{SH}} = 10^{9}$ and $n_{\mathrm{SH}} = 10^{17}$. As already shown in Fig. 2(a), the smaller the block size is, the larger the value of the minimum efficiency $\eta_{\mathrm{c,d}}$ that is required. For instance, for a block size as large as, say, $n_{\mathrm{SH}} = 10^{11}$, and if one considers the weaker set of security requirements S_1, the minimum efficiency is at least $\eta_{\mathrm{c,d}} \approx 96.4\%$. Also, for any given value of n_{SH}, the greater the detection efficiency considered (with respect to its minimum value), the closer the resulting secret key rates corresponding to the security settings S_1 and S_2 become. This is so because, in this situation, the effect of finite statistics is less prominent. Note that in the limit given by the asymptotic regime, the secret key rate K_∞ does not depend on the security sets S_1 and S_2, but these sets are only relevant in the finite-key regime.

Channel loss. In this subsection, we consider the effect of channel loss as modeled in the Methods section, where it is parametrised by the quantity $\Lambda = \alpha L$ measured in dB. Here and throughout this work, the transmission distance L is the distance between Alice's lab and Bob's lab. For example, when only Bob has a qubit amplifier, then L represents the distance between Alice's entanglement source ρ_{ab} (located inside Alice's lab) and Bob's qubit amplifier (located inside Bob's lab). Similarly, when both Alice and Bob have a qubit amplifier (see the Supplementary Information), L is the distance between Alice's qubit amplifier and Bob's qubit amplifier. Also, we set here the dark count rate of the detectors to $p_{\mathrm{d}} = 10^{-7}$, as the effect of dark counts becomes relevant in this scenario.

Figure 3 plots the secret key rate K as a function of Λ for various values of $\eta_{\mathrm{c,d}}$ and n_{SH}, and for the two qubit amplifier architectures under consideration. More precisely, we use two values for $\eta_{\mathrm{c,d}}$: the ideal one, *i.e.*, $\eta_{\mathrm{c,d}} = 100\%$, and another one close to the threshold value of 96.1% discussed above, say, $\eta_{\mathrm{c,d}} = 96.5\%$. Moreover, for each of these values of the efficiency $\eta_{\mathrm{c,d}}$, we plot three different secret key rates: the asymptotic one K_∞, and two finite-key rates, one for the security settings S_1 and another one for the security settings S_2. In both finite-key cases, we use a common block size n_{SH} close to the critical value obtained from Fig. 2(a). Specifically, we set $n_{\mathrm{SH}} = 10^7$ when $\eta_{\mathrm{c,d}} = 100\%$, and $n_{\mathrm{SH}} = 10^{11}$ when $\eta_{\mathrm{c,d}} = 96.5\%$. In doing so, and for the considered security analysis, we are simultaneously providing upper bounds (given by K_∞) and lower bounds (given by the finite-key rates) to the finite-key performance that could be achieved with the chosen detection and coupling efficiencies, and the security requirements. By increasing the value of n_{SH}, the finite-key rates approach the asymptotic scenario. Also, K_∞ with $\eta_{\mathrm{c,d}} = 100\%$ provides a clear upper bound for the achievable secret key rate with the security analysis introduced in Sec. IV B.

Figures 3(a) and 3(b) further show, as expected, that in the case of ideal sources the ESR architecture outperforms the PQA architecture also in the presence of channel loss.

As a final remark, we note that if Bob did not use a qubit amplifier, then the maximum possible value of Λ would be very limited. Indeed, it can be shown that in the case of ideal sources, and even if one sets $\eta_{\mathrm{c,d}} = 100\%$ and $n_{\mathrm{SH}} \to \infty$, the maximum value of Λ is as low as $\Lambda \lessapprox 0.7$ dB. See the Supplementary Information for further details.

Time constraints. In the discussion so far, we have not considered the duration of a DIQKD session, which is another crucial experimental parameter. Indeed, this parameter imposes strong restrictions on the loss that DIQKD can tolerate. We study it in this section.

According to the protocol described earlier, the post-processing block size, n_{SH}, is fixed a priori. This means, in particular, that the number of transmitted signals, N, and thus the duration of the distribution step of the protocol, which we shall denote by τ, are random variables. Their mean values are given by Eq. (4) and $\langle \tau \rangle = \nu \langle N \rangle$, respectively, where ν represents the clock rate of system. From Eq. (4) we have that, for a given n_{SH}, the value of $\langle N \rangle$ increases when the success probability of the qubit amplifier decreases, for instance, due to channel and/or

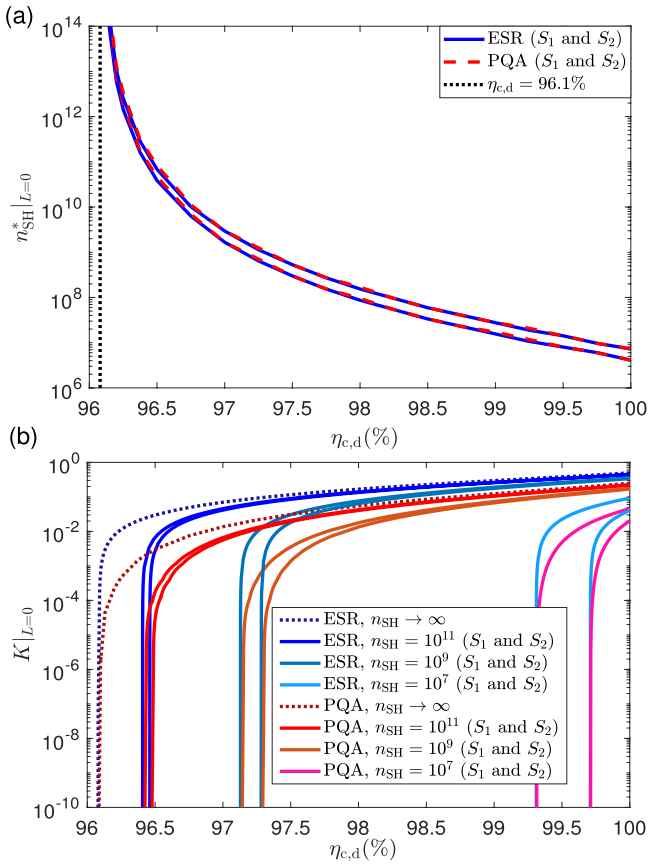

Figure 2. Performance evaluation of DIQKD with ideal photon sources at $L = 0$ km, for the setup given in Fig. 1. Bluish (reddish) lines are used for the ESR (PQA) architecture. (**a**) Minimum value of the detection and coupling efficiency, $\eta_{c,d}$, and minimum value of the block size, n_{SH}, required to obtain a zero-distance secret key rate $K|_{L=0} \geq 10^{-10}$. Both sets of security requirements, S_1 and S_2, are compared for each qubit amplifier. Any combination of parameters $\eta_{c,d}$ and n_{SH} must be above the lower (upper) lines to achieve a secret key rate above the threshold value with the security requirements given by the sets S_1 (S_2). The dotted black vertical line indicates the (asymptotic) minimum efficiency, $\eta_{c,d} \approx 96.1\%$, which is the smallest detection efficiency that delivers a zero-distance asymptotic secret key rate $K_\infty|_{L=0} \geq 10^{-10}$. (**b**) Zero-distance secret key rate, $K|_{L=0}$, as a function of $\eta_{c,d}$ for various values of the block size n_{SH}. For each qubit amplifier, four different block sizes are considered: $n_{SH} \to \infty$, $n_{SH} = 10^{11}$, $n_{SH} = 10^{9}$ and $n_{SH} = 10^{7}$. The finite secret key rates appear in pairs of solid lines, one for the security set S_1 (upper line) and another one for the security set S_2 (lower line). The asymptotic secret key rates corresponding to $n_{SH} \to \infty$ are illustrated with dotted lines.

detection loss. Indeed, according to Eqs. 5 and 6) we find that $\langle N \rangle$ at $L = 0$ km, which we will denote by $\langle N \rangle|_{L=0}$, is, in the case of an ESR, equal to

$$\langle N \rangle|_{L=0} = \frac{2n_{SH}}{\eta_{c,d}^2}, \tag{7}$$

while in the case of a PQA it satisfies

$$\begin{aligned} \langle N \rangle|_{L=0} &= \frac{n_{SH}}{(1-t)\eta_{c,d}^4[1-\eta_{c,d}^2(1-t)]} \\ &\approx \frac{n_{SH}}{(1-t)\eta_{c,d}^4}. \end{aligned} \tag{8}$$

This is illustrated in Fig. 4, which shows $\langle N \rangle|_{L=0}$ as a function of $\eta_{c,d}$ when $n_{SH} = \{10^7, 10^9, 10^{11}\}$. From Fig. 4 we find that the value of $\langle N \rangle|_{L=0}$ associated to the PQA presents a much steeper slope than that of the ESR architecture when $\eta_{c,d}$ decreases. This is because the optimal transmittance t of the PQA approaches 1 in that regime.

In the scenario where $L > 0$ km, the success probability of the qubit amplifier decreases exponentially with the channel loss. In particular, we find that the value of $\langle N \rangle|_{L\geq 0}$ in this case is given by

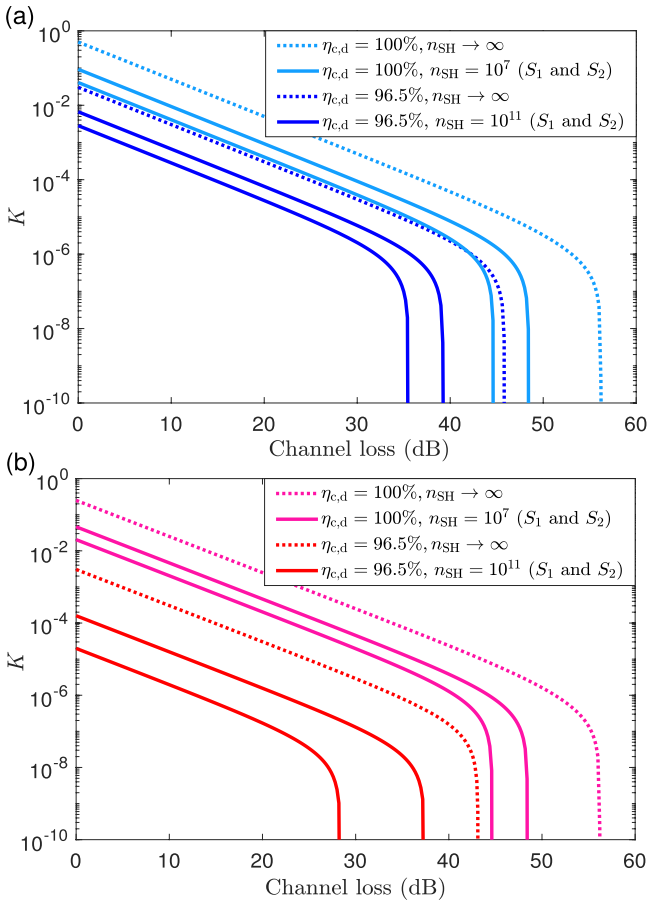

Figure 3. Secret key rate K as a function of the overall channel loss Λ measured in dB for the case of ideal photon sources. The considered setup is again that of Fig. 1. (**a**) Corresponds to the ESR architecture and (**b**) to the PQA architecture. In both figures, we use two different detection and coupling efficiencies, $\eta_{c,d} = 100\%$ and $\eta_{c,d} = 96.5\%$, each of them tagged with a different color. For each value of the efficiency, we plot the asymptotic secret key rate K_∞ (dotted line), together with two finite-key rates for different values of n_{SH} (solid lines). Each finite-key rate is plotted twice, the upper (lower) line corresponding to the security settings S_1 (S_2), and in both cases a common block size n_{SH} close to the critical one is assumed (see Fig. 2(a)). More precisely, we take $n_{SH} = 10^7$ when $\eta_{c,d} = 100\%$ and $n_{SH} = 10^{11}$ when $\eta_{c,d} = 96.5\%$. By increasing the value of $\eta_{c,d}$ and/or n_{SH} the finite-key rates approach those of the optimal scenario, which corresponds to K_∞ assuming $\eta_{c,d} = 100\%$.

$$\langle N\rangle|_{L\geq 0} = \frac{2n_{SH}}{\eta_{c,d}^2}\{(1-4p_d)\eta_{ch}\eta_{c,d}^2 + 4p_d[1+\eta_{ch}(1-2\eta_{c,d}^2)]\}^{-1}, \quad (9)$$

for the ESR architecture, and

$$\langle N\rangle|_{L\geq 0} = \frac{n_{SH}}{\eta_{c,d}^2[1-\eta_{c,d}^2(1-t)]}\{(1-10p_d)(1-t) \times \eta_{ch}\eta_{c,d}^2 + 4p_d(1-t+\eta_{ch}/2)\}^{-1}, \quad (10)$$

for the PQA. In these two equations, for simplicity, the success probability P_{SH} is computed to the first order in p_d.

We recall that Fig. 3 shows the overall channel loss that Alice and Bob can tolerate before the secret key rate drops down to zero, and which secret key rates they can attain depending on the channel loss. This information is complemented by Table 3, which, for every finite block size curve in the figure, tells us the value of $\langle N\rangle|_{L>0}$ required at the extreme channel loss where the key rate starts dropping down to zero. These values are easily translated into time constraints, and they are quite large from a practical point of view. Indeed, if one considers, for example, that the clock rate of the system is, say, 10 GHz, we find that when $\eta_{c,d} = 96.5\%$ it would take about 2.1 (37.0) days to establish a secret key of length 7.56×10^7 (8.64×10^7) bits—out of a block size $n_{SH} = 10^{11}$—over a channel loss of 39 dB (37 dB) when using the ESR (PQA) architecture and the security settings given by S_1. Of course, the result improves when $\eta_{c,d}$ increases. For instance, if $\eta_{c,d} = 100\%$ then it would take of the order of

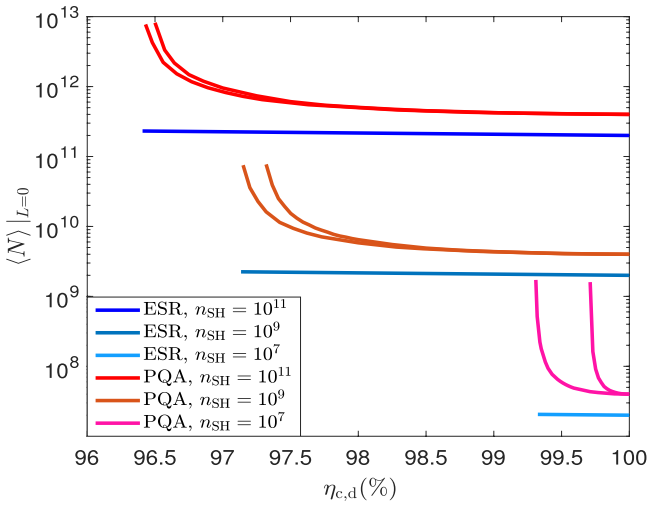

Figure 4. Average number of signals, $\langle N\rangle|_{L=0}$, that Alice needs to send Bob to collect a data block size equal to $n_{\rm SH}$ when using ideal photon sources, as a function of the detection and coupling efficiency $\eta_{\rm c,d}$ at $L = 0$ km. As in Eqs. 5 and 6), in this figure we disregard dark counts because their effect at $L = 0$ km is negligible. Also, we set the free experimental and security parameters to those values that optimise the secret key rate given by Fig. 2(b). The figure considers three different data block sizes, *i.e.*, $n_{\rm SH} = 10^7$, $n_{\rm SH} = 10^9$ and $n_{\rm SH} = 10^{11}$. All the plots are cut at the value of $\eta_{\rm c,d}$ for which the resulting secret key rate is below the threshold value of 10^{-10}. We note that, since in the case of the ESR the value of $\langle N\rangle|_{L=0}$ does not depend on any parameter to be optimised, the cases S_1 and S_2 only differ in the minimum $\eta_{\rm c,d}$ that still provides $K \geq 10^{-10}$, which can be extracted from Fig. 2. In the case of the PQA, $\langle N\rangle|_{L=0}$ depends on the transmittance t to be optimised, and therefore the cases S_1 and S_2 differ more from each other.

120 (250) seconds to establish a secret key of length 1.56×10^5 (1.58×10^5)—out of a block size $n_{\rm SH} = 10^7$—over 48 dB when using the ESR (PQA) architecture and the security settings given by S_1. These particular examples are given to illustrate the maximum duration of a DIQKD session, but the duration of a session with arbitrary values of $n_{\rm SH}$, $\eta_{\rm c,d}$ and L can be computed directly from Eqs. (9) and (10).

Generic sources. In this section we investigate the effect that vacuum pulses and multiple photon pairs, generated by practical entanglement sources, have on the performance of DIQKD. For concreteness, and also motivated by the results of the previous subsection, we focus on the ESR architecture for the qubit amplifier at Bob's lab, and we consider entanglement sources ρ_{ab} and ρ_{bc} (as in Fig. 1) that generate a coherent superposition of bipartite entangled states written as

$$|\psi\rangle_{ab} = \sqrt{p_0}\,|\varphi_0\rangle_{ab} + \sqrt{p_1}\,|\varphi_1\rangle_{ab} + \sqrt{p_2}\,|\varphi_2\rangle_{ab}, \tag{11}$$

where p_n, with $n \leq 2$ and $p_0 + p_1 + p_2 = 1$, stands for the probability of generating a $2n$-photon entangled state of the form

$$|\varphi_n\rangle_{ab} = \frac{1}{n!\sqrt{n+1}}(a_{\rm h}^\dagger b_{\rm v}^\dagger - a_{\rm v}^\dagger b_{\rm h}^\dagger)^n|0\rangle_{ab}. \tag{12}$$

In Eq. (12), $|0\rangle_{ab}$ is the vacuum state and $a_{\rm h}^\dagger$ and $a_{\rm v}^\dagger$ ($b_{\rm h}^\dagger$ and $b_{\rm v}^\dagger$) denote, respectively, the creation operators of horizontally and vertically polarised photons at the spatial mode a (b). Remarkably, we set $p_n = 0$ for $n \geq 3$ in Eq. (11). The underlying assumption is that the effect of multiple photon pairs is properly encompassed by the effect of double photon pairs, which is supported by our numerical simulations. A particular example of entanglement sources that sticks to the structure given by Eq. (12) are the parametric down conversion (PDC) sources[42,43], and a thorough analysis of their performance for DIQKD is given in the Supplementary Information (considering a contribution of up to $n = 3$ photon pairs). There, we show that PDC sources do not seem to be suitable for DIQKD, especially in the long-distance regime, since they require really long DIQKD sessions and deliver very low secret key rates.

For the evaluation of an entanglement source subject to Eq. (11), we characterise the photon-number statistics by means of two parameters alone: the probability p_0 of emitting vacuum, and the ratio $q = p_2/p_1$ between the probability of emitting a double photon pair and that of emitting a single photon pair. Of course, if one considers a practical entanglement source, the photon-number statistics p_n cannot be controlled separately, but they typically depend on an intensity parameter. For instance, in the case of PDC sources, we have that p_n is fixed for all n once we set the value of p_0 (or, equivalently, the intensity of the source), and in the low intensity regime the double-to-single photon pair ratio reads $q_{\rm PDC} = p_2/p_1 \approx (1 - p_0 - p_1)/p_1 = (p_0^{-1/2} - 1)(p_0^{-1/2} + 2)/2$. The case

S_1	$\eta_{c,d}$	n_{SH}	Λ_{cutoff}	K_{cutoff}	$\langle N \rangle$
ESR	100%	10^7	48 dB	1.3×10^{-7}	1.2×10^{12}
ESR	96.5%	10^{11}	39 dB	4.2×10^{-8}	1.8×10^{15}
PQA	100%	10^7	48 dB	6.3×10^{-8}	2.5×10^{12}
PQA	96.5%	10^{11}	37 dB	2.7×10^{-9}	3.2×10^{16}
S_2	$\eta_{c,d}$	n_{SH}	Λ_{cutoff}	K_{cutoff}	$\langle N \rangle$
ESR	100%	10^7	44 dB	2.1×10^{-7}	5.0×10^{11}
ESR	96.5%	10^{11}	35 dB	9.8×10^{-8}	7.2×10^{14}
PQA	100%	10^7	44 dB	1.0×10^{-7}	9.9×10^{11}
PQA	96.5%	10^{11}	28 dB	2.4×10^{-9}	4.0×10^{15}

Table 3. Average number of signals, $\langle N \rangle$, that Alice needs to send Bob to collect a data block size equal to n_{SH}, when using ideal photon sources and setting the channel loss to the cutoff value for which the secret key rate starts dropping down to zero in Fig. 3. The dark count rate of the photodetectors is set to $p_d = 10^{-7}$, and the detection and coupling efficiency is $\eta_{c,d}$. The considered combinations of $\eta_{c,d}$ and n_{SH} correspond to the cases illustrated in Fig. 3, and both sets of security settings, S_1 and S_2, are considered.

of ideal sources, on the other hand, corresponds to $p_0 = p_2 = 0$ and thus $q = 0$. Due to the poor performance of PDC sources when used for DIQKD (see the Supplementary Information), below we consider combinations of (p_0, q) that satisfy $0 \leq q < q_{PDC}$ for the corresponding $p_0 > 0$. In doing so, we investigate an intermediate scenario between the photon number statistics of ideal sources and those of PDC sources.

We remark, however, that the Supplementary Information includes a full mode analysis, both for the ESR and PQA architectures, which allows the evaluation of any desired photon number distribution for the different light sources, including the contribution of up to any wanted number of photon pairs per source.

The results for the simplified scenario discussed above are illustrated in Fig. 5, which shows the secret key rate as a function of the channel loss Λ for $n_{SH} = 10^9$ and the security requirements given by S_1. Regarding the detector and coupling efficiency, we use $\eta_{c,d} \in \{100\%, 98.7\%\}$. Note that the value $\eta_{c,d} = 96.5\%$ is not used here, as it is too close to the threshold efficiency with ideal sources. Instead, we choose $\eta_{c,d} = 98.7\%$, which in turn allows to simplify the comparison between this case and the one based on PDC sources in the Supplementary Information. For each value of $\eta_{c,d}$, we plot three different cases. The first (second) case, assumes that the entanglement source ρ_{bc} (ρ_{ab}) is an ideal entanglement source, while ρ_{ab} (ρ_{bc}) is characterised by the parameters (p_0, q). The third case considers that both ρ_{bc} and ρ_{ab} are characterised by the parameters (p_0, q), which, for simplicity, we assume are the same for both sources. In general, though, the optimal intensity for each source will depend of the value of the channel loss. In each figure, we evaluate two possible values for p_0: $p_0 = 0.5$ (solid lines) and $p_0 = 0.9$ (dotted lines). Also, we consider four different values for the parameter $q \in \mathcal{Q} = \{0, 10^{-2}, 10^{-1.5}, 10^{-1}\}$.

In all the plots within Fig. 5, if one compares the solid lines with the dotted lines, we observe that reducing the value of the probability p_0 for a fixed value of q basically leads to a rigid increase of the secret key rate (*i.e.*, an increase by a constant factor that keeps the slope of the curve in logarithmic scale). This is so because vacuum signals rarely lead to false heralding flags in the qubit amplifier: if ρ_{ab} (ρ_{bc}) emits a vacuum state, it is necessary that either ρ_{bc} (ρ_{ab}) emits more than one photon pair or that at least one dark count takes place at the detectors within the qubit amplifier in order to have a (spurious) successful heralding event. As a consequence, to a good extent, p_0 mainly affects the pre-factor P_{SH}, but not the conditional secret key rate, $K|_{SH}$. The greater the value of p_0, the smaller the value of P_{SH}, and thus the secret key rate rigidly decreases.

On the other hand, for a fixed value of p_0, increasing q significantly affects $K|_{SH}$, so that multiple photon pairs are responsible for the changing slope of the secret key rate as well as for the position of the cutoff point where the secret key rate starts dropping down to zero, as shown in Fig. 5. This is so because multiple photon pairs lead to spurious heralding events that limit the utility of the qubit amplifier, and, as expected, this effect is amplified when the detection and coupling efficiency $\eta_{c,d}$ decreases. In this regard, we also note that the performance of DIQKD seems to be more robust to the presence of multiple photon pairs in ρ_{ab} than in ρ_{bc}. The reason goes as follows. Multi-photons arising from ρ_{ab} need to undergo a lossy channel, but multi-photons from ρ_{bc} do not. Therefore, the latter are more likely to trigger a spurious success at the qubit amplifier when the input from the channel is a vacuum signal. Actually, from Fig. 5 we observe that the curves with an ideal source ρ_{bc}, and ρ_{ab} characterised with $q = 10^{-2}$ or $10^{-1.5}$ are relatively close to the curve corresponding to $q = 0$. This is so because the cutoff points of these curves at the high loss regime are due to the dark counts of the detectors at the qubit amplifier, as in the case $q = 0$, and not to the presence of multiple photon pairs in ρ_{ab}. On the contrary, all the curves with an ideal source ρ_{ab}, and ρ_{bc} characterised with a nonzero q, show an early cutoff point induced by the multiple photon pairs in ρ_{bc}.

Furthermore, we note that the cutoff points match for $p_0 = 0.5$ and $p_0 = 0.9$ if they are caused by the presence of multiple photon pairs, but they do not match if they are caused by the dark counts of the detectors. This is so because, in the former case, the cutoff point is roughly determined by the double-to-single photon pair ratio (*i.e.*, by the parameter q), while in the latter case it is determined by the dark count to single photon pair ratio, which is different for each curve. Either way, Fig. 5 suggests that the noise induced by multiple photon pairs generated by the sources, particularly those generated by the sources within the qubit amplifier, seems to be the major challenge to achieve long-distance DIQKD with the considered setup.

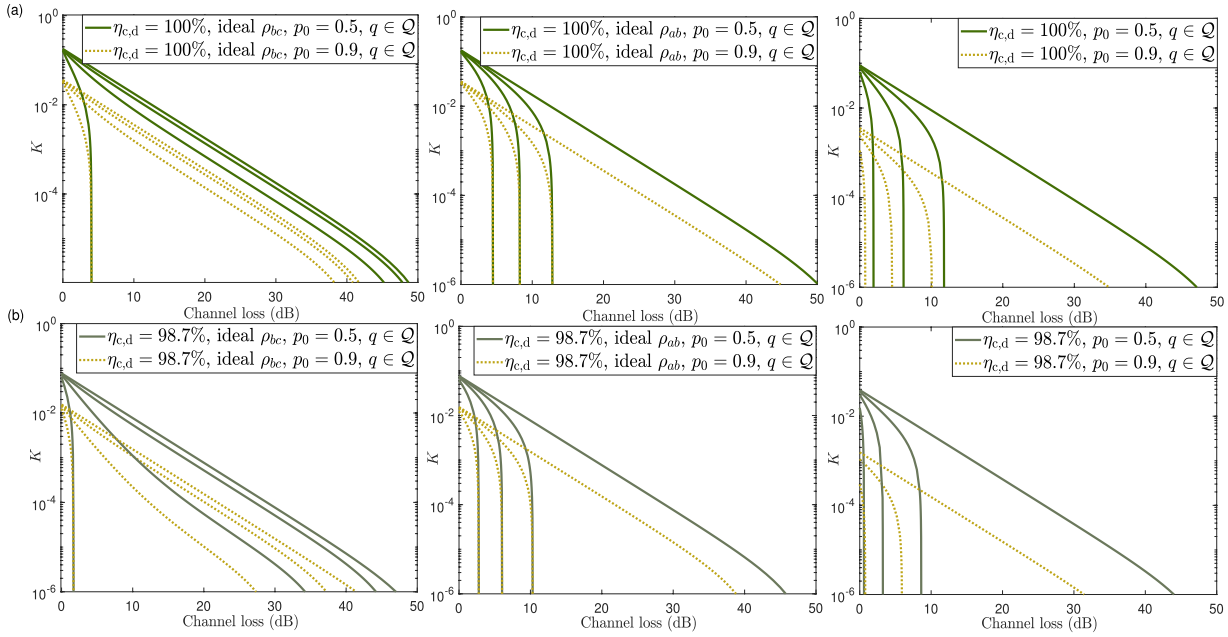

Figure 5. Secret key rate K as a function of the overall channel loss Λ measured in dB for generic photonic sources and assuming the ESR architecture. (**a**) considers a detection and coupling efficiency $\eta_{c,d} = 100\%$ and (**b**) considers $\eta_{c,d} = 98.7\%$. Each figure evaluates three different cases. The first (second) case, assumes that the entanglement source ρ_{bc} (ρ_{ab}) is an ideal entanglement source, while ρ_{ab} (ρ_{bc}) is characterised by the parameters p_0 and $q = p_2/p_1$. The third case considers that both ρ_{bc} and ρ_{ab} are characterised by the parameters p_0 and $q = p_2/p_1$. All figures consider two possible values for p_0, *i.e.*, $p_0 = 0.5$ (solid lines) and $p_0 = 0.9$ (dotted lines), and four different values for the parameter $q \in \mathcal{Q} = \{0, 10^{-2}, 10^{-1.5}, 10^{-1}\}$. Also, for concreteness, in all cases we set $n_{SH} = 10^9$ and choose the security settings S_1.

This effect is investigated further in Fig. 6, where we plot an upper bound on the maximum value of the parameter q, which we denote by q_{max}, to achieve $K \geq 0$ with $\langle N \rangle \leq 10^{15}$, as a function of the channel loss Λ. For this, we assume that the source ρ_{ab} is an ideal source and we parametrise the source ρ_{bc} with the quantity q. Note that since here we use the condition that the secret key rate is strictly greater than zero, we can set $p_0 = 0$ for ρ_{bc} as well. This is so because, as already explained, setting $p_0 > 0$ simply translates into a rigid decrease of the secret key rate, thus not affecting the value of q_{max}. That is, we define $q_{max} = \min_{p_1}\{(1 - p_1)/p_1 | K \geq 0\}$. For illustration purposes, we consider the extreme cases $\eta_{c,d} = 100\%$ and $\eta_{c,d} = 96.5\%$ again, and in addition we set $p_d = 0$ in order to investigate the limitations imposed by the noise due to multiple photon pairs alone. In this scenario, Fig. 6 suggests that, irrespectively of the block size n_{SH}, the value of the detector efficiency $\eta_{c,d}$ and the security settings, the double-to-single photon pair ratio q severely restricts the maximum distance that is achievable with DIQKD. Moreover, note that in a realistic situation with a non-ideal ρ_{ab}, q_{max} would be lower than the value shown in Fig. 6. The vertical cutoffs in the graphs indicate the points where $\langle N \rangle \approx 10^{15}$, as this value is already probably too large for a QKD session today. Since q_{max} is very small at these cutoff points, the corresponding values of Λ are very close (indistinguishable to our numerical precision) to those of the case $q = 0$, which are given by

$$\Lambda = 150 - 10\log_{10}\left(\frac{2n_{SH}}{\eta_{c,d}^4}\right) \tag{13}$$

for the different pairs $(\eta_{c,d}, n_{SH})$. This expression is directly obtained from Eq. (9) assuming $p_d = 0$. As a final remark, note that one might achieve a source whose parameter $q < q_{max}$ for a given distance by simply decreasing the intensity of the source. Indeed, this is the case, for example, of PDC sources, where one can reduce λ and thus q at the price of significantly increasing the probability p_0 of emitting vacuum. While this might provide a positive key rate according to Fig. 6 (by assuming still that ρ_{ab} is an ideal source), the resulting secret key rate might be probably too low to be practical because the probability of having a successful heralding event would be very low. The situation gets worse in the presence of dark counts.

Discussion

Device independence is a desirable feature for quantum key distribution (QKD) to ultimately defeat quantum hacking. However, it comes at a high price, in terms of achievable performance and required resources. Indeed, long distance device-independent QKD (DIQKD) requires the use of heralding devices, like for instance qubit amplifiers, which can herald the arrival of a photon and thus decouple channel loss from the measurement settings selection.

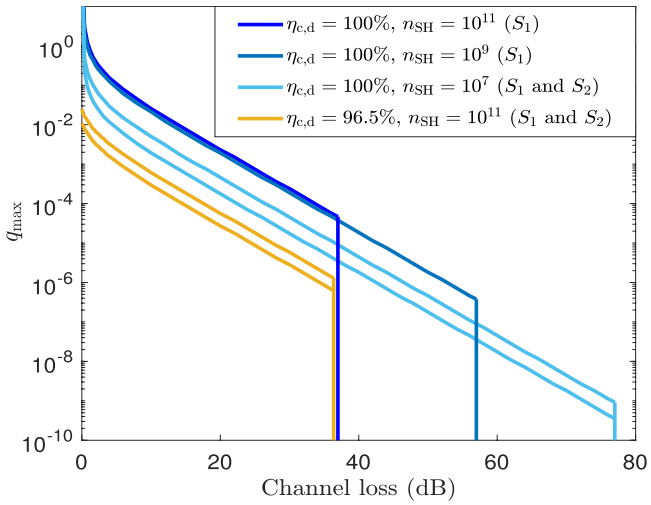

Figure 6. Upper bound on the maximum double-to-single photon pair ratio $q_{\max}$ of the entanglement source ρ_{b_c} required to achieve $K \geq 0$ with $\langle N \rangle \leq 10^{15}$, as a function of the channel loss Λ. Here, we set $p_d = 0$, so that the multiphotons generated in the qubit amplifier are the only source of noise in the system. The bluish lines use coupling and detection efficiency $\eta_{c,d} = 100\%$ and they include the block sizes $n_{SH} = 10^{11}, 10^{9}$ and 10^{7}, while the yellow lines use $\eta_{c,d} = 96.5\%$ and they only include the case $n_{SH} = 10^{11}$. This is so because $n_{SH} = 10^{9}$ and $n_{SH} = 10^{7}$ do not deliver a positive secret key rate for $\eta_{c,d} = 96.5\%$. Also, for each pair $(\eta_{c,d}, n_{SH})$, the graphs corresponding to both sets of security settings, S_1 and S_2, are included whenever they are significantly different. Otherwise, we only plot that of S_1 for simplicity. The vertical cutoffs in the graphs indicate the points where $\langle N \rangle \approx 10^{15}$. As expected, when $\eta_{c,d}$ decreases the value of $q_{\max}$ decreases as well.

In this work, we have investigated all-photonic DIQKD assisted by two general types of qubit amplifiers—entanglement swapping relays and polarization qubit amplifiers—in the finite-key regime. In doing so, we have quantified some crucial experimental parameters that are essential to achieve DIQKD over practical distances and within a reasonable time frame of signal transmission. This includes, for example, the minimum value of the detection efficiency of the photodetectors and the quality of the entanglement light sources, in terms of their vacuum and multi-photon contributions. In this regard, we have shown that, even if perfect entanglement sources and photon-number-resolving detectors were available, the ability to achieve large enough violations of a loophole-free CHSH test within a DIQKD session of a reasonable time duration already imposes very strong restrictions on the minimum detection efficiency ($\gtrsim 96.5\%$), which further increases quickly with the length of the transmission link. Similarly, we have shown that multi-photon pulses emitted by practical entanglement sources have a severe effect on the performance of DIQKD assisted by qubit amplifiers, as multiple photon pairs lead to spurious heralding events that strongly decrease the conditional secret key rate.

Altogether, our results suggest that the possibility of implementing optical DIQKD over long distances using the considered qubit amplifier architectures is probably quite far-off, as it seems to require a significant improvement of our current experimental capabilities.

Methods

Device models. In this section we briefly introduce the mathematical models that we used to derive the results exposed in Sec. II These models describe the main optical devices employed in a photonic implementation of a DIQKD setup, together with the behaviour of a typical lossy quantum channel.

Photodetectors. We consider that Alice and Bob have photon-number-resolving (PNR) detectors at their disposal, which are able to count the number of photons contained in each incoming optical pulse. In the relevant regime of low noise, they can be described by a positive operator valued measure (POVM) with the following elements:

$$\Pi_k = \begin{cases} (1 - p_d)\widetilde{\Pi}_0 & \text{if } k = 0, \\ (1 - p_d)\widetilde{\Pi}_k + p_d \widetilde{\Pi}_{k-1} & \text{if } k \geq 1, \end{cases} \tag{14}$$

where the quantity p_d stands for the dark count rate of the photodetectors, which is, to a good approximation, independent of the incoming signals. On the other hand, the operators $\widetilde{\Pi}_k$ that appear in Eq. (14), with $k \in \mathbb{N}$, are given by

$$\widetilde{\Pi}_k = \sum_{j=k}^{\infty} \binom{j}{k} \eta_d^k (1 - \eta_d)^{j-k} |j\rangle\langle j|, \tag{15}$$

with η_d denoting the detection efficiency of the detectors, and where $|j\rangle$ stands for a Fock state with j photons.

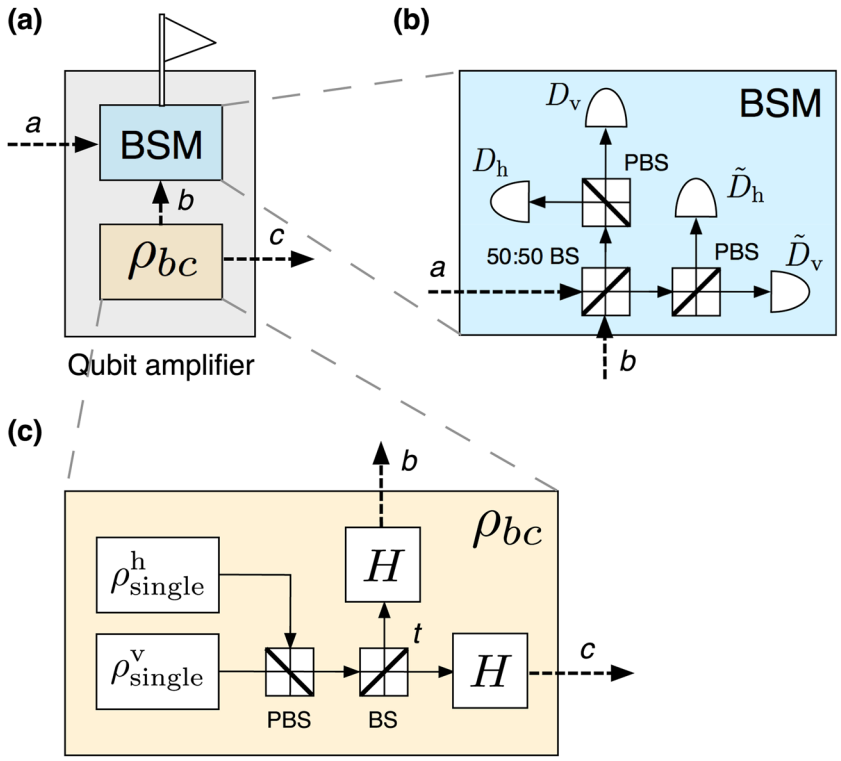

Figure 7. (**a**) Working principle of an heralded qubit amplifier based on teleportation[34–36]. A successful heralding is indicated with a flag. It notifies that a photon at the input port, a, of the qubit amplifier was teleported to a photon at its output port, c. For this, the qubit amplifier first generates a bipartite entangled state, ρ_{bc}, and then measures the signals in modes a and b with a BSM. In doing so, the state of the photon at mode a is teleported to that at mode c up to a unitary rotation. The only difference between the qubit amplifiers proposed in[34–36] is the mechanism to generate the entangled states ρ_{bc}. See the main text for further details. (**b**) Linear-optics BSM. The input states in modes a and b interfere at a 50:50 beamsplitter (BS). A polarizing BS (PBS) located at each output port of the BS separates vertically and horizontally polarised photons. Here we shall assume that all detectors are PNR detectors. A successful BSM corresponds to detecting two photons with orthogonal polarizations, *i.e.*, only when exactly two detectors record one input photon each for any of the following photodetector pairs: $(D_{\rm h}, D_{\rm v})$, $(D_{\rm h}, \widetilde{D}_{\rm v})$, $(\widetilde{D}_{\rm h}, D_{\rm v})$ or $(\widetilde{D}_{\rm h}, \widetilde{D}_{\rm v})$. (**c**) Scheme introduced in[35] to generate ρ_{bc}. A light source emits horizontally (vertically) polarised single-photons $\rho^{h}_{\rm single}$ ($\rho^{v}_{\rm single}$), which interfere at a PBS and then go through a BS of tunable transmittance t. Two Hadamard gates, denoted by H in the figure, are used to avoid (if one disregards noise effects) that input vacuum signals at mode a can produce a successful heralding flag when the BSM is that given by (**b**).

We remark that the mathematical model given by Eq. (14) assumes, for simplicity, that dark counts can only increment by one unit the number of photons observed in a given pulse. That is, if an optical pulse contains, say, k photons, we assume that the measurement outcome is at most $k + 1$ photons due to the dark counts, but not greater than this. This is a fair approximation given that $p_{\rm d}$ is sufficiently low, which indeed is typically the case in practice.

Heralded qubit amplifiers. To achieve long-distance DIQKD, we assume that Alice and Bob use heralded qubit amplifiers[34–36] to notify them the arrival of a photon before they select their measurement settings. That is, only after the qubit amplifier confirms that a photon has arrived, Alice (Bob) selects the measurement and measures the photon. If no successful heralding takes place, the optical pulse is simply discarded.

Typical qubit amplifiers consist in a teleportation gate[44]. That is, a successful heralding occurs when the state of the arriving photon is teleported to a photon at the output port of the qubit amplifier. The general mechanism is depicted in Fig. 7(a), while Fig. 7(b) shows the standard linear-optics BSM used by the qubit amplifiers introduced in[34–36] to teleport the input photon. More efficient BSMs exist[45,46] and could be used here as well, although they require complicated entangled ancilla states. Depending on the mechanism used to generate the bipartite entangled states, ρ_{bc}, illustrated in Fig. 7(a), one can distinguish two types of qubit amplifiers: polarization qubit amplifiers (PQAs)[34,35] and entanglement swapping relays (ESRs)[36].

PQAs, first introduced in[34] based on the seminal work reported in[47], typically employ practical single-photon sources to generate ρ_{bc}. For instance, the PQA proposed in[35] uses the linear-optics circuit shown in Fig. 7(c) for this purpose, where $\rho^{\rm h}_{\rm single}$ ($\rho^{\rm v}_{\rm single}$) represents the state of a single-photon pulse prepared in horizontal (vertical) polarization. In the ideal case of perfect single-photon sources and unit detection and coupling efficiencies, it is straightforward to show that the circuit given by Fig. 7(c) generates states $\rho_{bc} = |\varphi\rangle_{bc}\langle\varphi|$ with

$$|\varphi\rangle_{bc} = (1-t)|\psi\rangle_{bb} + t\,|\phi\rangle_{cc} - \sqrt{2t(1-t)}\;|\chi\rangle_{bc}, \tag{16}$$

where the parameter t is the transmittance of the tunable beamsplitter (BS) illustrated in Fig. 7(c), and the states $|\psi\rangle_{bb}$, $|\phi\rangle_{cc}$, and $|\chi\rangle_{bc}$ have the form

$$\begin{aligned} |\psi\rangle_{bb} &= \frac{1}{2}(b_{\mathrm{h}}^{\dagger 2} - b_{\mathrm{v}}^{\dagger 2})|0\rangle_b, \\ |\phi\rangle_{cc} &= \frac{1}{2}(c_{\mathrm{h}}^{\dagger 2} - c_{\mathrm{v}}^{\dagger 2})|0\rangle_c, \\ |\chi\rangle_{bc} &= \frac{1}{\sqrt{2}}(b_{\mathrm{h}}^{\dagger}c_{\mathrm{h}}^{\dagger} - b_{\mathrm{v}}^{\dagger}c_{\mathrm{v}}^{\dagger})|0\rangle_{bc}. \end{aligned} \tag{17}$$

In Eq. (17), the states $|0\rangle_b$, $|0\rangle_c$ and $|0\rangle_{bc}$ denote the vacuum states of the corresponding modes. The expression for the output states of the PQA in the practical scenario with non-ideal sources and non-unit detector and coupling efficiencies can be found in the Supplementary Information.

Let us continue assuming, for simplicity and for the moment, an ideal scenario where the BSM within the qubit amplifier uses perfect PNR detectors (*i.e.*, $p_{\mathrm{d}} = 0$ and $\eta_{\mathrm{d}} = 1$ in Eqs. 14 and 15) and lossless BSs. Then, from Eq. (16), it can be shown that whenever a single-photon pulse prepared in, say, the pure state $|\phi_{\mathrm{in}}\rangle_a = (\alpha a_{\mathrm{h}}^{\dagger} + \beta a_{\mathrm{v}}^{\dagger})|0\rangle_a$ (with $|\alpha|^2 + |\beta|^2 = 1$) arrives at the input port a of the qubit amplifier, a successful BSM occurs with probability $t(1-t)$. Also, in the case of a successful result, the state of the output photon at mode c (after applying an appropriate unitary transformation) is equal to $|\phi_{\mathrm{out}}\rangle_c = (\alpha c_{\mathrm{h}}^{\dagger} + \beta c_{\mathrm{v}}^{\dagger})|0\rangle_c$. That is, the state $|\phi_{\mathrm{in}}\rangle_a$ of the input photon is successfully teleported to an output photon. On the other hand, if a vacuum pulse, $|\phi_{\mathrm{in}}\rangle_a = |0\rangle_a$, arrives at the input port a of the qubit amplifier, this state can never lead to a spurious heralding event, at least in the ideal scenario. This is so because, when the BSM uses perfect PNR detectors with no dark counts, the state $|0\rangle_a\,|\varphi\rangle_{bc}$, with $|\varphi\rangle_{bc}$ given by Eq. (16), cannot produce two detection clicks associated to orthogonal polarizations if it is measured with the BSM shown in Fig. 7(b).

Finally, qubit amplifiers based on ESRs[36] directly prepare the state ρ_{bc} with practical entanglement light sources like, for example, PDC sources. Indeed, in contrast to the arguments presented in[34,48], it was shown in[36] that when this type of qubit amplifier is used in DIQKD, it can provide higher secret key rates than those achievable with the PQA introduced in[34] when using PDC sources.

Optical couplers. Our analysis in Sec. II considers a fiber-based implementation of DIQKD. Thus, we model the coupling of the photons generated by the light sources into the optical fibers by means of a BS of transmittance η_{c}. One input to the BS is the quantum signal, while the other input is a vacuum state. Similarly, one of the outputs of the BS is the optical fiber, while we assume that the other output is not accessible and represents the loss.

Quantum channel. For simplicity, we suppose that the quantum channel mainly introduces loss. That is, we disregard any noise effect due for example to polarization or phase misalignment.

The channel loss is modeled with a BS of transmittance $\eta_{\mathrm{ch}} = 10^{-\Lambda/10}$, where the parameter Λ (dB) is related to the transmission distance L (km) by an attenuation coefficient α (dB/km) via the expression $\Lambda = \alpha L$. The specific value of α depends on the considered channel. For instance, a typical value for α in the case of single-mode optical fibers in the telecom wavelength is $\alpha = 0.2$ dB/km.

Secret key length. We use the security analysis introduced in[28], which is valid against coherent attacks. Prior to the execution of the protocol, Alice and Bob agree on three parameters that tag the security of the final keys, K_{A} and K_{B}. These parameters are the secrecy parameter, ϵ_{sec}, the correctness parameter, ϵ_{cor}, and the robustness parameter, ϵ_{rob}.

In particular, a protocol is said to be ϵ_{sec}-secret, when implemented using a device D, if it satisfies

$$[1 - P(\mathrm{abort})]\,||\rho_{K_{\mathrm{A}}E} - \rho_{U_l} \otimes \rho_E||_1 \leq \epsilon_{\mathrm{sec}}, \tag{18}$$

where $P(\mathrm{abort})$ is the abortion probability of the protocol, $||\rho||_1 = \sqrt{\rho\rho^{\dagger}}$ stands for the trace norm, E is a quantum register held by the eavesdropper that may be initially correlated with D, $\rho_{K_{\mathrm{A}}E}$ is the output state of the DIQKD protocol describing Alice's key string K_{A} and the quantum register E conditioned on not aborting, $\rho_{U_l} = \sum_z \frac{1}{2^l}|z\rangle_{\mathrm{A}}\langle z\,|$ is the uniform mixture of all possible values of a l-bit string K_{A}, and $\rho_{U_l} \otimes \rho_{\mathrm{E}}$ is the perfectly secret output state.

The parameter ϵ_{sec} is upper bounded by

$$\epsilon_{\mathrm{sec}} \leq \epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{EA}}, \tag{19}$$

where $\epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{s}}$ is the total failure probability associated to the privacy amplification step, ϵ_{PA} being an upper bound on the error probability of the randomness extractor and ϵ_{s} being the smoothing parameter of the ϵ_{s}-smooth min-entropy[28]. The term ϵ_{EA} is the failure probability associated to the entropy accumulation theorem[30],

	Finite-key security parameters
ϵ_{sec}	Secrecy parameter
ϵ_{cor}	Correctness parameter
ϵ_{rob}	Robustness parameter
ϵ_{s}	Smoothing parameter of the min-entropy
ϵ_{rob}^{PE}	Abortion probability of parameter estimation
ϵ_{rob}^{IR}	Abortion probability of information reconciliation
ϵ_{rob}^{EA}	Abortion probability of entropy accumulation
ϵ_{EA}	Error probability of the entropy accumulation bound

Table 4. List containing the main finite-key security parameters.

which only guarantees that a certain lower bound on the ϵ_s-smooth min-entropy holds with a probability larger than $1 - \epsilon_{EA}$.

The correctness parameter, ϵ_{cor}, quantifies the probability that the final keys, K_A and K_B, are not equal. More precisely, a protocol is said to be ϵ_{cor}-correct if $P[K_A \neq K_B] \leq \epsilon_{cor}$. According to the protocol definition given in the previous section, we have that $\epsilon_{cor} = \epsilon_{IR}$.

Finally, a protocol is said to be ϵ_{rob}-robust for a specific honest implementation (*i.e.*, for a particular implementation where the eavesdropper does not intervene) if it aborts with a probability smaller than ϵ_{rob}. The protocol described above can only abort in two steps: the information reconciliation step, and the parameter estimation step. Therefore, we have that ϵ_{rob} satisfies

$$\epsilon_{rob} \leq \epsilon_{rob}^{IR} + \epsilon_{rob}^{PE}, \tag{20}$$

where ϵ_{rob}^{IR} (ϵ_{rob}^{PE}) is the probability of aborting at the information reconciliation (parameter estimation) step for the considered honest implementation. Moreover, we have that the quantity ϵ_{rob}^{PE} verifies

$$\epsilon_{rob}^{PE} \leq \epsilon_{rob}^{EA} + \epsilon_{IR}, \tag{21}$$

where ϵ_{rob}^{EA} is the probability of the fraction of CHSH wins, C_{SH}/n_{SH}, being lower than the threshold $\omega|_{SH}\gamma - \delta_{est}$. That is,

$$\epsilon_{rob}^{EA} = P\left(\omega|_{SH}\gamma - \frac{C_{SH}}{n_{SH}} > \delta_{est}\right). \tag{22}$$

Note that for fixed values of ϵ_{rob}^{EA} and n_{SH}, the minimum value of δ_{est} such that Eq. (22) holds satisfies[49]

$$\delta_{est} \geq \sqrt{\frac{1}{2n_{SH}}\ln\left(\frac{1}{\epsilon_{rob}^{EA}}\right)}. \tag{23}$$

Also, we note that the parameter ϵ_{IR} contributes to ϵ_{rob}^{PE} in Eq. (21) because, conditioned on not aborting the protocol in the error verification step, Bob performs the parameter estimation step by using his original bit string of outcomes, B, and his estimate, Z_B, of Alice's string, which is equal to Z_A except with probability ϵ_{IR}.

A list with the main parameters related to the security of the protocol is provided in Table 4.

Then, it turns out that, conditioned on not aborting, the DIQKD protocol presented in the Results section delivers ϵ_{cor}-correct and ϵ_{sec}-secret output keys, K_A and K_B, whose length, l, is given by

$$\begin{aligned} l \;=\; & n_{SH}(\eta_{opt} - \gamma) - 2\log 7\sqrt{1 - 2\log\left[\frac{\epsilon_s}{4}(\epsilon_{EA} + \epsilon_{IR})\right]} \\ & \times\sqrt{n_{SH}} - leak_{IR} - 3\log\left[1 - \sqrt{1 - \left(\frac{\epsilon_s}{4}\right)^2}\right] \\ & - 2\log\frac{1}{\epsilon_{PA}}. \end{aligned} \tag{24}$$

Here, the term η_{opt} represents a lower bound on the entropy generation rate of the CHSH game,

$$\eta_{opt}(\omega|_{SH}, n_{SH}, \gamma, \delta_{est}, \epsilon_s/4, \epsilon_{EA} + \epsilon_{IR}) = \max_{\frac{3}{4} < p_t < \frac{2+\sqrt{2}}{4}} \eta\left(\frac{\omega|_{SH}\gamma - \delta_{est}}{\gamma}, p_t, n_{SH}, \gamma, \epsilon_s/4, \epsilon_{EA} + \epsilon_{IR}\right), \tag{25}$$

where $\eta(p, p_t, n_{SH}, \gamma, \epsilon_1, \epsilon_2)$ has the form

$$\eta(p, p_t, n_{\mathrm{SH}}, \gamma, \epsilon_1, \epsilon_2) = f_{\min}(p, p_t) - \frac{2}{\sqrt{n_{\mathrm{SH}}}} \times \left[\log 13 + \frac{1}{\gamma}\frac{dg(p)}{dp}\Big|_{p_t}\right] \times \sqrt{1 - 2\log(\epsilon_1\epsilon_2)}. \quad (26)$$

In this equation, $f_{\min}(p, p_t)$ is given by

$$f_{\min}(p, p_t) = \begin{cases} g(p) & p < p_t \\ g(p_t) + \dfrac{dg(p)}{dp}\Big|_{p_t}(p - p_t) & p \geq p_t, \end{cases} \quad (27)$$

and the function $g(p)$ reads

$$g(p) = 1 - h\left[\frac{1}{2} + \frac{1}{2}\sqrt{16p(p-1) + 3}\right], \quad (28)$$

where the winning probability p lies in the interval $0 \leq p \leq (2 + \sqrt{2})/4$. Similarly, $h(x)$ is the binary entropy function, $h(x) = -x\log x - (1 - x)\log(1 - x)$.

On the other hand, the information reconciliation leakage term in 24, $leak_{\mathrm{IR}}$, depends not only on the expected conditional quantum bit error rate of the key rounds, $Q|_{\mathrm{SH}}$, but also on the expected conditional winning rate of the test rounds, $\omega|_{\mathrm{SH}}$. It can be written as

$$leak_{\mathrm{IR}}(Q|_{\mathrm{SH}}, \omega|_{\mathrm{SH}}, n_{\mathrm{SH}}, \gamma, \epsilon_{\mathrm{IR}}, \epsilon^{\mathrm{IR}}_{\mathrm{rob}}) = n_{\mathrm{SH}}[(1-\gamma)h(Q|_{\mathrm{SH}}) + \gamma h(\omega|_{\mathrm{SH}})] + 4\sqrt{n_{\mathrm{SH}}}\log(2\sqrt{2} + 1)\sqrt{2\log\left[\frac{8}{\epsilon'^2_{\mathrm{IR}}}\right]} + \log\left[\frac{8}{\epsilon'^2_{IR}} + \frac{2}{2 - \epsilon'_{IR}}\right] + \log\left(\frac{1}{\epsilon_{\mathrm{IR}}}\right), \quad (29)$$

where $\epsilon^{\mathrm{IR}}_{\mathrm{rob}} = \epsilon'_{\mathrm{IR}} + \epsilon_{\mathrm{IR}}$.

Recently, a slightly improved bound on the smooth min-entropy was derived for the entropy accumulation theorem[31], thus enabling an improvement of the secret key length given by Eq. (24). However, the results reported in[29,31] suggest that such improvement is small and does not probably have a significant impact in the regime of block sizes required by practical DIQKD.

Finally, in an actual execution of the protocol that required the transmission of N signals, the secret key rate is defined as

$$K = \frac{l}{N}. \quad (30)$$

We remark that, in the limit where $n_{\mathrm{SH}} \to \infty$, Eq. (30) matches the asymptotic secret key rate against general attacks reported in[17], which is given by

$$K_\infty = \lim_{n_{\mathrm{SH}}\to\infty}\frac{n_{\mathrm{SH}}\eta_{\mathrm{opt}} - leak_{\mathrm{IR}}}{N} = P_{\mathrm{SH}}\left\{1 - h\left[\frac{1}{2} + \frac{1}{2}\sqrt{16\omega|_{\mathrm{SH}}(\omega|_{\mathrm{SH}} - 1) + 3}\right] - h(Q|_{\mathrm{SH}})\right\}. \quad (31)$$

Data availability

No datasets were generated or analysed during the current study.

Received: 3 June 2019; Accepted: 5 November 2019;
Published online: 28 November 2019

References

1. Wiesner, S. Conjugate Coding. *SIGACT News* **15**, 78–88 (1983).
2. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE Int. Conf. Comp. Systems Signal Processing*, 175–179 (1984).
3. Scarani, V. *et al*. The security of practical quantum key distribution. *Reviews of Modern Physics* **81**, 1301 (2009).

4. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Reviews of Modern Physics* **74**, 145 (2002).
5. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nature Photonics* **8**, 595 (2014).
6. IdQuantique, http://www.idquantique.com.
7. Qi, B., Fung, C. H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation* **7**, 73–82 (2007).
8. Zhao, Y., Fung, C. H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A* **78**, 042333 (2008).
9. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A* **74**, 022313 (2006).
10. Lydersen, L. *et al*. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4**, 686–689 (2010).
11. Gerhardt, I. *et al*. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications* **2**, 349 (2011).
12. Weier, H. *et al*. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics* **13**, 073024 (2011).
13. Jain, N. *et al*. Device calibration impacts security of quantum key distribution. *Physical Review Letters* **107**, 110501 (2011).
14. Mayers, D. & Yao, A. C. C. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, 503–509 (1998).
15. Acín, A. *et al*. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters* **98**, 230501 (2007).
16. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications* **2**, 238 (2011).
17. Vazirani, U. & Vidick, T. Fully device-independent quantum key distribution. *Physical Review Letters* **113**, 140501 (2014).
18. Ekert, A. & Renner, R. The ultimate physical limits of privacy. *Nature* **507**, 443 (2014).
19. Miller, C. A. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM* **63**(4), 33 (2016).
20. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Physical Review Letters* **110**, 010503 (2013).
21. Curty, M. & Lo, H.-K. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *npj Quantum Information* **5**, 14 (2019).
22. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Reviews of Modern Physics* **86**, 419 (2014).
23. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika* **1**(3), 195 (1964).
24. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Physical Review Letters* **23**, 880 (1969).
25. Hensen, B. *et al*. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
26. Shalm, L. K. *et al*. A strong loophole-free test of local realism. *Physical Review Letters* **115**, 250402 (2015).
27. Giustina, M. *et al*. Significant-loophole-free test of Bell's theorem with entangled photons. *Physical Review Letters* **115**, 250401 (2015).
28. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications* **9**, 459 (2018).
29. Murta, G., van Dam, S. B., Ribeiro, J., Hanson, R. & Wehner, S. Towards a realization of device-independent quantum key distribution. *Quantum Science and Technology* (2019).
30. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. Preprint arXiv:1607.01796 (2016).
31. Dupuis, F. & Fawzi, O. Entropy accumulation with improved second-order. Preprint arXiv:1805.11652 (2018).
32. Pearle, P. M. Hidden-variable example based upon data rejection. *Physical Review D* **2**, 1418 (1970).
33. Gisin, N. & Gisin, B. A local hidden variable model of quantum correlation exploiting the detection loophole. *Physics Letters A* **260**, 323–327 (1999).
34. Gisin, N., Pironio, S. & Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Physical Review Letters* **105**, 070501 (2010).
35. Pitkanen, D., Ma, X., Wickert, R., van Loock, P. & Lütkenhaus, N. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Physical Review A* **84**, 022325 (2011).
36. Curty, M. & Moroder, T. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Physical Review A* **84**, 010304 (2011).
37. Seshadreesan, K. P., Takeoka, M. & Sasaki, M. Towards practical device-independent quantum key distribution with spontaneous parametric downconversion sources, on-off photodetectors and entanglement swapping. Preprint arXiv:1512.06876 (2015).
38. Máttar, A. *et al*. Device-independent quantum key distribution with single-photon sources. Preprint arXiv:1803.07089 (2018).
39. Minder, M. *et al*. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics* **13**(5), 334 (2019).
40. Liu, Y. *et al*. Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending. *Physical Review Letters* **123**(10), 100505 (2019).
41. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Physical Review Letters* **123**, 100506 (2019).
42. Kok, P. & Braunstein, S. L. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Physical Review A* **61**, 042304 (2000).
43. Ma, X., Fung, C. H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Physical Review A* **76**, 012307 (2007).
44. Bennett, C. H. *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters* **70**, 1895 (1993).
45. Grice, W. P. Arbitrarily complete Bell-state measurement using only linear optical elements. *Physical Review A* **84**, 042331 (2011).
46. Ewert, F. & van Loock, P. 3/4-efficient Bell measurement with passive linear optics and unentangled ancillae. *Physical Review Letters* **113**, 140403 (2014).
47. Ralph, T. C. & Lund, A. P. Nondeterministic noiseless linear amplification of quantum systems. In *AIP Conference Proceedings* **1110**(1), 155–160 (2009).
48. Sangouard, N. *et al*. Faithful Entanglement Swapping Based on Sum-Frequency Generation. *Physical Review Letters* **106**, 120403 (2011).
49. Hoeffding, W. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association* **58**, 13–30 (1963).

Acknowledgements
We thank Rotem Arnon-Friedman for very useful discussions related to the security analysis. We thank the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grants TEC2014-54898-R and TEC2017-88243-R, and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662 (project QCALL) for financial support. VZ gratefully acknowledges support from a FPU scholarship from the Spanish Ministry of Education.

Author contributions
V.Z. performed the analytical calculations and the numerical simulations, M.C. triggered the consideration of this research project, and both authors analysed the results and contributed to the writing.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information is available for this paper at https://doi.org/10.1038/s41598-019-53803-0.

Correspondence and requests for materials should be addressed to V.Z.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.