Satellite-Based Quantum Key Distribution in the Presence of Bypass Channels

Masoud Ghalaii,[1,*] Sima Bahrani,[2] Carlo Liorni,[3] Federico Grasselli,[3] Hermann Kampermann,[3] Lewis Wooltorton,[2,4,5] Rupesh Kumar,[6,7] Stefano Pirandola,[8] Timothy P. Spiller,[6,7] Alexander Ling,[9,10] Bruno Huttner,[11] and Mohsen Razavi[1]

[1] *School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, United Kingdom*
[2] *Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom*
[3] *Institute für Theoretische Physik III, Heinrich Heine Universität, D-40225 Düsseldorf, Germany*
[4] *Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory, University of Bristol, Bristol BS8 1FD, United Kingdom*
[5] *Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom*
[6] *School of Physics, Engineering and Technology, University of York, York YO10 5DD, United Kingdom*
[7] *York Centre for Quantum Technologies, University of York, York, United Kingdom*
[8] *Department of Computer Science, University of York, York YO10 5GH, United Kingdom*
[9] *Centre for Quantum Technologies, National University of Singapore, 117543, Singapore*
[10] *Department of Physics, Faculty of Science, National University of Singapore, 117551, Singapore*
[11] *ID Quantique, Geneva, Switzerland*

(Received 20 December 2022; revised 28 April 2023; accepted 25 September 2023; published 1 November 2023)

The security of prepare-and-measure satellite-based quantum key distribution (QKD), under restricted eavesdropping scenarios, is addressed. We particularly consider cases where the eavesdropper, Eve, has limited access to the transmitted signal by Alice and/or Bob's receiver station. This restriction is modeled by lossy channels between relevant parties, where the transmissivity of such channels can, in principle, be bounded by monitoring techniques. An artifact of such lossy channels is the possibility of having *bypass* channels, those that are not accessible to Eve but that may not necessarily be characterized by the users either. This creates interesting unexplored scenarios for analyzing QKD security. In this paper, we obtain generic bounds on the key rate in the presence of bypass channels and apply them to continuous-variable QKD protocols with Gaussian encoding with direct and reverse reconciliation. We find regimes of operation in which the above restrictions on Eve can considerably improve system performance. We also develop customized bounds for several protocols in the BB84 family and show that, in certain regimes, even the simple protocol of BB84 with weak coherent pulses is able to offer positive key rates at high channel losses, which would otherwise be impossible under an unrestricted Eve. In this case, the limitation on Eve would allow Alice to send signals with larger intensities than the optimal value under an ideal Eve, which effectively reduces the effective channel loss. In all these cases, the part of the transmitted signal that does not reach Eve can play a nontrivial role in specifying the achievable key rate. Our work opens up new security frameworks for spaceborne quantum communications systems.

DOI: 10.1103/PRXQuantum.4.040320

I. INTRODUCTION

Satellite-based quantum communications links [1–12] can be part of a global solution to quantum key distribution (QKD) networks or, more generally, the quantum Internet [13–16]. QKD provides two parties with a secret key that can be used in cryptographic protocols, such as one-time pad encryption. In the absence of practical quantum repeaters, however, point-to-point fiber-based QKD links are often limited to a distance of several hundred kilometers [17–21]. In contrast, free-space QKD relying on ground-to-satellite, satellite-to-ground, and/or satellite-to-satellite quantum communications links can potentially offer secure key exchange over thousands of kilometers [22,23]. The successful launch of the Chinese QKD satellite in 2017 and the experiments carried out since then [22–25] have particularly been a game changer in bringing

*m.ghalaii@leeds.ac.uk

the field into a new exciting development phase, while a substantial global effort is being directed at finding practical solutions to the wide-scale deployment of QKD systems. That said, satellite-based quantum communications comes at an additional price for launching and operating possibly dedicated satellites, as well as with some restrictions on accessibility and the achievable key rate. This paper seeks solutions that can enhance the benefits reaped from investing in this technology by looking into relevant threat models to a line-of-sight link, as in satellite-based QKD, while maintaining the key security features of QKD systems.

To make the above vision possible, and, in particular, to deploy satellite-based QKD in large scales, certain technological challenges must be addressed. For instance, a secure satellite-based QKD system must combat loss and noise effects in the link. A satellite-to-ground link would also face additional challenges due to pointing errors and atmospheric turbulence, which impact system performance. Ultimate limits, as well as achievable rates of specific QKD protocols, have recently been investigated considering diffraction, extinction, background noise, and fading in such links [26–29]. Such analyses, as well as recent experimental demonstrations, suggest that a typical low-Earth-orbit (LEO) satellite-to-ground link could suffer around 30–40 dB of loss for a modest-size receiver telescope [22] and possibly with night operation only in order to minimize the background noise. This would imply that, under nominal security assumptions that give Eve maximum possible control over the channel, many QKD protocols may struggle to offer sufficiently high, if any, positive key rates.

The above limitations are partly because of the assumptions made in our security analysis, e.g., that the channel in its entirety is assumed to be under the control of a potential eavesdropper. Whether such an assumption is necessary and/or realistic in satellite-based QKD, which relies on line-of-sight links, needs to be scrutinized. Relaxing this assumption could open up new opportunities that have been discounted but which, if proved to be viable, could offer additional options for implementation and commercial exploitation.

With the above idea in mind, recently, several works have addressed the security of satellite-based QKD in wire-tap channels [30–32], while earlier the security of QKD in the framework of physical-layer security has been considered [33]. The work in Ref. [30] considers a passive eavesdropping scenario for a wire-tap channel [34] and compares the key rate achievable under an unrestricted Eve for several QKD protocols with alternative schemes that they refer to as photon key distribution (PKD). Overall, they observe more resilience to noise in high-loss regimes for their PKD schemes, which allows them to cover longer distances. The work in Refs. [31,32] considers the in-principle achievable key rate, in a wire-tap channel, when only one of Alice and Bob measures their signal and the other one holds onto a quantum state, on which they can, in principle, do an optimal measurement to maximize the key rate. They will then observe a boost in the key rate so long as the channel between Alice and Eve is lossier than that of Alice and Bob. In Ref. [32], the authors further claim that by considering a protected zone around Alice (the satellite) and Bob (the ground station), they can ensure that the above condition holds if the presence of an eavesdropper in orbit can be ruled out. For the latter, they will then consider some constraints on celestial mechanics to show how difficult it would be for Eve to eavesdrop in this line-of-sight link.

In this paper, we study the security of prepare-and-measure (P&M) satellite-based QKD for a restricted Eve without restricting ourselves to the case of the wire-tap channel. This allows us to consider more generic cases and takes an important step toward having a verifiable set of assumptions. In the case of the wire-tap channels considered in Refs. [31,32], it will be difficult to ensure through experimental observations that the channel is indeed a wire-tap channel or to specify the relevant channel parameters. One can potentially use monitoring techniques to rule out the possibility of having eavesdropping objects in the line-of-sight link. Even if we trust our employed monitoring technique, any such technique would, however, be bound by a certain resolution and it is still possible that they will miss objects smaller than a certain size. The potential users should then choose whether they are satisfied with these assumptions or whether, for provable security, they wish to use a full QKD protocol.

Note that the physical size of the devices an eavesdropper may have used has not been a matter of contention in conventional QKD systems. In conventional security proofs, we only care about the impact Eve may have on the quantum signals that Alice and Bob exchange and they bound the leaked information to Eve based on the observations that they make in the quantum communication part of the protocol. By introducing monitoring techniques, we are not directly measuring the quantum interactions that Eve may have with the exchanged quantum signals but, instead, we are trying to bound some classical aspects, such as the size, of Eve's apparatus. While a superpowerful Eve could, in principle, fool our monitoring system too, in practice, this would add an additional layer of complexity to Eve's attack.

In our case, the primary assumption that we make about the potential eavesdropper is on the collection efficiency of her apparatus when it comes to interacting with the transmitted signal from Alice's telescope. This collection efficiency can then be bounded based on the size of devices that Eve has employed within the line-of-sight link. The corresponding size can, in principle, be bounded using reliable monitoring techniques that can be employed in parallel to quantum signal transmission. The same argument

and methodology can be used to bound the loss between Eve and Bob.

It is interesting to note that specifying the minimum loss that Alice's signal would go through before being collected by Eve does not specify the entire channel between Alice and Bob and it is still possible that part of Alice's signal reaches Bob without going through Eve. This latter channel, which we refer to as a *bypass* channel, has a nontrivial role in the achievable key rate and one of our key contributions here is to analyze QKD security in the presence of such bypass channels. Moreover, unlike the wire-tap channel model, we can now consider scenarios where the Alice-Eve loss is lower than that of Alice-Bob. By performing the security analysis under the above conditions, we can then bound the achievable key rate for a restricted Eve using a set of assumptions that are in-principle verifiable. This turns out to offer better performance, as compared to unrestricted eavesdropping, without necessarily compromising on our security assumptions.

Note that there is a difference between "bypass" channels, to which eavesdroppers do not have access, although they may still indirectly use them to their advantage, and "side" channels, which are assumed to be fully accessible to the eavesdropper. While the issue of side channels has been considered for years in the QKD literature [35–37], the topic of bypass channels is quite new and we believe that this paper offers an intriguing formulation of this problem and then derives relevant generic and customized security bounds for the emerging settings.

The key contributions of this paper are as follows:

(i) We develop models for restricted eavesdropping the elements of which can, in principle, be characterized using monitoring techniques.
(ii) We obtain generic bounds on achievable key rates in P&M QKD setups in the presence of an uncharacterized bypass channel not accessible to Eve.
(iii) We show that, in certain practical regimes, such bounds enable continuous-variable (CV) QKD to offer positive key rates in satellite-based implementations.
(iv) We develop customized bounds for discrete-variable (DV) QKD systems that rely on photon-number channels and improve their performance under restricted eavesdropping.

The rest of this paper is organized as follows. In Sec. II, we describe our setting and the motivations behind the model we have adopted for the restricted Eve. In Sec. III, we offer some generic results applicable to QKD protocols in the presence of bypass channels. We apply these results to CV-QKD protocols, in Sec. IV, and customize them to the case of DV QKD protocols, such as BB84 [38], in Sec. V. We conclude the paper in Sec. VI with some discussions on the relevance of the results obtained and the way forward for other cases not considered in this paper.

II. GENERIC MODELS FOR RESTRICTED EAVESDROPPING

In this section, we model the key restriction that we consider in this work on potential eavesdroppers in a satellite-based QKD system. One of the distinctive features of a satellite link, as compared to a fiber link, is that it is a line-of-sight link. While it may not be possible, for a link of around 500 km of length in the LEO case, to fully monitor the channel between Alice and Bob, one can employ monitoring techniques, such as light detection and ranging (LIDAR), to detect objects of a certain minimum size along the path. In fact, the same system and the corresponding optics that are being used for tracking and acquisition purposes can also be used to detect unwanted objects along the beam. In free-space LIDAR, the power received by the detection site is proportional to the effective area of the object and scales inversely with the fourth power of the distance between the object and the LIDAR source. If the collected power is below a certain noise threshold, we cannot conclusively declare the detection of an object but we might be able, at any given distance, to set a bound on the maximum size that any undetected object may have. In fact, our preliminary calculations suggest that for a 500-km-long satellite link and for low-power LIDAR systems used at both Alice's and Bob's stations, with some nominal assumptions, the largest undetected object within the beam width of our LIDAR sources is around a few centimeters in diameter (see Appendix A). This is important because, for any effective eavesdropping activity in the P&M scenario, Eve requires (i) to somehow collect the signals transmitted by Alice or reflect them to some other collection point and/or (ii) to somehow be able to send her own signals toward Bob's receiver. In the satellite scenario, full power collection or reflection requires telescopes or optical tools of a certain size, corresponding to the beam width and manipulation of Bob's receiver might need powerful laser sources, especially if Eve's source is not fully aligned with Bob's telescope. This implies that the combination of limited-size telescopes and/or devices used in the line-of-sight link for Eve and a monitored and/or protected zone around Alice's box could restrict Eve to only receiving a fraction of what Alice has sent. This would be the first point of departure from a maximally powerful Eve. In the second case, where Eve cannot replace the channel between herself and Bob with an ideal channel, any active attack by Eve will be affected by potentially a lossy channel that the protection zone around the receiver would enforce. This could further restrict Eve in implementing her attack scenario.

In this work, we model the restrictions explained above, which can, in principle, be characterized by the employed monitoring systems, by lossy channels between Alice and Eve and between Eve and Bob. In particular, as shown in Fig. 1(a), we assume that a lossy channel with

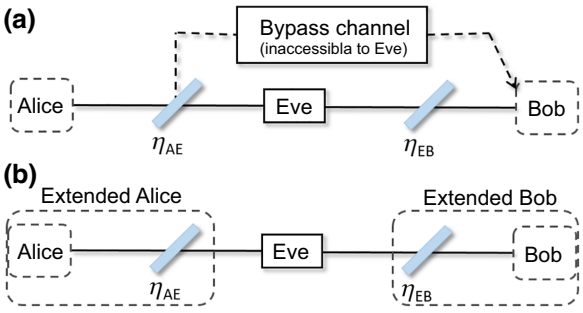

FIG. 1. (a) The restrictions imposed on Eve in terms of her collection efficiency, modeled by a beam splitter with transmissivity η_{AE}, and her access to Bob's telescope via a beam splitter with transmissivity η_{EB}. The part of the transmitted signal that does not go through Eve may still reach Bob via a bypass channel inaccessible to Eve. The signal lost at the second beam splitter, with transmissivity η_{EB}, is assumed to be inaccessible to all parties. (b) A simplified model where the bypass channel in (a) is assumed to be not accessible to Bob. This assumption would effectively reduce the channel model in (a) to a typical P&M QKD scenario with extended Alice's and Bob's boxes that contain some trusted lossy elements.

transmissivity η_{AE} connects Alice to Eve and that Eve has no access to the signals lost in this channel. Note that part of the lost signal can still reach Bob and we cannot discount this possibility. This creates an interesting QKD scenario, where, in addition to the channel controlled by Eve, there is a *bypass* channel via which some signals can reach Bob. Eve has no access to this bypass channel but Alice and Bob cannot necessarily characterize this channel either. The study of QKD security in the presence of such a bypass channel would generate interesting scenarios that we analyze in this paper. Similarly, we assume that every signal sent by Eve to Bob would go through a lossy channel with transmissivity η_{EB}, where Eve (and Bob) have no access to the lost signals on this channel. We do not impose any other restrictions on Eve, except being bound by the laws of quantum mechanics. We investigate how these two restrictions affect the performance of a QKD system ran on such a link.

There are different scenarios that one can consider with the above generic restrictions. One possible scenario, shown in Fig. 2(a), is when Eve's telescope is sufficiently large to capture all signals that would end up on Bob's telescope but not necessarily large enough to capture the entire signal sent by Alice. This case corresponds to $\eta_{AE} < 1$ but possibly with η_{EB} close to one. Note that when we are speaking of Eve, she is not restricted to operate only from one point in space. Another possibility is when Eve's telescope is assumed to be too small to capture the entire signal that would be received by Bob, in which case part of Alice's signal may reach Bob without Eve's intervention [see Fig. 2(b)]. This case would result in intriguing scenarios, especially when $\eta_{AE} \ll 1$. We look at how we can capitalize on this restriction to increase the secret-key rate in forthcoming sections. One last case, shown in Fig. 2(c), is for when Eve is simply a passive receiver of Alice's signal without sending anything to Bob. This case corresponds to a small η_{AE} and $\eta_{EB} = 0$ and captures a passive attack on a wire-tap channel [30]. These are just a few examples but the important point is that the generic model proposed here for a natural restriction on Eve can capture many practical cases that could happen in reality, as well as the few cases considered thus far in the literature [30–32].

Our objective in this paper is to find bounds on the secret-key generation rate under the assumption that η_{AE} and η_{EB} are known to Alice and Bob. We separate the issue of how, in practice, we can find an upper bound for these parameters from the security proof that follows once this restrictive assumption is used. The latter will be discussed in Sec. III, with particular examples on CV and DV QKD in Secs. IV and V, respectively. For the former, in Appendix A we consider a simple model to calculate the reflected power from an object (or a collection of objects with a similar effective size) with a certain reflectivity, in the line-of-sight link, assuming that a LIDAR system has been employed on both the satellite and the ground station. If our LIDAR system detects an object of a certain size, we can then use that to bound η_{AE} and η_{EB}. Even if the LIDAR systems do not detect any object, by making some nominal assumptions on the power budget on satellite and Earth, the sensitivity of the LIDAR system, and the reflectivity of space objects, we can then find the maximum object size that may remain undetected by our LIDAR systems and then accordingly upper bound η_{AE} and η_{EB}. This preliminary analysis suggests that, in nominal working conditions, η_{EB} is greater than η_{AE} and can be close to 1, whereas η_{AE} can remain small. In our analysis in Secs. IV and V, we then only consider the special case of $\eta_{AE} < 1$ at $\eta_{EB} = 1$, which is of practical interest.

In what follows, we first find some generic results for the key rate of the setup in Fig. 1(a). Throughout the paper, the satellite is assumed to have the QKD encoder and the ground station would decode the received signals. We therefore mainly focus on P&M schemes in the forthcoming sections. In particular, we consider the BB84 protocol with different types of sources and CV QKD with Gaussian encoding. One interesting point about the restricted-Eve scenario is the possibility of designing new protocols that capitalize on Eve's imposed restrictions. For instance, as shown in Ref. [30], in the case of a passive Eve, one can relax the requirement for using two mutually unbiased bases to come up with simpler protocols. Or, in the case of an ideal single-photon source (SPS) with a passive Eve, no privacy amplification may be needed [39]. In our setting, the bypass channel in Fig. 1(a) can play a

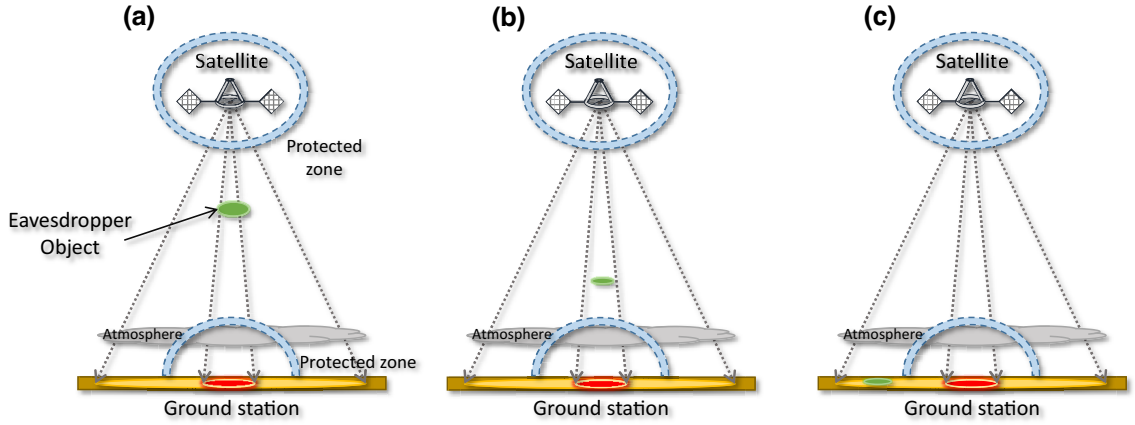

FIG. 2. A schematic view of a satellite-to-ground QKD link, with different restricted eavesdropping scenarios: (a) a semipowerful Eve who, while she does not capture the entire beam sent by the satellite (Alice), has access to the part that will be collected by the ground station (Bob); (b) An Eve with a telescope too small to capture the entire signal that reaches Bob; and (c) A passive Eve in a wire-tap channel.

nontrivial role in determining the key rate, as we investigate next.

III. SECURITY PROOF

In this section, we aim at finding generic bounds on the secret-key generation rate for the setup in Fig. 1(a). The key assumption in our analysis is that Alice and Bob can reliably characterize parameters η_{AE} and η_{EB} in Fig. 1(a). Otherwise, we do not need to know the nature of the bypass channel; and the bypass channel, while inaccessible to Eve, remains uncharacterized by Alice and Bob. This is in contrast with what is typically assumed in physical-layer security, or earlier work on restricted eavesdropping, in which certain channel models are assumed [30–33].

To gain some insight into the setting of Fig. 1(a), one simplifying assumption, as shown in Fig. 1(b), is to ignore the bypass channel and assume that no information would reach Bob via the bypass channel. This assumption would effectively reduce the channel model in Fig. 1(a) to a typical P&M QKD scenario with extended Alice's and Bob's boxes that contain some trusted lossy elements. The secret-key rate calculations in Fig. 1(b) would then reduce to modifying existing security proofs to account for the trusted loss in the channel. This would provide us with a reference point to which we can compare the key rate of QKD systems with bypass channels as in Fig. 1(a). On the one hand, having a bypass channel that Eve has no access to may suggest that Alice and Bob can share their secret key more easily implying that the key rate in the scenario in Fig. 1(b) is a lower bound to that of Fig. 1(a). On the other hand, because the bypass channel is not fully characterized by Alice and Bob, they need to consider the worst-case scenario, compatible with their observations, in which case Eve may end up being the beneficiary of the bypass channel.

One of our key contributions is to prove that, under a given set of experimental observations, the key rate of Fig. 1(a) is always upper bounded by that of Fig. 1(b). We label this result as Theorem 1 and will prove it in this section. That said, by properly formulating the problem, we can also see how the other intuition comes into play and under what scenarios it may prevail. Lemma 1 will capture this other result. But first, let us diligently formulate the two settings in Fig. 1.

In Figs. 3(a) and 3(b), we have presented generic attack models in the entanglement-based picture for, respectively, the scenarios in Figs. 1(a) and 1(b). Here, $|\psi_{AB}\rangle$ represents the initial bipartite entangled state generated by Alice, where one of its components is measured by measurement operator M_A to give the classical outcome X and its other component is sent to Bob. In Fig. 3, we have used the same notation for the field modes at the input and output of a quantum operation. For instance, mode B would go through the initial beam splitter and then through Eve's system, followed by the second beam splitter before entering Bob's telescope, modeled by operator $\mathcal{E}_T$ and measurement operator M_B, resulting in a classical variable Y. The measurement operator M_B effectively models the corresponding QKD measurements in the respective QKD protocol. Given that the bypass channel and Eve-controlled channels represent two independent spatial modes, the operator $\mathcal{E}_T$ effectively combines these two modes to generate outcome Y. For a physical telescope, these two modes are defined by what the telescope actually collects. In that case, this operation has to model a unitary evolution. We therefore assume that $\mathcal{E}_T$ is a unitary map, in which case we need to introduce a second output mode, which we have denoted by F_0. In our setup, mode F_0 is not accessible

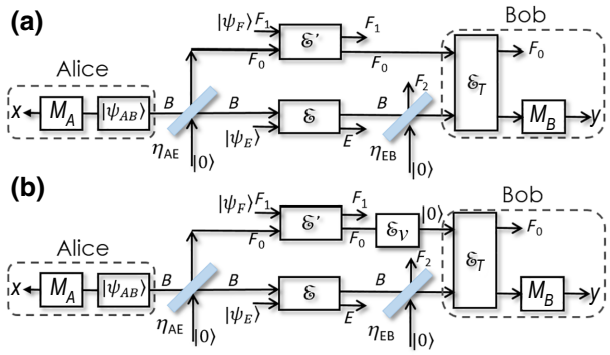

FIG. 3. (a) A generic attack model for a QKD system under restrictive assumptions on the collection efficiency and transmission efficiency of Eve's apparatus. (b) The attack model assuming that the bypass channel includes an infinitely high loss and only produces the vacuum state at its output. The notation is defined in the text.

to Bob but it would be interesting to see what, in principle, is achievable for Alice and Bob if F_0 is available to Bob. Lemma 1 below considers this case. Other important components of Figs. 3(a) and 3(b) are completely positive trace-preserving (CPTP) maps $\mathcal{E}$ and $\mathcal{E}'$, which, respectively, model the channel controlled by Eve and the bypass channel, with pure input states denoted by $|\psi_E\rangle$ and $|\psi_F\rangle$. In order to match the model in Fig. 3(b) with that of Fig. 1(b), we have introduced a trivial map $\mathcal{E}_V$ that maps every incoming state to the vacuum state $|0\rangle$. More specifically, the map $\mathcal{E}_V$ is a CPTP map with the following Kraus representation:

$$\mathcal{E}_V(\rho) = \sum_i K_i \rho K_i^\dagger, \quad K_i := |0\rangle\langle e_i|, \tag{1}$$

with $\{|e_i\rangle\}$ being an orthonormal basis for the Hilbert space in which the input state ρ lies. This operation ensures that nothing but the vacuum state would be transferred via the bypass channel, which corresponds to the simplified scenario in Fig. 1(b). Finally, the second input to both beam splitters in Fig. 3 is the vacuum state to model a lossy channel.

For the above-detailed settings, we now investigate how the key rate achievable in Fig. 3(a), which corresponds to the main restrictions imposed on Eve in our work, compares with that of Fig. 3(b), which further simplifies the channel and makes additional assumptions. As discussed earlier, because Eve has no access to the bypass channel, one may expect that the former cannot be lower than the latter. In Lemma 1, we prove that this intuition is correct in the case of direct reconciliation (DR), provided that Eve's attack (map $\mathcal{E}$) is fixed in both scenarios of Figs. 3(a) and 3(b) and mode F_0 is available to Bob. However, from a security perspective, we cannot ensure that Eve would perform the same attack independently of the physical channel(s) linking Alice and Bob. Interestingly, when allowing for the worst-case attack by Eve in each scenario of Fig. 3 and conditioned on the observed parameters in the QKD experiment, the achievable key rate in Fig. 3(a) turns out to be upper bounded by that of Fig. 3(b), as we prove in Theorem 1. Note that the bypass channel $\mathcal{E}'$ is not necessarily known to Alice and Bob.

Let us first consider the case where mode F_0 is available to Bob and Eve's attack is identical in both scenarios of Fig. 3.

Lemma 1.—For a quantum Bob with access to modes B and F_0 and a unitary map $\mathcal{E}_T$, the in-principle achievable asymptotic key rates r_a and r_b, with one-way *direct reconciliation*, corresponding, respectively, to the setups in Figs. 3(a) and 3(b), satisfy

$$r_b \leq r_a. \tag{2}$$

The proof is given in Appendix B. The proof of Lemma 1 hinges on the fact that the scenario in Fig. 3(b) can be recovered from Fig. 3(a) by applying an additional map on Bob's systems—effectively, the extra map $\mathcal{E}_V$ that maps everything to the vacuum. Such a map does not affect Eve's uncertainty about Alice's X outcomes while it increases Bob's uncertainty, by possibly increasing the quantum bit error rate (QBER) in a QKD experiment. This implies that under the conditions of Lemma 1, the in-principle achievable key rate in Fig. 3(b) should not be higher than that of Fig. 3(a).

The result of Lemma 1, however, holds for a quantum Bob under fixed attack by Eve performed in the two scenarios of Fig. 3 and might not be of use when evaluating the secret-key rate produced in a given QKD experiment. As a matter of fact, in a QKD experiment, what we are interested in is a bound on the leaked information to Eve conditioned on the set of observations made in the corresponding QKD experiment, in either configuration in Fig. 3. Considering that the scenario in Fig. 1(b) is equal to the scenario in Fig. 1(a) except for possibly an additional noise-increasing map, by fixing the observed amount of noise, we may conclude that the required attack by Eve can be less powerful in Fig. 1(b) than in Fig. 1(a), such that the resulting noise is effectively the same in the two scenarios. A less powerful attack could amount to less information leaked to Eve; hence a higher secret-key rate in the case of Fig. 3(b). This leads us to the opposite conclusion from what we draw in Lemma 1, namely, that in the P&M QKD setting, the secret-key rate in Fig. 3(a) cannot be larger than that of Fig. 3(b). An alternative way to look at this problem is that, from Alice's and Bob's point of view, they have to find the worst-case attack in the space spanned by valid choices of $\{\mathcal{E}, \mathcal{E}'\}$, for Fig. 3(a), and in the space of $\{\mathcal{E}, \mathcal{E}_V\}$ for Fig. 3(b). The latter turns out to be a subset of the former, which implies that Eve might come up with a

more effective attack in the setup of Fig. 3(a). We formalize this argument in the following theorem, which rigorously proves the above insight in the finite-key scenario and for both direct- and reverse-reconciliation (RR) cases.

Theorem 1.—Consider an ε-secure QKD protocol, with one-way direct (or reverse) information reconciliation and $\varepsilon = 2\bar{\varepsilon} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}}$, where $\varepsilon_{\mathrm{EC}}$ and $\varepsilon_{\mathrm{PA}}$ are, respectively, the security parameters for the error-correction and privacy-amplification steps. Let n be the number of signals used for key generation and let $\{Q_1^{\mathrm{obs}}, Q_2^{\mathrm{obs}}, \dots\}$ be the parameters observed by Alice and Bob in the parameter-estimation rounds. Then, the achievable secret-key rates R_a and R_b of the scenarios in Figs. 3(a) and 3(b), respectively, obtained with the above protocol in the finite-key regime, satisfy

$$R_a \leq R_b. \tag{3}$$

Proof.—The claim follows directly from the definitions of the achievable secret-key rate for the scenarios in Figs. 3(a) and 3(b) in the finite-key regime. To see this, let us first consider the state $\rho_{X^n Y^n E}$ representing the raw keys of Alice and Bob, together with Eve's quantum side information. For simplicity, we assume that Bob assigns a random outcome in the case of no detection in a key-generation round. A similar proof would hold in the case where Alice and Bob apply a sifting map to their outcomes in order to discard the rounds where Bob had no detection. Let us denote the initial state of all subsystems, before any map is applied, by ρ, given by

$$\begin{aligned}\rho := |\psi_{AB}\rangle\langle\psi_{AB}|^{\otimes n} \otimes |0\rangle\langle 0|_{F_0}^{\otimes n} \otimes |\psi_F\rangle\langle\psi_F| \\ \otimes |\psi_E\rangle\langle\psi_E| \otimes |0\rangle\langle 0|_{F_2}^{\otimes n}.\end{aligned} \tag{4}$$

Then, for the scenario in Fig. 3(a), we have

$$\begin{aligned}\rho_{X^n Y^n E}^{(\mathcal{E},\mathcal{E}')} = \mathrm{Tr}_{F_0F_1F_2}\Big[M_B \circ \mathcal{E}_T \circ \mathcal{B}_{\eta_{\mathrm{EB}}} \circ \mathcal{E}' \\ \circ \mathcal{E} \circ \mathcal{B}_{\eta_{\mathrm{AE}}} \circ M_A(\rho)\Big]\end{aligned} \tag{5}$$

and for the scenario in Fig. 3(b),

$$\begin{aligned}\rho_{X^n Y^n E}^{(\mathcal{E})} = \mathrm{Tr}_{F_0F_1F_2}\Big[M_B \circ \mathcal{E}_T \circ \mathcal{B}_{\eta_{\mathrm{EB}}} \circ \mathcal{E}_V \\ \circ \mathcal{E} \circ \mathcal{B}_{\eta_{\mathrm{AE}}} \circ M_A(\rho)\Big],\end{aligned} \tag{6}$$

where we denote the maps of the two beam splitters by $\mathcal{B}_{\eta_{\mathrm{AE}}}$ and $\mathcal{B}_{\eta_{\mathrm{EB}}}$ and we discard the map $\mathcal{E}'$ in Eq. (6) since it would have no effect on the state. Then, the state in Eq. (6) can be obtained from Eq. (5) by replacing $\mathcal{E}'$ with $\mathcal{E}_V$, i.e., $\rho_{X^n Y^n E}^{(\mathcal{E})} = \rho_{X^n Y^n E}^{(\mathcal{E},\mathcal{E}_V)}$.

For the scenario in Fig. 3(a), the achievable secret-key rate obtained from the n detected key-generation rounds, in the case of DR, is given by [40]

$$\begin{aligned}R_a = \frac{1}{n}\Bigg[\min_{(\mathcal{E},\mathcal{E}')\in\mathcal{S}(\{Q_1^{\mathrm{obs}},Q_2^{\mathrm{obs}},\dots\},\bar{\varepsilon})} H_{\min}^{\bar{\varepsilon}}(X^n|E)_{\rho^{(\mathcal{E},\mathcal{E}')}} \\ - I_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{EC}}} - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\Bigg],\end{aligned} \tag{7}$$

where the minimization is performed over all possible attacks by Eve, $\mathcal{E}$, and all possible actions of the bypass channel, $\mathcal{E}'$, compatible with the observed parameters, while I_{EC} is the amount of error-correction information publicly revealed by Alice and $H_{\min}^{\bar{\varepsilon}}$ is the $\bar{\varepsilon}$-smooth min-entropy function. More specifically, the set $\mathcal{S}(\{Q_1^{\mathrm{obs}}, Q_2^{\mathrm{obs}}, \dots\}, \bar{\varepsilon})$ contains all pairs of maps $(\mathcal{E}, \mathcal{E}')$ such that the parameters $\{Q_1^n, Q_2^n, \dots\}$, computed from the resulting state $\rho_{X^n Y^n}^{(\mathcal{E},\mathcal{E}')}$ in Eq. (5), are close to the observed parameter values $\{Q_1^{\mathrm{obs}}, Q_2^{\mathrm{obs}}, \dots\}$, except for a small probability fixed by $\bar{\varepsilon}$.

Similarly, for the scenario in Fig. 3(b), the achievable secret-key rate is given by

$$\begin{aligned}R_b = \frac{1}{n}\Bigg[\min_{\mathcal{E}\in\mathcal{T}(\{Q_1^{\mathrm{obs}},Q_2^{\mathrm{obs}},\dots\},\bar{\varepsilon})} H_{\min}^{\bar{\varepsilon}}(X^n|E)_{\rho^{(\mathcal{E})}} \\ - I_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{EC}}} - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\Bigg],\end{aligned} \tag{8}$$

where in this case the set $\mathcal{T}(\{Q_1^{\mathrm{obs}}, Q_2^{\mathrm{obs}}, \dots\}, \bar{\varepsilon})$ contains all possible maps $\mathcal{E}$ such that the parameters $\{Q_1^n, Q_2^n, \dots\}$, computed from the resulting state $\rho_{X^n Y^n}^{(\mathcal{E})}$ in Eq. (6), are close to the observed values $\{Q_1^{\mathrm{obs}}, Q_2^{\mathrm{obs}}, \dots\}$, except for a small probability fixed by $\bar{\varepsilon}$.

For a fixed set of values $\{Q_1^{\mathrm{obs}}, Q_2^{\mathrm{obs}}, \dots, \bar{\varepsilon}\}$, Eqs. (7) and (8) are identical expect for their smooth min-entropy terms. Moreover, we observe that the minimization set in Eq. (8) is a subset of the minimization set in Eq. (7). In particular, the smooth min-entropy term in Eq. (8) is calculated for $\rho_{X^n Y^n}^{(\mathcal{E})} = \rho_{X^n Y^n}^{(\mathcal{E},\mathcal{E}_V)}$, which is a subset of all the states $\rho_{X^n Y^n}^{(\mathcal{E},\mathcal{E}')}$ that are considered in Eq. (7). In other words, we have that $\mathcal{T} \times \{\mathcal{E}_V\} \subseteq \mathcal{S}$. We therefore conclude that the minimization in Eq. (7) can only produce a smaller or equal rate than the minimization in Eq. (8), thus proving the claim that $R_a \leq R_b$.

Note that the same proof can straightforwardly be extended to the RR case, by replacing Alice's raw key X^n with Bob's raw key Y^n in the smooth min-entropy terms. We again observe that by minimizing the achievable key rate over the uncharacterized maps of the setups in Fig. 3, namely, $\mathcal{E}$ and $\mathcal{E}'$ in Fig. 3(a) and $\mathcal{E}$ in Fig. 3(b), the scenario in Fig. 3(b) can be seen as a particular case of the scenario in Fig. 3(a). Thus, the optimal key rate in Fig. 3(a) should be smaller than or equal to the optimal key rate in Fig. 3(b). However, this also suggests that a partial characterization of the map $\mathcal{E}'$ in the bypass channel would

prevent us from viewing Fig. 1(b) as a particular case of Fig. 1(a), leading to a potentially different relation between the key rates R_a and R_b. ■

Theorem 1 provides an easy way to obtain upper bounds on the key rate in the generic setup of Fig. 3(a), which includes a bypass channel, using existing techniques and bounds for the setup of Fig. 3(b), which includes extended Alice's and Bob's boxes. While this is an important result, in QKD, we are often interested in lower bounds on the key rate, by which we can specify the required amount of privacy amplification in a real experiment. In the following sections, we will further study the relationship between such lower and upper bounds in the case of certain CV- and DV-QKD protocols. In particular, we numerically check in the case of CV QKD how the two bounds are close to, or deviate from, each other in certain practical scenarios. In the case of DV QKD, we also use the photon-number nature of the channel in certain BB84 protocols to come up with customized lower bounds in the setups with a bypass channel.

An alternative way to lower bound the min-entropy term in Eq. (7), in the DR case, is to calculate $H_{\min}^{\bar{\varepsilon}}(X^n|B')$, where, in Figs. 3(a) and 3(b), B' represents mode B right after the first beam splitter, which is in the state given by $\rho_{B'} = \mathrm{Tr}_{AF_0}[\mathcal{B}_{\eta_{\mathrm{AE}}}(|\psi_{AB}\rangle\langle\psi_{AB}|^{\otimes n} \otimes |0\rangle\langle 0|_{F_0}^{\otimes n})]$. To prove this, consider that the min-entropy in Eq. (7) is computed on the state in Eq. (5), where the system Y^n is traced out. This allows us to simplify some of the quantum maps in the state in Eq. (5), since they have no effect once the systems on which they act are traced out. We thus have that the min-entropy term in Eq. (7) is computed on the following state:

$$\rho_{X^nE} = \mathrm{Tr}_{F_0B}\Big[\mathcal{E} \circ \mathcal{B}_{\eta_{\mathrm{AE}}} \circ M_A(|\psi_{AB}\rangle\langle\psi_{AB}|^{\otimes n} \otimes |0\rangle\langle 0|_{F_0}^{\otimes n} \otimes |\psi_E\rangle\langle\psi_E|)\Big]. \tag{9}$$

Then, we can use the strong subadditivity of the smooth min-entropy function [41] to obtain the following lower bound:

$$H_{\min}^{\bar{\varepsilon}}(X^n|E) \geq H_{\min}^{\bar{\varepsilon}}(X^n|BE), \tag{10}$$

where the entropy on the right-hand side is computed on the state

$$\rho_{X^nBE} = \mathrm{Tr}_{F_0}\Big[\mathcal{E} \circ \mathcal{B}_{\eta_{\mathrm{AE}}} \circ M_A(|\psi_{AB}\rangle\langle\psi_{AB}|^{\otimes n} \otimes |0\rangle\langle 0|_{F_0}^{\otimes n} \otimes |\psi_E\rangle\langle\psi_E|)\Big]. \tag{11}$$

By using the data-processing inequality given in Ref.[41], the entropy can be further bounded as follows:

$$H_{\min}^{\bar{\varepsilon}}(X^n|BE) \geq H_{\min}^{\bar{\varepsilon}}(X^n|B'E), \tag{12}$$

where the entropy on the right-hand side is now computed on the state without the eavesdropper's map $\mathcal{E}$, i.e.,

$$\rho_{X^nB'E} = \mathrm{Tr}_{F_0}\Big[\mathcal{B}_{\eta_{\mathrm{AE}}} \circ M_A(|\psi_{AB}\rangle\langle\psi_{AB}|^{\otimes n} \otimes |0\rangle\langle 0|_{F_0}^{\otimes n})\Big] \otimes |\psi_E\rangle\langle\psi_E|. \tag{13}$$

Because system E is separate from all other systems in Eq. (13), it follows that its contribution to the conditional entropy vanishes, i.e., $H_{\min}^{\bar{\varepsilon}}(X^n|B'E) = H_{\min}^{\bar{\varepsilon}}(X^n|B')$. By combining this with Eqs. (10) and (12), we then obtain

$$H_{\min}^{\bar{\varepsilon}}(X^n|E) \geq H_{\min}^{\bar{\varepsilon}}(X^n|B'), \tag{14}$$

which proves our claim. Note that in certain regimes of operation, Eq. (14) would allow us to obtain an effective lower bound on the key rate, as we will see in Sec. IV.

IV. CONTINUOUS-VARIABLE QKD WITH RESTRICTED EVE

Here, we focus on CV-QKD protocols, in which data are encoded on the quadratures of light. We consider a particular protocol in the family of GG02 protocols [42,43], in which Alice uses Gaussian encoding and Bob performs homodyne detection. CV QKD is not an obvious choice when it comes to highly lossy channels [44] such as the ones we may face in the satellite-based QKD scenario. But, for that very reason, it is a particularly interesting case to study because, in our setting, the initially trusted loss η_{AE} could alleviate some of the problems that CV QKD faces in high-loss channels. Note that by using the fading nature of the atmospheric part of the link [45], along with relevant binning or clustering techniques, it might also be possible to find working regimes of operation for satellite-based CV QKD [46–48]. In this work, however, we only focus on the benefits that we may reap by imposing access restrictions on Eve, particularly, at the transmitter end, by assuming $\eta_{\mathrm{AE}} \leq 1$ while $\eta_{\mathrm{EB}} = 1$. For the same reason, we only focus on the asymptotic case, which also makes the analysis a bit easier to follow.

To be able to obtain concrete results, for the most of this section, we study a special case of the setup in Fig. 3(a), which we expect to encounter in practice. A schematic diagram of this case is given in Fig. 4, in which the bypass channel is modeled as a pure loss channel with transmissivity η_S. This is a reasonable assumption considering scenarios that we may face in practice. Alternatively, a thermal-loss channel could have been assumed for the bypass channel but, as we will see later, the insights that we obtain into the effects of the bypass channel on the performance would not change majorly. The second assumption is in modeling the telescope action as a coupling beam splitter with transmissivity η_T. As we will show in Appendix C, this is partly the result of the mode definitions in Fig. 3(a) and partly because of the light-collecting

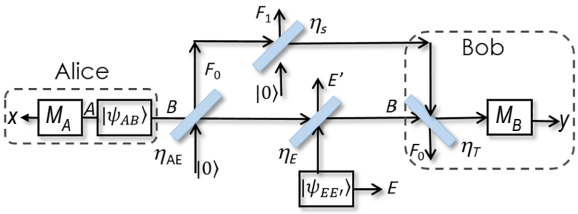

FIG. 4. A special setting for the setup of Fig. 3(a), where the bypass channel and the telescope actions are modeled by beam splitters. Eve's attack has also been modeled using an entangling cloner, assuming that the Eve-controlled section of the channel is also lossy.

nature of a telescope. Finally, whenever Eve's action needs to be explicitly modeled, we assume that Eve is implementing an entangling cloner attack. This would implicitly imply that the channel controlled by Eve is of thermal-loss nature. This may not be necessarily the case, especially in our setting where the bypass channel can offer other pathways to the receiver. But, again, it is what we may expect to be the case in a realistic scenario and it also considerably reduces the search space when we look for worst-case configurations.

The key rate of a CV-QKD protocol, in the asymptotic limit of infinitely many signals, in the DR and RR cases, are, respectively, given by

$$K_{\mathrm{DR}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{AE}}, \tag{15}$$

$$K_{\mathrm{RR}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{16}$$

where β is the reconciliation efficiency, I_{AB} is the mutual information between the variables, X and Y, that Alice and Bob, respectively extract their secret key from, and χ_{AE} (χ_{BE}) is the Holevo information between Alice (Bob) and Eve. Under optimal collective Gaussian attacks [49–51], the mutual-information and Holevo-information terms can both be bounded by using the covariance matrix (CM) of Alice, Bob, and Eve in the equivalent entanglement-based picture of the protocol. In the unrestricted-Eve scenario, it can be assumed that Eve holds a purification of Alice's and Bob's joint states. This enables us to calculate all relevant terms just as a function of the CM of Alice and Bob, which can directly be measured in the experiment. In the restricted-Eve scenario, however, this purification assumption does not hold, as there are other modes, such as F_0, F_1, and F_2 in Fig. 3, that are not accessible to any of the parties. This would require us to redo some of the calculations in the simulation cases that we consider in this section.

Throughout this section, we assume that the CM measured by Alice and Bob implies a channel with a total equivalent excess noise, at the transmitter end, ξ, and a total transmissivity $T_{\mathrm{eq}} = \eta_{\mathrm{ch}}\eta_{\mathrm{d}}$, where η_{d} is the receiver efficiency, corresponding to the measurement operator M_B, which is a trusted source of loss that can be characterized by the users, and η_{ch}, representing the channel transmissivity, is defined as the ratio between the two observed parameters T_{eq} and η_{d}. Note that in the asymptotic case considered in our analysis, the observed values for T_{eq} and ξ effectively represent the corresponding average values for, respectively, transmissivity and excess noise, over the entire set of exchanged quantum states. This does not imply or require that the channel parameters need to be fixed throughout the experiment. In fact, in the satellite-to-ground channels, the turbulence effect can indeed result in a fading channel with a time-dependent gain. But, our security proof only relies on the average values derived from our observations, based on which the amount of information leaked to Eve can be bounded. Given that, in practice, such an overall effect often resembles a lossy channel, in our simulations, we only consider scenarios where $T_{\mathrm{eq}} \leq \eta_{\mathrm{ch}} \leq 1$. We also assume that the mutual-information term, I_{AB}, which is an observable in the experiment, is given by

$$I_{\mathrm{AB}} = \frac{1}{2}\log_2 \frac{V + \chi_{\mathrm{tot}}}{1 + \chi_{\mathrm{tot}}}, \tag{17}$$

corresponding to a thermal-loss channel identified by T_{eq} and ξ. In Eq. (17), V is the variance of the two-mode squeezed vacuum (TMSV) state at the source (in the entanglement-based picture) and $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{hom}}/\eta_{\mathrm{ch}}$ is the total noise, calculated at the transmitter end, where $\chi_{\mathrm{line}} = (1 - \eta_{\mathrm{ch}})/\eta_{\mathrm{ch}} + \xi$ and $\chi_{\mathrm{hom}} = (1 - \eta_{\mathrm{d}})/\eta_{\mathrm{d}} + \nu_{\mathrm{el}}/\eta_{\mathrm{d}}$ are, respectively, the noise terms due to the channel and the homodyne receiver. Here, ν_{el} denotes the receiver's electronic noise.

In the following, we obtain a lower bound on the secret-key generation rate under the above assumptions for the setup in Fig. 4 in the RR and DR cases and compare it with the corresponding upper bounds that can be obtained from Theorem 1.

A. Reverse reconciliation

Reverse reconciliation is typically the default choice for CV-QKD systems in highly lossy channels. We first consider this case under the restricted-Eve scenario of $\eta_{\mathrm{AE}} \leq 1$, while $\eta_{\mathrm{EB}} = 1$ in Fig. 4. The key question that we would like to explore is how the achievable key rate in the setup with a bypass channel compares with the upper bound that can be obtained from the setup of Fig. 3(b). Interestingly, we find that, under the assumptions outlined above, the two are numerically very close to each other in certain practical regimes of interest.

Let us first explain the limitations that we have considered in the special setup shown in Fig. 4. Given that this is a linear channel and that our encoding is Gaussian, a Gaussian attack is expected to be the optimal collective attack by Eve. In principle, for any given values of η_{AE}, η_S, and η_T, there could be a Gaussian attack by Eve that

is compatible with the observed values for total transmissivity $T_{\rm eq}$ and the total equivalent excess noise ξ at the transmitter end. The Gaussian operation by Eve could take different forms. Here, we only focus on one particular form of attack, which can be modeled by the conventional entangling cloner setup as shown in Fig. 4. Here, Eve combines a TMSV state with variance $V_{\rm E}$, at a beam splitter with transmissivity $\eta_{\rm E}$, with the signal she receives from Alice. The implicit assumption here is that Eve's channel is lossy, corresponding to the condition that $\eta_{\rm E} \leq 1$. The conclusions that we draw in this section will then only be valid for this type of attack.

In Appendix D, we have calculated the corresponding CM for all parties in Fig. 4, from which the expected values for our key observables, $T_{\rm eq}$ and ξ are obtained and, respectively, given by Eqs. (D5) and (D6). In the following, in order to focus on the impact of the restrictions imposed on Eve, we assume that the receiver has no loss, i.e., $\eta_{\rm d} = 1$, and no electronic noise, i.e., $\nu_{\rm el} = 0$. For any given values of $\eta_{\rm AE}$, η_S, and η_T, we can then find the corresponding values for $\eta_{\rm E}$ and V_E that are compatible with the observed values of $T_{\rm eq}$ and ξ. For the sake of our simulation, we assume that the resulting $\eta_{\rm E}$ is less than or equal to one, to be compatible with the entangling cloner attack considered here.

In order to calculate the key rate for the setup of Fig. 4, we use the CM given in Eq. (D3), from which all relevant terms can be calculated. $I_{\rm AB}$ is already given by Eq. (17). To calculate the Holevo-information term, we have

$$\chi_{\rm BE} = H(EE') - H(EE'|B), \tag{18}$$

where $H(EE')$ and $H(EE'|B)$ can, respectively, be obtained from the corresponding symplectic eigenvalues of the CM for EE' and $EE'|B$ (for notation, see Fig. 4). The former, $\mathbf{V}_{EE'}$, is specified by tracing out modes A and B in the CM of Eq. (D3). We then numerically find its symplectic eigenvalues, which we denote by Λ_1 and Λ_2. The latter CM, $\mathbf{V}_{EE'|B}$, can also be obtained by applying a homodyne measurement on mode B:

$$\mathbf{V}_{EE'|B} = \mathbf{V}_{EE'} - \frac{1}{V_B}\Sigma_{BEE'}\Pi\Sigma_{BEE'}^T, \tag{19}$$

where $\Sigma_{BEE'}^T = [C_{BE}\mathbb{Z} \;\; C_{BE'}\mathbb{1}]$ and $\Pi = \mathrm{diag}(1,0)$, with $\mathbb{Z} = \mathrm{diag}\{1,-1\}$ and $\mathbb{1}$ being the identity matrix of dimension two [52]. In the above, V_B, C_{BE}, and $C_{BE'}$ are defined in Eq. (D4). Denoting the symplectic eigenvalues of $\mathbf{V}_{EE'|B}$ by Λ_3 and Λ_4, the Holevo-information term in the RR case is given by

$$\chi_{\rm BE} = g(\Lambda_1) + g(\Lambda_2) - g(\Lambda_3) - g(\Lambda_4), \tag{20}$$

where $g(x) = \left(\frac{x+1}{2}\right)\log_2\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log_2\left(\frac{x-1}{2}\right)$. Note that in the above calculations, we account for the fact that the state corresponding to $ABEE'$ is not a pure state. This prevents us from calculating all the terms from the CM of A and B, as it is common in the unrestricted case.

Let us now fix the observed values for $T_{\rm eq}$ and $\xi_{\rm eq}$ and compare the achievable secret-key rates in Fig. 4 with the corresponding scenario where the bypass channel is removed or, equivalently, when $\eta_S = 0$. In both cases, some optimization needs to be done to find the lower bound on the key rate. In Fig. 4, while the telescope is part of Bob's secure station, it is not clear how this parameter can be characterized. For any key-rate analysis, one should then consider the space of feasible values of η_S and η_T and go with the worst case possible. In Fig. 4, this corresponds to going over all possible values of η_S and η_T that are compatible with $T_{\rm eq}$ and $\xi_{\rm eq}$ and then finding $K_{\rm RR}^{(a)} \equiv \min_{\eta_S,\eta_T}\{K_{\rm RR}\}$. Similarly, for the extended Alice model, we can set $\eta_S = 0$, and optimize over η_T. For a fixed loss in the link, the higher η_T, the more control is given to Eve. The minimum guaranteed key rate in this case is then given by $K_{\rm RR}^{(b)} \equiv K_{\rm RR}(\eta_S = 0, \eta_T = 1)$. We can then compare $K_{\rm RR}^{(a)}$ with $K_{\rm RR}^{(b)}$.

In order to gain some insight into our optimization problem, in Fig. 5 we have plotted $K_{\rm RR}$ versus each of η_S and η_T, while keeping the other parameter constant. To mainly focus on the impact of the channel parameters in Fig. 4, we have assumed that $\beta = 1$, which results in the optimal V being very large. We have fixed V at 300 in shot-noise units (SNU), which gives us close-to-optimum key-rate values. In Fig. 5(a), η_T and $\eta_{\rm AE}$ are fixed at 0.5, while, for different values of $T_{\rm eq}$, we look at how $K_{\rm RR}$ varies versus η_S. We observe a decreasing behavior for the key rate within the acceptable range of values for η_S. Note that within the assumptions in our model, e.g., that $0 \leq \eta_{\rm E} \leq 1$, such a range becomes narrower with a decrease in $T_{\rm eq}$. This is because in Eq. (D5), the maximum value for η_S is given by $\eta_S^{\max} = T_{\rm eq}/[(1-\eta_{\rm AE})(1-\eta_T)]$ at $\eta_{\rm E} = 0$, i.e., when Alice's signal reaches Bob only via the bypass channel. Interestingly, at such a point, the key rate is at a minimum, while $\chi_{\rm EB}$, shown in the inset, is at a maximum. A justification for this behavior is that, at $\eta_{\rm E} = 0$, Eve can keep the entirety of the signal she has received from Alice for herself and use it to obtain information about Bob's key. In fact, in this scenario, the bypass channel helps Eve with masquerading the transmissivity of the channel without requiring her to give up any information she can extract from her share of Alice's signal. This observation also explains why the scenario with no bypass channels offers an upper bound on the key rate. In the latter case, i.e., when $\eta_S = 0$, we see a similar behavior with regard to the optimum value of $\eta_{\rm E}$ from Eve's perspective. As shown in Fig. 5(b), in this case, the key rate goes down with an increase in $\eta_T \geq T_{\rm eq}$. The larger η_T, the smaller will be $\eta_{\rm E} = T_{\rm eq}/\eta_T$, meaning that Eve has more control

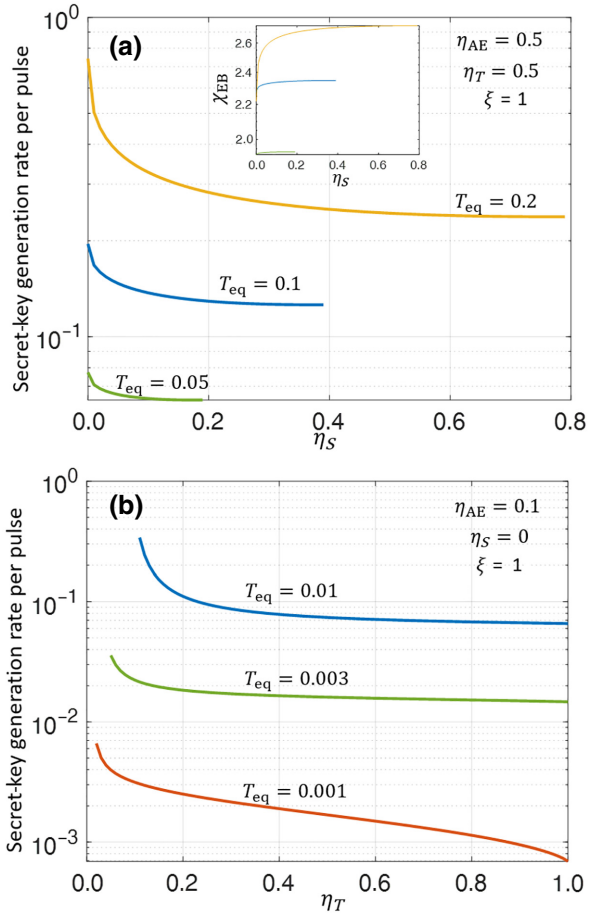

FIG. 5. The secret-key generation rate for the CV-QKD protocol in Fig. 4, with RR, versus (a) η_S and (b) η_T, for different values of observed transmissivity and a fixed value of excess noise. In (a), the bound on the leaked information to Eve, χ_{EB}, is also shown in the inset. In both figures, $V = 300$ in SNU, $\beta = 1$, $\eta_d = 1$, and $v_{el} = 0$. Other parameters are specified on the plot.

on the channel. This observation agrees with our earlier definition of $K_{RR}^{(b)}$.

Putting together the points made above, it may seem that the gap between $K_{RR}^{(a)}$ and $K_{RR}^{(b)}$ could be large in certain regimes of operation. In Fig. 5(a), it is, however, interesting to see that the difference between the maximum value of K_{RR} at $\eta_S = 0$ and its minimum value, obtained at η_S^{max}, shrinks down as T_{eq} decreases. This would give us the hope that, in practical regimes of operation for satellite QKD with a total loss of 30–40 dB, the difference between $K_{RR}^{(a)}$ and $K_{RR}^{(b)}$ could be reasonably low. This has been verified, as a function of η_{AE}, in Fig. 6(a) at $T_{eq} = 0.001$ for different values of the excess noise. As can be seen, $K_{RR}^{(a)}$ and $K_{RR}^{(b)}$ almost overlap in the entire region, with the exception of when $\eta_{AE} \ll 1$. Numerically speaking, the optimum value for $K_{RR}^{(a)}$ is often obtained at $\eta_S = 1$, which effectively maximizes η_T and minimizes η_E. The latter two favor Eve, while the former makes the bypass channel a reliable replacement for what Eve should have done in the absence of the bypass channel. This also suggests that while our model in Fig. 4 is just a special case of what could happen in reality, a no-loss, and possibly no-noise, bypass channel, as we are dealing with in the case of $K_{RR}^{(a)}$, could be the worst-case scenario for Alice and Bob. We have briefly examined this hypothesis by considering a thermal-loss bypass channel and observed the following:

(i) The key change in the CM elements is for the excess-noise expression in Eq. (D6), which now gets an additional term, $(1-\eta_S)(1-\eta_T)(V_S-1)$, due to the bypass channel, where V_S is the variance of the TMSV state that models thermal noise in the bypass channel.
(ii) At $\eta_S < 1$ and $V_S > 1$, we see an increase in the key rate as compared to the case of $V_S = 1$, corresponding to no thermal noise in the bypass channel.
(iii) The minimum key rate is, however, still obtained at $\eta_S = 1$, in which case the effect of additional term in the excess noise vanishes and we will obtain the same result for $K_{RR}^{(a)}$ as the pure-loss bypass channel.

We should note that we still limit our search space to the feasibility assumptions we have made in Fig. 4. While the above claim needs to be analytically verified, based on our numerical results, in practical regimes of operation for satellite QKD, it seems safe to use the upper bound given by Theorem 1 as a reliable approximation to the lower bound on the key rate for CV-QKD systems with RR.

Another reassuring result in Fig. 6(a) is that the achievable key rate is a decreasing function of η_{AE}, i.e., the more restriction we set on Eve, the higher is the key rate that Alice and Bob can securely achieve. The impact in certain cases can be quite instrumental. For instance, at a total equivalent excess noise of $\xi = 0.1$ at the transmitter end, while no key can be exchanged under unrestricted Eve, positive key rates can be obtained for $\eta_{AE} < 0.9$. The same happens for $\xi = 1$ but with higher restrictions on Eve at $\eta_{AE} < 0.1$. This is particularly promising because the excess noise in satellite-to-ground links is expected to increase because of the fading effect in the atmospheric part of the link [53, Ch. 8]. Interestingly, when η_{AE} is sufficiently low, the key rate will become almost independent of the amount of excess noise and rather large key rates can be obtained.

The overall results explained above seem to be unchanging when we account for other sources of imperfection in our system. In particular, in Fig. 6(b), we have accounted for nonideal values for the reconciliation efficiency parameter β. It can be seen that the overlap between the upper and lower bounds on the key rate still holds when $\beta < 1$ and that the key rate goes down as η_{AE} increases. The difference is that the threshold value for η_{AE} to give us

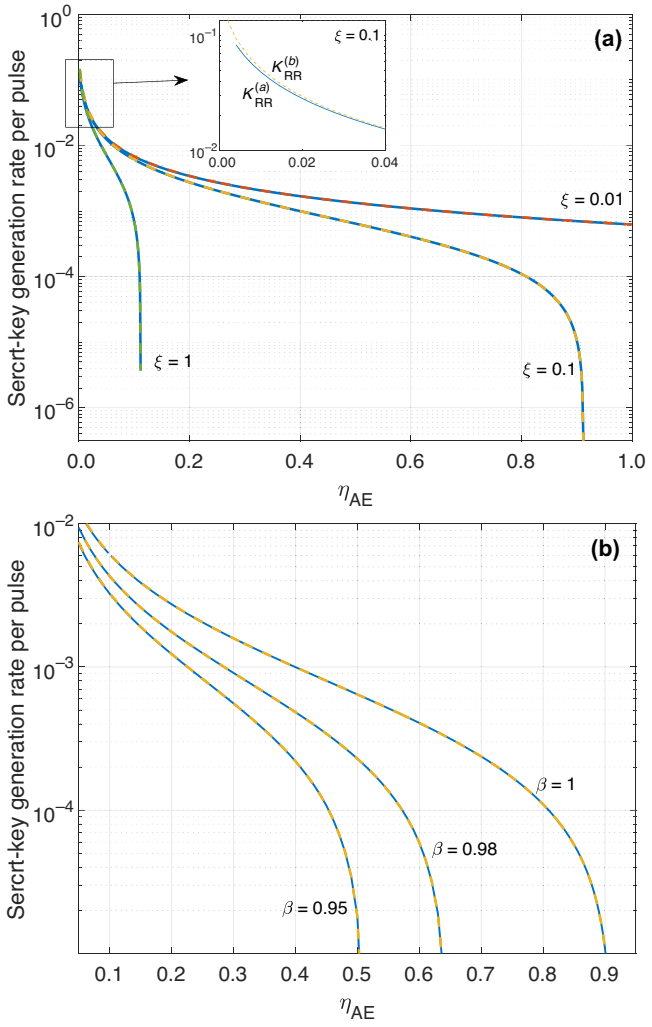

FIG. 6. The secret-key generation rate for the CV-QKD protocol in Fig. 4, with RR, versus η_{AE}. The solid lines represent $K^{(a)}_{RR}$ and the dashed lines represent $K^{(b)}_{RR}$. As shown in the inset, the two curves are very close to each other and mostly overlap except for small values of η_{AE}. In (a), $T_{eq} = 0.001$, $V = 300$ in SNU, $\beta = 1$, $\eta_d = 1$, $v_{el} = 0$, and the excess noise is shown in the graphs. In (b), we consider imperfect reconciliation efficiencies characterized by parameter β. The other parameters are $T_{eq} = 0.001$, $\xi = 0.1$, and $V = 3.5$ in SNU.

positive key rates goes down as we decrease β. This is understandable because, by reducing the mutual-information term by a factor of β, we now need further restrictions on Eve to bring down the Holevo-information term in Eq. (16). The transition to positive key rates happen at around 0.5 for η_{AE} at $\beta = 0.95$, which is still an attainable value. Note also that when $\beta < 1$, the optimal value for the modulation variance, V, drops to small finite values, which in practice correspond to very low amounts of transmitted energy per pulse.

B. CV QKD with direct reconciliation

In Sec. IV A, we saw how the proposed restrictions on Eve can improve the key rate of CV-QKD systems in highly lossy channels. Here, we apply the results of Sec. III to the case of CV QKD with DR under a restricted Eve. In the DR case, with no restriction on Eve, the maximum loss that we can tolerate is only 3 dB. It would be interesting to see how that would change when we impose restrictions on Eve's access to Alice's signal. In the following, we consider two extremes: when $\eta_{AE} > T_{eq}$, in which case, the entangling cloner attack as in Fig. 4 is the optimal attack by Eve, and when $\eta_{AE} < T_{eq}$, where we can use Eq. (14) to directly find a lower bound on the key rate.

1. Method 1: Entangling cloner attack

Here, we assume that $T_{eq} < \eta_{AE}$ and use the results of Appendix D to calculate the key rate for the setup of Fig. 4. As in the RR case, we optimize the key rate over uncharacterized system parameters η_S and η_T as follows:

$$\begin{aligned} K^{(a)}_{DR} &\equiv \min_{\eta_S,\eta_T}\{K_{DR}(\eta_S,\eta_T)\},\\ K^{(b)}_{DR} &\equiv \min_{\eta_T}\{K_{DR}(0,\eta_T)\} = K_{DR}(0,1), \end{aligned} \tag{21}$$

where K_{DR} is defined in Eq. (15), with

$$\chi_{AE} = H(EE') - H(EE'|A_x), \tag{22}$$

where A_x represents the homodyne-measurement result on one of the quadratures of mode A after going through the 50:50 beam splitter in the heterodyne measurement M_A. The above entropy terms can be calculated using the CM in Eq. (D3) with some modifications due to the 50:50 beam splitter in M_A. The joint CM for modes A_xEE' is then given by

$$\mathbf{V}_{A_xEE'} = \begin{pmatrix} (V+1)/2\mathbb{1} & 0\mathbb{1} & C_{AE'}/\sqrt{2}\mathbb{Z} \\ 0\mathbb{1} & V_E\mathbb{1} & C_{EE'}\mathbb{Z} \\ C_{AE'}/\sqrt{2}\mathbb{Z} & C_{EE'}\mathbb{Z} & V_{E'}\mathbb{1} \end{pmatrix}, \tag{23}$$

where $\mathbb{Z} = \mathrm{diag}\{1,-1\}$, $\mathbb{1}$ is the identity matrix of dimension two, and all other parameters are given by Eq. (D4). Eve's state $\rho_{EE'}$ is then described by the CM $\mathbf{V}_{EE'}$, which is given by the 4×4 submatrix in the lower right of $\mathbf{V}_{A_xEE'}$ given in Eq. (23). We then have

$$H(EE') = g(\Lambda_1) + g(\Lambda_2), \tag{24}$$

where Λ_1 and Λ_2 are the symplectic eigenvalues of $\mathbf{V}_{EE'}$. Similarly, the conditional term $H(EE'|A_x) = g(\Lambda_3) + g(\Lambda_4)$, where Λ_3 and Λ_4 are the symplectic eigenvalues

of $\mathbf{V}_{EE'|A_x}$, given by

$$\mathbf{V}_{EE'|A_x} = \mathbf{V}_{EE'} - \frac{2}{V+1}\Sigma_{A_xEE'}\Pi\Sigma^T_{A_xEE'}, \tag{25}$$

where we have applied a homodyne measurement on mode A_x [52] and $\Sigma_{A_xEE'} = \begin{pmatrix} 0\mathbb{1} \\ C_{AE'}/\sqrt{2}\mathbb{Z} \end{pmatrix}$.

2. Method 2: Generic lower bound

In method 2, we use Eq. (14), which basically uses the state before Eve's operation, to bound χ_{AE}. The advantage of this technique is that here we do not need to impose any conditions on the observed values of η_{ch} and η_{AE}. In particular, we can now cover the case of $\eta_{\mathrm{AE}} < \eta_{\mathrm{ch}}$, which is the extreme case where Eve's collection efficiency is worse than Bob; e.g., as in Fig. 2(c). In this case, we use Eq. (14) to upper bound χ_{AE} by

$$\chi_{AB'} = H(B') - H(B'|A_x), \tag{26}$$

where B' is mode B right after the first beam splitter in Fig. 3(a). Note that in this approach, we do not need to restrict ourselves to the assumptions in Fig. 4. In the above equation, $H(B')$ is the von Neumann entropy of the thermal state B' with variance $V_{B'} = \eta_{\mathrm{AE}}V + 1 - \eta_{\mathrm{AE}}$. We then use the fact that the symplectic eigenvalue of a single-mode thermal state is indeed equal to its variance to obtain $H(B') = g(V_{B'})$. Similarly, to calculate the term $H(B'|A_x)$, we need to find the symplectic eigenvalues for the conditional covariance matrix $\mathbf{V}_{B'|A_x}$. Given that the CM of A_xB' is given by

$$\mathbf{V}_{A_xB'} = \begin{pmatrix} (V+1)/2\mathbb{1} & \sqrt{\eta_{\mathrm{AE}}(V^2-1)/2}\mathbb{Z} \\ \sqrt{\eta_{\mathrm{AE}}(V^2-1)/2}\mathbb{Z} & V_{B'}\mathbb{1} \end{pmatrix}, \tag{27}$$

we have, after the homodyne detection on A_x,

$$\begin{aligned}\mathbf{V}_{B'|A_x} &= V_{B'}\mathbb{1} - \frac{\eta_{\mathrm{AE}}(V^2-1)}{V+1}\mathbb{Z}\Pi\mathbb{Z}^T \\ &= \begin{pmatrix} 1 & 0 \\ 0 & V_{B'} \end{pmatrix}.\end{aligned} \tag{28}$$

An upper bound on χ_{AE} can then be calculated from the following:

$$\chi_{\mathrm{AE}} \le g(V_{B'}) - g(\sqrt{V_{B'}}). \tag{29}$$

3. Numerical results

Figure 7(a) shows the key rate versus η_{AE}, for $\eta_{\mathrm{AE}} > T_{\mathrm{eq}}$, using method 1 for different values of $T_{\mathrm{eq}} > 0.5$. We have plotted the upper bound $K^{(b)}_{\mathrm{DR}}$ (dashed lines) as well as the optimized lower bound $K^{(a)}_{\mathrm{DR}}$ (solid lines). Unlike the RR case, in the DR scenario, the two bounds are not close and effectively we cannot guarantee higher key rates than what we can obtain in the unrestricted case. In particular, for $T_{\mathrm{eq}} < 0.5$, similar to the unrestricted case, we do not get a positive key rate for $K^{(a)}_{\mathrm{DR}}$. The optimum value of $K^{(a)}_{\mathrm{DR}}$ is again numerically obtained at $\eta_S = 1$ but this time the optimum η_{E} takes rather large nonzero values around 0.5. The larger η_{AE} is, the larger is the η_{E} that we get at the optimum point. This could be because, at η_{AE} close to one, the main path through Eve should offer a transmissivity close to 0.5, or higher, to get positive key rates, whereas, as η_{AE} goes down, the bypass channel helps Eve more with the total observed T_{eq} to the extent that the initial restriction on Eve becomes irrelevant.

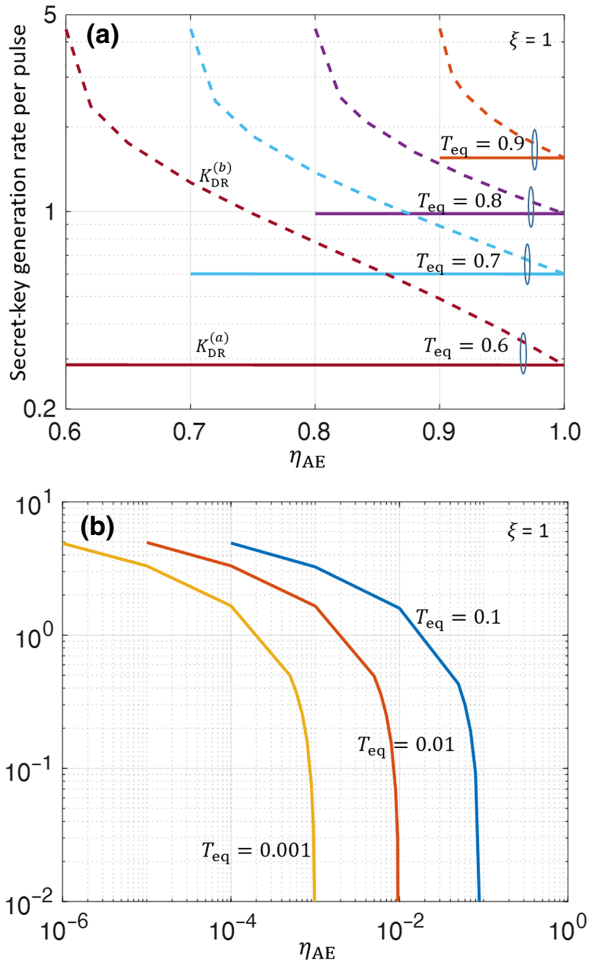

FIG. 7. The secret-key generation rate at $V = 10^7$ in SNU, obtained from (a) method 1 and (b) method 2, versus η_{AE} for CV-QKD systems using DR. The results are shown for an observed channel with different values of T_{eq}, $\xi = 1$ SNU, $\eta_{\mathrm{d}} = 1$, $\nu_{\mathrm{el}} = 0$, and $\beta = 1$. In (a), the solid (dashed) lines represent $K^{(a)}_{\mathrm{DR}}$ ($K^{(b)}_{\mathrm{DR}}$).

We can, however, gain some advantage in the restricted case in the extreme case of $\eta_{\mathrm{AE}} < T_{\mathrm{eq}}$. Here, we can use the generic lower bound in Eq. (29) to obtain the key rate. The

results are shown in Fig. 7(b). As can be seen, in this case, the key rate can be improved by orders of magnitude by decreasing η_{AE}. The seemingly flat curves at the left-hand side of the graph are mainly because of the choice of a finite value for V. In principle, the key rate would continue going up in the asymptotic limit of $V \to \infty$. However, the growth happens very slowly, e.g., for a variance as large as $V = 10^{20}$, the key rate is only about 25. Considering the limitations on the transmitted power, a maximum V can be chosen in practice to offer the maximum key rate in such settings where Eve is disadvantaged as compared to Bob, as in the case of the wire-tap channel.

V. DISCRETE-VARIABLE QKD WITH RESTRICTED EVE

In this section, we consider several DV-QKD protocols, mainly focusing on the BB84 protocol [54] and its variants. We consider the original BB84 with single-photon sources (SPSs) as well as its variant with phase-randomized weak coherent pulses (WCPs) [55]. In all these cases, we deal with a photon-number channel from Eve's perspective. We assume that $\eta_{\mathrm{EB}} = 1$, i.e., we only consider Eve's restriction on her signal-collection capabilities. The case of $\eta_{\mathrm{EB}} < 1$ will be the subject of another investigation. In the following, we present a method to obtain a lower bound for the secret-key rate in the restricted-Eve case. In this paper, we only consider the asymptotic regime where infinitely many signals are exchanged and focus on how restrictions on Eve can affect system performance.

A. General lower bounds for secret-key rate

The secret-key rate of BB84 protocols, in the asymptotic regime, in an unrestricted-Eve scenario is lower bounded by [56]

$$R \geq qQ\left[-fh(E_b) + \frac{Q_1}{Q}(1 - h(e_1)) + \frac{Q_0}{Q}\right], \tag{30}$$

where f is the error-correction inefficiency, q is the basis reconciliation factor, and $h(\cdot)$ represents Shannon's binary entropy function, defined as $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. In Eq. (30), Q, E_b, and e_1, respectively, denote the total gain, the QBER, and the single-photon error rate. The parameters Q_0 and Q_1 are given by

$$\begin{aligned} Q_0 &= Y_0 p_0, \\ Q_1 &= Y_1 p_1, \end{aligned} \tag{31}$$

where Y_i is the probability of Bob's detection under the condition that Alice has sent i photons and p_i denotes the probability that Alice sends i photons.

The general idea behind Eq. (30) is that, in photon-number channels, the information gained by Eve depends on the number of photons in the signal received by Eve. For the events in which Eve receives two or more photons, one may assume that Eve can obtain full information about the transmitted key bit using the photon-number splitting (PNS) attack [57]. In the events in which Eve receives one photon, the maximum information that she can gain is $h(e_1)$. Finally, if Eve receives no photon, her information is zero, assuming that DR is used.

In our restricted-Eve scenario, for every sifted bit, we find an upper bound, I_{E}, on Eve's information, in the DR case, based on the number of photons transmitted by Alice and received by Eve, denoted, respectively, by n and m, as follows:

$$I_{\mathrm{E}} = \begin{cases} 0, & m = 0, n \geq 0, \\ 1, & m > 1, n \geq m, \\ h(\varepsilon_{11}), & m = 1, n = 1, \\ 1, & m = 1, n > 1, \end{cases} \tag{32}$$

where ε_{11} denotes an upper bound on the error rate of the signals for which $n = m = 1$. Here, we have pessimistically assumed that Eve can distinguish between the cases where $m = n = 1$ versus $m = 1$ but $n > 1$. This assumption would allow Eve, in the latter case, to keep the photon to herself and wait to see if one of the remaining photons is received by Bob. To find a lower bound on the secret-key rate, we define the parameters W_{ij} and p_{ij} as follows:

$$\begin{aligned} W_{ij} &= \Pr(\text{Bob's detection} | n = i, m = j), \\ p_{ij} &= \Pr(n = i, m = j). \end{aligned} \tag{33}$$

In the asymptotic case where Alice sends infinitely many signals, a lower bound on the secret-key rate can be obtained by

$$R \geq qQ\left[-fh(E_b) + \frac{S_{11}}{Q}(1 - h(\varepsilon_{11})) + \frac{S_0}{Q}\right], \tag{34}$$

where

$$\begin{aligned} S_0 &= \sum_{i=0}^{\infty} W_{i0} p_{i0}, \\ S_{11} &= W_{11} p_{11}. \end{aligned} \tag{35}$$

Effectively, the last two terms in Eq. (34) have replaced that of Eq. (30), in the case of no bypass channel and represent part of the shared key that can be used for privacy amplification.

In the following, we find bounds on the key parameters in Eq. (34). In a typical QKD protocol, it may not be possible to measure the exact values of S_0, S_{11}, and ε_{11}. Instead, we try to find lower bounds on S_0 and S_{11} and an upper

bound on ε_{11}. To find a lower bound on S_0 and S_{11}, in the first step we find a lower bound on $S_0 + S_{11}$. Note that

$$1 \geq Q = \sum_{i=0}^{\infty} \sum_{j=0}^{i} W_{ij} p_{ij} = S_0 + S_{11} + S_{\text{other}}, \tag{36}$$

where

$$S_{\text{other}} = \sum_{j=2}^{\infty} \sum_{i=j}^{\infty} W_{ij} p_{ij} + \sum_{i=2}^{\infty} W_{i1} p_{i1}. \tag{37}$$

Using Eqs. (35)–(37), we can obtain

$$\begin{aligned} S_0 + S_{11} &= Q - S_{\text{other}} \geq S^L_{0+11} \\ &\equiv Q - \left(\sum_{j=2}^{\infty} \sum_{i=j}^{\infty} p_{ij} + \sum_{i=2}^{\infty} p_{i1} \right), \end{aligned} \tag{38}$$

where S^L_{0+11} denotes the lower bound on $S_0 + S_{11}$. Now, we consider the following two inequalities:

$$\begin{aligned} S_0 &\leq \sum_{i=0}^{\infty} p_{i0}, \\ S_{11} &\leq p_{11}. \end{aligned} \tag{39}$$

Note that $\sum_{i=0}^{\infty} p_{i0}$ is the probability that Eve receives no photon, i.e., $m = 0$. We denote this probability by p_0^{Eve}. Then, we can write

$$\begin{aligned} S_0 &\geq S^L_{0+11} - S_{11} \geq S^L_{0+11} - p_{11}, \\ S_{11} &\geq S^L_{0+11} - S_0 \geq S^L_{0+11} - p_0^{\text{Eve}}. \end{aligned} \tag{40}$$

Substituting Eq. (38) into the above inequalities, it can be concluded that

$$\begin{aligned} S_0 &\geq S_0^L \equiv \max\left\{ Q - (1 - p_0^{\text{Eve}}), 0 \right\}, \\ S_{11} &\geq S_{11}^L \equiv \max\left\{ Q - (1 - p_{11}), 0 \right\}. \end{aligned} \tag{41}$$

The above bounds have an easy explanation. Let us look at S_0^L, for instance. The term $1 - p_0^{\text{Eve}}$ is the probability that Eve has got a nonvacuum state. This sets an upper bound on the number of detection events that Bob can get because of nonvacuum states. Any other click must come from cases where Eve has received no photons, which gives us the expression in Eq. (41).

Note that in the case of restricted Eve, the bound on S_0 is likely to become relevant for small values of η_{AE}. This is because, for S_0^L to be strictly positive, $1 - p_0^{\text{Eve}}$ should be smaller than Q. In the nominal mode of operation, when no Eve is present, Q often scales with channel transmissivity and, for coherent-state inputs, $1 - p_0^{\text{Eve}}$ is expected to scale with η_{AE}. This suggests that as η_{AE} becomes smaller and smaller, there could be a non-negligible contribution from the S_0 term, which is often ignored in the conventional unrestricted-Eve case. In the latter case, $1 - p_0$ is often a fixed value, which, in high loss regimes, can become greater than the value of Q. Even if Q happens to be larger than $1 - p_0$, the contribution from S_0 is likely to be canceled out by the additional error correction that Alice and Bob need to do for the clicks resulted from the vacuum states sent by Alice. In the restricted-Eve scenario, however, the bypass channel can, in principle, provide a route to obtaining correlated data between Alice and Bob without necessarily increasing the QBER. This could allow Alice and Bob to extract more secret-key bits from their measured data as compared to the conventional scenario. We will look more carefully at the effect of the above bounds on S_0 and S_{11} later in this section.

To find an upper bound on ε_1, we note that

$$E_b Q = \sum_{i=0}^{\infty} \sum_{j=0}^{i} \varepsilon_{ij} S_{ij}, \tag{42}$$

where $S_{ij} = W_{ij} p_{ij}$. Using the above equation, we can write

$$E_b Q \geq \varepsilon_{11} S_{11} \geq \varepsilon_{11} S^L_{11} \Rightarrow \varepsilon_{11} \leq \frac{E_b Q}{S^L_{11}}. \tag{43}$$

Using Eqs. (41) and (43), the secret-key rate, in the restricted-Eve case, in the limit of infinitely long key is lower bounded by

$$R \geq qQ \left[-f h(E_b) + \frac{S^L_{11}}{Q} (1 - h(\varepsilon^U_{11})) + \frac{S^L_0}{Q} \right], \tag{44}$$

where $\varepsilon^U_{11} = \min\{E_b Q / S^L_{11}, 1/2\}$ gives an upper bound on $h(\varepsilon_{11})$.

B. BB84 performance under restricted eavesdropping

In the following, we discuss the secret-key rate of BB84 protocols considering different sources. We find the relevant parameters needed in each case to calculate R as given by Eq. (44).

1. BB84 with single-photon sources

If an ideal single-photon source is used at Alice's side, we have $S_0 + S_{11} = Q$, $p_0^{\text{Eve}} = 1 - \eta_{\text{AE}}$ and $p_{11} = \eta_{\text{AE}}$. Hence, from Eq. (41), we have

$$\begin{aligned} S_0^L &= \max\left\{ Q - \eta_{\text{AE}}, 0 \right\}, \\ S_{11}^L &= \max\left\{ Q - (1 - \eta_{\text{AE}}), 0 \right\}. \end{aligned} \tag{45}$$

By substituting Eq. (45) into Eqs. (43) and (44), we can calculate a lower bound on the secret-key rate.

In the case of an ideal single-photon source, there are alternative ways of calculating lower bounds on the key rate by directly using Eqs. (34) and (30). For instance, because $S_0 + S_{11} = Q$, Eq. (34) turns into

$$\begin{aligned} R &\geq qQ\left[-fh(E_b) + 1 - \frac{S_{11}}{Q}h(\varepsilon_{11})\right] \\ &\geq qQ\left[-fh(E_b) + 1 - h(\varepsilon_{11}^U)\right]. \end{aligned} \tag{46}$$

Alternatively, one can directly use Eq. (30) by setting $Q_0 = 0$. In Sec. V B 3, we use the best of these three bounds to specify the lower on the key rate.

2. BB84 with WCP sources

Phase-randomized WCP (or, in short, WCP) sources follow Poisson distribution in photon generation. If the average number of photons of the WCP source is μ, then p_{ij} can be obtained by

$$\begin{aligned} p_{ij} &= \Pr(n = i)\Pr(m = j\,|n = i) \\ &= \frac{e^{-\mu}\mu^i}{i!}\binom{i}{j}\eta_{\rm AE}^j(1-\eta_{\rm AE})^{i-j}. \end{aligned} \tag{47}$$

By substituting the above equation into Eqs. (39) and (41), we obtain

$$\begin{aligned} S_0 &\geq S_0^L = \max\left\{Q - (1 - e^{-\mu\eta_{\rm AE}}), 0\right\}, \\ S_{11} &\geq S_{11}^L = \max\left\{Q - (1 - \mu\eta_{\rm AE}e^{-\mu}), 0\right\}. \end{aligned} \tag{48}$$

The lower bound R can then be obtained by substituting the above two equations into Eqs. (43) and (44).

3. Numerical results

In this subsection, we consider a satellite-based QKD system, using the BB84 protocol, and evaluate its performance in different regimes of operation. The nominal values used for the system parameters are listed in Table I. It is noteworthy that we calculate the key rate at a channel transmissivity of $\eta_{\rm ch} = 10^{-3}$, corresponding to the recent efficiency measurements for the Micius satellite [58]. We have also assumed that the ground station is equipped with superconducting single-photon detectors of 90% efficiency but to account for possible background noise in the link [32], the dark-count probability per pulse for the receiver is assumed to be $p_{\rm dc} = 10^{-7}$. For a system running at 100 MHz, this is one order of magnitude higher than the typical dark counts for such detectors [59]. We also assume that we use the efficient version of the BB84 protocol [60], in which the reconciliation factor q approaches one.

We consider two types of sources, SPS and WCP, for the encoder at Alice's side, i.e., the satellite. In a real QKD experiment, the parameters related to the overall gain and the QBER, i.e., Q and E_b in Eq. (44), are obtained by measurement. Here, we assume that the measured values for these parameters are equal to those that can be obtained analytically as calculated in Ref. [61, Appendix A].

TABLE I. The nominal values used for the system parameters.

Parameter	Value
Average channel loss, $\eta_{\rm ch}$	30 dB
Error-correction inefficiency, f	1.16
Basis reconciliation factor, q	1
Total dark and background probability, $p_{\rm dc}$	10^{-7}
Misalignment error, e_d	0.01
Quantum efficiency of detectors, $\eta_{\rm d}$	0.9

Figure 8(a) shows the secret-key rate versus $\eta_{\rm AE}$ for the SPS and WCP protocols. We have optimized the key rate over μ in the WCP case. The optimum values of μ are shown in Fig. 8(b). There are several interesting points to highlight in Fig. 8:

(i) At the channel loss of 30 dB, the WCP protocol cannot provide any secret key under unrestricted Eve's assumption. In the restricted-Eve case, however, we start having positive key rates for roughly $\eta_{\rm AE} < 8.1 \times 10^{-4}$. This suggests that a simple phase-randomized laser source is sufficient for key exchange in this regime.

(ii) The WCP protocol performance exceeds that of the SPS protocol at small values of $\eta_{\rm AE}$. This is interesting, as the SPS source conventionally corresponds to the ideal BB84 protocol. In our example system, this happens at roughly $\eta_{\rm AE} < 8 \times 10^{-4}$. This is mainly because of the extra laser power that Alice can now use to generate signals with a larger number of photons without worrying much about photon-number-splitting attacks. We do not have this possibility with SPSs; hence such sources would not allow us to benefit from Eve's restrictions in this case.

(iii) Among the three techniques proposed in Sec. V B for the SPS source, the one obtained from Eq. (30) offers the highest key rate. That is why the corresponding curve in Fig. 8 remains constant. Mathematically, this can be seen by comparing Eq. (46) with Eq. (30) and noting that $h(\varepsilon_{11}^U) \geq h(e_1)$. The worst-case assumption made in Eq. (32) seems to not offer any advantage in the single-photon case. To check if there is any room for improvement, we have verified if the bound can be improved by using numerical techniques for bounding the key rate [62,63]. We have, however, observed no change in the achievable rate and the result presented in Fig. 8 seems to be the optimum case for the SPS

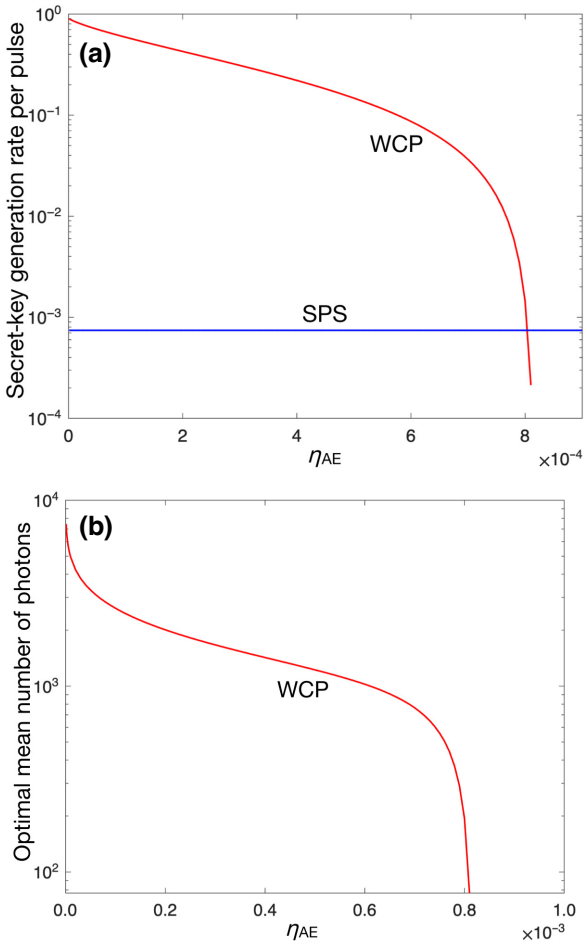

FIG. 8. (a) The secret-key generation rate versus η_{AE} for WCP and SPS sources. (b) The optimal values of μ versus η_{AE} for WCP sources.

source. The full details of the numerical approach will be the subject of a separate publication.

(iv) As mentioned earlier, the case of $\eta_{AE} < \eta = \eta_{ch}\eta_d$ is of special interest. This is when the bound S_0^L in Eq. (48) can take nontrivial values. We can see this effect in the parameter values chosen for our simulation, where $Q = 1 - (1 - p_{dc})^2 e^{-\eta\mu}$. In this case, we have $Q - (1 - p_0^{Eve}) = e^{-\mu'} - (1 - p_{dc})^2 e^{-\eta\mu} > e^{-\eta_{AE}\mu} - e^{-\eta\mu}$. The latter term would get a positive value when $\eta_{AE} < \eta$, resulting in a positive value for S_0^L.

VI. DISCUSSION AND CONCLUSIONS

We have studied the security of P&M QKD systems under certain restrictions on the eavesdropper. We have relaxed some of the assumptions on the eavesdropper's unrestricted capabilities in collecting and retransmitting QKD signals. Such restrictions could particularly find relevance in satellite-based QKD protocols. Our restrictive assumptions have resulted in an under-explored scenario, where the channel between Alice and Bob is not entirely controlled by Eve but, rather, an uncharacterized bypass channel could also carry signal. We have found generic upper bounds on the key rate for QKD systems in the presence of bypass channels and in the case of CV QKD with RR, we have shown that the upper and lower bounds on the key rate are very close to each other in certain practical regimes of interest. Such an upper bound offers a considerable boost to the key rate that can be achieved under unrestricted eavesdropping. In the case of CV QKD with DR, or that of BB84 protocols, the advantage offered by our customized bound is limited to certain scenarios where Eve's access to Alice's signal is significantly hampered, as is the case in, e.g., wire-tap channels. Nevertheless, our approach to security proof relies only on a few assumptions, which can, in principle, be verified with monitoring techniques.

The analysis of QKD systems in the presence of bypass channels can certainly be extended in several directions, where each is worth a separate investigation. For instance, the difference between RR and DR in the CV-QKD case raises the question of whether DV QKD with RR could offer any better performance. One way to answer such questions is by developing numerical techniques for finding tight bounds on the key rate in such setups, which is ongoing research. While Theorem 1 is applicable to finite-size key settings, the issue of statistical fluctuations in the presence of the bypass channel needs to be further investigated. Whether the bypass channel affects non-P&M QKD protocols, e.g., entanglement-based QKD, also needs to be investigated. In this work, we mainly focused on LEO-satellite scenarios but, in principle, the same techniques could also find application in medium-Earth-orbit and geostationary satellite missions. The practicality of this needs to be investigated, as monitoring techniques would become less efficient at long distances. Overall, while the key application of such an analysis could be in satellite-based systems, the whole area of QKD security under unconventional assumptions is a less explored territory, which deserves more attention. One generic direction of travel is to consider the classical limitations that one can impose on Eve. This work has effectively been concerned with limiting the size of an eavesdropping object but this can be extended to other classically measurable attributes of Eve. We hope that works such as this paper can open new avenues of research in this area.

All data generated in this paper can be reproduced by the provided methodology and equations.

ACKNOWLEDGMENTS

M.R. is grateful to Norbert Lütkenhaus, Xiongfeng Ma, and Charles C. W. Lim for fruitful discussions around the security analysis. This work has been partially sponsored

by the White Rose Research Studentship, the Engineering and Physical Sciences Research Council (EPSRC) via the UK Quantum Communications Hub with Grants No. EP/M013472/1 and No. EP/T001011/1, and the European Union Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 675662 [Quantum Communications for ALL (QCALL)]. M.G. would like to additionally acknowledge support from the European Union via "Continuous Variable Quantum Communications" (CiViQ, Grant Agreement No. 820466). F.G. and H.K. acknowledge support from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy—Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769. H.K. also acknowledges support by the QuantERA project QuICHE, via the German Ministry for Education and Research (BMBF) Grant No. 16KIS1119K.

APPENDIX A: ESTIMATING η_{AE} AND η_{EB} PARAMETERS

In this appendix, we find nominal values for parameters η_{AE} and η_{EB} if Alice and Bob are equipped with the LIDAR technology for detecting unwanted objects around them.

1. Optical setup

In this section, we specify the optical setup considered in our calculation for the two authorized QKD parties, Alice (A) and Bob (B), and the eavesdropper, Eve (E). We assume that Alice is located on a LEO satellite, traveling in a circular orbit at an altitude L above the ground. It is equipped with a QKD source and a telescope with aperture radius r_A. Bob is instead placed on the surface of the Earth and he collects the light sent by Alice using a telescope with radius r_B. We address the static situation in which the satellite is at a fixed position right above the optical ground station, so that the length of the link is exactly L. In the following calculations, we will allow Eve to have two distinct satellites, one for collecting and one for resending the light, with appropriate values of the aperture radius and position. However, it turns out that the configuration of a single satellite is indeed optimal for her. We can therefore assume that Eve is represented by a spacecraft equipped with two telescopes, one for collection (pointed toward Alice) and one for transmission (pointed toward Bob), both of radius r_E. We also assume, as the worst-case scenario, that the aperture of the telescope represents the whole projected area of Eve's spacecraft.

We assume that Alice's telescope sends the QKD signals in the form of a Gaussian beam, with initial beam width W_0, equal to its radius r_A, at wavelength λ. For the light propagation, we neglect the action of the atmosphere and the contribution of pointing errors. We use the standard expressions for Gaussian optics, corrected through the quality factor M^2 in order to replicate the far-field divergence of real optical elements. Eve's telescope is instead perfect, meaning that she can send Gaussian beams with $M^2 = 1$.

In the following, we will call z the coordinate along the propagation path, so that Alice is at $z = 0$ and Bob at $z = L$. After a propagation of length $z \in [0, L]$, the beam width can be expressed as

$$W(z) = W_0\sqrt{1 + \left(\frac{zM^2}{z_R}\right)^2}, \tag{A1}$$

where $z_R = \pi W_0^2/\lambda$ represents the Rayleigh range of the beam. Comparison between the far-field divergence of a perfect Gaussian beam and the divergence measured for the Micius satellite suggests a value of $M^2 \approx 3$. The transmittance of such a beam, when impinging at the center of a circular collecting aperture of radius ρ can be expressed as

$$\eta(\rho, z) = 1 - \exp\left[-2\frac{\rho^2}{W^2(z)}\right]. \tag{A2}$$

This expression can be used to compute the transmittance of Alice's beam through Bob's telescope, by setting $z = L$ and $\rho = r_B$:

$$\eta_{AB} = 1 - \exp\left[-2\frac{r_B^2}{W^2(L)}\right], \tag{A3}$$

which describes the efficiency of the QKD channel, apart from additional losses such as the atmospheric absorption, detection efficiency, and transmittance of the optical elements. The same formula can express the efficiency with which Eve can collect Alice's signals, while she is at position z and has a collecting aperture of radius $r_E(z)$:

$$\eta_{AE}(z) = 1 - \exp\left[-2\frac{r_E(z)^2}{W^2(z)}\right]. \tag{A4}$$

We assume here that Eve is positioned at the exact center of the beam. The way in which we model the dependence of $r_E(z)$ on the distance from Alice and Bob will be specified in Sec. A 2.

We can use a similar approach to estimate the ability of Eve to resend the signals that she has intercepted toward Bob. In order to take full advantage of her optical system, we allow Eve to send focused beams. It is not necessary to take this into account in the case of Alice, because for a typical LEO satellite, the total propagation length L is much larger than the Rayleigh range $z_R \approx 70$ km, so focusing would not give much advantage. For our calculations, we suppose that Eve has a lens of focal length f just in front of her sending aperture. We can then use

the ray-transfer-matrix formalism and obtain the following expression for the optimized width of a focused beam at distance d from its transmitter [64]:

$$W_{\rm E}(z) = \frac{\lambda d}{\pi r_{\rm E}(z)} = \frac{\lambda(L-z)}{\pi r_{\rm E}(z)}\,, \tag{A5}$$

which agrees with Eq. (A1) when $z \gg z_R$ and $r_{\rm E} = W_0$. Now, using Eq. (A2), we can compute the transmittance of Eve's beam through Bob's aperture as follows:

$$\eta_{\rm EB}(z) = 1 - \exp\left[-2\frac{r_{\rm B}^2}{W_{\rm E}(z)^2}\right]. \tag{A6}$$

We point out that, even in this case, the dependence of $r_{\rm E}(z)$ on the length of Alice-to-Eve and Eve-to-Bob links is important and will be modeled in Sec. A 2.

2. Techniques for channel monitoring

In this section, we obtain an upper bound on the size of an undetected Eve's spacecraft, depending on the distance from Alice's or Bob's position, if some sort of channel monitoring system is employed. Typical techniques are radar, LIDAR, and direct optical detection. We will not analyze the last of these, as it requires rather stringent conditions: Eve's spacecraft must be illuminated by the Sun while the receiver is in eclipse and the sky must be clear. A radar is very power consuming, so we will address this technique as operated only from Bob, on the ground (although examples of radars on spacecraft can also be found). LIDARs, on the other hand, require much less power and share similar optical elements as those used for QKD, so may be placed on both Alice's and/or Bob's sides.

The operation of a radar or LIDAR system can be described by the so-called radar equation:

$$d_{\rm max} = \left(\frac{P_T G^2 \lambda \sigma}{P_{\rm min}(4\pi)^3 \kappa}\right)^{1/4}, \tag{A7}$$

which expresses the maximum distance at which an object with radar cross section σ can be detected. We are interested in the inverse dependence for the maximum $\sigma(z)$, for a space object at location z, i.e., at distance $L - z$ from Bob, which is given by

$$\begin{aligned}\sigma(z) &= \frac{P_{\rm min}(4\pi)^3 \kappa d_{\rm max}^4}{P_T G^2 \lambda^2} \\ &= \frac{P_{\rm min}(4\pi)^3 \kappa (L-z)^4}{P_T G^2 \lambda^2}.\end{aligned} \tag{A8}$$

Here, $P_{\rm min}$ represents the minimum power measurable by the receiving system, P_T is the total power emitted, G is the gain of the radar antenna, and κ is a parameter that accounts for all additional sources of loss.

In order to assess the applicability of a radar system on Bob's end, we use the following parameter values:

(i) $G = 4\pi\ E_{\rm ant}\ \pi\ r_{\rm ant}^2/\lambda_R^2$, where $E_{\rm ant} = 0.6$ is the antenna efficiency, $r_{\rm ant} = 2$ m is the radius of the circular parabolic antenna and $\lambda_R = 4$ cm is the wavelength of the radar signals. We choose $r_{\rm ant} = 2$ m as a reasonable size for a dish to be put alongside an optical ground station.
(ii) $P_T = 10^5$ W, as it is the power usually used in systems of this size (such as the ones used in airports).
(iii) $P_{\rm min} = k_B T F_n B$, where k_B is the Boltzmann constant, T is the temperature, $F_n = 8$ dB is the so-called noise figure, and $B = 2.5 \times 10^6$ Hz is the effective noise bandwidth of the setup.
(iv) $\kappa = 7$ dB, which takes into account attenuation from atmospheric effects, filters, and other sources.
(v) We also assume that $L = 500$ km, corresponding to a LEO satellite.

In general, the radar cross section σ is not equal to the geometric projected area and it strongly depends on the shape of the object. These two quantities only coincide for spherical objects and this is the case that we consider here. In this way, we can set the radius of Eve's telescope to $r_{\rm E} = \sqrt{\sigma/\pi}$. Figure 9 shows the minimum size of $r_{\rm E}$, calculated from Eq. (A8) at the above parameter values, if a radar is located at Bob's site, i.e., at $z = L$. Figure 9 suggests that if we only use radar at Bob's end, we can easily miss eavesdropping objects of a few meters in radius. This implies that we may not achieve useful bounds on $\eta_{\rm AE}$ and $\eta_{\rm EB}$, in Eqs. (A4) and (A6), if we only rely on radar as a monitoring system. Even assuming that low-power radar could be employed on the satellite to monitor the first tens of kilometers around it, a telescope of 3 m in radius at 100 km from Alice would be able to intercept and resend with transmittances very close to 1. In practice, radar techniques are currently used to monitor the number of objects present in low orbits around the Earth [65]. However, much bigger facilities (antenna radius $\gtrsim 10$ m) are necessary for such missions and the information is usually not in real time but used to build and update catalogs of the objects. We would therefore consider the radar solution insufficient for our purposes, while passive monitoring could always provide additional information. Next, we consider the LIDAR option.

Much better performance can be achieved using LIDARs. The working principle is the same as radars, but in this case light in the near-ultraviolet, visible, or near-infrared range is sent and recorded after reflection from the object under study. In this case, instead of enormous antennas, we only need telescopes of reasonable sizes. For example, the same telescopes used for exchanging QKD

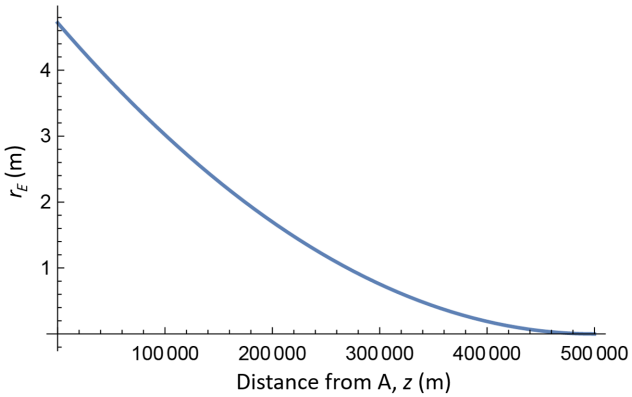

FIG. 9. The minimum radius for Eve's telescope aperture detectable by a typical radar system located at Bob's site. Note that the distance from Bob is measured by $L - z$. An object 500 km away from Bob must have a radius greater than 4 m, for our chosen parameter values, to be detectable by Bob's radar system.

signals, or alignment, can be used for LIDAR operation. Moreover, instead of powers of tens of kilowatts, lasers with power on the order of 1 W are sufficient, meaning that this technique can rather easily be implemented on even small satellites, as well as on Bob's side. As expected, the big advantage comes from the much shorter wavelength of the employed light with respect to the microwave signals used in the radar technique, resulting in much less diffraction of the electromagnetic beams.

In this case, we can again try to use the standard radar equation of Eq. (A8), with suitably chosen parameters. We report here a simple calculation, again using Gaussian optics, that gives a result very similar to the radar equation (with LIDAR parameters), for when the LIDAR is placed on the satellite. A similar calculation can be used for a LIDAR based in the ground station. We use Eq. (A5) and modify it to take into account the realistic quality factor M^2 as estimated before,

$$W_{\mathrm{LIDAR}}(z) = \frac{\lambda_{\mathrm{LIDAR}} z M^2}{\pi W_0}, \tag{A9}$$

where λ_{LIDAR} is the LIDAR wavelength. The intensity distribution of such a beam can be expressed as

$$I(r,z) = \frac{2P_T}{\pi W_{\mathrm{LIDAR}}(z)^2} \exp\left[\frac{2r^2}{W_{\mathrm{LIDAR}}(z)^2}\right], \tag{A10}$$

where P_T is the total power carried by the beam and r is the distance from the beam center in the plane transversal to the direction of propagation. We assume that the reflecting object is at the center of the beam.

We compute the total power incident on the object by integrating Eq. (A10) in the area corresponding to Eve's spacecraft, as follows:

$$P(z) = \int_{|r|<r_{\mathrm{E}}} I(r,z) dr d\theta = \\ = P_T\left(1 - \exp\left[-\frac{2r_{\mathrm{E}}^2}{W_{\mathrm{LIDAR}}(z)}\right]\right). \tag{A11}$$

We assume that the light is reflected back isotropically by the object under study, with reflectivity α, resulting in a received light intensity of

$$I_R(z) = \frac{P(z)\alpha}{4\pi z^2} = \\ = \frac{P_T \alpha}{4\pi z^2}\left(1 - \exp\left[-\frac{2r_{\mathrm{E}}^2}{W_{\mathrm{LIDAR}}(z)}\right]\right). \tag{A12}$$

The total collected power reaching the satellite LIDAR is then $P_R(z) = I_R(z)\pi r_{\mathrm{A}}^2 \kappa$, where we account for any additional loss encountered during transmission and collection by factor κ. In order to obtain the bound on the size of Eve's object, we can then invert this expression and equate $P_R(z)$ to the minimum power P_{min} measurable by the receiving setup, as follows:

$$r_{\mathrm{E}}(z)^2 = -\left(\ln\left[1 - \frac{2P_{\mathrm{min}} k z^2}{\alpha P_T W_0^2}\right]\right)\left(\frac{\lambda_{\mathrm{LIDAR}} z M^2}{\pi W_0}\right)^2. \tag{A13}$$

For the rest of this section, unless otherwise noted, we use the following parameter values. We set $\lambda_{\mathrm{LIDAR}} = 800$ nm and assume that $\kappa = 0.25$. The transmitted power is set to $P_T = 1$ W due to the limit on the power consumption on small satellites. For the ground-based LIDAR, the transmitted power can be higher, but this may only offer a small advantage, due to atmospheric scattering, as we show by the end of this section. We choose a rather conservative value for the reflectivity of the object, $\alpha = 0.1$, considering that for different metals it is usually around $\alpha = 0.5$ or more. Coating can be used to lower this value; however, measurements at different wavelengths could limit the effectiveness of this technique. We also assume that $M^2 = 3$, $r_{\mathrm{A}} = 15$ cm, and $r_{\mathrm{B}} = 50$ cm. These values are compatible with the instruments used in the Chinese satellite mission Micius. All other relevant parameters are the same as in the radar case.

Figure 10 shows the estimated maximum radius of Eve's object that does not trigger our LIDAR monitoring system, versus its distance from the satellite. The results obtained by using Eqs. (A13) and (A8) are both shown. They differ because the efficiency of the transmitter and the reflectivity of the object are modeled in different ways. We see that the bound on the size of undetectable objects, r_{E}, is much smaller as compared to the values shown in Fig. 9 using the radar technique, giving hope that the values obtained for

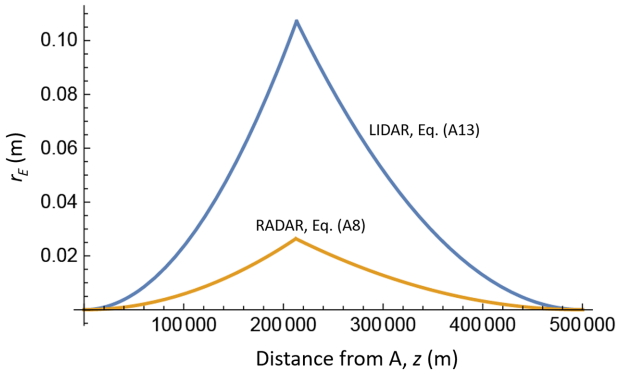

FIG. 10. The minimum radius for Eve's telescope aperture detectable by LIDAR measurements performed, simultaneously, from the satellite and from the ground. The bound on this quantity is obtained from two different techniques: the blue curve is obtained from Eq. (A13), while the orange curve is from the radar equation [Eq. (A8)], using parameters suitable for a LIDAR system.

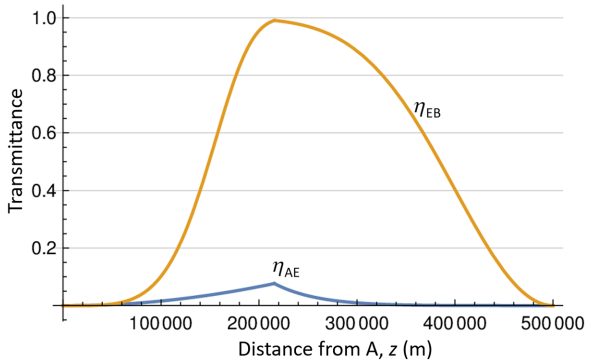

FIG. 11. The values of η_{AE} and η_{EB}, for an undetected Eve, computed using Eqs. (A4) and (A6), respectively.

η_{AE} and η_{EB} in this case may be low enough to be useful in the enhancement of the secret-key rate.

The minimum measurable power $P_{\min}$ used in Fig. 10 is obtained by calculating the background light collected by the satellite in normal working conditions. For the LIDAR placed on the satellite, the main source of background light during night-time operation is represented by the light of the Moon reflected by the Earth [1], which can be expressed as follows:

$$P^{A}_{\min} = \alpha_E \alpha_M R_M^2 r_{\mathrm{A}}^2 \frac{\Omega_{\mathrm{fov}}}{d_{\mathrm{EM}}^2} H_{\mathrm{Sun}} B_{\mathrm{filter}} , \tag{A14}$$

where α_E and α_M are the albedo of the Earth and the Moon, respectively, R_M is the radius of the Moon, d_{EM} is the Earth-Moon distance, H_{Sun} is the irradiance of the Sun at λ_{LIDAR}, and Ω_{fov} is the field of view of the telescope and B_{filter} is the bandwidth of the spectral filters. For the LIDAR on the ground, we estimate the background light from the analysis in Ref. [66], as follows:

$$P^{B}_{\min} = H_b \Omega_{\mathrm{fov}} \pi r_{\mathrm{B}}^2 B_{\mathrm{filter}} , \tag{A15}$$

where H_b is the brightness of the sky background. The typical value for such background lights is very small suggesting that in order to obtain some statistics about such sources, we may need to use single-photon detectors in our LIDAR system [67].

The previous analysis does not take into account the fact that the LIDAR detection from the ground will be strongly affected by the presence of the atmosphere. The air can back-scatter the light sent by Bob's LIDAR, especially when the sky is not completely clear, giving a signal that can be attributed to Eve's object. This means that without additional analysis, every time we measure a reflected power greater than $P_{\min}$, we will think that this is because of Eve's apparatus and the measured power will be used to bound its size. If part of the back-scattered light is due to the atmosphere, we will end up over-estimating the size of Eve's object and consequently its collecting efficiency. In that sense, while this issue can loosen our lower bound on the key rate, it does not make our analysis unreliable.

3. Bounds on η_{AE} and η_{EB}

In this section, we report the numerical results for Eve's collecting and resending efficiencies, obtained using the analysis provided in the previous sections. Figure 11 shows the values of η_{AE} and η_{EB}, computed, respectively, from Eqs. (A4) and (A6), as a function of z. In both graphs, the maximum value happens somewhere in the middle of the orbit. This is because we are using LIDAR on both Alice and Bob and the maximum value is achieved at the point where Eve's telescope is the biggest, which is roughly in the middle. This happens because the widths of the beams, during the propagation, vary linearly with z, while the bound on Eve's size is proportional to z^2 (equivalently, the cross section in Eq. (A8) is proportional to z^4). We see that η_{AE} remains below 0.1, while η_{EB} grows up to about 1. There are two main reasons for this behavior. First, we allow Eve to use perfect optics that generate Gaussian beams with minimal divergence and second, Bob's telescope aperture is bigger than Alice's.

Figure 12 shows the values of some quantities of the setup as a function of the coordinate z, which are useful to understand the behavior observed in Fig. 11. The r_{E} curve close to the x axis is the same as the upper curve in Fig. 10, which shows the maximum radius of the undetected Eve. The W_{E} curve represents the width of the beam, sent by Eve at distance z from Alice with a telescope of radius $r_{\mathrm{E}}(z)$, when it arrives at Bob's receiving plane. The W_{LIDAR} curve is, instead, the width of the beam sent by Alice as it propagates toward Bob. We see that when it arrives at Bob, after 500 km of traveling, the beam is about 2.5 m in radius, which is several times larger than that of Bob's

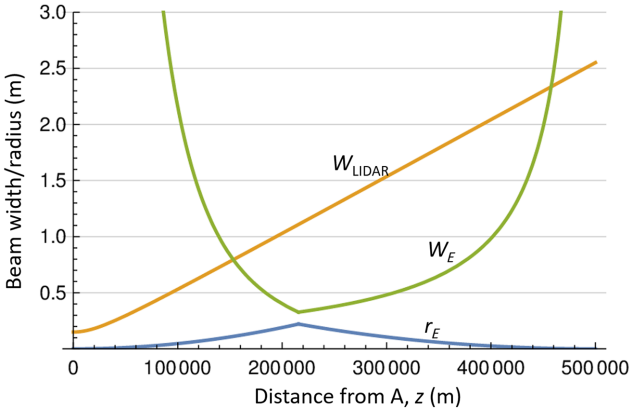

FIG. 12. The maximum radius, r_{E}, of the undetected Eve's object, the width of the propagating beam, W_{LIDAR}, sent by Alice, and the width of signal sent by Eve at point Bob, W_{E}, versus z.

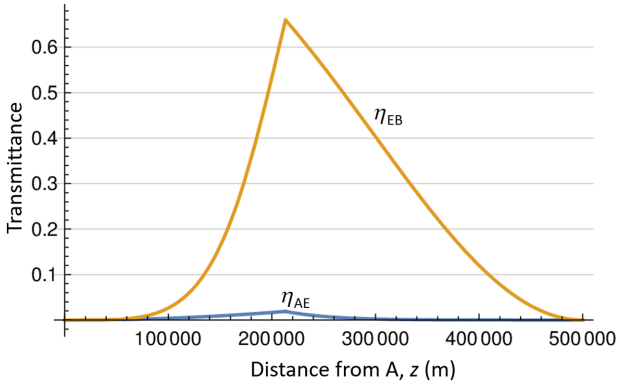

FIG. 13. The values of η_{AE} and η_{EB} for an undetected Eve, computed using Eqs. (A4) and (A6), for a power of 4 W.

telescope, giving a transmittance between the legitimate parties of $\eta_{\mathrm{AB}} = 0.05$ (only considering diffraction losses, without collection and detection losses). As for Eve, however, the minimum of the W_{E} curve is roughly 30 cm at Bob, which is smaller than Bob's telescope size, resulting in $\eta_{\mathrm{EB}} \simeq 1$. Note that W_{E}, in Eq. (A5), is inversely proportional to $r_{\mathrm{E}}(z)(L-z)$, which justifies the asymmetry in the graph.

The values in Fig. 11 can be lowered by raising the value of LIDAR's transmitted power. Note that $r_{\mathrm{E}} \propto P_T^{1/2}$, so if we raise the power by a factor of 4, to 4 W, the bound on Eve's size will be halved. In this case, smaller values of η_{AE} and η_{EB} are expected, as shown in Fig. 13. η_{AE}, in particular, reaches a maximum of about 3%, giving big room for improvement in the achievable key rate. This bound depends very strongly on the minimum measurable power P_{min}. Any improvement in the filtering techniques (defined by the parameters B_{filter} and Ω_{fov}) will improve the performance. In the same way, going to lower wavelengths will reduce the diffraction losses and improve the bound. We point out that, in practice, the monitoring can possibly be repeated with a rather low frequency, leaving the remaining time for the QKD signal exchange. This means that the power actually consumed during monitoring operation should be manageable even by small satellites. On the other hand, if QKD missions are merged with remote sensing missions used for Earth observations, then large satellite payloads and, therefore, high-power LIDAR systems can be used, which considerably improves the bounds on η_{AE} by 1–2 orders of magnitude. Examples include the 562-W LIDAR used in CALIPSO and that of 1865 W in LITE missions.

The LIDAR technique, in the simplified approach that we have used in these calculations, is sensitive to the total power reflected by objects illuminated by the transmitted light. This means that we are safe even in the situation where Eve places more flying objects, which taken alone would be smaller than the detectable size. If we detect that one object or more are passing between Alice and Bob, by measuring a received power $P_R > P_{\mathrm{min}}$, we can assume that they are all malicious, estimate their size by replacing P_{min} with P_R in the above expressions, and bound η_{AE} and η_{EB} in the real case.

We point out again that the presence of back-reflections from the atmosphere would give an over-estimation of the size of Eve when measured from Bob, which has not been considered here, leading to higher values of η_{AE} and η_{EB}. More sophisticated techniques, e.g., using the timing information obtained when using the LIDAR in the pulsed regime, should be able to address this problem. The advantage introduced by sending a beam with higher power, analyzed in Fig. 13, would be less effective for Bob, because it would also correspond to more light back-reflected by the atmosphere.

Until now we have considered the static case where the satellite is fixed at the position closest to the ground station. We study now how the maximum values of η_{AE} and η_{EB} (optimal for Eve) vary during the passage of the satellite. We show the results in Fig. 14 at $P_T = 1$ W of transmitted power for the LIDAR system, and in Fig. 15 at $P_T = 4$ W. As can be seen, both configurations perform well for high elevation angles; however, the higher power level is required to put useful bounds at low elevation angles. As pointed out before, if the available power output is limited, one can achieve the same performance by changing other parameters of the setup.

For comparison, we report in Fig. 16 the behavior of η_{AB}, from Eq. (A3), as a function of the position of the satellite. The upper curve represents only the diffraction losses, while in the lower curve other sources of loss are also considered. In particular, we assume the detection loss is 50% and transmittance of the receiving optics is 80%. The absorption in the atmosphere is accounted for by $\chi_{\mathrm{ext}} = \exp\left[-\beta \sec(\theta)\right]$, where $\beta = 0.7$ at $\lambda_{\mathrm{LIDAR}} = 800$ nm, with

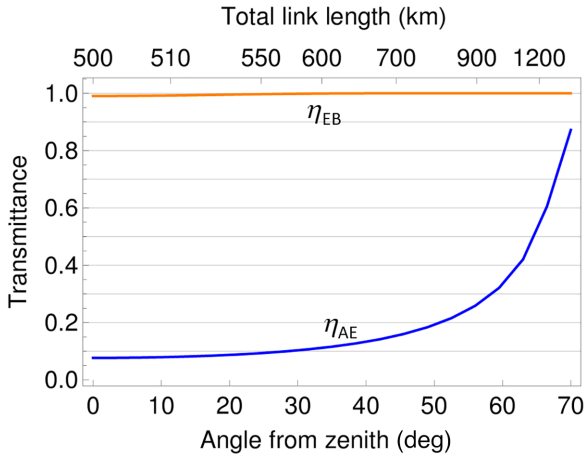

FIG. 14. The maximum values of η_{AE} and η_{EB} for an undetected Eve, as a function of the position of the satellite, for a LIDAR transmitted power of 1 W.

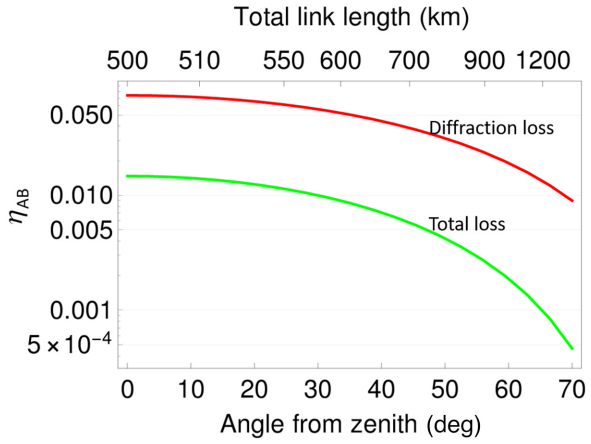

FIG. 16. The transmittance of the beam sent by A through B's aperture η_{AB} [Eq. (A3)], as a function of the position of the satellite.

θ being the angle from zenith. Note that the expression for χ_{ext} is an approximate value at large values of θ. We have, however, compared our results with that obtained from software tools such as MODTRAN 5 and the results are within an acceptable range for the purpose of this study. The inclusion of pointing errors should have a fairly small impact, about 2–3 dB.

In the previous analysis, we fixed the reflectivity of Eve's spacecraft to bound its size. The value chosen at the end of Sec. A 2, $\alpha = 0.1$, is conservative enough if one considers standard spacecraft. However, lower values of the reflectivity parameters can be reached if specific technologies are used. For example, nanostructured coatings [68] can be laid over opaque surfaces and can enable reflectivity values $< 10^{-2}$. Similar values can be obtained on transparent surfaces (such as lenses), using multilayer interferometric coatings. In Fig. 17, we report the minimum value of reflectivity parameter of Eve's surfaces to achieve $\eta_{AE} < 1$, for different positions of the satellite with respect to the ground station. This means that, by fixing all other parameters, any value of reflectivity $\alpha < \alpha_{min}$ will lead to $\eta_{AE} = 1$, so only values $\alpha > \alpha_{min}$ lead to useful bounds in our analysis. We see from Fig. 17 that if Eve uses such high-performance coatings, the LIDAR setup is no longer sensitive enough. In this case, we have to compensate for the lower reflectivity by increasing the emitted power P_T, increasing the directionality of the beam (smaller λ_{LIDAR} and/or larger W_0) or decreasing the minimum measurable power P_{min}.

APPENDIX B: PROOF OF LEMMA 1

Here, we prove Lemma 1.

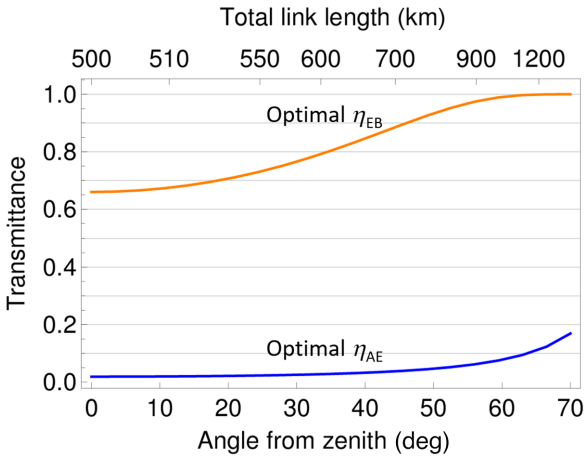

FIG. 15. The maximum values of η_{AE} and η_{EB} for an undetected Eve, as a function of the position of the satellite, for a LIDAR transmitted power of 4 W.

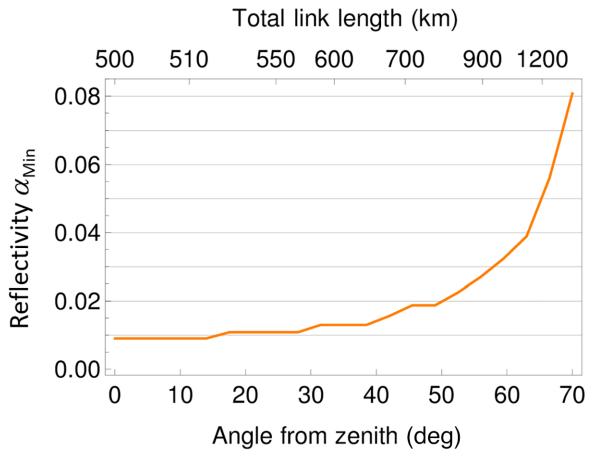

FIG. 17. The minimum value of the reflectivity parameter of E's surfaces to achieve $\eta_{AE} < 1$, as a function of the angle of the satellite with respect to the zenith of the ground station.

Proof.—Under the condition of a quantum Bob with access to B and F_0 modes, the in-principle achievable asymptotic key rate of the QKD protocol in Fig. 3 is given by the Devetak-Winter bound [15,69]:

$$r_k = H(X|E)_k - H(X|BF_0)_k, \quad k = a, b, \tag{B1}$$

where, for scenario $k = a, b$ in Fig. 3, $H(X|E)_k$ is the conditional von Neumann entropy of Alice's classical outcome X given Eve's quantum information E, whereas $H(X|BF_0)$ is the conditional entropy of Alice's outcome X given Bob's quantum information, which includes the joint state BF_0 at the output of the telescope. This is effectively a classical quantum quantum (CQQ) scenario, where Alice has a classical state but Eve and Bob hold on to their quantum states.

The entropy functions in Eq. (B1) are computed on the quantum states ρ_{XE} and ρ_{XBF_0}, which in turn are the reduced density operators of the single-round global quantum state $\rho_{XBF_0F_1F_2E}$. In the following, we compute the latter state for the setups in Figs. 3(a) and 3(b). We denote by $\mathcal{B}$ the map corresponding to the beam splitters and add subscripts on the map symbols to indicate the subsystems on which they act.

The global state obtained after one round of the protocol in the setting of Fig. 3(a) is given by

$$\begin{aligned}\rho^{(a)}_{XBF_0F_1F_2E} = \mathcal{E}_T \circ \mathcal{B}_{BF_2} \circ \mathcal{E}'_{F_0F_1} \circ \mathcal{E}_{BE} \circ \mathcal{B}_{BF_0} \circ M_A \\ \Big(|\psi_{AB}\rangle\langle\psi_{AB}| \otimes |0\rangle\langle 0|_{F_0} \otimes |\psi_F\rangle\langle\psi_F| \\ \otimes |\psi_E\rangle\langle\psi_E| \otimes |0\rangle\langle 0|_{F_2}\Big).\end{aligned} \tag{B2}$$

Then, the reduced state on subsystems XE, over which the entropy $H(X|E)$ is computed, is given by

$$\begin{aligned}\rho^{(a)}_{XE} &= \mathrm{Tr}_{BF_0F_1F_2}[\rho^{(a)}_{XBF_0F_1F_2E}] \\ &= \mathrm{Tr}_{BF_0}\Big[\mathcal{E}_{BE} \circ \mathcal{B}_{BF_0} \circ M_A(|\psi_{AB}\rangle\langle\psi_{AB}| \otimes \\ &\quad |0\rangle\langle 0|_{F_0} \otimes |\psi_E\rangle\langle\psi_E|)\Big],\end{aligned} \tag{B3}$$

where we have used the Kraus theorem to remove the outer quantum maps that act on the subsystems that are traced out.

Similarly, the global state for Fig. 3(b) is given by

$$\begin{aligned}\rho^{(b)}_{XBF_0F_1F_2E} = \mathcal{E}_T \circ \mathcal{E}_V \circ \mathcal{B}_{BF_2} \circ \mathcal{E}'_{F_0F_1} \circ \mathcal{E}_{BE} \circ \mathcal{B}_{BF_0} \circ M_A \\ \Big(|\psi_{AB}\rangle\langle\psi_{AB}| \otimes |0\rangle\langle 0|_{F_0} \otimes |\psi_F\rangle\langle\psi_F| \\ \otimes |\psi_E\rangle\langle\psi_E| \otimes |0\rangle\langle 0|_{F_2}\Big).\end{aligned} \tag{B4}$$

Note that compared to Eq. (B2), we only have the additional CPTP map $\mathcal{E}_V$ in Eq. (B4). For the reduced state, we obtain

$$\begin{aligned}\rho^{(b)}_{XE} &= \mathrm{Tr}_{BF_0F_1F_2}[\rho^{(b)}_{XBF_0F_1F_2E}] \\ &= \mathrm{Tr}_{BF_0}\Big[\mathcal{E}_{BE} \circ \mathcal{B}_{BF_0} \circ M_A(|\psi_{AB}\rangle\langle\psi_{AB}| \\ &\quad \otimes |0\rangle\langle 0|_{F_0} \otimes |\psi_E\rangle\langle\psi_E|)\Big].\end{aligned} \tag{B5}$$

From Eqs. (B3) and (B5), we observe that the reduced states on XE are the same for both scenarios, i.e., $\rho^{(a)}_{XE} = \rho^{(b)}_{XE}$, which implies that

$$H(X|E)_a = H(X|E)_b, \tag{B6}$$

since the entropy functions are computed on the same quantum state.

From Eqs. (B2) and (B4), we observe that $\rho^{(b)}_{XBF_0F_1F_2E}$ can be obtained from $\rho^{(a)}_{XBF_0F_1F_2E}$ through the following CPTP map:

$$\rho^{(b)}_{XBF_0F_1F_2E} = \mathcal{R}_{BF_0}(\rho^{(a)}_{XBF_0F_1F_2E}), \tag{B7}$$

where

$$\mathcal{R}_{BF_0} := \mathcal{E}_T \circ \mathcal{E}_V \circ \mathcal{E}_T^{-1}. \tag{B8}$$

By tracing over F_1F_2E in Eq. (B7), the reduced state of XBF_0 in Fig. 3(b) can be obtained by applying the CPTP map $\mathcal{R}_{BF_0}$ to the reduced state of Fig. 3(a), i.e.,

$$\rho^{(b)}_{XBF_0} = \mathcal{R}_{BF_0}(\rho^{(a)}_{XBF_0}). \tag{B9}$$

By the fact that quantum maps applied on the conditioning system can only increase the conditional von Neumann entropy [70], we have that

$$H(X|BF_0)_a \leq H(X|\mathcal{R}(BF_0))_a = H(X|BF_0)_b. \tag{B10}$$

Finally, by inserting Eqs. (B6) and (B10) into Eq. (B1), we obtain

$$r_b \leq r_a, \tag{B11}$$

which concludes the proof. ■

APPENDIX C: A TYPICAL TELESCOPE MODEL

In this appendix, we look at the implications of the two-mode model that we have in Fig. 3 and deduce that the telescope action can be modeled by a beam-splitter-like operation, where only one output mode is accessible. The gist of the idea is as follows. Let us denote by a_r the field operator that will be collected by the telescope, after proper focusing, at point r on the outer surface S of the receiver

telescope. We then have $[a_r, a_{r'}^\dagger] = \delta(r - r')$ and the corresponding annihilation operator for the collected optical mode, in a particular polarization, is given by

$$a = \int_S \mathrm{d}r g(r) a_r, \tag{C1}$$

where $\int_S \mathrm{d}r |g(r)|^2 = 1$; hence $[a, a^\dagger] = 1$. Here, we have assumed that the collected light is coupled to a single-mode fiber.

In principle, the operator $\mathcal{E}_T$, acting in input modes B and F_0, should give us the same output relationship as in Eq. (C1). In reality, in addition to the bypass channel and Eve's channel, the telescope could capture other background modes as well. In the worst-case scenario, however, we can always assume that all these other modes are controlled by Eve and that she can decide whether leave them as they are or control them, via its operator $\mathcal{E}$. The implication of this assumption is that we can assume that $\mathcal{E}_T$ is a unitary map, which fully models the action of the telescope. In particular, the collected light from mode F_0 combined with the collected light from mode B must fully recover the action modeled by Eq. (C1). That is, if we model the collected light for mode F_0 by

$$a_F = \int_S \mathrm{d}r f(r) a_r, \tag{C2}$$

with $\int_S \mathrm{d}r |f(r)|^2 = 1$, and the collected light for mode B by

$$a_B = \int_S \mathrm{d}r h(r) a_r, \tag{C3}$$

with $\int_S \mathrm{d}r |h(r)|^2 = 1$, we should then have $[a_F, a_B] = 0$, as they originate from different spatial modes, and

$$a = \alpha a_F + \beta a_B, \tag{C4}$$

to make sure that the two modes fully model the light collected by the telescope. The choice of linear combination above matches what a typical telescope does to different impinging modes of light. The first condition implies that the weight functions f and h must satisfy the orthogonality condition $\int_S \mathrm{d}r f(r) h^*(r) = 0$, whereas the second condition implies that

$$g(r) = \alpha f(r) + \beta h(r), \tag{C5}$$

which results in

$$\alpha = \int_S \mathrm{d}r g(r) f^*(r), \beta = \int_S \mathrm{d}r g(r) h^*(r). \tag{C6}$$

In addition, given that g, f, and h are normalized and the latter two are orthogonal, we have $|\alpha|^2 + |\beta|^2 = 1$, which results in the following relationship:

$$a = \sqrt{\eta_T} a_B + \sqrt{1 - \eta_T} a_F, \tag{C7}$$

where

$$\eta_T = \int_S \mathrm{d}r g(r) h^*(r) = 1 - \int_S \mathrm{d}r g(r) f^*(r). \tag{C8}$$

The expression in Eq. (C7) resembles one output of a beam splitter with transmissivity η_T, following our use in the main text.

APPENDIX D: COVARIANCE-MATRIX CALCULATIONS

In this appendix, we calculate the CM for the setting given in Fig. 4. While this is a special channel configuration, with proper choices of parameters, it can be used to model several cases of interest to our work. For instance, by choosing η_S to be zero, we effectively remove the bypass channel and the remaining setup would then correspond to an optimal attack by Eve in the extended Alice-Bob model so long as the values assigned to η_{AE}, η_{E}, and η_T are within 0 and 1.

To calculate the CM between all parties involved, i.e., Alice, Bob, and Eve, we consider the entanglement-based picture in Fig. 4 and start with the CM corresponding to the TMSV state $|\psi_{AB}\rangle$ with variance V, given by

$$\mathbf{V}_{AB} = \begin{pmatrix} V\mathbb{1} & c\mathbb{Z} \\ c\mathbb{Z} & V\mathbb{1} \end{pmatrix}, \tag{D1}$$

where $c = \sqrt{V^2 - 1}$. On one leg of this TMSV state, Alice performs a heterodyne measurement, while she sends the other beam toward Bob. On its way, the latter beam experiences some pure loss, modeled by η_{AE}, which splits the signal into two beams. One undergoes Eve's attack, whereby it would interfere, at a beam splitter with transmissivity η_{E}, with Eve's TMSV state $|\psi_{EE'}\rangle$ with variance V_E, and the following CM:

$$\mathbf{V}_{EE'} = \begin{pmatrix} V_E\mathbb{1} & c_E\mathbb{Z} \\ c_E\mathbb{Z} & V_E\mathbb{1} \end{pmatrix}, \tag{D2}$$

where $c_E = \sqrt{V_E^2 - 1}$. The other output of η_{AE} beam splitter undergoes additional loss, which is modeled via the beam splitter with transmissivity η_S. Eventually, the two beams reconcile at the last beam splitter with transmissivity η_T.

Using linear optics algebra, we have modeled the above beam-splitter operations using relevant matrices to find the CM of the purified state between all modes, i.e.,

$ABEE'F_0F_1$. After tracing out modes F_0 and F_1, as they are assumed inaccessible to all parties, we obtain

$$\mathbf{V}_{ABEE'} = \begin{pmatrix} V\mathbb{1} & C_{AB}\mathbb{Z} & 0\mathbb{1} & C_{AE'}\mathbb{Z} \\ C_{AB}\mathbb{Z} & V_B\mathbb{1} & C_{BE}\mathbb{Z} & C_{BE'}\mathbb{1} \\ 0\mathbb{1} & C_{BE}\mathbb{Z} & V_E\mathbb{1} & C_{EE'}\mathbb{Z} \\ C_{AE'}\mathbb{Z} & C_{BE'}\mathbb{1} & C_{EE'}\mathbb{Z} & V_{E'}\mathbb{1} \end{pmatrix}, \quad \text{(D3)}$$

where the first row and column correspond to mode A and its covariance elements with other modes, the second to B, and the third and fourth to E and E', respectively. In Eq. (D3),

$$\begin{aligned} C_{AB} &= \sqrt{T_{\rm eq}}c, \\ C_{AE'} &= -\sqrt{\eta_{\rm AE}(1-\eta_{\rm E})}c, \\ V_B &= T_{\rm eq}(V-1)+1+\xi_{\rm eq}^{\rm Rx}, \\ C_{BE} &= \sqrt{(1-\eta_{\rm E})\eta_T}c_E, \\ C_{BE'} &= \sqrt{\eta_{\rm E}(1-\eta_{\rm E})\eta_T}\Big(-\big(\eta_{\rm AE}(V-1)+1\big)+V_E\Big) \\ &\quad -\sqrt{\eta_{\rm AE}(1-\eta_{\rm AE})(1-\eta_{\rm E})\eta_S(1-\eta_T)}(V-1), \\ C_{EE'} &= \sqrt{\eta_{\rm E}}c_E, \\ V_{E'} &= (1-\eta_{\rm E})[\eta_{\rm AE}(V-1)+1]+\eta_{\rm E}V_E, \end{aligned} \quad \text{(D4)}$$

where

$$T_{\rm eq} = \Big(\sqrt{\eta_{\rm AE}\eta_{\rm E}\eta_T}+\sqrt{(1-\eta_{\rm AE})\eta_S(1-\eta_T)}\Big)^2, \quad \text{(D5)}$$

appearing in the coefficient of C_{AB} entry, is the observed value of transmissivity in the link, and

$$\xi_{\rm eq}^{\rm Rx} = T_{\rm eq}\xi = (1-\eta_{\rm E})\eta_T(V_E-1) \quad \text{(D6)}$$

is effectively the observed value of excess noise at the receiver, with ξ being its equivalent at the transmitter end. As one would expect, the excess noise is a function of Eve's variance V_E and is simply the amount of noise that enters Bob's receiver via the two beam splitters on the path between Bob and Eve. Similarly, $\sqrt{T_{\rm eq}}$ in Eq. (D5) is the sum of the amplitudes in the two pathways from Alice to Bob. Similar calculations show that if instead of the pure-loss bypass channel, we assume a thermal-loss bypass channel with a noise variance V_S, there would be an additional term for $\xi_{\rm eq}^{\rm Rx}$, given by $(1-\eta_S)(1-\eta_T)(V_S-1)$, which accounts for the noise coming from the bypass channel, with no change in $T_{\rm eq}$.

The above CM can be used to calculate the key rate in different scenarios. For any given observed value of $T_{\rm eq} \leq 1$ and $\xi \geq 0$, we can search the $\eta_S - \eta_T$ space for the minimum guaranteed key rate. One could also account for other sources of trusted noise at the receiver, such as electronic noise, by adjusting the above parameters but for the purpose of our discussion on CV QKD in the restricted case, the above framework is sufficiently detailed.

[1] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, Feasibility of satellite quantum key distribution, New J. Phys. **11**, 045017 (2009).

[2] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links, IEEE J. Sel. Areas Commun. **27**, 1582 (2009).

[3] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss, Phys. Rev. A **84**, 062326 (2011).

[4] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, Corrigendum: A comprehensive design and performance analysis of low Earth orbit satellite quantum communication (2013 New J. Phys. **15** 023006), New J. Phys. **16**, 069502 (2014).

[5] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon, Entanglement over global distances via quantum repeaters with satellite links, Phys. Rev. A **91**, 052325 (2015).

[6] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook, IEEE Commun. Surv. Tutorials **21**, 881 (2018).

[7] R. Bedington, J. M. Arrazola, and A. Ling, Advances in quantum teleportation, Nat. Commun. **3**, 30 (2017).

[8] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Air-to-ground quantum communication, Nat. Photon. **7**, 382 (2013).

[9] J.-Y. Wang *et al.*, Direct and full-scale experimental verifications towards ground-satellite quantum key distribution, Nat. Photon. **7**, 387 (2013).

[10] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations, Phys. Rev. A **92**, 052339 (2015).

[11] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Experimental satellite quantum communications, Phys. Rev. Lett. **115**, 040502 (2015).

[12] K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, C. R. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, and G. Leuchs, Quantum-limited measurements of optical signals from a geostationary satellite, Optica **4**, 611 (2017).

[13] H. J. Kimble, The quantum Internet, Nature **453**, 1023 (2008).

[14] S. Pirandola and S. L. Braunstein, Unite to build the quantum Internet, Nature **532**, 169 (2016).

[15] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and

P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).
[16] C. Liorni, H. Kampermann, and D. Bruß, Quantum repeaters in space, New J. Phys. **23**, 053021 (2021).
[17] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).
[18] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photonics **15**, 530 (2021).
[19] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).
[20] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Large scale quantum key distribution: Challenges and solutions, Opt. Express **26**, 24260 (2018).
[21] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution over 1000 km fiber distance, arXiv:2303.15795 [quant-ph] (2023).
[22] S.-K. Liao *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).
[23] S.-K. Liao *et al.*, Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. **120**, 030501 (2018).
[24] S.-K. Liao *et al.*, Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, Nat. Photon. **311**, 509 (2017).
[25] J.-G. Ren *et al.*, Ground-to-satellite quantum teleportation, Nature **549**, 70 (2017).
[26] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Res. **3**, 013279 (2021).
[27] S. Pirandola, Satellite quantum communications: Fundamental bounds and practical security, Phys. Rev. Res. **3**, 023130 (2021).
[28] M. Ghalaii and S. Pirandola, Quantum communications in a moderate-to-strong turbulent space, Commun. Phys. **5**, 38 (2022).
[29] M. Ghalaii and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution in free-space channels, arXiv:2212.06687 (2022).
[30] T. Vergoossen, R. Bedington, J. A. Grieve, and A. Ling, Satellite quantum communications when man-in-the-middle attacks are excluded, Entropy **21**, 387 (2019).
[31] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, Secret-key distillation across a quantum wiretap channel under restricted eavesdropping, Phys. Rev. Appl. **14**, 024044 (2020).
[32] A. Vázquez-Castro, D. Rusca, and H. Zbinden, Quantum keyless private communication versus quantum key distribution for space links, Phys. Rev. Appl. **16**, 014006 (2021).
[33] M. Sasaki, Quantum networks: Where should we be heading?, Quantum Sci. Technol. **2**, 020501 (2017).
[34] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J. **54**, 1355 (1975).
[35] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[36] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).
[37] C. Zhang, X.-L. Hu, C. Jiang, J.-P. Chen, Y. Liu, W. Zhang, Z.-W. Yu, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental side-channel-secure quantum key distribution, Phys. Rev. Lett. **128**, 190503 (2022).
[38] *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* (1984).
[39] M. Legre and B. Huttner, Quantum-enhanced physical layer cryptography: A new paradigm for free-space key distribution (2017), qCrypt 2017.
[40] V. Scarani and R. Renner, Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing, Phys. Rev. Lett. **100**, 200501 (2008).
[41] M. Tomamichel, *Quantum Information Processing with Finite Resources* (Springer International Publishing, London, 2016).
[42] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. **88**, 057902 (2002).
[43] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature **421**, 238 (2003).
[44] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photonics **9**, 397 (2015).
[45] L. Ruppert, C. Peuntinger, B. Heim, K. Gunthner, V. C. Usenko, D. Elser, G. Leuchs, R. Filip, and C. Marquardt, Fading channel estimation for free-space continuous-variable secure quantum communication, New J. Phys. **21**, 123036 (2019).
[46] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, Feasibility of satellite-to-ground continuous-variable quantum key distribution, npj Quantum Inf. **7**, 3 (2021).
[47] I. Derkach and V. C. Usenko, Applicability of squeezed- and coherent-state continuous-variable quantum key distribution over satellite links, Entropy **23**, 55 (2021).
[48] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel, Quantum Eng. **2**, e50 (2020).
[49] R. García-Patrón and N. J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, Phys. Rev. Lett. **97**, 190503 (2006).
[50] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian attacks in continuous-variable quantum cryptography, Phys. Rev. Lett. **97**, 190502 (2006).
[51] S. Pirandola, S. L. Braunstein, and S. Lloyd, Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography, Phys. Rev. Lett. **101**, 200504 (2008).

[52] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).
[53] L. T. Vidarte, Ph.D. thesis, Université Paris-Saclay, 2019.
[54] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).
[55] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* (IEEE, Chicago, 2004), p. 136.
[56] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).
[57] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).
[58] J. Yin *et al.*, Entanglement-based secure quantum cryptography over 1,120 kilometres, Nature **582**, 501 (2020).
[59] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Detecting single infrared photons with 93% system efficiency, Nat. Photonics **7**, 210 (2013).
[60] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptol. **18**, 133 (2005).
[61] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, Memory-assisted measurement-device-independent quantum key distribution, New J. Phys. **16**, 043005 (2014).
[62] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, Quantum **2**, 77 (2018).
[63] D. Bunandar, L. C. G. Govia, H. Krovi, and D. Englund, Numerical finite-key analysis of quantum key distribution, npj Quantum Inf. **6**, 104 (2020).
[64] B. E. A. Saleh and M. C. Teich, in *Fundamentals of Photonics* (New Jersey, John Wiley & Sons, Ltd, 2007), 2nd ed., Chap. 3.
[65] H. Klinkrad, Monitoring space—efforts made by European countries (2004).
[66] M. Er-long, H. Zheng-fu, G. Shun-sheng, Z. Tao, D. Dasheng, and G. Guang-can, Background noise of satellite-to-ground quantum key distribution, New J. Phys. **7**, 215 (2005).
[67] J. Tachella, Y. Altmann, N. Mellado, A. McCarthy, R. Tobin, G. S. Buller, J.-Y. Tourneret, and S. McLaughlin, Real-time 3D reconstruction from single-photon LIDAR data using plug-and-play point cloud denoisers, Nat. Commun. **10**, 1 (2019).
[68] J. Xi, M. F. Schubert, J. K. Kim, E. Fred Schubert, M. Chen, S.-Y. Lin, W. Liu, and J. A. Smart, Optical thin-film materials with low refractive index for broadband elimination of fresnel reflection, Nat. Photonics **1**, 176 (2007).
[69] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A: Math., Phys. Eng. Sci. **461**, 207 (2005).
[70] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010), 10th ed.