# Quantum Keyless Private Communication Versus Quantum Key Distribution for Space Links

A. Vázquez-Castro,[1,*] D. Rusca,[2] and H. Zbinden[2]

[1] *Autonomous University of Barcelona and Center of Space Studies and Research, CERES (IEEC-UAB), Campus de Bellaterra, Barcelona 08290, Spain*

[2] *Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, Geneva 4 CH-1211, Switzerland*

(Received 4 December 2020; revised 10 April 2021; accepted 9 June 2021; published 2 July 2021)

We study information-theoretical security for space links between a satellite and a ground station. Quantum key distribution (QKD) is a well-established method for information-theoretical secure communication, giving the eavesdropper unlimited access to the channel and technological resources limited by only the laws of quantum physics. But QKD for space links is extremely challenging, the achieved key rates are extremely low, and daytime operating impossible. However, eavesdropping on a channel in free space without being noticed seems complicated, given the constraints imposed by orbital mechanics. If we also exclude the eavesdropper's presence in a given area around the emitter and receiver, we can guarantee that he has access to only a fraction of the optical signal. In this setting, quantum keyless private (direct) communication based on the wiretap channel model is a valid alternative to provide information-theoretical security. Like for QKD, we assume that the legitimate users are limited by state-of-the-art technology, while the potential eavesdropper is only limited by physical laws: either by specifying her detection strategy (Helstrom detector) or by bounding her knowledge, assuming the most powerful strategy through the Holevo information. Nevertheless, we demonstrate information-theoretical secure communication rates (positive keyless private capacity) over a classical-quantum wiretap channel using on-off keying of coherent states. We present numerical results for a setting equivalent to the recent experiments with the Micius satellite and compare them to the fundamental limit for the secret key rate of QKD. We obtain much higher rates compared with QKD with an exclusion area of less than 13 m for low earth orbit satellites. Moreover, we show that the wiretap channel quantum keyless privacy is much less sensitive to noise and signal dynamics and daytime operation is possible.

DOI: 10.1103/PhysRevApplied.16.014006

## I. INTRODUCTION

Quantum key distribution (QKD) was proposed in 1984 by Bennet and Brassard [1]. Today, commercial fiber-based systems are available with operational distances steadily increasing [2,3]. Recently, QKD has also been realized between the Chinese satellite Micius and ground stations [4,5]. Currently, there are several national initiatives to deploy a QKD network, including terrestrial and space links. In particular, there is an increasing and unprecedented interest in space telecommunication networks; our scenarios of interest as illustrated in Fig. 1 (this work focuses on the blue link).

A QKD protocol assumes that two distant legitimate parties, Alice and Bob, have at their disposal the following resources: secure offices, access to an untrusted quantum channel and an authenticated classical public channel, and perfectly random numbers. A potential eavesdropper, Eve, has complete control of the quantum channel. In particular, she can intercept all quantum states and perform any measurement allowed by quantum mechanics, including entangling the states with some auxiliary system and storing them in perfect quantum memories. Moreover, she can send signals to Bob over a lossless channel. Despite this extreme power limited only by the laws of quantum physics, QKD protocols are now well established and furnished with security proofs [6–9]. So the generated keys together with encoding using one-time-pad guarantee information-theoretical secure communication [10,11]. Alternatively, physical-layer security also relies on information-theoretical principles in the sense that Eve has unlimited computing power. However, she has a physical disadvantage with respect to the legitimate

[*] angeles.vazquez@uab.es

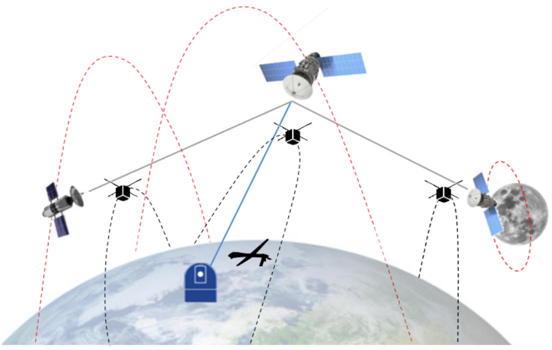

FIG. 1. Our scenarios of interest: celestial mechanics dictates orbit dynamics for legitimate parties and eavesdroppers.

users. In particular, Eve can intercept only a fraction of the signal sent by Alice. In 1975, Wyner proposed a protocol based on a so-called degraded wiretap channel (for a classical channel) [12–14]. The information leakage to the eavesdropper is determined with an information-theoretical measure, which has been strengthened from Wyner's (weak) security to the so-called strong security criterion by Csiszár and Körner [15] and Maurer [16], until achieving cryptographic semantic security [17]. In a quantum setting, where Alice and Bob use an authenticated quantum channel for (keyless) secure direct communication, the asymptotically achievable rate, the private capacity, subject to the strong security criterion was determined by Cai *et al.* [18] and Devetak [19,20].

On the one hand, QKD with satellites is extremely challenging due to the small signal strength of the order of one photon per pulse, the high channel loss, delays due to the iterative protocol, and the sensitivity to background noise, which does not allow key exchanges during daytime. On the other hand, eavesdropping without being noticed seems to be very complicated as well in a free-space scenario. So it makes a lot of sense to consider a few reasonable assumptions that limit the power of Eve. Indeed, due to the laws of celestial mechanics, a satellite cannot be parked in the line of sight between Alice's satellite and Bob's ground station (or satellite), which prevents intercept and resend attacks. Eve could position her satellite very close or eventually attach it to Alice's satellite. This would allow Eve to exploit side channels (e.g., monitoring electronic signals), but this scenario is excluded in QKD that relies by definition on secure offices. Similarly, Eve could place a telescope close to Bob's, but again we may introduce an exclusion region under the control of Bob, within which Eve cannot install a big telescope.

There is some initial work investigating the consequences of restricted power for Eve on the performance of QKD links [21–24]. However, given their additional, reasonable assumptions, we find exactly the scenario where keyless private communication is possible. This type of secret transmission and its practical comparison with QKD have been studied in Refs. [25,26]; however, without assuming a quantum channel.

In this paper, we show that physical layer encryption is a reasonable choice for satellite communication over the quantum space channel. In Sec. II, we introduce the one-way wiretap protocol and identify its asymptotic information-theoretical secure and reliable rate: the private capacity. In Sec. III, we propose a simple yet accurate channel model using binary modulated coherent states [on-off keying (OOK)], and derive and analyze the private capacity for Bob using realistic, state-of-the-art photon counting detectors while the signal reception by Eve is limited by only the laws of physics. Finally, we present numerical results for a realistic scenario taking the performance of the Micius system as a reference and compare it to the fundamental limit for the secret key rate of QKD [27].

## II. DESCRIPTION OF THE PROTOCOL

Our protocol is based on the classical one-way wiretap protocol proposed in Refs. [12,15] where secret bits are channel encoded and sent over $n$ uses of a physical channel. In this protocol, Alice sends messages to Bob through a communication channel denoted as the main channel, but her signal also reaches Eve through another channel, called the wiretap channel. The fundamental difference in our protocol with respect to the classical protocol is that we use a quantum carrier of information and exploit quantum properties at the detection. We assume OOK for lighter analytical treatment, but other binary modulations can be used, e.g., binary phase shift keying.

The protocol contains the following steps.

1. *Encoding.* Alice, the legitimate information transmitter, sends a stream of secret information bits (any data, video, pictures, etc.) to a stochastic wiretap encoder. Information theoretically, this encoding is described as Alice selects a codeword $X^n$ to send her secret message $M$. The signal is meant for Bob, but part of it is leaked to the environment represented by the omnipresent Eve. The secrecy depends on the structure of this encoder, which is characterized by the rate $R = k/n$ (where $k$ is the number of secret bits), the error probability $\epsilon_n$, and the information leakage measured by an information-theoretical measure, which we denote as $\delta_n$.

2. *State preparation.* For each use of the channel, the legitimate information transmitter (Alice) prepares a coherent state modulated by the random variable $X \in \mathcal{X} = \{0, 1\}$, where $X = 0$ with probability $q$ and $X = 1$ with probability $1 - q$. The OOK states transmitted by Alice are the vacuum state, $|\alpha_0\rangle = |0\rangle$, and

$$|\alpha_1\rangle = e^{-|\alpha_1|^2/2} \sum_{n=0}^{\infty} \frac{\alpha_1^n}{(n!)^{1/2}} |n\rangle . \quad (1)$$

The probability $q$ is not decided *a priori* as part of the protocol; it needs to be optimized depending on the assumptions at the detection and the physical propagation channel (Sec. III).

3. *Measurement.* After $n$ transmissions over the quantized propagating field, Bob receives $B^n$ and Eve $E^n$. Bob estimates his received coherent state after measuring the arriving light and obtains $Y^n$. He disposes of state-of-the-art (but not perfect) detectors, whereas Eve may apply the best quantum detection strategy to obtain $Z^n$.
4. *Decoding.* Bob and Eve send their estimated received states to the decoder. The concrete construction of encoder and decoder are assumed to be publicly known. The values of $\epsilon_n$ and $\delta_n$ depend on the choice of this code.

According to the wiretap theory, even if the eavesdropper is computationally unbounded, the wiretap code ensures that if $R$ is an achievable rate, both $\epsilon_n$ and $\delta_n$ (after decoding) tend to zero for large $n$,

$$\lim_{n\to\infty} \epsilon_n = \lim_{n\to\infty} \delta_n = 0, \tag{2}$$

which means that the error probability and the information leakage towards Eve can be made arbitrarily low. Upper bounds are also known for the speed of convergence rate of leaked information [28]. Hence, the protocol jointly provides information-theoretical reliable and secure communication. The supremum of rates given in step 1 of our protocol, $R$, is called the private capacity and for the classical-quantum wiretap channel subject to the (average) error probability for $\epsilon_n$ and strong security criterion for the security parameter $\delta_n$, it has been determined in Refs. [18,19] (see therein for the exact definitions of parameters $\epsilon_n$ and $\delta_n$). The meaning of strong security is that, given a uniform distribution of the message to be transmitted through the channel, the eavesdropper shall obtain no information about it [29]. This criterion is the most common security criterion in classical and quantum information theory. The metric of strong security is the amount of mutual information leaked to Eve.

When Bob's channel is degradable, the private capacity of the quantum wiretap protocol (with quantum channel and information) is [20]

$$C_P(\mathcal{N}) = \sup_{\rho_{\text{in}}} I_c(\rho_{\text{in}}, \mathcal{N}), \tag{3}$$

where $\rho_{\text{in}}$ is the input density matrix, $\mathcal{N}$ denotes the classical-quantum channel (see Fig. 2), and $I_c(\rho_{\text{in}}, \mathcal{N})$ is the coherent information defined as

$$I_c(\rho_{\text{in}}, \mathcal{N}) = S[\mathcal{N}_B(\rho_{\text{in}})] - S[\mathcal{N}_E(\rho_{\text{in}})] \tag{4}$$

with $S$ the von Neumann entropy. In the next sections we characterize the degradable channel of our practical (energy-constrained) protocol over space links, which we use to derive the private capacity.

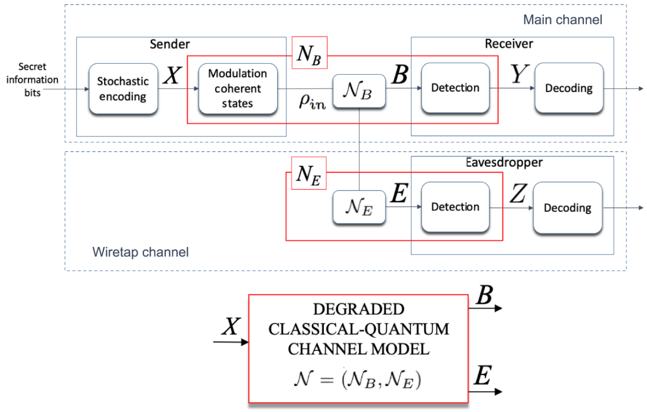

FIG. 2. The main channel and the wiretap channel (top) and the information-theoretical representation of the degraded classical-quantum channel (bottom).

The (physical) description of our protocol is illustrated in Fig. 2 (top). The figure shows encoded bits modulating coherent states, the quantum channel $\mathcal{N} = (\mathcal{N}_B, \mathcal{N}_E)$, the resulting classical channel after detection $N = (N_B, N_E)$, as well as the information-theoretical representation (bottom).

## III. CALCULATION OF THE PRIVATE CAPACITY $C_P$

First, we build a model for the classical-quantum channel of our protocol. The legitimate transmitter, Alice, is on a satellite while the legitimate receiver, Bob, is on Earth. We assume a single-mode free-space quantum bosonic channel (for the wiretap channel in the semiclassical regime, see Ref. [30]). The overall efficiency of Bob's channel is $\eta$. The coefficient $\gamma \in (0, 1)$ characterizes the channel degradation. Hence, the efficiency of Eve's channel is $\gamma\eta$.

According to step 2 of our protocol, the received states are simply the vacuum, or $|\sqrt{\eta}\alpha_1\rangle$ and $|\sqrt{\eta\gamma}\alpha_1\rangle$ for Bob and Eve, respectively. The wiretap channel transition probabilities depend on the coherent states received by Bob and Eve and by their detection strategies. For practical purposes, we assume that Bob uses standard single-photon detectors, i.e., a threshold detector. For Bob, we also take into account the limited detection efficiency (included in $\eta$), the dark count probability $p_{\text{dark}}$ and the stray light with a Poisson photon number distribution, and average $\eta_0\Delta$, where $\eta_0$ is the optical loss between the telescope input lens and the detector, and $\Delta$ is the average number of noise photons for a given collection angle and the given frequency and temporal windows (see Appendix D). The conditional probabilities that Bob detects $y$ given that Alice sent $x$ are illustrated in Fig. 3 with $\epsilon_0 = (1 - p_{\text{dark}})e^{-\eta_0\Delta}$

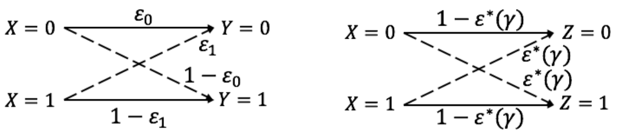

FIG. 3. Probabilistic detection models assumed for Bob and Eve to obtain $Y$ and $Z$, respectively.

and $\epsilon_1 = (1-p_{\text{dark}})e^{-(\eta\mu+\eta_o\Delta)}$, where we have set $\mu = |\alpha_1|^2$.

Eve instead performs an optimal quantum detection. For the single observation, this leads to the optimal error probability $\epsilon^*$, which can be calculated as (see Refs [31,32] and Lemma 3.1 of Ref. [33])

$$\begin{aligned}\epsilon^* &= \min_{0\leq\Pi\leq\mathbf{1}} [q\,\text{Tr}(\mathbf{1}-\Pi)\rho_1 + (1-q)\text{Tr}\,\Pi\rho_0]\\ &= \tfrac{1}{2} - \tfrac{1}{2}\|q\rho_1 - (1-q)\rho_0\|_1, \end{aligned}\tag{5}$$

where $\Pi$ is the positive operator valued measure element corresponding to $\rho_1$, and $\|\cdot\|_1$ stands for the trace norm. In the binary source scenario, this bound is achieved by the Holevo-Helstrom projector [34,35], for which several practical implementations have been proposed, such as the Kennedy receiver [36], the Dolinar receiver [37], or the Sasaki-Hirota receiver [38,39]. The optimal error probability of Eve resulting from Eq. (5) becomes

$$\epsilon^*(\gamma) = [1-\sqrt{1-4q(1-q)e^{-\eta\gamma\mu}}]/2. \tag{6}$$

The private capacity for our wiretap channel model coincides with the classical secrecy capacity and is defined as

$$C_P(\gamma) = \max_q\{I(X;Y) - I(X;Z|\gamma)\}, \tag{7}$$

where $I(X,Y)$ is the Shannon mutual information of Alice using a state-of-the-art photon counting detector and $I(X;Z|\gamma)$ is the maximum Shannon mutual information that Eve can physically detect. For our setting as presented in Sec. IV, a uniform input probability (i.e., $q=0.5$) is very close to optimum (see Appendix A), and we have

$$C_P(\gamma) = \left[h[\epsilon^*(\gamma)] + h\left(\frac{\epsilon_0+\epsilon_1}{2}\right) - \frac{h(\epsilon_1)+h(\epsilon_0)}{2} - 1\right]_+, \tag{8}$$

where $[\cdot]_+$ means the positive part and we have used the notation $h(\cdot)$ as the binary Shannon entropy. If we now restrict Eve to the laws of quantum electrodynamics, we obtain the Devetak-Winters rate [40] for our protocol,

$$R_{\text{DW}}(\gamma) = I(X,Y) - \chi(X;E|\gamma), \tag{9}$$

where $I(X;Y)$ is the Shannon mutual information of Alice's choice for the input probability, measured by a state-of-the-art photon counting detector.

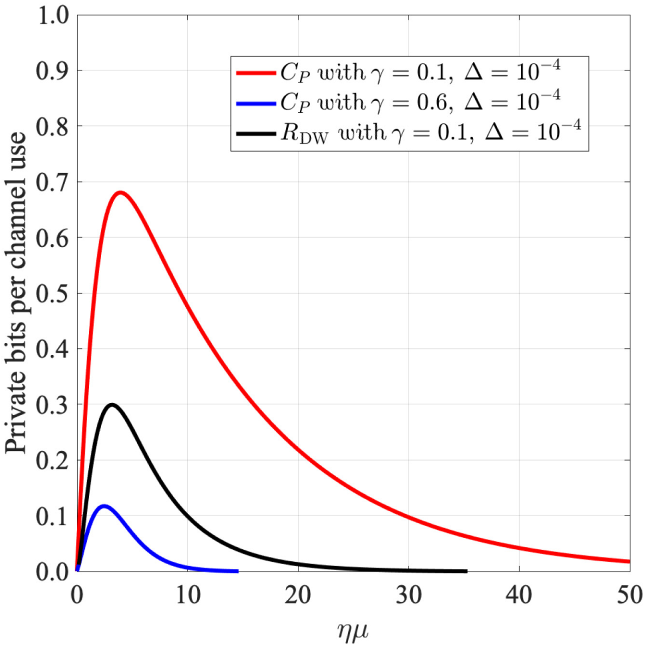

FIG. 4. Private capacity of OOK for $\gamma=0.1$ and $\gamma=0.6$ ($p_{\text{dark}}\approx 0$, $\eta_o=1$, $\Delta=10^{-4}$). For comparison, we also plot the numerical values of $R_{\text{DW}}$ for $\gamma=0.1$.

The quantity $\chi(X;E|\gamma)$ is the Holevo bound for the eavesdropper, which for OOK modulation and uniform priors (i.e., $q=0.5$), reduces to $\chi(X;E|\gamma) = S[(\langle 0\,|0\rangle + \langle\sqrt{\eta\gamma}\alpha_1\,|\sqrt{\eta\gamma}\alpha_1\rangle)/2]$. Letting $\epsilon(\gamma) = \langle 0\,|\sqrt{\eta\gamma}\alpha_1\rangle$, for uniform priors (i.e., $q=0.5$), it is easy to show that

$$\begin{aligned}R_{\text{DW}}(\gamma) = \Bigg[&h\left(\frac{\epsilon_0+\epsilon_1}{2}\right) - \frac{h(\epsilon_1)+h(\epsilon_0)}{2}\\ &- h\left(\frac{1+\epsilon(\gamma)}{2}\right)\Bigg]_+. \end{aligned}\tag{10}$$

The numerical calculation is shown in Fig. 4. We observe that the private rate in Eq. (7) is as high as 0.68 for $\gamma=0.1$ (with little sensitivity to noise, see Appendix B). And even for adverse channel conditions ($\gamma$ close to 1), there is a positive secrecy rate for reasonable noise (e.g., up to $\gamma=0.6$ for $\Delta=10^{-4}$); however, we show below that in practice it is best to aim for $\gamma<0.1$. For comparison, we have also plotted Eq. (10) for $\gamma=0.1$. We observe a substantial decrease, which is also affected by noise; however, we still get significant positive rates. In the following, we assume the realistic setting of Eve using Helstrom detection.

## IV. THE MICIUS SATELLITE: A CONCRETE EXAMPLE OF AN ORBIT-EARTH OPTICAL LINK

As a realistic physical scenario, we use as a reference the recent experiment of QKD with the Chinese low earth orbit (LEO) satellite Micius [4,5]. The geometry is shown

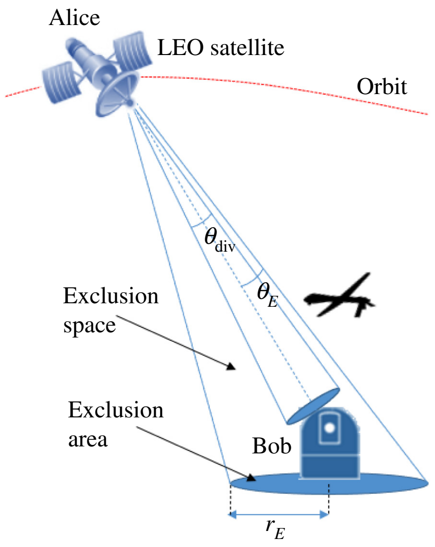

FIG. 5. Geometry for the secure and reliable communication of our wiretap protocol showing the exclusion radius $r_E$.

in Fig. 5. The satellite has an orbit of about 500 km above the Earth's surface and exchanges keys over distances up to 1200 km if the satellite is close to the horizon. The transmitter is equipped with a 300 mm Cassegrain telescope featuring a far-field divergence $\theta_{\text{div}}$ of 10 $\mu$rad (full angle at $1/e^2$). The receiver at the ground station has a telescope with a diameter $D_R$ of 1 m.

We can approximate the fraction of the light collected by Bob, the free-space loss $\eta_f^B$, as the ratio of the telescope area and the footprint area,

$$\eta_f^B = \frac{A_R}{A_F} = \frac{\pi(D_R/2)^2}{\pi(D_F/2)^2} = \frac{D_R^2}{\theta_{\text{div}}^2 d_B^2} \tag{11}$$

with

$$D_F \approx \theta_{\text{div}} d,$$

where $d_B$ is the distance between the transmitter and receiver.

The number of photons detected by Bob is given by $\eta\mu = \eta_f^B \eta_b \mu$, where $\eta_b$ is the total additional loss of Bob depending on the experimental situation. In the Micius experiment those are an atmospheric turbulence of 3–8 dB ($\eta_{\text{atm}}$), pointing errors ($\eta_p$) less than 3 dB, an overall optical loss ($\eta_o$) from the telescope input lens to detector 7.4 dB detector, and a detector efficiency $\eta_{\text{det}}$ of 50% (3 dB) (see Appendix D). In the following we calculate with a loss $\eta_b$ of 20 dB (1%).

For Eve, we calculate $\eta_f^E$ as in Eq. (11), but we add a factor that takes into account the light intensity outside the exclusion angle, supposing a Gaussian angular distribution of the beam of

$$\eta_f^E = \frac{(D_R^E)^2}{\theta_{\text{div}}^2 d_E^2} e^{-2(2\theta_E/\theta_{\text{div}})^2}. \tag{12}$$

Then, the number of photons detected by Eve becomes simply $\eta_f^E \mu = \gamma\eta\mu$, as we assume no additional loss for Eve. Hence, for fixed antenna sizes, we can easily calculate $\gamma$ as

$$\gamma(d_B, d_E, \eta_b, \theta_E, \theta_{\text{div}}) = \frac{1}{\eta_b}\left(\frac{d_B}{d_E}\right)^2 \left(\frac{D_R^E}{D_R^B}\right)^2 e^{-2(2\theta_E/\theta_{\text{div}})^2}. \tag{13}$$

For $d_B = d_E = 1200$ km and $\theta_E = r_E/d$, for the Micius system parameters and assuming a very large eavesdropper's receiving antenna $D_R^E$ of 2 m and a small exclusion radius $r_E = 12.5$ m, we obtain

$$\gamma = 0.07 < 0.1.$$

For the remainder of the paper, we fix the exclusion radius such that $\gamma < 0.1$. Indeed, this value seems to be a good choice as it leads to high secret capacities greater than 0.6 (see Fig. 4), little sensitivity to noise, and signal fluctuations for reasonable exclusion radii, as discussed in Appendix B. This sensitivity is driven by the distinguishability of the coherent states at Eve's Holevo-Helstrom detector, as shown in Appendix E; the lower $\gamma$, the less is the distinguishability sensitive to the signal dynamics.

## V. PRIVATE RATES FOR DIFFERENT PRACTICAL SETTINGS AND COMPARISON WITH QKD

We can now calculate the private capacity for different geometrical configurations, supposing that Alice and Bob have a satellite and a ground station equivalent to the Micius experiment. We consider OOK with a clock rate of 1 GHz. With a time window of 1 ns, state-of-the-art single-photon detectors feature a $p_{\text{dark}} < 10^{-7}$, so the detector noise has no significant effect on the secret capacity. Table I in Ref. [41] indicates the expected number of noise photons for different collection angles, filter bandwidths, and temporal windows. Based on that, average numbers of $10^{-4}$ and $10^{-7}$ for $\Delta$ are achievable values for a clear daytime sky and a full moon clear night, respectively. During a cloudy day, one could expect a $\Delta$ of $10^{-2}$, and still positive private rates (this is under the assumption that transmission of the channel is affected in the same way for Bob and Eve). See Fig. 9 for the sensitivity to noise.

Given the clock rate and the maximum private capacity from Fig. 4, we obtain a private rate of 680 Mb/s for $\gamma = 0.1$. This value is the same for any channel efficiency $\eta$ as long as the received power $\eta\mu$ is optimized. We can

TABLE I. Comparison of the achievable secret key rates for QKD and the private rates for the wiretap channel presented in this work. The values are extrapolated from experimental data from the Micius satellite [4] for $\eta_f^B = 22$ dB (at 1200 km) and $\eta_b = 20$ dB (except for the theoretical PLOB bound [27] with $\eta_b = 1$). The exclusion radii $r_E$ for $\gamma = 0.1$ are calculated based on the Micius beam parameters. Note that, for Micius and PLOB, we consider nighttime operation, in contrast to the case of the wiretap channel where daytime operation is possible. LEO, MEO and GEO refer to low, medium and geostationary earth orbits, respectively.

| | | | QKD (night) $\Delta = 10^{-7}$ | | Wiretap channel (day) $\Delta = 10^{-4}$ | | |
|---|---|---|---|---|---|---|---|
| Configuration | Distance (km) | Channel loss ($\eta_f^B$) | Micius | PLOB ($\eta_b = 1$) | Exclusion radius $r_E$ (m) | Gamma | Private rate (MHz) |
| LEO | 500–1200 | 22 dB | < 10 kHz | 10 MHz | 12.5 | 0.1 | 700 |
| MEO | 10 000 | 40 dB | ... | 100 kHz | 100 | 0.1 | 700 |
| GEO | 36 000 | 52 dB | ... | 6 kHz | 340 | 0.1 | 700 |

compare these rates with the key rates obtained by QKD in the Micius experiment and a potential perfect quantum communication scheme. Indeed, Pirandola *et al.* [27] showed that there is an upper bound, the so-called PLOB bound, of the achievable secret key rate of a QKD protocol for a given channel transmission $\eta$:

$$R_{\mathrm{QKD},\infty}(\eta) = -\log_2(1-\eta). \qquad (14)$$

(Note that, very recently, specific free-space and satellite versions of the PLOB bound have been introduced [42,43].)

Table I presents all these rates for LEO, MEO, and GEO satellites. As expected, the private capacity of a wiretap channel outperforms QKD dramatically in terms of rate and, most importantly, in terms of resistance against noise.

Certainly, if the eavesdropper is restricted, the performance of QKD can also be substantially improved. As a comparison, we estimate the theoretically achievable secret key rate for QKD following Appendix B in Ref. [21], choosing the parameters such that they are equivalent to our assumptions, notably $\Delta = 10^{-4}$ and $\gamma = 0.1$. We obtain a similar rate of 360 Mbit/s. However, keyless private communication is arguably easier to implement in practice. The OOK protocol is particularly simple to realize on the sender side as well as on the receiver side, whereas, e.g., for BB84, four different quantum states have to be generated and measured. Moreover, it does not need two-way communication for reconciliation, which is an advantage in the setting of satellite communication.

There is also a scheme called quantum secure direct communication [44] that combines quantum communication and the possibility to detect the presence of an eavesdropper with encoding like for the wiretap channel. However, the implementation of this scheme is very challenging for a satellite link, in particular because the quantum signal has to travel back and forth between the satellite and ground station.

Finally, some practical remarks. The necessary laser powers to reach an optimal signal strength of about four photons on average is about 15 mW and 15 $\mu$W for the GEO and LEO settings, respectively, and therefore it is no limitation. However, due to the high signal strength, a gigahertz repetition rate implies high detection rates at Bob's receiver, which are still a challenge for single-photon detectors [45].

## VI. DISCUSSION AND CONCLUSIONS

We show the feasibility, practicality, and performance of unconditionally secure links for space, and show the required exclusion radius. A protection area is needed for any kind of secure communication, including QKD. In this paper, we discuss a downlink; however, similarly, we could also consider an uplink and estimate the channel degradation $\gamma$ for reasonable assumptions on Eve's satellites.

Our protocol is certainly susceptible to jamming attacks, but so are QKD protocols.

Given these boundary conditions, we demonstrate that physical layer encryption can also provide information-theoretically secure communication in the case of Eve being limited by only the laws of quantum physics. As for the wiretap codes, explicit constructions are available that can provide the strong security. Well-known constructions are based on either coset codes with random codeword choice within a coset [46,47] or concatenation of encryption functions (e.g., hashing) with conventional capacity-achieving codes [30,48] (e.g., low-density parity code, polar code, or Reed Muller codes).

The achievable private rates are considerably higher than the QKD rates for an unrestricted Eve in the asymptotic regime. Furthermore, due to the high detection rates, big block sizes, i.e., long codewords, are not an issue for our protocol and therefore the reduction of the rates in the finite-length regime can be made negligible; see, e.g., Ref. [49]. Moreover, direct private communication is also possible close to illuminated cities and even during daytime in contrast to QKD. Given the low rates in practice, the secret keys generated by QKD are likely to be used in combination not with the one-time pad, but with symmetric encryption systems like the advanced encryption standard. This means that legitimate users may choose between trusting physical security, including exclusion areas around

Alice and Bob, or the computational security of encryption algorithms.

Overall, physical layer encryption seems to be a reasonable choice for satellite communication.

## ACKNOWLEDGMENTS

We would like to acknowledge Antonio Acín, Andreas Winter, Masahito Hayashi, Christoph Wildfeuer, and Mikael Afzelius for useful discussions. D.R. acknowledges the support of the European Union's Horizon 2020 program under the Marie Skłodowska-Curie project QCALL (Grant No. GA 675662).

## APPENDIX A: OPTIMIZED INPUT PROBABILITY

The optimization of the private capacity given in Eq. (7) also provides the optimal input probability that Alice should choose to transmit the OOK symbols. Figure 6 shows the optimized input probability as a function of the received average number of photons and intensity of stray light. It is interesting to observe that our wiretap channel can be considered nearly symmetric. However, optimal private rates require small deviations from the symmetric channel.

## APPENDIX B: THE APPROPRIATE VALUE OF $\gamma$ AND THE CORRESPONDING EXCLUSION RADIUS

In this section we give a justification for the value for $\gamma = 0.1$ as a good trade-off between, on the one hand, a high secrecy capacity, and on the other hand, the required exclusion area and resilience to experimental fluctuations.

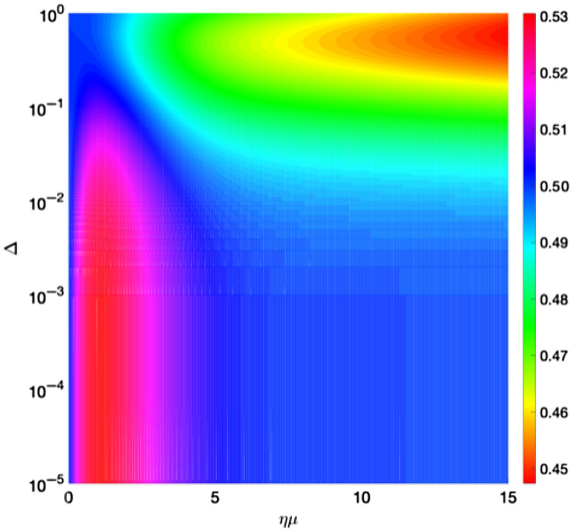

FIG. 6. Optimal value of input probability, $q$, as a function of the average number of photons received by Bob $\eta\mu$ and the intensity of the stray-light $\Delta$ ($\gamma = 0.1$).

We consider the situation in which the adversary Eve is going to collect the light with a telescope from a location close to Bob, and hence at the same distance $d$ from Alice's satellite. Alice. In this case, if $\gamma$ is fixed, the value of the exclusion ratio is given by the formula

$$r_{\text{ex}} = \frac{1}{2}\theta_{\text{div}} d \sqrt{\left\{\frac{1}{2}\log\left[\frac{1}{\gamma}\frac{1}{\eta_b}\left(\frac{D_R^E}{D_R^B}\right)^2\right]\right\}}, \tag{B1}$$

where $\theta_{\text{div}}$ is the far-field divergence angle for the Gaussian beam, $\eta_b$ is the efficiency of the detection system of Bob, and $D_R^E$ and $D_R^B$ are respectively the radius of the antennas of Eve and Bob.

As can be seen from Fig. 7, the requested exclusion radius depends linearly on the satellite-to-ground distance and it amounts to about 350 m for a geostationary orbit (around 35 000 km) for $\gamma = 0.1$. It can also be seen that increasing the value of $\gamma$, e.g., $\gamma = 0.9$, does not allow us to reduce the exclusion radius significantly.

A more conservative approach consist in giving Eve all the optical power outside the exclusion radius. This correspond to assuming that Eve can collect all the light outside the cone from the satellite to the secure area. In this case the exclusion ratio can be extrapolated from the following implicit function once $\gamma$ is fixed:

$$e^{-2(r_{\text{ex}}/\theta_{\text{div}} d)^2} = \gamma\left(1 - e^{-2(D_R^B/\theta_{\text{div}} d)^2}\right). \tag{B2}$$

Also, in this case the relation between the exclusion radius and the satellite-to-ground distance is almost linear. However, the value is 2–3 times higher than in the previous scenario. Still, the exclusion radius for the geostationary orbit remains below 1 km.

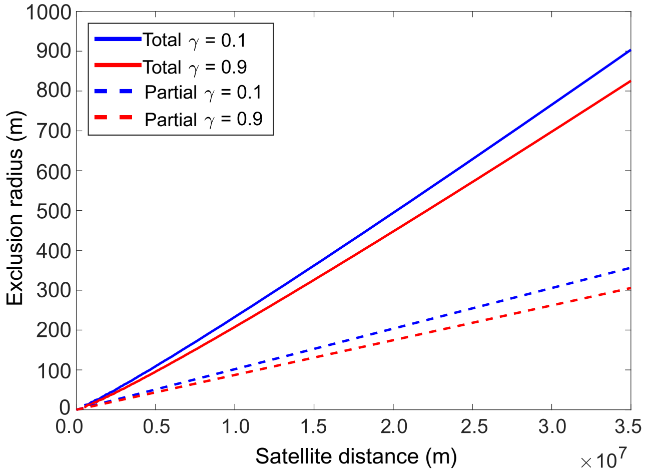

FIG. 7. Exclusion radius versus the satellite distance for different $\gamma$ and eavesdropper models. "Partial" stands for a telescope of 2 m diameter; "total" stands for an eavesdropper collecting all light outside the exclusion region.

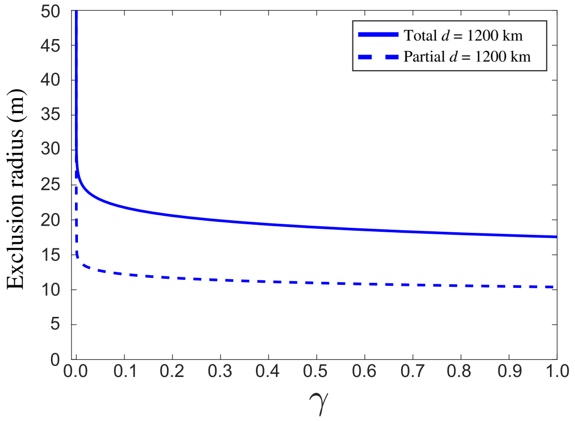

FIG. 8. The exclusion radius needed to achieve a given value of $\gamma$.

Figure 8 shows the dependence of the exclusion radius on the parameter $\gamma$ when the satellite-to-ground distance is fixed to 1200 km (a distance similar to the Micius satellite). It illustrates that indeed (for a finite detection area as well as for the unlimited case) the required exclusion radius is almost constant with respect to $\gamma$ for values higher than 0.1. This means that a value of $\gamma$ higher than 0.1 brings only a little advantage in terms of the exclusion radius, but at the cost of a significant reduction of the secrecy rate, detrimental for the performance of the protocol. Moreover, in this range, a small uncertainty in the radius, or a bad pointing stability, may lead to a large variation in $\gamma$ and threaten the security of the protocol. Therefore, choosing values of $\gamma < 0.1$ seems to be pertinent in the case of optical communication with well-defined Gaussian beams.

Finally, in Fig. 9 we show the behavior of the private capacity $C_p$ for $\gamma$ equal to 0.1, with respect to the stray light $\Delta$ and the received light by Bob $\eta\mu$ (both in units of the average number of photons per time and frequency bin). We note that if we fix a secret capacity of say 0.5, the protocol can resist high fluctuations in the received light intensity and a high amount of stray light (remember, we expect a $\Delta$ of 0.0001 for a clear sky during daytime). This security margin would be considerably reduced for a $\gamma$ of 0.6 for instance.

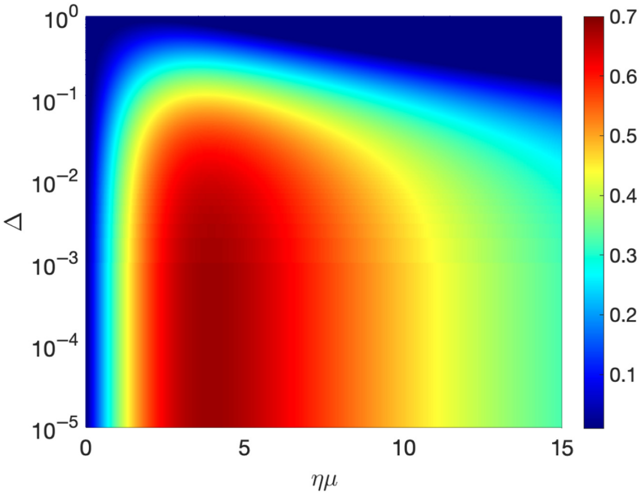

FIG. 9. Private capacity $C_p$ for $\gamma = 0.1$ as a function of the average number of photons received by Bob and the intensity of the stray light.

## APPENDIX C: BASIC CELESTIAL MECHANICS

Since, as discussed above, Eve can get only limited information by positioning a receiver station on the ground next to Bob's telescope, the natural question would be: what happens if Eve tries to attack Alice's satellite instead? In this section we argue that, similarly to the previous case, it is sufficient to assume a reasonable exclusion radius around Alice's satellite in order to assure the security of our protocol. A complete treatment of the question is beyond the scope of this paper, and so we just present some simple, general considerations (see, e.g., Ref. [50] for more information).

For simplicity, we assume that Bob's station is positioned on the equator and that Alice's and Eve's satellites have two circular orbits in the equator plane (see Fig. 10). This is an extreme simplification of Eve's task, since this guarantees that at some time Eve will be exactly in the line of sight of Alice and Bob. Indeed, if the two orbits and Bob are not in the same plane, Eve will have a hard time intersecting the beam that has a diameter of less than 1 m close to Alice. So arguably, her best strategy would be to attach her satellites directly on Alice's. But, as for the ground case, we impose an exclusion radius around Alice (in agreement with the general assumption also valid for QKD), which sets the minimal distance between Alice's and Eve's orbits. Note that all objects in space are well monitored and that this assumption can be verified with reasonable effort [51].

Both Alice's and Eve's angular velocities have the same direction as Bob on earth. Let us consider first a single passage of the satellites over the ground station. In order to calculate $\gamma$, we trace the instantaneous collection efficiency of Bob and Eve with respect to time, where time zero is fixed, such as when Alice, Eve, Bob, and the center

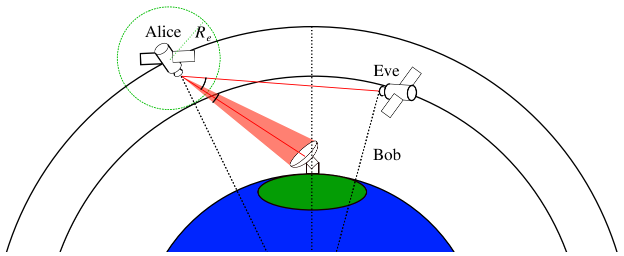

FIG. 10. Sketch of the orbits of Alice and Eve with respect to Bob.

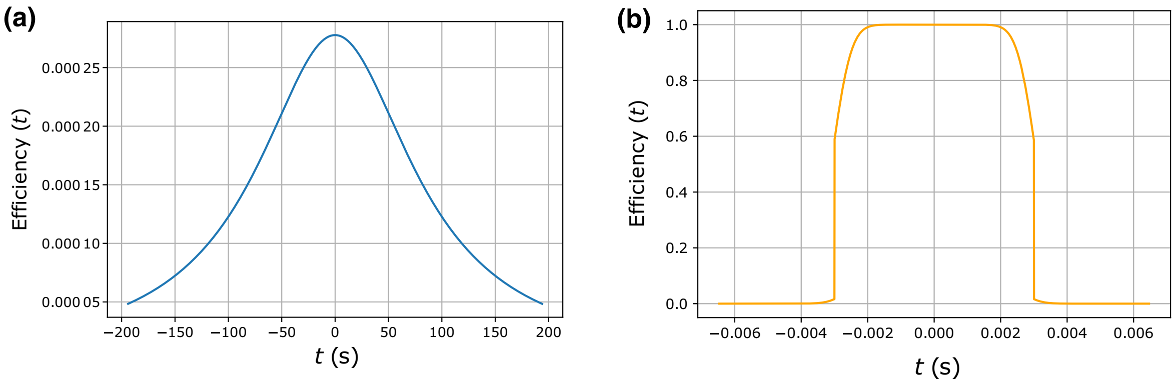

FIG. 11. Instantaneous channel efficiencies of Bob (a) and Eve (b) versus time for a single passage of Alice's satellite.

of the Earth are aligned. We conservatively assume that if Eve completely intersects the beam, she resends the signals to Bob and is consequently not detected directly. Finally, we integrate the instantaneous efficiency over the period of communication between Alice and Bob. The instantaneous efficiency with respect to time are respectively calculated for Bob and Eve as

$$\eta^B(t) = \eta_b * \frac{D_R^2}{\theta_{\text{div}}^2 d_B(t)^2}, \tag{C1}$$

$$\eta^E(t) = \frac{2}{\pi} \iint_{A(t)} \frac{e^{-2[(x^2+y^2)/\theta_{\text{div}}^2 d_E(t)^2]}}{\theta_{\text{div}}^2 d_E(t)^2} dxdy, \tag{C2}$$

where $d_B(t)$ and $d_E(t)$ are the distances between Alice and Bob and Alice and Eve with respect to time, and the integral is considered over the area of Eve's telescope $A(t)$ moving with respect to Alice's telescope. In the end, in order to calculate $\gamma$, we evaluate the ratio between the average efficiency integrated over a period of communication between Alice and Bob:

$$\gamma = \frac{\int_{-T}^{T} \eta^B(t)dt}{\int_{-T}^{T} \eta^E(t)dt}. \tag{C3}$$

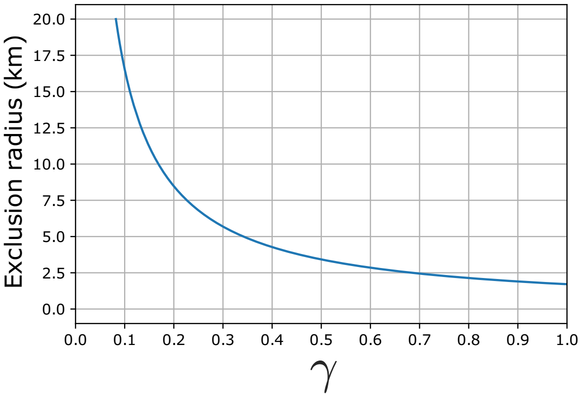

FIG. 12. Exclusion radius versus $\gamma$ (for a single passage).

Here $T = 400$ s, as can be seen from Fig. 11(a).

Figures 11(a) and 11(b) show the instantaneous efficiencies of Bob and Eve, respectively, for a configuration with an exclusion radius around Alice's satellite of 16 km and with Alice's orbit 600 km above ground. The communication is considered to begin and end when the satellite is 20° above the horizon with respect to Bob. As can be seen, the communication between Alice and Bob lasts for over 400 s, while Eve's time of interception is only a few hundred millisecond. If the efficiency is averaged over the passage of the satellite, we can again calculate the factor $\gamma$. Figure 12 shows the needed exclusion radius in order to obtain a given $\gamma$. We can see that, for an exclusion radius above 16 km, a value of $\gamma$ lower than 0.1 can again be assured. Note that this is for Eve's telescope being 2 m in size, which would be very easy to spot.

This value of $\gamma$ is true for a single passage; however, a passage of Alice over Bob occurs at a much higher frequency than the perfect alignment of Alice, Eve and Bob. The closer Eve is to Alice, the longer the beating period will be. This means that in order to implement such an attack, it is not sufficient to use a single satellite in a fixed orbit. The active strategy would involve either a constellation of satellites or a satellite with an adjustable orbit. Just to give an idea, for the parameters considered here (an orbit of 600 km above ground for Alice with Eve 15 km below her), the period between two links from Alice to Bob is around 1.7 h, while the period between two intercept events for Eve (Eve is in between Alice and Bob during communication) would be of 20 days.

Overall, these estimations, although based on a worst-case scenario, show that it is possible to guarantee a $\gamma$ as low as 0.1.

## APPENDIX D: PHYSICAL PROBABILISTIC CHANNEL MODEL

Figure 13 represents our (degraded) quantum wiretap channel model, which is a physical-probabilistic model. It shows the impairments undergone by the transmitted

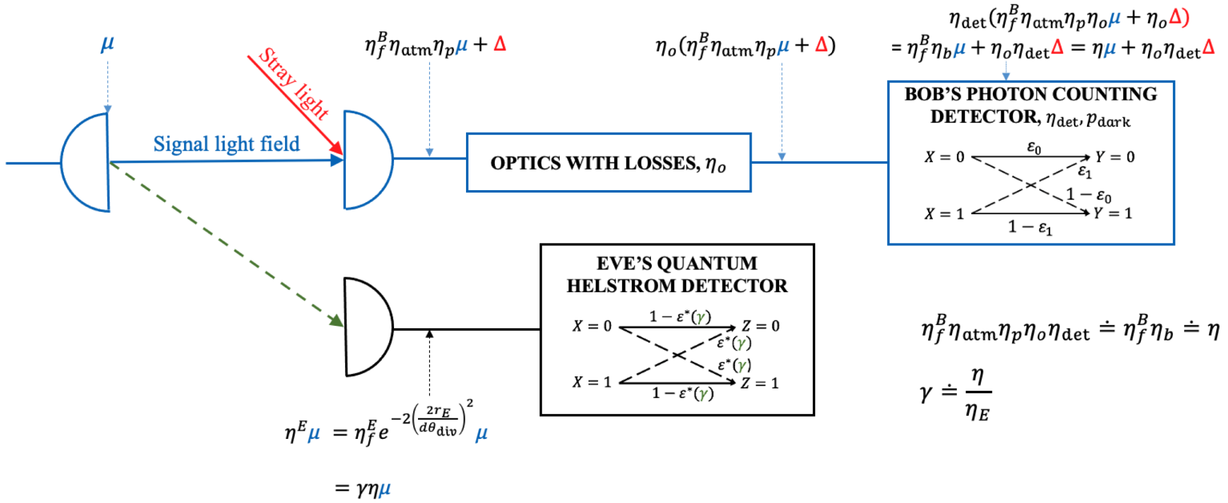
$\mu$
Stray light
Signal light field
$\eta_f^B\eta_{\mathrm{atm}}\eta_p\mu+\Delta$
$\eta_o(\eta_f^B\eta_{\mathrm{atm}}\eta_p\mu+\Delta)$
$\eta_{\mathrm{det}}(\eta_f^B\eta_{\mathrm{atm}}\eta_p\eta_o\mu+\eta_o\Delta)$
$=\eta_f^B\eta_b\mu+\eta_o\eta_{\mathrm{det}}\Delta=\eta\mu+\eta_o\eta_{\mathrm{det}}\Delta$
OPTICS WITH LOSSES, $\eta_o$
BOB'S PHOTON COUNTING DETECTOR, $\eta_{\mathrm{det}}, p_{\mathrm{dark}}$
$X=0$
$X=1$
$Y=0$
$Y=1$
$\varepsilon_0$
$\varepsilon_1$
$1-\varepsilon_0$
$1-\varepsilon_1$
EVE'S QUANTUM HELSTROM DETECTOR
$X=0$
$X=1$
$Z=0$
$Z=1$
$1-\varepsilon^*(\gamma)$
$\varepsilon^*(\gamma)$
$\varepsilon^*(\gamma)$
$1-\varepsilon^*(\gamma)$
$\eta^E\mu=\eta_f^E e^{-2\left(\frac{2r_E}{d\theta_{\mathrm{div}}}\right)^2}\mu$
$=\gamma\eta\mu$
$\eta_f^B\eta_{\mathrm{atm}}\eta_p\eta_o\eta_{\mathrm{det}}\doteq\eta_f^B\eta_b\doteq\eta$
$\gamma\doteq\frac{\eta}{\eta_E}$

FIG. 13. Graphical representation of our degraded quantum wiretap channel model.

average number of photons, $\mu=|\alpha_1|^2$, over the main and wiretap channels.

Bob's channel power attenuation has the following contributions: $\eta_f^B$ (free space), $\eta_{\mathrm{atm}}$ (atmospheric, e.g., turbulences), $\eta_p$ (pointing), and $\eta_o$ (optical loss from the telescope input lens to detector). The detector efficiency, $\eta_{\mathrm{det}}$, is included in the overall losses parameter $\eta$. The channel transition probabilities are also affected by the dark current noise, modeled by $p_{\mathrm{dark}}$. Then, the probabilistic model of the detector is fully described by the probabilities $\epsilon_0=(1-p_{\mathrm{dark}})e^{-\eta_o\Delta}$ and $\epsilon_1=(1-p_{\mathrm{dark}})e^{-(\eta|\alpha_1|^2+\eta_o\Delta)}$.

Eve's channel is only affected by propagation in free space, $\eta_f^E$, and by the Gaussian angular distribution of the beam, modeled as $e^{-2(2\theta_E/\theta_{\mathrm{div}})^2}$, or $e^{-2(2r_E/d\theta_{\mathrm{div}})^2}$, since $\theta_E\approx r_E/d$ with $\theta_E$ Eve's exclusion angle, $\theta_{\mathrm{div}}$ the divergence angle, and $d$ the distance between Alice and Bob. In our model, we express the number of photons at Eve's detector as a fraction of those received by Bob as $\eta^E(\gamma)=\gamma\eta$. This modeling makes the parameter $\gamma$ a design choice that controls the distinguishability of the coherent states at Eve's detector.

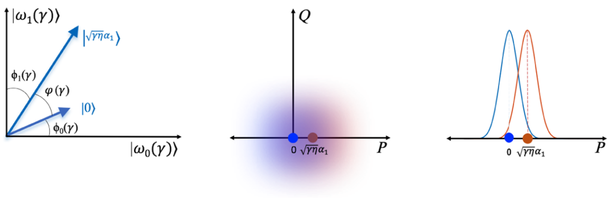
$|\omega_1(\gamma)\rangle$
$|\sqrt{\gamma\eta}\alpha_1\rangle$
$\phi_1(\gamma)$
$\varphi(\gamma)$
$|0\rangle$
$\phi_0(\gamma)$
$|\omega_0(\gamma)\rangle$
$Q$
0 $\sqrt{\gamma\eta}\alpha_1$
$P$
0 $\sqrt{\gamma\eta}\alpha_1$
$P$

FIG. 14. Representation of the coherent states sent by Alice and received by Eve in the qubit space, in the classical phase space, and as histograms on the quadrature $P$ (respectively from left to right).

## APPENDIX E: DISTINGUISHABILITY OF EVE'S COHERENT STATES WITH $\gamma$ AT EVE'S DETECTION

Our design parameter $\gamma$ controls the distinguishability (orthogonality) of the coherent states at Eve's detection. This dependency can be visualized in different representations, as shown in Fig. 14, in which we present the representation of the (rank-2) Hilbert space spanned by the coherent states at Eve's reception (left), where $\varphi(\gamma)$ is the angle between the coherent states; the $P$-$Q$ phase space with the (unitary variance) Gaussian uncertainty of each state (center); and the representation of the Gaussian distribution along the $P$ quadrature (right). Given the angle $\varphi(\gamma)=\cos^{-1}(\langle 0,\sqrt{\gamma\eta}\alpha_1\rangle)$, the Holevo-Helstrom optimization induces $\epsilon^*(\gamma)$ and the symmetric space $\phi_0^*(\gamma)=\phi_1^*(\gamma)=0.5[\pi/2-\varphi(\gamma)]$.

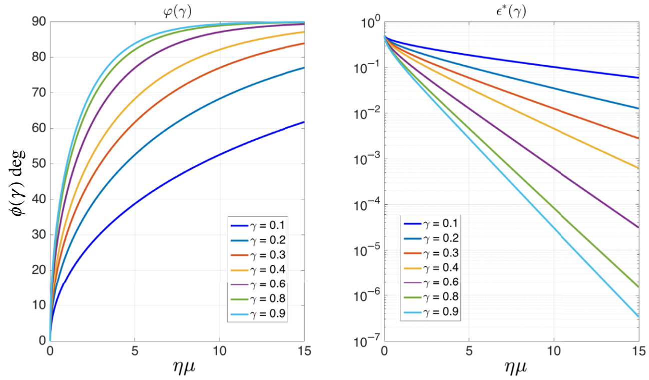

FIG. 15. The angle $\phi(\gamma)$ (left) and the error probability $\epsilon^*(\gamma)$ versus the received number of photons $\eta\mu$ for different values of $\gamma$.

Figure 15 shows the sensitivity of $\varphi(\gamma)$ to variations of the received number of photons. The lower the $\gamma$, the less sensitivity.

We observe that, for $\eta\mu = 4$, we have $\varphi(0.1) = 35^\circ$ and $\epsilon^*(0.1) = 0.2$ with an increase in orthogonality of 10% and a decrease of 5% in the (uncoded) error probability for a fluctuation around 1 photon.

[1] C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. Computers, Systems and Signal Processing* (Steering Committee, Bangalore, 1984).

[2] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussieres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure Quantum Key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[3] X. T. Fang, P. Zeng, H. Liu, *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[4] S. K. Liao, W. Q. Cai, W. Y. Liu, *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[5] J. Yin, Y. H. Li, S. K. Liao, *et al.*, Entanglement-based secure quantum cryptography over 1120 km, Nature **582**, 501 (2020).

[6] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[7] D. Mayers, Unconditional security in quantum cryptography, J. ACM **48**, 351 (2001).

[8] G. Kat and K. Tamaki, Security of six-state quantum key distribution protocol with threshold detectors, Sci. Rep. **6**, 30044 (2016).

[9] M. Curty, K. Azuma, and H. K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[10] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusěk, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[12] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J. **54**, 8 (1975).

[13] A. D. Wyner, Capacity and error exponent for the direct detection photon channel—Part I, IEEE Trans. Inf. Theory **34**, 6 (1998).

[14] A. D. Wyner, Capacity and error exponent for the direct detection photon channel—Part II, IEEE Trans. Inf. Theory **34**, 6 (1998).

[15] I. Csiszár and J. Körner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory **24**, 3 (1978).

[16] U. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 3 (1993).

[17] M. Bellare, S. Tessaro, and A. Vardy, in *Proc. Advances in Cryptology* (Springer-Verlag, Berlin, Heidelberg, 2012).

[18] N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channels, Probl. Inf. Transm. **40**, 4 (2004).

[19] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, IEEE Trans. Inf. Theory **51**, 1 (2005).

[20] I. Devetak and P. W. Shor, The capacity of a quantum channel for simultaneous transmission of classical and quantum information, Commun. Math. Phys. **256**, 287 (2005).

[21] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, Secret Key Distillation Over a Pure Loss Quantum Wiretap Channel Under Restricted Eavesdropping, Phys. Rev. Appl. **14**, 024044 (2020).

[22] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, in *Proc. IEEE Int. Symp. on Inf. Theory* (IEEE, Paris, 2019).

[23] T. Vergoossen, R. Bedington, J. A. Grieve, and A. Ling, Satellite quantum communications when man-in-the-middle attacks are excluded, Entropy **21**, 9 (2019).

[24] M. Fujiwara, T. Ito, M. Kitamura, H. Endo, O. Tsuzuki, M. Toyoshima, H. Takenaka, Y. Takayama, R. Shimizu, M. Takeoka, R. Matsumoto, and M. Sasaki, Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link, Opt. Exp. **26**, 15 (2018).

[25] H. Endo, T. S. Han, T. Aoki, and M. Sasaki, Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels, IEEE Photonics J. **7**, 5 (2015).

[26] H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, Y. Takayama, H. Takenaka, R. Shimizu, N. Laurenti, G. Vallone, P. Villoresi, T. Aoki, and M. Sasaki, Free-space optical channel estimation for physical layer security, Opt. Express **24**, 8940 (2016).

[27] S. Pirandola, R. Laurenza, C. Ottavani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[28] M. Hayashi, Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information, IEEE Trans. Inf. Theory **61**, 10 (2015).

[29] U. M. Maurer, *The Strong Secret Key Rate of Discrete Random Triples*, Communication and Cryptography (Springer, Boston, 1994).

[30] M. Hayashi and A. Vázquez-Castro, Physical layer security protocol for poisson channels for passive man-in-the-middle attack, IEEE Trans. Inf. Forensics Security **15**, 2295 (2020).

[31] K. M. R. Audenaert, J. Casamiglia, R. Munoz-Tapia, E. Bagan, Ll. Masanes, A. Acín, and F. Verstraete, Discriminating States: The Quantum Chernoff Bound, Phys. Rev. Lett. **98**, 160501 (2007).

[32] K. M. R. Audenaert, M. Nussbaum, A. Szkoła, and F. Verstraete, Asymptotic error rates quantum hypothesis testing, Commun. Math. Phys. **279**, 251 (2008).

[33] M. Hayashi, *Quantum Information. An Introduction* (Springer, Berlin, Heidelberg, New York, 2006).

[34] Carl W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering, Vol. 123 (Academic Press, New York, 1976).

[35] A. S. Kholevo, On asymptotically optimal hypothesis testing in quantum statistics, Probab. Appl. **23**, 411 (1978).

[36] R. S. Kennedy, A near-optimum receiver for the binary coherent state channel, Rep. 108, MIT RLE. Quarterly Progress Report, 1973.

[37] S. J. K. Dolinar, An optimum receiver for the binary coherent state quantum channel, Rep. 111, MIT RLE Quarterly Progress Report, 1973.

[38] M. Takeoka and M. Sasaki, Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-Gaussian near-optimal receivers, Phys. Rev. A **78**, 022320 (2008).

[39] K. Tsujino, D. Fukuda, G. Fujii, S. Inoue, M. Fujiwara, M. Takeoka, and M. Sasaki, Quantum Receiver beyond the Standard Quantum Limit of Coherent Optical Communication, Phys. Rev. Lett. **106**, 250503 (2011).

[40] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. London, A **461**, 2053 (2005).

[41] 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).

[42] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Res. **3**, 013279 (2021).

[43] S. Pirandola, Satellite quantum communications: Fundamental bounds and practical security, Phys. Rev. Res. **3**, 023130 (2021).

[44] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, Implementation and security analysis of practical quantum secure direct communication, Light Sci. Appl. **8**, 22 (2019).

[45] M. Perrenoud, M. Caloz, E. Amri, C. Autebert, Ch. Shönenberger, H. Zbinden, and F. Bussières, Operation of parallel SNSPDs at high detection rates, Supercond. Sci. Technol. **34**, 024002 (2021).

[46] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, Applications of LDPC codes to the wiretap channel, IEEE Trans. Inf. Theory **53**, 8 (2007).

[47] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. Kwak, LDPC codes for the Gaussian wiretap channel, IEEE Trans. Inf. Forensics Security **6**, 3 (2011).

[48] H. Tyagi and A. Vardy, Universal hashing for information-theoretic security, Proc. IEEE **103**, 10 (2015).

[49] A. Vázquez-Castro and Masahito Hayashi, Physical layer security for RF satellite channels in the finite-length regime, IEEE Trans. Inf. Forensics Security **14**, 981 (2018).

[50] B. Tapley, B. Schutz, and G. Born, *Statistical Orbit Determination* (Elsevier, 2004).

[51] See e.g., https://www.esa.int/Safety_Security/Space_DebrisESA Space Debris Office.