22 Vol. 4, No. 1 / 25 February 2026 / Optica Quantum Research Article

OPTICA QUANTUM

Quantum key distribution in the Iberian Peninsula

Victoria Domínguez Tubío,[1,2,7,†] Mario Badás Aldecocea,[3,*,†] David L. Bakker,[4] Gustavo C. Amaral,[4] Diego López,[5] and Johannes Borregaard[6]

[1]QuTech, Delft University of Technology, 2628 CJ Delft, The Netherlands
[2]Kavli Institute of Nanoscience, Delft University of Technology, 2628 CJ, Delft, The Netherlands
[3]Space Engineering Department, Delft University of Technology, 2629 HS Delft, The Netherlands
[4]Quantum Technology Department, The Netherlands Organization for Applied Scientific Research, 2628 CK Delft, The Netherlands
[5]Telefónica gCTIO/I+D, Madrid, Spain
[6]Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA
[7]vicky.dotu@gmail.com
[†]These authors contributed equally to this work.
*mbadasaldecoce@tudelft.nl

Received 16 October 2025; revised 6 December 2025; accepted 6 December 2025; published 7 January 2026

A promising use of quantum networking is quantum key distribution (QKD), which can provide information-theoretic security unattainable by classical means. While optical fiber-based QKD networks suffer from exponential loss, satellite-assisted quantum communication offers a scalable solution for long-distance secure key exchange. In this work, we propose and evaluate a satellite-based QKD setup covering the Iberian Peninsula, linking Madrid with Barcelona, Bilbao, and Lisbon. Our proposed setup uses a Low-Earth-Orbit (LEO) state-of-the-art satellite equipped with a spontaneous parametric down-conversion (SPDC) source to distribute entangled photon pairs to ground stations. Considering vibrations in the satellite, we optimize the beam waist to enhance the transmission probability and improve the secret key rate (SKR). Our results show that key rates sufficient for real-world applications, such as secure communication between hospitals, using hybrid classical-quantum protocols, are feasible with existing protocols. Our results highlight the viability of near-term satellite-based QKD networks for national-scale secure communications.

https://doi.org/10.1364/OPTICAQ.581903

1. INTRODUCTION

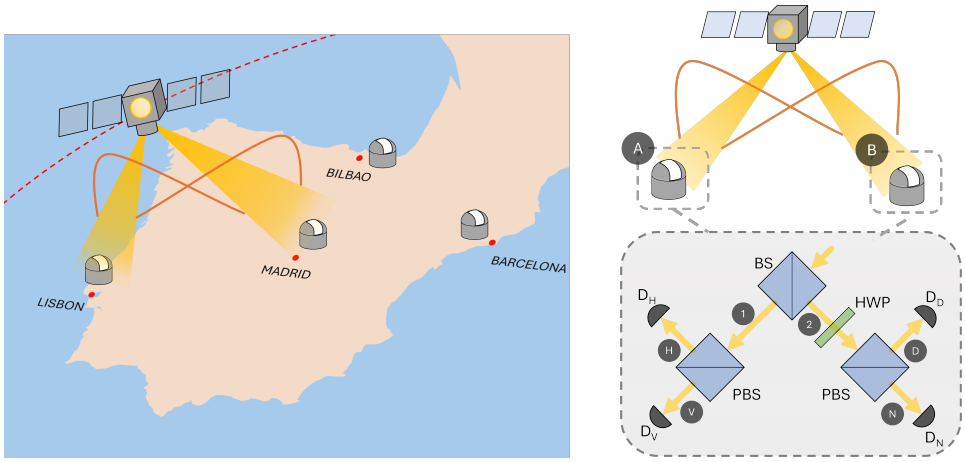
The realization of a quantum internet holds the potential to revolutionize multiple fields, including secure communication [1–3], high-precision sensing networks [4–6], and distributed quantum computing [7]. In particular, quantum key distribution (QKD) enables communication with information-theoretic security, a level of protection unattainable by classical methods.

Quantum communication relies on photons to carry quantum information. However, their transmission is limited by loss and, unlike classical signals, quantum signals cannot be amplified using conventional techniques due to the no-cloning theorem [8]. To mitigate this, quantum repeater architectures have been proposed. These divide the total distance into shorter segments, where quantum information can be transmitted directly. The segments are then connected using quantum teleportation [9,10] or quantum error correction [11,12] at the repeater nodes, enabling faithful transmission over the total distance. In fiber-based systems, however, signal attenuation increases exponentially with distance, requiring hundreds of repeater nodes for continental-scale coverage.

Satellite-based free-space QKD offers a promising alternative for long-distance communication without the need for complex repeater infrastructures. Notably, the Micius satellite has demonstrated QKD over distances from 500 to 7,000 km using a trusted-node architecture [13,14]. More recently, entanglement-based QKD was successfully achieved without relying on a trusted node, decreasing the risk of eavesdroppers, reaching up to 1,200 km [15,16]—distances well beyond the capability of terrestrial fiber networks.

Fiber-based QKD has also made significant progress, enabling high-speed, secure communication across metropolitan areas. Recent demonstrations include the protection of multiple VPNs [17] and secure data exchange between hospitals in the Madrid area via a trusted-node QKD network [18]. The next logical step is to extend these capabilities from city-scale to national-scale coverage.

To this end, we propose a satellite-based QKD architecture to interconnect major cities across the Iberian Peninsula—Madrid with Barcelona, Bilbao, and Lisbon—as shown in Fig. 1(a). Our system employs a satellite like Micius in a Low-Earth-



(a) (b)

Fig. 1. Experimental setup. (a) Ground stations of the regional quantum key distribution (QKD) network that we want to implement. The central node is Madrid, and the key distribution is always between Madrid and any of the other cities (Barcelona, Bilbao, and Lisbon). (b) We consider a downlink scenario, with an entangled photon source firing photons from the satellite to the ground stations. At the ground stations, the photons are randomly measured in the X or Z basis. To perform such a measurement, the photons go through a 50/50 beam splitter (BS), followed by a half-wave plate (HWP) in one of the outputs, which changes the basis of the input photons. Finally, before measuring, the photons go through a polarizing beam splitter (PBS) such that we measure different polarizations- horizontal (D_H), vertical (D_V), diagonal (D_D) and antidiagonal (D_N)- at the output ports of the B.S. The measurement results are fed into a classical memory from which we can then extract secret keys for the two applications we consider.

Orbit (LEO) equipped with a spontaneous parametric down-conversion (SPDC) source to distribute entangled photon pairs to multiple ground stations, implementing the BBM92 protocol [16]. In our setup, we consider the vibrations in the satellite and propose a novel optimization of the beam waist that generalizes the static Gaussian beam clipping problem [19], to the dynamic regime. Unlike classical optical communication links that prioritize signal stability to minimize fading outages [20], our method maximizes the average photon yield even at the cost of higher signal variance. This optimization allows us to mitigate the detrimental effects of pointing jitter and consequently increase the photon transmission probability to the ground stations.

We evaluate the system's performance with and without optimization, demonstrating that the latter significantly enhances the secret key rate (SKR)—by a factor of approximately 10. The non-optimized beam refers to a Gaussian with a beam waist of radius $w_{0,\text{non-opt}} = 2.7$ cm, which is compatible with the 10 µrad divergence at a wavelength of 850 nm, as reported [21] for the Micius satellite. In our model, we also consider atmospheric conditions in real time, following the work done in [22]. In other words, the weather data are collected for the desired experiment duration at the target locations using the Free Weather API software [23] and fed into an empirical mathematical model [22] that extracts the attenuation experienced by an optical beam operating at the wavelength of 1550 nm. A single-satellite link proves sufficient to support secure communication across the Iberian Peninsula. Our results show that the SKR is adequate to support existing QKD use cases, such as hospital-to-hospital encryption demonstrated in the MAD-QCI project, using hybrid protocols where the quantum layer handles key generation, and classical layers manage key expansion via IPsec [18]. Furthermore, we check that for more demanding use cases such as supporting VPN services using the ETSI-QKD-014 protocol [17], we would need to improve the entangled photon pair source rate by 3 orders of magnitude, i.e., 1 GHz. While such a high rate has not currently been demonstrated on a satellite, it is compatible with performances demonstrated in laboratory environments simulating LEO satellite conditions [24].

2. MODEL

We focus on a downlink configuration, where photons are transmitted from a satellite to ground stations. This setup is preferred because atmospheric disturbances are generally less severe than in the uplink case, where photons travel from the ground to the satellite [25,26]. The satellite carries an onboard entangled photon source that probabilistically generates polarization-entangled photon pairs. Specifically, we consider a single satellite like Micius, with telescopes of radius of 15 cm, a rate of entangled pairs per second of $5.9 \cdot 10^6$ ph/s and pointing jitters of $\sim 10^{-6}$ rad [16,27], in a Low-Earth-Orbit (LEO) at an altitude of approximately 400 km, following a medium-inclination trajectory at a latitude of 42°, passing over the Iberian Peninsula, as illustrated in Fig. 1(b).

We consider the BBM92 protocol [16], where the photons are measured randomly in either the Z or X basis at the ground stations. Only photon pairs detected in the same basis are retained in classical memories through postselection. We employ the BBM92 protocol, following the approach demonstrated by the Micius satellite [16]. The figure of merit that we base our analysis on is the extracted key material; in general, the value is presented as a certain amount of **bits per second** (bps), but eventually it may also be convenient to also express it in terms of **bits per satellite pass**. The calculation involves three main steps, which are discussed in the Sections to follow: the model of the photonic qubit states generated by the entangled photon pair source on-board the satellite; the effect of the optical channels between the satellite and the ground stations; and the effect of the measurement performed by the receivers in the presence of noise.

A. Entangled Photon Pair Source

A pump laser is used to drive a nonlinear optical crystal in both the clockwise and anticlockwise directions simultaneously, generating down-converted polarization-entangled photon pairs with orthogonal polarizations [15,28].

$$
\begin{aligned}
|\psi_{\text{source}}\rangle \approx (1-\lambda)\,\big(&|0,0\rangle_{\text{A,B}} \\
&+ \frac{\sqrt{2}\lambda^{1/2}}{(1-\lambda)^{1/2}}\frac{1}{\sqrt{2}}\left(|H\rangle_{\text{A}}|V\rangle_{\text{B}} + |V\rangle_{\text{A}}|H\rangle_{\text{B}}\right) \\
&+ \frac{\sqrt{3}\lambda}{1-\lambda}\frac{1}{\sqrt{3}}\left(|2H\rangle_{\text{A}}|2V\rangle_{\text{B}} + |HV\rangle_{\text{A}}|HV\rangle_{\text{B}}\right. \\
&+ \left.|2V\rangle_{\text{A}}|2H\rangle_{\text{B}}\right) + O\left(\sqrt{n+1}\,\frac{\lambda^{n/2}}{(1-\lambda)^{n/2}}\right)\Big),
\end{aligned}
\tag{1}
$$

where the subscripts A and B correspond to two different spatial modes directed toward the ground stations of Alice and Bob, respectively, $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization states, respectively. The state $|\Psi^+\rangle = 1/\sqrt{2}\,(|H\rangle_{\text{A}}|V\rangle_{\text{B}} + |V\rangle_{\text{A}}|H\rangle_{\text{B}})$ denotes the desired state which corresponds to a maximally entangled state with anticorrelated polarization.

The term $\mu = 2\lambda$ is the average number of photon pairs generated per pulse, characterized by the brightness of the SPDC source [28]. The source operates in a weak-pump regime, where $\lambda \ll 1$, implying that the probability of emitting a photon pair is low. However, operating in this regime is necessary since it suppresses multi-photon events ($\propto |2H\rangle_{\text{A}}|2V\rangle_{\text{B}} + |HV\rangle_{\text{A}}|HV\rangle_{\text{B}} + |2V\rangle_{\text{A}}|2H\rangle_{\text{B}}$), which causes errors and lowers the secret key rate. In other words, there is tradeoff between the rate and the fidelity of entanglement. In our simulation, we optimize λ to obtain the highest SKR.

B. Photon Transmission

Photon loss during transmission to the two ground stations will change the received state from the one emitted by the SPDC source. We model this by passing the state in Eq. (1) through fictitious beam splitters in each spatial mode, where one output of the beam splitters corresponds to the loss, while the other is the transmitted mode. In general, the two spatial modes experience different transmission probabilities due to the various distances from the satellite to each of the ground stations. This is also relevant during satellite orbit, since the photons from the same pair can only be captured by both OGSs when the satellite is within their mutual range. In the calculations that follow, the maximum zenith angle of each OGS that determines whether it is in range of the satellite or not during the orbital movement is seventy-five degrees.

The free-space transmission probability is estimated from the model in Ref. [29], which includes divergence, atmospheric absorption, and pointing jitter. For a more accurate estimation of the number of entangled photon pairs captured by the ground station per second, an optical propagation model based on Ref. [30], which accounts for the clipping of the beam in the transmitter's telescope, is used (see Appendix A). Previous works often assume a Gaussian beam where clipping of the beam in the transmitter can be neglected. Instead, we explicitly take this effect into account using the model from Ref. [30]. This model enables the accurate evaluation of the average photon capture probability of each downlink channel, accounting for both the diffraction effects and the pointing jitter. By changing the beam waist w_0 of the transmitted spatial Gaussian mode, the average photon capture probability $\overline{\eta}$ can be maximized. Figure 2 shows the optimization of the beam waist for the apertures used in the present work. The results show that an optimum beam waist can be found that maximizes the average photon capture probability (this maximum barely changes with the distance between the terminals). This maximum is the result of two counteracting effects when increasing the beam waist. On the one hand, increasing the beam waist increases the collimation of the beam and therefore results in a smaller spread of the spatial mode on the receiver aperture plane. On the other hand, as the beam waist increases, the clipping effects due to the finite aperture of the transmitter start to be relevant. These clipping effects account for the telescope's transmission probability and the diffraction induced due to the edges of the aperture.

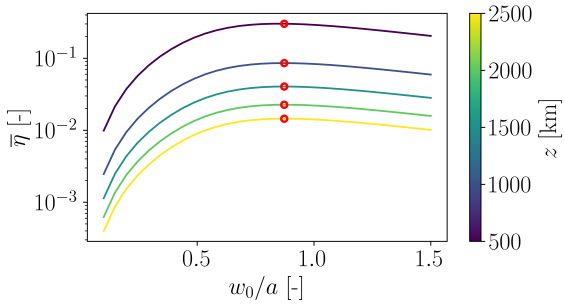


Fig. 2. Optimization of the average photon capture probability $\overline{\eta}$ as a function of the ratio w_0/a, where w_0 is the beam waist transmitted from the satellite and a is the satellite aperture radius. The simulation assumes a pointing jitter $\sigma_{\text{PJ}} = 0.47\,\mu\text{rad}$ [16,27], a satellite aperture radius $a = 15\,\text{cm}$, and a ground station aperture radius of 60 cm. Curves correspond to different link distances z.

As a result of this optimization, the spatial spread of the single-photon mode in the ground station's aperture plane can be significantly reduced, compared to a case in which $w_0 \ll a$ (where a is the transmitter's telescope radius). This optimum beam, when combined with the pointing jitter statistics, results in a higher average photon capture probability $\overline{\eta}$. This formulation generalizes the classic optimization of static on-axis irradiance [19] to include the dynamic and stochastic effects of the pointing jitter. While the static approach maximizes the peak far-field intensity, our optimization targets the average collected power by explicitly integrating over the probability density function of the pointing jitter (see Appendix A). Consequently, the optimal beam-to-aperture ratio is not fixed, but strictly depends on the magnitude of the pointing jitter as shown in Supplement 1. However, the maximization of the average photon capture probability comes along with an increase in the fluctuation of the photon capture probability η around the average $\overline{\eta}$. Although these fluctuations can be very detrimental in classical communication links [30], this is not the case for quantum entanglement distribution. As shown in Supplement 1, the average photon capture probability is what matters on quantum entanglement distribution protocols affected by the pointing jitter stochastic process. These differences arise because classical systems decode information from large correlated bit strings, which require to have a stable power to get as many of these correlated bits as possible. Then, classical error correction codes are applied to correct the bits flipped in the transmission. If the probability of being below a certain power threshold is high, the classical error correction codes cannot compensate for the flipped bits, and information contained in the full bit string is

lost. For quantum key distribution, however, we detect individual independent events on each receiver. Hence, in this case, the maximization of the number of photons captured in each receiver can be pursued.

The effect of the atmospheric channel in the performance of the system has also been modeled. The atmospheric attenuation and scattering model presented in [22] has been used. Regarding the atmospheric turbulence, under weak turbulence conditions, the effect of beam spread and wander has been considered negligible for the downlinks at limited zenith angles considered in this work [25]. Moreover, the turbulence induced scintillation and the resulting coupling efficiency on the detector is accounted for on the coupling efficiency (CL)—this efficiency is obtained assuming an adaptive optics system on the ground station [31]. Enforcing wavefront correction can be achieved by spectrally multiplexing a beacon channel alongside the photonic qubit beam on the downlink path, as shown in [32]. We assume that a spectral channel separation of a few tens of nanometers is enough to guarantee both an optimal fibre-coupling performance of the photonic qubits via the adaptive optics and efficient spectral filtering with free-space and fibre filters. Furthermore, based on satellite-to-ground experimental observations reported in [33], the depolarizing effect induced by atmospheric turbulence can be regarded as negligible.

Other dynamic atmospheric effects that significantly impact the quality of the QKD link depending on time of day and weather are also taken into account. This is possible due to the framework developed in [22], where the sun irradiance—used to calculate the stray light impinging on the single-photon detectors—and atmospheric parameters—such as cloud coverage factor, weather visibility, and the relative angle between the satellite and the ground station telescope—are extracted at the ground station locations and used to determine noise levels and photon losses dynamically. To limit the analysis to reliable links, we exclude observations where the satellite's zenith angle exceeds 75° with respect to the ground stations. We also model false detections assuming that there is a probability p_{dark} that a detector clicks despite no photon being received. We assume that this event translates into a detected state with zero fidelity with respect to the desired entangled state, leading to a lower bound in the overall fidelity measured at the ground.

C. Photon Measurement

At the ground stations, the incoming photons are randomly measured in either the Z basis—defined by the states $|H\rangle$ (horizontal) and $|V\rangle$ (vertical)—or the X basis, defined by $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ (diagonal) and $|N\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ (antidiagonal). To implement this random-basis measurement, the photons first pass through a 50/50 beam splitter (BS). At one of the BS output ports, a half-wave plate (HWP) is used to rotate the measurement basis from Z to X. Both outputs are then directed into a polarizing beam splitter (PBS), which spatially separates the polarization components, as illustrated in Fig. 1(b).

Assuming the maximally entangled state $|\Psi^+\rangle$ is received at the ground stations, it evolves as follows:

$$\begin{aligned}&\frac{1}{\sqrt{2}}(|H\rangle_{\text{A}}|V\rangle_{\text{B}} + |V\rangle_{\text{A}}|H\rangle_{\text{B}}) \xrightarrow{\text{B.S.}} \\ &\quad\frac{1}{\sqrt{2}}\Bigg[\frac{1}{\sqrt{2}}(|H\rangle_{\text{A1}} + i|H\rangle_{\text{A2}})\,\frac{1}{\sqrt{2}}(|V\rangle_{\text{B1}} + i|V\rangle_{\text{B2}}) \\ &\qquad+ \frac{1}{\sqrt{2}}(|V\rangle_{\text{A1}} + i|V\rangle_{\text{A2}})\,\frac{1}{\sqrt{2}}(|H\rangle_{\text{B1}} + i|H\rangle_{\text{B2}})\Bigg].\end{aligned} \tag{2}$$

Here, the subscripts A1, A2, B1, and B2 refer to the different spatial modes after the beam splitter for photons A and B, respectively. The different spatial modes are shown in Fig. 1(b). The output ports labelled A2 and B2 undergo a basis transformation via a HWP: $|H\rangle \to |D\rangle$ and $|V\rangle \to |N\rangle$.

Subsequently, each output passes through a PBS, which separates the polarization components before detection. The resulting state just before measurement is:

$$\begin{aligned}&|\psi_{\text{final}}\rangle \\ &= \frac{1}{2\sqrt{2}}\big[|H\rangle_{\text{AH}}|0\rangle_{\text{AV}}|0\rangle_{\text{BH}}|V\rangle_{\text{BV}} + i|H\rangle_{\text{AH}}|0\rangle_{\text{AV}}|0\rangle_{\text{BD}}|N\rangle_{\text{BN}} \\ &\quad+ i|D\rangle_{\text{AD}}|0\rangle_{\text{AN}}|0\rangle_{\text{BH}}|V\rangle_{\text{BV}} - |D\rangle_{\text{AD}}|0\rangle_{\text{AN}}|0\rangle_{\text{BD}}|N\rangle_{\text{BN}} \\ &\quad+ |0\rangle_{\text{AH}}|V\rangle_{\text{AV}}|H\rangle_{\text{BH}}|0\rangle_{\text{BV}} + i|0\rangle_{\text{AH}}|V\rangle_{\text{AV}}|D\rangle_{\text{BD}}|0\rangle_{\text{BN}} \\ &\quad+ i|0\rangle_{\text{AD}}|N\rangle_{\text{AN}}|H\rangle_{\text{BH}}|0\rangle_{\text{BV}} - |0\rangle_{\text{AD}}|N\rangle_{\text{AN}}|D\rangle_{\text{BD}}|0\rangle_{\text{BN}}\big],\end{aligned} \tag{3}$$

where the first subscript corresponds to the ground stations (A or B) and the second subscript to the detector path (H, V, D, or N), as depicted in Fig. 1(b). From Eq. (3), we observe that in half of the cases, the photon pairs are measured in the same basis (either Z or X). Consequently, during post-selection, approximately 50% of the events are discarded to ensure only measurements in matching bases are kept. The fidelity, F, of the final state, relevant to the calculations of secret key rate in the next section, is taken with respect to a maximally entangled Bell state as (refer to Appendix B for the full calculation).

3. PERFORMANCE

A. Secret Key Rate Calculation

The computation of the SKR follows the model shown in [22], where both the assumption of a depolarizing channel and Werner states produced by the entangled photon pair source have been used. This analysis provides a lower bound on the achievable secret key rate and takes as input the calculated fidelity of the state measured on the ground. Furthermore, the model enables one to split the effect of losses and decoherence (loss of fidelity) in the channel, calculating them separately only to combine them when calculating the final secret key rate expression:

$$\text{SKR} = R_{\text{final}} \cdot (\max(0, 1 - (1+\xi)\,\mathcal{H}(\text{QBER}))). \tag{4}$$

In the expression above, $\mathcal{H}$ is Shannon's entropy function, ξ is a factor representing the inneficiency of the classical protocol required for key extraction [28], and the QBER is calculated based on the total state fidelity (see Appendix B).

$$\text{QBER} = \frac{1 - \frac{3F+1}{4}}{2}. \tag{5}$$

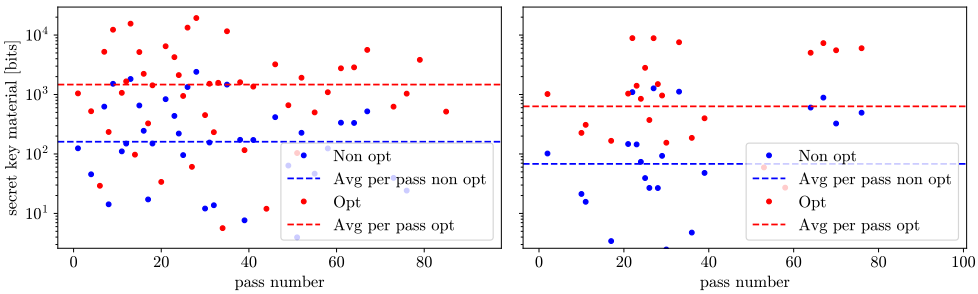


Fig. 3. Secret key material between Madrid and Barcelona (left), and Madrid and Bilbao (right). The blue data shows the usable key without carrying out the beam optimization, and the red data shows the results when applying the optimization of the beam. The discontinuous red line shows the average key per pass. In the link Madrid-Barcelona, the successful passes, where key is shared between the satellite and the ground stations, are around 39% for the non-optimized case and 48% for the optimized case. While in the Madrid-Bilbao link, the successful passes for the non-optimized case are around 22% and for the optimized case 24%, leading to a lower average of secret key material.

$R_{\text{final}} = R\, p_{\text{T,A}}\, p_{\text{T,B}}$ depends on the rate R of the source in the satellite and the total channel efficiency, i.e., source-to-ground-stations transmission probabilities. This term can be decomposed into three main ones: the free-space path loss, governed by the divergence of the beam; the atmospheric attenuation factor, governed by the weather condition; and the detector efficiency, which varies significantly in case one chooses cryogenically cooled detectors (higher efficiency, but fibre coupling is required), or free-space-coupled detectors (lower efficiency, no fibre coupling). For the purpose of this analysis, we choose to operate under the assumption that fibre coupling can be efficiently implemented via adaptive optics correction strategies, leading to an overall net improvement in the channel quality with the more efficient superconducting nanowire single-photon detectors (SNPDs). This assumption is also tied to a lower system jitter and lower detector dead times, which lead to a higher signal-to-noise ratio (due to narrower available detection time windows and detection saturation rates). For the purposes of this study, the fibre-coupling efficiency is set to 40%; inclusion of the turbulence and wavefront correction on the QKD link performance is left as future work.

In summary, the transmission from the satellite to the ground stations follows the expression:

$$p_{\text{T,A}} = \overline{\eta}_{\text{Sat-GndA}}\, \text{ATML}_{\text{Sat-GndA}}\, \text{CL}_{\text{Sat-GndA}}, \quad \textbf{(6)}$$

$$p_{\text{T,B}} = \overline{\eta}_{\text{Sat-GndB}}\, \text{ATML}_{\text{Sat-GndB}}\, \text{CL}_{\text{Sat-GndB}}. \quad \textbf{(7)}$$

$\overline{\eta}$ accounts for the diffraction and pointing jitter losses (see Section 2.B), ATML for atmospheric attenuation and scattering loss, CL for coupling loss, and GndA/GndB for the two ground stations of interest. A coupling loss of CL = 0.5 is considered in agreement with simulations and experimental data in optical downlink channels with adaptive optics and single-mode fiber coupling [31,34,35]. Further detailed description of how each of these terms is evaluated can be found in Supplement 1. The reason for evaluating the two paths individually is the channel asymmetry during satellite transit, not only in terms of the dynamic conditions (such as weather conditions) but also the distance between the spacecraft and either ground station.

Equipped with the overall loss term, the probabilities—per attempt—associated with the detection of a valid pair can be translated into raw detection rates via the source pair emission rate R. These are further translated into expected secret key rate using a key extraction algorithm that implements: basis reconciliation, error correction, and privacy amplification. As mentioned before, depending on the channel quality, the raw detection material that must be spent in order to produce a final key will change according to the classical protocols being used. Since this procedure can be quite computationally intensive and would have to be executed for each time step at each satellite pass, a look-up table was generated by feeding the software with a grid of parameters (QBER and block length)—refer to Appendix C for discussions and results.

B. Representative System Evaluation

For the course of one month, specifically June 2025, we compute the SKR per satellite pass that reached the ground stations, while accounting for real-time weather conditions. Our analysis focuses on three links: Madrid–Barcelona (504 km), Madrid–Bilbao (322 km), and Madrid–Lisbon (503 km). We begin by computing the SKR per pass and, based on this, derive the usable secret key material per pass. By averaging the usable key material per pass and taking into account the percentage of successful passes, i.e., the passes where communication between the satellite and the ground stations is established, we obtain the average secret key material rate, which we then compare against the requirements of Telefónica and JPMorgan use cases.

In Fig. 3, we present the secret key material per satellite pass and its average for both the non-optimized and optimized cases on the Madrid–Barcelona and Madrid–Bilbao links. The non-optimized beam refers to a Gaussian with a beam waist of radius $w_{0,\text{non-opt}} = 2.7$ cm, which is compatible with the 10 μrad divergence at a wavelength of 850 nm, as reported in Ref. [21] for the Micius satellite. The figure shows that beam optimization results in an increase of the average secret key material by an order of magnitude, which increases the SKR to a point where enough secret bits are produced to run the applications.

Table 1 summarizes the computed results for the different links and compares them against two use cases: Telefónica [18], which requires 256-bit keys every 12 hours (equivalent to 0.006 bits/s), and JPMorgan [17], which requires 256-bit keys every 2 minutes (2.13 bits/s). For the Telefónica case, the 256-bit size ensures compliance with the standard RFC 8784, while the 12-hour rotation is a conservative reduction of the NIST 24-hour recommendation to protect sensitive medical data [36]. We observe that the 12-hour key renewal, used for communication between hospitals, is achieved across all links when the beam optimization is carried out. We do also see that for the link Madrid-Barcelona, this last use case can also be implemented

Table 1. Summary of Results for an Entangled Photon Source (Micius-like, $5.9 \cdot 10^6$ Hz [16])[a]

	Non-Optimized Scenario			Optimized Scenario		
Link	**Rate [Keys/s]**	**Telefónica**	**JPMorgan**	**Rate [Keys/s]**	**Telefónica**	**JPMorgan**
		Req. met?	*Req. met?*		*Req. met?*	*Req. met?*
Mad-Bilb	0.003	No	No	0.028	Yes	No
Mad-Bcn	0.012	Yes	No	0.132	Yes	No
Mad-Lis	0.004	No	No	0.055	Yes	No

[a]The Table details whether the achievable key rates meet the distinct service requirements for Telefónica (0.006 Keys/s) and JPMorgan (2.13 Keys/s).

without the optimization. This is due to the high percentage of successful passes, i.e., the key is shared between the satellite and the ground stations, we observe in that link during the month we are evaluating: around 40% for the non-optimized case and 50% for the optimized. This contrasts with the other two links, where the percentage of successful passes is around 20–25%, and up to 34% for the optimized case between Madrid and Lisbon. The passes where the communication is established between the satellite and the ground station are higher in the optimized case due to the fact that in those cases the overall channel efficiency improves; therefore, there will be cases where the SKR is zero in the non-optimized cases and non-zero in the optimized case.

However, for the more demanding use case of QKD-based VPNs, where the key must be refreshed every 2 minutes, the required key rate is not met. To get to such key requirements, we would need to improve the entangled photon source rate to the order of 1 GHz [24] (for more details, check Appendix D). Additionally, we could also boost the SKR by not only increasing the photon source rate but also combining it with the decrease in coupling loss, CL, which we consider 0.5 due to the scintillation effect of the lowest parts of the atmosphere [31,34,35]. This coupling efficiency could be increased by considering free-space coupling into the single-photon detectors [37], or multimode fiber coupling [38,39]. For distances beyond the Iberian Peninsula, constellations of satellites could be used.

4. CONCLUSION

In summary, we have demonstrated how single-satellite architectures enable the extension of quantum key distribution (QKD) from metropolitan-scale deployments [18] to national-scale distances. Our approach employs an entanglement-based QKD protocol, which eliminates the need for trusted nodes in the key distribution process, thereby reducing the risk of eavesdropping. Furthermore, we introduced a beam optimization method that accounts for satellite pointing jitter and the clipping effects due to the finite size of the transmitter's aperture, maximizing the transmission probability. This optimization allows us to meet the key rate requirement for the current use cases of secure communication between two hospitals [18], using state-of-the-art satellite technology [16]. Furthermore, by upgrading the rate of the entangled photon source to 1 GHz, which can be reached with current technology [24], we could also meet the requirement for the most demanding use case [17].

In those use cases, hybrid quantum algorithms are employed, where only the first layer involves quantum processing. As a natural progression, future work should investigate fully quantum algorithms and their corresponding key rate requirements.

Additionally, in our current setup, we assume trusted ground stations for classical information storage. Incorporating quantum memories at the ground level would allow for the use of untrusted ground stations and enable the distribution of entanglement across nodes. This would open the door to a broader range of quantum technologies beyond QKD, including blind quantum computing [40,41] and quantum-enhanced sensing networks [4–6].

APPENDIX A: FREE-SPACE CHANNEL MODEL

In this appendix, we discuss the details of our free-space channel model. This model considers the effects of the beam propagation and the pointing jitter in a coupled manner. Furthermore, as the maximum average photon capture probability is obtained when the spatial Gaussian mode describing the single photon in the transmitter aperture is highly clipped, the model presented in this appendix also accounts for the diffraction effects due to this clipping. A more detailed explanation of this model can be found in [30].

The beam waist w_0 of the spatial Gaussian mode is located at the satellite's telescope aperture. The telescope on board the satellite has a radius a. The field at the ground station's aperture plane, located at a distance z, can be computed numerically through Fresnel propagation [42]. This propagation gives the probability density function of the spatial location of the single photon, i.e., $I(x, y)$, in the ground station's aperture plane. Then, a convolution can be performed to compute the probability of capturing the single photon $g(x_0, y_0)$ when the center of the beam is displaced to (x_0, y_0) in the ground station's reference system. This convolution can be computed using the convolution theorem by:

$$g(x_0, y_0) = \mathcal{F}^{-1}\mathcal{F}(I) \cdot \mathcal{F}(A), \tag{A1}$$

where $A(x, y)$ is the aperture function of the ground station's telescope and $\mathcal{F}$ is the bidimensional Fourier transform. The satellite pointing jitter is modeled as a bidimensional Gaussian probability density function of the location of the center of the beam at the ground station frame of reference (x_0, y_0):

$$f_{\mathrm{PJ}}(x_0, y_0) = \frac{1}{2\sigma^2} \exp\left(-\frac{x_0^2 + y_0^2}{2\sigma^2}\right), \tag{A2}$$

where $\sigma = z\sigma_{\mathrm{PJ}}$, and σ_{PJ} is the angular pointing jitter. By combining the previous equations, the probability density function of the photon capture probability can be computed as [43]:

$$f(\eta) = \iint_{\mathbb{R}^2} f_{\mathrm{PJ}}(x_0, y_0)\, \delta[\eta - g(x_0, y_0)]\, dx_0\, dy_0, \tag{A3}$$

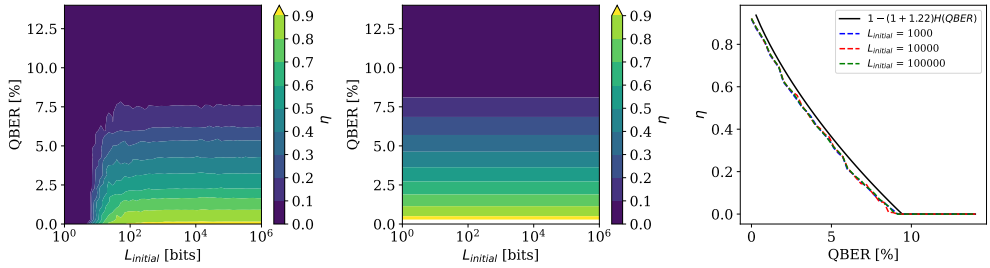


Fig. 4. Key extraction efficiency—look up table. The heatmap shows the value of η_{LUT} (Eq. (C1)) as a function of the block length and the estimated QBER.

where $\delta(x)$ is the Dirac delta function. Finally, the average of this probability density function gives the average photon capture probability. As shown in Supplement 1, the latter is to be maximized in the context of quantum entanglement-based QKD for optimal performance of the system. This maximization is done by varying the beam waist w_0 of the spatial Gaussian mode transmitted.

APPENDIX B: FIDELITY OF THE FINAL STATE

In this appendix, we provide a more detailed calculation of how we compute the fidelity required for the secret key rate computation. The final state is of the form:

$$\rho_{\mathrm{final}} = A|\psi\rangle\langle\psi| + B\rho_{\mathrm{deph}} + C\rho_{\mathrm{garb}}, \tag{B1}$$

where $|\psi\rangle$ is the desired target state which gives fidelity 1, ρ_{deph} are the multi-photon states, where one photon for each elementary link has been lost, resulting in a dephased states which gives fidelity smaller than one, and ρ_{garb} is the non-specified 'garbage' density matrix with zero overlap with the desired target state. The (normalized) density matrix of the dephased state is the following:

$$\begin{aligned}\rho_{\mathrm{deph}} = \frac{1}{12}\,(&5|H\rangle|V\rangle\langle H|\langle V| + 5|V\rangle|H\rangle\langle V|\langle H| + |H\rangle|H\rangle\langle H|\langle H| \\ &+|V\rangle|V\rangle\langle V|\langle V|)\,,\end{aligned} \tag{B2}$$

being the fidelity of the previous state:

$$F_{\mathrm{deph}} = \langle\psi|\rho_{\mathrm{deph}}|\psi\rangle = 5/12. \tag{B3}$$

Therefore, the overall fidelity is:

$$F = \frac{\langle\psi|\rho_{\mathrm{final}}|\psi\rangle}{Tr(\rho_{\mathrm{final}})} = \frac{A + \frac{5}{12}B}{A + B + C}, \tag{B4}$$

where the parameters A, B, C are the following:

$$A = \lambda(1-\lambda)p_{\mathrm{T,A}}p_{\mathrm{T,A}}, \tag{B5}$$

$$B = 5\lambda^2 p_{\mathrm{T,A}}p_{\mathrm{T,B}}(1-p_{\mathrm{T,A}})(1-p_{\mathrm{T,B}}), \tag{B6}$$

$$\begin{aligned}C = \lambda(1-\lambda)\,&\big(p_{\mathrm{T,A}}(1-p_{\mathrm{T,B}})p_{\mathrm{dark}} + p_{\mathrm{T,B}}(1-p_{\mathrm{T,A}})p_{\mathrm{dark}} \\ &+ (1-p_{\mathrm{T,A}})(1-p_{\mathrm{T,B}})p_{\mathrm{dark}}^2\big) \\ &+ \lambda^2\,\big(3p_{\mathrm{T,A}}(1-p_{\mathrm{T,A}})(1-p_{\mathrm{T,B}})^2 p_{\mathrm{dark}} \\ &+3p_{\mathrm{T,B}}(1-p_{\mathrm{T,B}})(1-p_{\mathrm{T,A}})^2 p_{\mathrm{dark}} \\ &+\frac{3}{2}(1-p_{\mathrm{T,A}})^2(1-p_{\mathrm{T,B}})^2 p_{\mathrm{dark}}^2\big) \\ &+ \frac{1}{2}(1-\lambda)^2 p_{\mathrm{dark}}^2.\end{aligned} \tag{B7}$$

APPENDIX C: KEY EXTRACTION

The key extraction protocol is performed after the quantum state transmission and reception phase of QKD, leading to a so-called block of detection events. The two communicating parties in the BBM92 configuration transmit the time-tagged information about the (in this case, passively) chosen measurement bases. Basis reconciliation and time filtering allow both parties to discard all events that correspond to mismatched bases or those that fall outside the time window of acceptance. It is important to note that time synchronization, in this case, must be enforced between the receiving parties, i.e., the OGSs. Therefore, ground-based solutions, such as the White Rabbit Protocol [44], can be used to achieve synchronization with precision down to tens of picoseconds. At this point, the protocol requires the parties to sacrifice a subset of the remaining events by disclosing the detection outcome in order to calculate the QBER. If the value is below the threshold for security—at 11% for BBM92 [45]—the protocol moves on to the next stage. Depending on the value of the QBER, however, the amount of privacy amplification rounds will vary: for low values of QBER, the expected mutual information between the communicating parties and a potential adversary is low, indicating that the security of the key is high; if the value of the QBER approaches the threshold, more rounds are necessary to reduce the mutual information and enforce security of the key material.

The factor on the right-hand side of Eq. (4) of the Main Text indicates the ratio between the amount of raw detection events before privacy amplification and error correction rounds and the final amount of secure bits output by the protocol. Practical operation of QKD systems requires online computation of the QBER and execution of the subsequent rounds of classical communication that enable producing a key. The complexity of the steps, and the fact that they may be executed several times, lead to the development of dedicated hardware to tackle this problem efficiently and ensuring that it does not represent a bottleneck in the key distribution link. For the analysis presented in this work, several satellite passes have been evaluated over multiple days, which translates into a heavy computational task to execute the classical protocol for each block of raw detection events. Therefore, a look-up table (LUT) was created allowing one to efficiently and accurately estimate the value of the so-called **key extraction efficiency** (η_{LUT}) given a block length and the corresponding QBER value. In other words:

$$\begin{aligned}\mathrm{SKR} &= R_{\mathrm{final}} \cdot (\max\,(0, 1-(1+\xi)\,\mathcal{H}\,(\mathrm{QBER}))) \\ &= R_{\mathrm{final}} \cdot \eta_{\mathrm{LUT}}\,[L_{\mathrm{block}}; \mathrm{QBER}]\,.\end{aligned} \tag{C1}$$

The look-up table was generated by artificially inputting bit strings—of different length and error rate—to a key extraction

Table 2. Summary of Results for an Entangled Photon Source of 10^9 Hz[a]

	Non-Optimized Scenario			Optimized Scenario		
Link	**Rate [Keys/s]**	**Telefónica**	**JPMorgan**	**Rate [Keys/s]**	**Telefónica**	**JPMorgan**
		Req. met?	*Req. met?*		*Req. met?*	*Req. met?*
Mad-Bilb	0.565	Yes	No	5.005	Yes	Yes
Mad-Bcn	2.367	Yes	Yes	22.978	Yes	Yes
Mad-Lis	1.031	Yes	No	10.378	Yes	Yes

[a]The table details whether the achievable key rates meet the distinct service requirements for Telefónica (0.006 Keys/s) and JPMorgan (2.13 Keys/s).

software implementing the Cascade error correction protocol [46,47]. For each combination of $[L_{\text{block}}; \text{QBER}]$, η_{LUT}—presented as a heatmap in Fig. 4(a)—outputs a value of that can be immediately used to calculate the expected key material generated by the QKD protocol. In Fig. 4(b), we present the same calculations but considering a static value of $\xi = 1.22$, which approximates the realistic results for large block lengths ($L \geq 10^4$). Due to the limited availability of the satellite during the pass, and the dynamic weather conditions that can significantly diminish the key material generated on the ground, the regime of $L \leq 10^4$ is relevant for the analysis of the results and justifies the use of η_{LUT}.

APPENDIX D: RESULTS WITH AN ENTANGLED PAIR PHOTON SOURCE RATE OF 10^9 HZ

In this appendix, we provide the results we get with an entangled photon source rate 3 orders of magnitude higher than Micius. As we see in Table 2, we always get the key requirements for Telefónica´s use case, and with the optimization we get the more demanding use case of refreshing the key each two minutes from JPMorgan.

Funding. Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Project QSC No. 024.003.037, P19-13); Amazon Web Services (Quantum Discovery Fund).

Acknowledgment. V.D.T. acknowledges helpful discussions with Antonio Agustín Pastor Perales and María Ruiz Fernández de Arcaya. V.D.T. and J.B. acknowledge funding from the NWO Gravitation Program Quantum Software Consortium (Project QSC No. 024.003.037). J.B. acknowledges support from The AWS Quantum Discovery Fund at the Harvard Quantum Initiative. M.B. acknowledges the funding from the NWO Perspectief FREE Program (P19-13).

Disclosures. The authors declare no conflicts of interest.

Data availability. The data of the results of this paper are openly available on 4TU.ResearchData: Data underlying the publication "Quantum Key Distribution in the Iberian Peninsula" at Ref. [48].

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci. **560**, 7–11 (2014).
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
3. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
4. P. Kómár, E. M. Kessler, M. Bishof, *et al.*, "A quantum network of clocks," Nat. Phys. **10**, 582–587 (2014).
5. X. Guo, C. R. Breum, J. Borregaard, *et al.*, "Distributed quantum sensing in a continuous-variable entangled network," Nat. Phys. **16**, 281–284 (2020).
6. L.-Z. Liu, Y.-Z. Zhang, Z.-D. Li, *et al.*, "Distributed quantum phase estimation with entangled photons," Nat. Photonics **15**, 137–142 (2021).
7. H. Buhrman and H. Röhrig, "Distributed quantum computing," in *Mathematical Foundations of Computer Science 2003*, B. Rovan and P. Vojtáš, eds. (Springer, 2003), Lecture Notes in Computer Science, pp. 1–20.
8. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
9. L. M. Duan, M. D. Lukin, J. I. Cirac, *et al.*, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413–418 (2001).
10. N. Sangouard, C. Simon, H. de Riedmatten, *et al.*, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys. **83**, 33–80 (2011).
11. S. Muralidharan, J. Kim, N. Lütkenhaus, *et al.*, "Ultrafast and fault-tolerant quantum communication across long distances," Phys. Rev. Lett. **112**, 250501 (2014).
12. W. J. Munro, A. M. Stephens, S. J. Devitt, *et al.*, "Quantum communication without the necessity of quantum memories," Nat. Photonics **6**, 777–781 (2012).
13. J. Yin, Y. Cao, Y.-H. Li, *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," Phys. Rev. Lett. **119**, 200501 (2017).
14. S.-K. Liao, W.-Q. Cai, J. Handsteiner, *et al.*, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).
15. J. Yin, Y.-H. Li, S.-K. Liao, *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature **582**, 501–505 (2020).
16. J. Yin, Y. Cao, Y.-H. Li, *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140–1144 (2017).
17. O. Alia, A. Huang, H. Luo, *et al.*, "Quantum-safe 10 Gbps site-to-site IPsec VPN tunnel over 46 km deployed fibre," in *2024 Optical Fiber Communications Conference and Exhibition (OFC)* (2024), pp. 1–3.
18. Telefónica and Vithas, "Telefónica and Vithas test shielding against quantum attacks in two hospitals," (2025). Press release, https://www.telefonica.com/es/sala-comunicacion/prensa/telefonica-vithas-prueban-blindaje-frente-ataques-cuanticos-hospitales/.
19. A. E. Siegman, *Lasers* (University Science Books, 1986).
20. A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," J. Light. Technol. **25**, 1702–1710 (2007).
21. C.-Y. Lu, Y. Cao, C.-Z. Peng, *et al.*, "Micius quantum experiments in space," Rev. Mod. Phys. **94**, 035001 (2022).
22. D. L. Bakker, Y. Jong, B. P. F. Dirks, *et al.*, "A best-path approach to the design of a hybrid space–ground quantum network with dynamic constraints," Photonics **11**, 268 (2024).
23. P. Zippenfenig, "Open-Meteo.com Weather API," GitHub, 2025, https://github.com/open-meteo/open-meteo .
24. J. Merolla, B. Pages, J. Cussey, *et al.*, "High-performance 1560 nm entangled photon source for high secure key rates QKD satellite-based communications," in *ICSOS International Conference on Space Optics (ICSO 2022)* (2022), pp. 1–12.
25. L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media* (SPIE, 2005).

26. M. Gündoğan, J. S. Sidhu, V. Henderson, *et al.*, "Proposal for space-borne quantum memories for global quantum networking," NPJ Quantum Inf. **7**, 128 (2021).
27. X. Wang, X. Wang, C. Li, *et al.*, "Angular micro-vibration of the Micius satellite measured by an optical sensor and the method for its suppression," Appl. Opt. **60**, 1881–1887 (2021).
28. X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," Phys. Rev. A **76**, 012307 (2007).
29. V. D. Tubío, M. B. Aldecocea, J. van Dam, *et al.*, "Satellite-assisted quantum communication with single photon sources and atomic memories," arXiv (2024).
30. M. Badás, P. Piron, J. Bouwmeester, *et al.*, "Seidel optical aberrations and optimum truncated Gaussian beams on intersatellite free space optical communications," Opt. Express **33**, 33686–33703 (2025).
31. M. Chen, C. Liu, and H. Xian, "Experimental demonstration of single-mode fiber coupling over relatively strong turbulence with adaptive optics," Appl. Opt. **54**, 8722–8726 (2015).
32. M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, *et al.*, "Adaptive-optics-enabled quantum communication: a technique for daytime space-to-earth links," Phys. Rev. Appl. **16**, 014067 (2021).
33. A. Carrasco-Casado, H. Kunimori, H. Takenaka, *et al.*, "LEO-to-ground polarization measurements aiming for space QKD using small optical TrAnsponder (SOTA)," Opt. Express **24**, 12254–12266 (2016).
34. V. Marulanda Acosta, D. Dequal, M. Schiavon, *et al.*, "Analysis of satellite-to-ground quantum key distribution with adaptive optics," New J. Phys. **26**, 023039 (2024).
35. M. T. Gruneisen, M. B. Flanagan, and B. A. Sickmiller, "Modeling satellite-Earth quantum channel downlinks with adaptive-optics coupling to single-mode fibers," Opt. Eng. **56**, 1 (2017).
36. E. Barker, Q. Dang, S. Frankel, *et al.*, "Guide to IPsec VPNs," *Tech. Rep. NIST SP 800-77r1* (National Institute of Standards and Technology, 2020).
37. A. S. Mueller, B. Korzh, M. Runyan, *et al.*, "Free-space coupled superconducting nanowire single-photon detector with low dark counts," Optica **8**, 1586–1587 (2021).
38. D. Zheng, Y. Li, E. Chen, *et al.*, "Free-space to few-mode-fiber coupling under atmospheric turbulence," Opt. Express **24**, 18739–18744 (2016).
39. P. V. Trinh, D. R. Kolev, K. Shiratama, *et al.*, "Experimental verification of fiber coupling characteristics for FSO downlinks from the international space station," Opt. Express **31**, 9081–9097 (2023).
40. J. F. Fitzsimons, "Private quantum computation: an introduction to blind quantum computing and related protocols," NPJ Quantum Inf. **3**, 11 (2017).
41. R. Van Meter and S. J. Devitt, "The path to scalable distributed quantum computing," Computer **49**, 31–42 (2016).
42. J. W. Goodman, *Introduction to Fourier Optics*, 3rd ed. (Roberts Co., 2005).
43. V. K. Rohatgi and A. K. M. E. Saleh, *An Introduction to Probability and Statistics*, 2nd ed. (John Wiley Sons, Incorporated, 2001).
44. P. Moreira, J. Serrano, T. Wlostowski, *et al.*, "White rabbit: sub-nanosecond timing distribution over Ethernet," in *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication* (IEEE, 2009), pp. 1–5.
45. E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," Phys. Rev. A **65**, 052310 (2002).
46. T. Attema, J. W. Bosman, and N. M. Neumann, "Optimizing the decoy-state BB84 QKD protocol parameters," Quantum Inf. Process **20**, 154 (2021).
47. N. Neumann, R. Wezeman, and A. Amadora, "Github—key extraction protocol," GitHub (2023), https://github.com/TNO-Quantum/communication.qkd$_{key_rate}$.
48. V. Domínguez Tubio, M. Badás Aldecocea, D. Bakker, *et al.*, "Data underlying the publication 'quantum key distribution in the Iberian Peninsula'," 4TU.ResearchData (2025), https://doi.org/10.4121/eda0897b-8157-4ab3-9a1b-db10d1baf33e.v1.