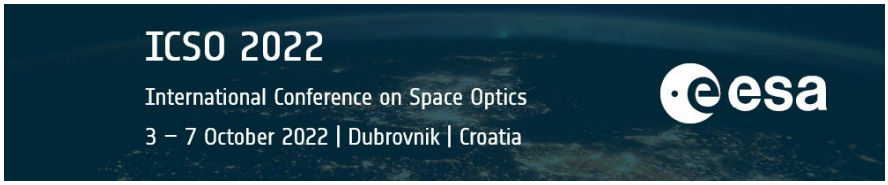
International Conference on Space Optics—ICSO 2022

Dubrovnik, Croatia

3–7 October 2022

Edited by Kyriaki Minoglou, Nikos Karafolas, and Bruno Cugny,



Dual-downlink quantum key distribution with entangled photons: Prospects for daylight operation

International Conference on Space Optics — ICSO 2022, edited by Kyriaki Minoglou, Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 12777, 1277726 · © 2023 ESA and CNES · 0277-786X · doi: 10.1117/12.2689971

Dual-downlink quantum key distribution with entangled photons: Prospects for daylight operation

Andrej Kržič[a,b], Daniel Heinig[a], Matthias Goy[a], and Fabian Steinlechner[a,c]

[a]Fraunhofer Institute for Applied Optics and Precision Engineering, Albert-Einstein-Str. 7, 07745 Jena, Germany
[b]Friedrich Schiller University Jena, Faculty of Physics and Astronomy, Max-Wien-Platz 1, 07743 Jena, Germany
[c]Abbe Center of Photonics, Friedrich Schiller University Jena, Albert-Einstein-Str. 6, 07745 Jena, Germany

ABSTRACT

In recent years, quantum key distribution (QKD) has seen the first proof-of-concept demonstrations from space. Next on the agenda towards a full-blown global quantum internet is to address the more practical aspects, such as efficiency, flexibility, and accessibility of QKD services. One of the main challenges that remains to be solved in this regard is to enable operation in the presence of daylight noise. Here, we present a complete framework for modelling daylight QKD from an orbiting satellite. We include the effects of atmospheric turbulence and adaptive optics correction at the receivers. We consider single- and multi-mode fibre coupling as a means of spatial filtering, for which we derived simple formulas for estimating coupling efficiencies of signal as well as noise. Using our framework, we identify the most critical system parameters for daylight operation and discuss the choice of signal wavelength and detection technology. Finally, we provide simulation results for various parameter combinations in a hypothetical daylight QKD between Berlin and Munich via a satellite in a low Earth orbit. The results show a clear advantage of 800 nm signal wavelength over 1550 nm with the currently available technology. Moreover, we show the relevance of single-mode fibre coupling and the importance of detectors with low timing jitters. We anticipate our work will provide valuable insight and tools to aid the future feasibility studies of daylight QKD in dual-downlink configurations.

Keywords: quantum key distribution, quantum entanglement, dual downlink, daylight noise, adaptive optics

1. INTRODUCTION

Quantum key distribution[1] is a form of quantum communication, where the communicating parties attempt to establish a secret key, of which security is based on the laws of quantum mechanics. Since fibre-based implementations are limited to a few hundred kilometres,[2] there is an ever growing interest in satellite implementations for bridging larger distances.

There are two popular but fundamentally different ways to perform QKD from space: with attenuated lasers (also called prepare-and-measure) or with entangled photons. Although still behind the technological maturity of prepare-and-measure schemes, recent developments towards ultra-bright and space-suitable entangled photon sources have considerably increased interest in entanglement-based QKD for space applications. Here, we focus on the latter and consider a dual-downlink configuration, where an entangled photon source (EPS) on board of a satellite is used to establish a secret key between two ground stations. This configuration offers several advantages. First of all, the EPS does not need to be trusted, allowing the satellite to act as an untrusted node. Furthermore, the EPS generates entangled photons in a completely passive manner, essentially requiring no access to the inner workings of the satellite by the users on ground. This further gives users on ground

Send correspondence to:
Andrej.Krzic@iof.fraunhofer.de
Fabian.Steinlechner@iof.fraunhofer.de

much more flexibility in terms of the choice of protocol, quantum measurement, and post-processing, since these considerations are to a large degree independent of the EPS.

One of the main remaining challenges in practical QKD is the daylight noise. During daytime, a vast amount of sunlight enters receiver telescopes and may end up completely masking the weak quantum signal upon detection. The background noise primarily consists of photons that are scattered in the Earth's atmosphere, thus changing the direction of propagation and ending up within the field of view of the receiver system. In order to reduce the noise to acceptable levels, we therefore need strong filtering in all the possible degrees of freedom: temporal, spectral and spatial. In QKD with entangled photons, temporal filtering is automatically realized by the coincidence-based detection and typically provides the strongest rejection of the noise. The level of temporal filtering we can apply is dictated by the detector time jitter. Similarly, the level of spectral filtering is usually dictated by the signal bandwidth and realized by off-the-shelf components. Temporal and spectral filtering can therefore be realized with relative ease and their effect can be typically predicted to a good degree. Moreover, they do not depend on the link conditions. Spatial filtering, on the other hand, is more complex, because it usually depends on the ability to focus the incoming light, which deteriorates in the presence of atmospheric turbulence. Adaptive optics (AO) is therefore often considered in the context of spatial filtering, making the system design much more demanding and complex. Coupling the signal into optical fibres is one of the ways to realize spatial filtering. While notable daylight QKD experiments have been recently reported over terrestrial links,[3–5] all the satellite-based QKD demonstrations have thus far been performed at night.

Here, we present a complete framework to model daylight QKD with entangled photons from an orbiting satellite. We review the established models for secure key and link efficiency calculations. We further derive simple formulas for estimating signal coupling efficiency into single- and multi-mode fibres in the presence of atmospheric turbulence. We also derive relations for estimating the sky background noise rate at the detectors for the case of both single- and multi-mode fibres. We then discuss important open questions, such as the choice of signal wavelength and the available detector technology, and provide insight into into state-of-the-art sources. We finally provide simulation results for various parameter combinations in a hypothetical daylight QKD between Berlin and Munich via a satellite in a low Earth orbit (LEO).

2. SATELLITE-BASED QUANTUM KEY DISTRIBUTION WITH ENTANGLED PHOTONS

In QKD in a dual-downlink configuration, an EPS on board of a satellite generates pairs of entangled photons, which are transmitted to two separate optical ground stations (OGSs). Two communicating users, commonly called Alice and Bob, each associated with one OGS, perform measurements on the incoming photons according to a specific protocol from which they try to extract a secret key. For modelling the link geometry dynamics for a particular orbit and ground station locations, we used the Skyfield package*.

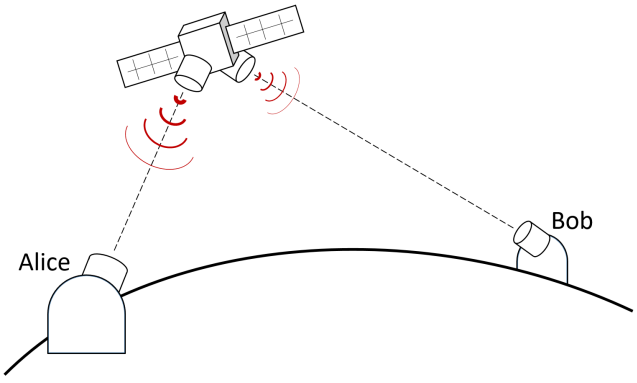


Figure 1. Dual-downlink configuration for entanglement-based quantum key distribution.

*http://rhodesmill.org/skyfield/

2.1 Secure Key Rate Calculation

Here, we consider the BBM92 protocol,[6] which is the most commonly considered protocol for entanglement-based QKD. For secure key rate calculations, we adapted the model from Ref. 7. Consider a continuous-wave pumped EPS that generates pairs of polarization-entangled photons with the rate G. Note, that this is the intrinsic pair generation rate, meaning that no loss – not even of the source optics – is yet considered. One photon of each generated pair is sent towards Alice and the other one towards Bob via their respective channels, which are characterized by their total channel efficiencies η_{A} and η_{B}.

Secure key generation is based on correlation of simultaneous detection events – coincidences – at Alice and Bob, and this correlation is provided by the quantum entanglement of the signal photon pairs. Coincidences are defined as events when a single-photon detection at one site happens within $\pm\frac{\tau}{2}$ of a detection time at the other site, where τ is called coincidence window. Due to channel losses, many pairs do not make it to their respective detectors, in turn reducing the rate of desirable coincidences, called true coincidences. But what is even worse, is that some photons lose their partner photons while they alone make it to a detector. There is a chance that two such partner-less photons – one at each site – still produce simultaneous clicks, which are called accidental coincidences.

In order to estimate the secure key rate, the relationship between true and accidental coincidences need to be established. True coincidence rate is simply the pair generation rate reduced by the combined total loss of both channels,

$$C_{\mathrm{true}} = \eta^{\mathrm{A}}\eta^{\mathrm{B}}G\,. \tag{1}$$

Accidental coincidences, on the other hand, are determined by the single photons detected locally at each site. For high-loss scenarios, which certainly is the case for space links, accidental coincidence rate can be approximated by[7]

$$C_{\mathrm{acc}} = \frac{\left(1-e^{-S^{\mathrm{A}}_{\mathrm{det}}\tau}\right)\left(1-e^{-S^{\mathrm{B}}_{\mathrm{det}}\tau}\right)}{\tau}\,, \tag{2}$$

where $S^{\mathrm{A}}_{\mathrm{det}}$ and $S^{\mathrm{B}}_{\mathrm{det}}$ are the local single-photon detection rates at Alice and Bob, respectively. Since not only the signal but also noise contributes to the detected single-photon rates, we break them down as

$$S^{\mathrm{i}}_{\mathrm{det}} = S^{\mathrm{i}}_{\mathrm{true}} + S^{\mathrm{i}}_{\mathrm{back}} + S^{\mathrm{i}}_{\mathrm{dark}}\,. \tag{3}$$

where $S^{\mathrm{i}}_{\mathrm{dark}}$ is the dark count rate, $S^{\mathrm{i}}_{\mathrm{back}}$ is the background noise rate, and $S^{\mathrm{i}}_{\mathrm{true}}$ is the rate of true single photon detection events that originate from the EPS, given by

$$S^{\mathrm{i}}_{\mathrm{true}} = \eta^{\mathrm{i}}G\,. \tag{4}$$

We introduced $\mathrm{i}\in[A,B]$, which indicates Alice or Bob. Note, that these are total rates, therefore $S^{\mathrm{i}}_{\mathrm{dark}}$ is a sum of dark count rates of all 4 detectors used at site i.

We may now combine true and accidental coincidences into the total detected coincidence rate,

$$C_{\mathrm{det}} = \eta_{\mathrm{coin}}C_{\mathrm{true}} + C_{\mathrm{acc}}\,, \tag{5}$$

where we introduced coincidence detection efficiency η_{coin} that only applies to coincidence and not to single-photon detection. It is given by

$$\eta_{\mathrm{coin}} = \mathrm{erf}\left[\frac{1}{2\sqrt{2}}\frac{\tau}{\sqrt{{\sigma^{\mathrm{A}}_{\mathrm{det}}}^2+{\sigma^{\mathrm{B}}_{\mathrm{det}}}^2}}\right]\,, \tag{6}$$

where $\sigma^{\mathrm{i}}_{\mathrm{det}}$ is the total detection timing jitter at the ground station i. Strictly speaking, $\sigma^{\mathrm{i}}_{\mathrm{det}}$ should in addition to detector jitters include also effects of dispersion and photon coherence times, however, these are often negligible compared to detector jitters. Some of the true coincidences may nevertheless cause erroneous (uncorrelated) outcomes. This is characterized by the baseline error rate e_0, which accounts for the source imperfections and

imperfect alignment of polarization frame of reference between Alice and Bob. We calculate the rate of erroneous coincidences as

$$C_{\mathrm{err}} = \eta_{\mathrm{coin}} C_{\mathrm{true}} e_0 + \frac{1}{2} C_{\mathrm{acc}} \,. \tag{7}$$

Note, that not all the accidental coincidences contribute to errors – some may completely by chance produce a correlated outcome, which also contributes to the secret key, hence the factor of 1/2. The quantum bit error rate (QBER) is then given by

$$E = \frac{C_{\mathrm{err}}}{C_{\mathrm{det}}} \,. \tag{8}$$

Assuming that one of the two mutually unbiased measurement bases is selected with 50:50 probability, secure key rate is finally given by

$$K = \frac{1}{2} C_{\mathrm{det}} \left[1 - f_{\mathrm{EC}} \mathrm{H}_2(E) - \mathrm{H}_2(E)\right] \,, \tag{9}$$

where H_2 is the binary entropy function defined as

$$\mathrm{H}_2(x) = -x \log_2(x) - (1-x) \log_2(1-x) \,, \tag{10}$$

and f_{EC} is the error correction efficiency factor. In general, f_{EC} depends on E and the chosen error correction algorithm, but for simulations we may set it to a conservative fixed value, e.g. $f_{\mathrm{EC}} = 1.22$.[8] Note, that this is the asymptotic secure key rate, which assumes infinitely large blocks of raw key, before post-processing is applied to distil the final secret key. Finite key analysis is an important aspect of practical QKD – even more so for space links, where the satellite is available for only short periods of time – however, it is beyond the scope of this work.

2.2 Link Loss Model

As shown in Sec. 2.1, we need to know the total loss for each of the two channels to calculate the key rate. We now go step by step through the entire channel and identify each individual loss contribution. We start by defining the total efficiency of the channel i as

$$\eta^{\mathrm{i}} = \eta^{\mathrm{i}}_{\mathrm{EPS}} \eta^{\mathrm{i}}_{\mathrm{Tx}} \eta^{\mathrm{i}}_{\mathrm{DL}} \eta^{\mathrm{i}}_{\mathrm{Rx}} \eta^{\mathrm{i}}_{\mathrm{FC}} \eta^{\mathrm{i}}_{\mathrm{det}} \,, \tag{11}$$

Here, $\eta^{\mathrm{i}}_{\mathrm{EPS}}$ is the source efficiency, which accounts for all the losses for the i-channel photons, before they leave the source module. All the remaining losses of the transmitter optics are combined in $\eta^{\mathrm{i}}_{\mathrm{Tx}}$. The downlink efficiency is given by[9]

$$\eta^{\mathrm{i}}_{\mathrm{DL}} = G^{\mathrm{i}}_{\mathrm{Tx}} L^{\mathrm{i}}_{\mathrm{p}} L^{\mathrm{i}}_{\mathrm{FS}} L^{\mathrm{i}}_{\mathrm{atm}} L^{\mathrm{i}}_{\mathrm{BS}} G^{\mathrm{i}}_{\mathrm{Rx}} \,, \tag{12}$$

where the individual factors represent transmitter gain, pointing loss, free-space loss, atmospheric loss (absorption and scattering), beam spreading loss (due to atmospheric turbulence), and receiver gain, respectively. These factors can be calculated using well established formulas, which are listed in Appendix A, and depend on signal wavelength λ^{i}, transmitted beam waist w^{i}_0, transmitter pointing jitter $\sigma^{\mathrm{i}}_{\mathrm{p}}$, downlink path length z^{i}, receiver primary aperture diameter $D^{\mathrm{i}}_{\mathrm{Rx}}$, atmospheric transmittance at zenith $\eta^{\mathrm{i}}_{\mathrm{zen}}$, and satellite altitude angle α^{i}, as seen from the ground station i.

The model for fiber coupling $\eta^{\mathrm{i}}_{\mathrm{FC}}$ is fundamentally different for a single-mode (SM) or a multi-mode (MM) fibre. In literature, the Strehl ratio has been suggested as an estimator for SM fibre coupling efficiency.[10] In the presence of atmospheric turbulence, the Strehl ratio can be approximated as[11]

$$SR \approx \left[1 + \gamma (D_{\mathrm{Rx}}/r_0)^{5/3}\right]^{-6/5} \,, \tag{13}$$

where r_0 is the Fried parameter that characterizes atmospheric turbulence. Factor γ accounts for the level of AO correction and is given by

$$\gamma = \begin{cases} 1 & \text{for no correction,} \\ 0.28 & \text{for tip-tilt correction,} \\ 0 & \text{for full AO correction.} \end{cases} \tag{14}$$

Note, that only perfect correction is considered here, meaning that the tip-tilt correction completely removes the tip and the tilt contribution to the wavefront error, while full AO correction removes all the aberrations, resulting in a diffraction limited spot.

But even a perfectly corrected wavefront, having a flat phase, would not result in 100% coupling efficiency due to the unavoidable mismatch of the amplitude profiles. The mode of the SM fibre can be well approximated with a Gaussian function.[12] Since the aperture plane and the focal plane are related via a Fourier transform, perfect coupling could only be achieved with a matching Gaussian beam in the aperture of the coupling optics. The long-term average of the incoming light, however, is expected to have a flat-top amplitude profile, allowing at most 81% average coupling efficiency.[13] In the case of MM coupling, we calculate the corresponding efficiency by integrating the focal plane intensity profile, as expected in the presence of atmospheric turbulence, over the area of the MM core (for derivation, see Appendix B). Assuming the coupling optics is chosen for the optimal coupling efficiency, we then estimate the coupling efficiency as

$$\eta_{\mathrm{FC}}^{\mathrm{i}} = \begin{cases} 0.81\left[1+\gamma(D_{\mathrm{Rx}}/r_0)^{5/3}\right]^{-6/5} & \text{for SM fibre,} \\ 1-\exp\left[-\frac{d_{\mathrm{MM}}^2}{8\sigma_{\mathrm{PSF}}^2}\right] & \text{for MM fibre,} \end{cases} \tag{15}$$

where

$$\sigma_{\mathrm{PSF}}^2 = \frac{\lambda^2\left[1+\gamma(D_{\mathrm{Rx}}/r_0)^{5/3}\right]}{2\pi^2\mathrm{NA}_{\mathrm{MM}}^2}, \tag{16}$$

and the multi-mode fibre is characterized by its fibre core diameter d_{MM} and numerical aperture $\mathrm{NA}_{\mathrm{MM}}$.

Finally, $\eta_{\mathrm{det}}^{\mathrm{i}}$ is the detection efficiency of the detectors. Note, that some of the parameters above are very likely to be the same for Alice and for Bob channel, but for the sake of generality we made no such assumptions so far.

2.3 Fibre Coupling of Background Noise

We model the background noise as an incoherent Lambertian source with radiance B. The amount of noise power that eventually couples into a MM fibre is given by[14]

$$P_{\mathrm{noise}} = M\frac{B\lambda^2}{2}, \tag{17}$$

with

$$M = \frac{1}{2}\left(\frac{\pi d_{\mathrm{MM}}\mathrm{NA}_{\mathrm{MM}}}{\lambda}\right)^2, \tag{18}$$

where M represents the number of guided modes. According to Ref. 14, Eq. (17) can be used even in the case of a SM fibre, where we simply take $M = 2$ (one fundamental mode for each of the two orthogonal polarizations).

The actual sky brightness is usually given in terms of spectral radiance B_λ, from which we calculate radiance as $B = B_\lambda\Delta\lambda$, where $\Delta\lambda$ is the bandwidth of the spectral filter employed at the receiver. With the energy of a single photon being hc/λ, we can now express the rate of detected background noise photons as

$$S_{\mathrm{back}} = \begin{cases} \eta_{\mathrm{Rx}}\eta_{\mathrm{det}}\frac{B_\lambda\Delta\lambda\lambda^3}{hc} & \text{for SM fibre,} \\ \eta_{\mathrm{Rx}}\eta_{\mathrm{det}}\frac{B_\lambda\Delta\lambda\lambda}{hc}\left(\frac{\pi d_{\mathrm{MM}}\mathrm{NA}_{\mathrm{MM}}}{2}\right)^2 & \text{for MM fibre,} \end{cases} \tag{19}$$

where h is the Planck constant and c is the speed of light in vacuum.

2.4 Signal Wavelength Considerations

When it comes to the choice of the signal wavelength for potential daylight QKD, there are several important aspects to consider. First of all, we need a source of high-fidelity entangled photons with high generation rates, and these are available only at certain wavelengths. Secondly, single-photon detectors with high detection efficiencies are required at the corresponding wavelengths. It is also crucial that that the Earth's atmosphere

has a high transmittance at these wavelengths. Based on these considerations, two wavelength ranges of interest have been established in the satellite-based QKD community: one around 800 nm and the other one at about 1550 nm.

The most obvious advantage of the roughly half smaller ∼800 nm wavelengths is considerably smaller diffraction, resulting in a much more concentrated photon flux at the OGS, improving the product $G^{\mathrm{i}}_{\mathrm{Tx}} L^{\mathrm{i}}_{\mathrm{FS}} G^{\mathrm{i}}_{\mathrm{Rx}}$ approximately by a factor of 4, see Eqs. (20), (22), and (29). In turn, however, smaller transmitted beam cone results in higher pointing loss, Eq. (21), making the overall effect on the link loss much less trivial. Furthermore, atmosphere transmittance is about 10% lower at ∼800 nm than it is at 1550 nm.[4] Beam spreading loss due to atmospheric turbulence is in the case of downlinks substantially smaller compared to other losses,[11] therefore it does not need to be considered here. Atmospheric turbulence does, however, distort the wavefront of lower wavelengths more,[11] which would have an impact on single-mode fibre coupling or spatial filtering in general, unless corrected for.

All of the above is applicable to satellite-based QKD in general, but there are further considerations that are particularly relevant for daylight QKD. Spectral radiance of the daytime sky is generally about an order of magnitude higher at ∼800 nm than at 1550 nm.[9] By mimicking the actual tracking of a satellite across the sky with their telescope, Liao *et al.*[3] measured the single photon counts at 1550 nm to be a factor of 22.5 larger than at 850 nm. Based solely on the argument of smaller noise, plus the argument of better compatibility with established fibre-optical communication infrastructure, they chose 1550 nm for their groundbreaking terrestrial daylight QKD experiments. Gruneisen *et al.*,[4] on the other hand, took several more aspects including wavelength-dependent link loss into consideration. They conclude that at 780 nm signal-to-noise ratio would be about 1.8 higher and overall signal level about 3.6 times larger than at 1550 nm, finally choosing 780 nm for their terrestrial daylight QKD experiments.

Although we can narrow down the choice of wavelength to only two ranges, we can see that the final choice between the two is far from trivial. In the near-term, the community will therefore very likely to keep investigating and developing the relevant technologies in both domains.

2.5 Detection Technology

Another crucial consideration that can have an enormous impact on the achievable secure key rates is the choice of single-photon detection technology. Performance of single-photon detectors is typically characterized by their detection efficiency, dark count rate, and detection time jitter. Dark count rates, although critical for some other applications, are usually negligible compared to orders of magnitude higher background noise rates from the day-lit sky. Detection efficiency directly influences the rate of detected coincidences C_{det} in Eq. (9), therefore it is trivial to recognize its importance in achieving high secure key rates. The importance of low time jitters, however, is even more important but much less trivial to see. The entangled pair sources most commonly used for QKD are based on spontaneous parametric down-conversion (SPDC), which convert pump photons into pairs of entangled photons. To achieve a higher pair generation rate G, one may therefore simply increase the pump power. But even though higher G generally increase detected coincidences C_{det} and in turn secure key rate K, as can be seen from Eq. (9), there exists an optimal pair generation rate, which is dictated by the detector time jitter.

In practice, accidental coincidences can often be approximated by $C_{\mathrm{acc}} \approx S^{\mathrm{A}}_{\mathrm{det}} S^{\mathrm{B}}_{\mathrm{det}} \tau$,[7] meaning that they scale quadratically with the pair generation rate G. True coincidences, which primarily contribute to the generation of the secure key, scale only linearly with G, as seen in Eq. (1). For this reason, increasing G would lead to higher QBER, eventually reaching the threshold value of about 10%, which is imposed by H_2 in Eq. (9), at which generation of positive secure key rate becomes impossible. What can also be appreciated from the approximation above is that we may decrease the rate of accidental coincidence by decreasing the coincidence window τ. This would allow for higher G before reaching the error threshold. Shorter τ also leads to better temporal filtering of the background noise, as discussed above, and is therefore particularly desired for daylight QKD. Through Eq. (6), however, time jitters of the detectors impose a lower bound on the choice of τ, since reducing τ below time jitter substantially reduces the coincidence detection efficiency. In conclusion, lower detector jitter allows for a shorter coincidence window, which in turn allows for a higher pair generation rate and reduces the background noise rate, finally leading to a higher secure key rate.

Here we focus on the two most popular yet fundamentally different families of devices: single-photon avalanche detectors (SPADs) and superconducting nanowire single-photon detectos (SNSPDs). Table 1 shows parameters for typical commercially available SPADs and SNSPDs for ∼800 nm and 1550 nm, taken from the manufacturer data sheets. The efficiency of Si-based SPADs for ∼800 nm has tremendously improved over the past years and is now almost reaching similar levels as SNSPDs. InGaS-based SPADs for 1550 nm, on the other hand, still suffer from very low detection efficiencies and high dark count rates. An order of magnitude lower timing jitter of SNSPDs is, however, expected to allow for considerably higher key rates even at ∼800 nm, based on the arguments given above. While SNSPD is without a doubt a far superior technology in terms of performance, it is considerably more bulky and an order of magnitude more expensive, therefore making the more accessible SPAD technology still an option worth considering.

Table 1. Typical parameters for commercially available single-photon detectors.

	SPAD @ 800 nm	SPAD @ 1550 nm	SNSPD @ 800 nm	SNSPD @ 1550 nm
Model	IDQ ID120	IDQ ID Qube NIR	Single Quantum Eos	Single Quantum Eos
Efficiency	80%	25%	90%	85%
Dark count rate	300 s^{-1}	6000 s^{-1}	1 s^{-1}	10 s^{-1}
Timing jitter	400 ps	150 ps	15 ps	25 ps

3. CHOICE OF SIMULATION SCENARIOS AND PARAMETERS

In this section, we discuss the choice of the link geometry for our simulations and provide justifications for individual parameters.

3.1 Satellite Orbit and Ground Station Selection

For all the simulations presented here, we chose the orbit of the Chinese Quantum Science Satellite – also known as Micius – which is a Sun-synchronous low Earth orbit. Micius was the first satellite to have ever demonstrated dual-downlink QKD with entangled photons.[15] The orbit parameters were retrieved from CelesTrak online database[†] in the form of a two-line element (TLE) set, shown in Tab. 2. For explanation of the TLE data format, please refer to CelesTrak documentation. We also chose transmitter aperture diameter of $D_{\mathrm{Tx}} = 180$ mm (we assume $w_0 = D_{\mathrm{Tx}}/3$) and pointing jitter of $\sigma_{\mathrm{p}} = 1$ µrad according to Micius.[16] For transmitter efficiency, we take the value of 75%, which roughly corresponds to 6 silver mirror surfaces.

Table 2. Two-line element set of Micius used for simulations.

Line 1	`1 41731U 16051A 22221.10474242 .00001628 00000+0 63650-4 0 9992`
Line 2	`2 41731 97.3322 131.2551 0014121 117.8778 353.5535 15.27206413332907`

As the two ground station sites, we choose the European cities of Berlin and Munich, and their coordinates are shown in Tab. 3. The minimal surface distance (great-circle distance) between the two cities is about 500 km and an optical fibre connecting them would be even longer. QKD over such distances is infeasible due to exponential loss along optical fibres,[2] therefore the only alternative is a satellite link, making these two sites a suitable choice for our feasibility study. We assume both sites are equipped with a $D_{\mathrm{Rx}} = 800$ mm telescope, having a central obstruction diameter of 328 mm (e.g. commercially available ASA AZ800). As the optical efficiency of the rest of the receiver system, we take the value of 60%.

QKD can only be performed when the satellite can be seen from both ground sites simultaneously, i.e. its altitude angle at both sites needs to be positive. We further limit ourselves to satellite altitude angles that are

[†] https://celestrak.org/NORAD/elements/

Table 3. Coordinates of the two ground sites used for simulations.

	Latitude	Longitude	Elevation
Berlin	52.5200° N	13.4050° E	34 m
Munich	48.1375° N	11.5750° E	520 m

larger than 30°, since for smaller altitude angles the atmospheric models employed here are not valid anymore.[9] Based on these considerations, we define a satellite pass as the time when the satellite altitude angle is above 30° at both ground sites simultaneously.

We chose all such passes in the year 2022 as our sample of possible satellite-Alice-Bob geometry dynamics for subsequent key calculations. Note, that about half of these passes actually happen around midnight and the other half around noon (ground station time), which is due to the fact that Micius is in a Sun-synchronous orbit. Nevertheless, the distribution of geometry dynamics is essentially the same for day and night passes. Although we are interested in investigating daylight QKD here, we use all these passes for the QKD simulations to have a larger and a more representative sample of link geometry dynamics.

Fig. 2 shows the distribution of this sample by the pass duration. In the year 2022, there is a total of 571 passes of Micius over Berlin and Munich simultaneously, with 271 happening during the day. The longest pass lasts 141 s and the mean pass duration is 102 s. Note, that these times would increase, should we allow lower satellite altitude angles. In Fig. 3, we show the link geometry dynamics for an example pass of which the duration roughly matches the median pass duration of 113 s.

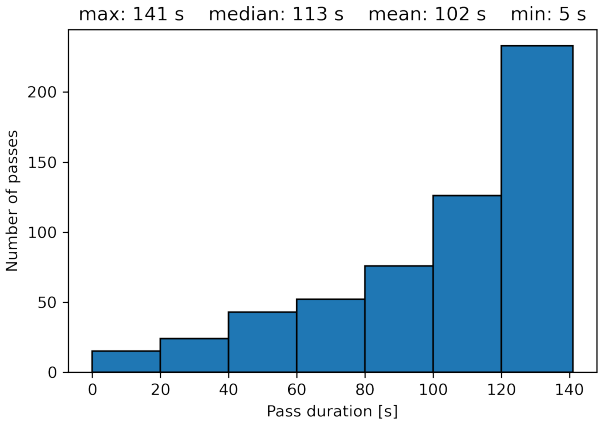


Figure 2. Distribution of simultaneous passes of Micius over Berlin and Munich in 2022 by their duration.

3.2 Source and Detection Parameters

As discussed in Sec. 2.4, the choice between ∼800 nm and 1550 nm as the signal wavelength is far from trivial and there remains a high interest in both within the community. Similarly, both SPAD and SNSPD detector technologies are worth considering for the reasons given in Sec. 2.5. We therefore perform simulations for all the four combinations of these wavelengths and detector technologies, using parameters from Tab. 1. As the coincidence window, we chose $\tau = 5\sigma_{\text{det}}$, which corresponds to $\eta_{\text{coin}} \approx 92\%$, according to Eq. (6).

While the optimal source pair generation rate heavily depends on the detector parameters, we do not expect it to change considerably during a pass and between different passes. Moreover, optimizing it on the fly would be extremely difficult in practice. For this reason, we optimize the pair generation rate for a single satellite position for each of the four wavelength-detector combinations. The background noise was set to zero for the

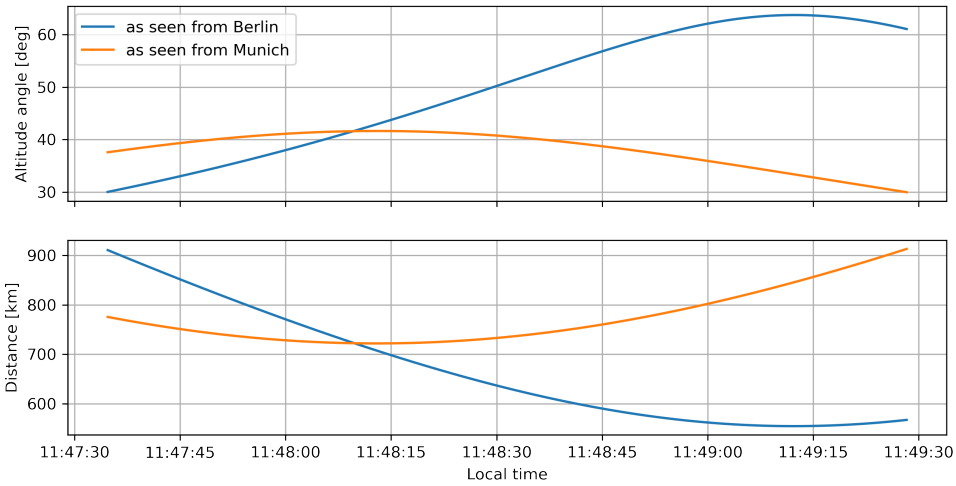


Figure 3. Typical dynamics of link geometry parameters for a Micius pass over Berlin and Munich (14/07/2022).

optimization. The resulting pair generation rates are shown in Tab. 4 and were used for all the simulations with the corresponding wavelength-detector combination.

Table 4. Entangled pair source parameters used for simulations.

	SPADs & 800 nm	SNSPDs & 800 nm	SPADs & 1550 nm	SNSPDs & 1550 nm
Pair generation rate	42.4 Mpairs/s	1.14 Gpairs/s	67.2 Mpairs/s	0.681 Gpairs/s
Efficiency	80%	80%	47.8%	47.8%

An example ∼800 nm source from Ref. 17 can generate 6.25 Mpairs/s/mW with $\eta_{\mathrm{EPS}} = 80\%$. Note, that these values are calculated from the reported measured values, by taking into account the reported detector efficiency. To achieve the desired optimal pair generation rates, we would therefore need to pump such a source with less than 7 mW, if SPAD detectors are used, or with about 182 mW, if SNSPD detectors are used. At 1550 nm, an example source from Ref. 18 can generate 18.9 Mpairs/s/mW with $\eta_{\mathrm{EPS}} = 47.8\%$. We would therefore need to pump it with less than 4 mW in the case of SPADs or with about 36 mW in the case of SNSPDs. Pumping the source on board of a satellite with such powers should be feasible in practice.

For the spectral filter bandwidth, we took 3 nm, as this should be broad enough to work with the bandwidth of the example sources in Refs. 17 and 18, and such filters are readily available on the market. We set the baseline error rate to $e_0 = 0.02$, which is in line with the above mentioned sources and allows for some polarization basis alignment error.

3.3 Sky Brightness and Atmosphere Parameters

Sky spectral radiance B_λ depends on the relative geometry of the Sun, satellite and the corresponding ground station location. In general, it therefore differs for Alice and Bob, and varies as the the receiver tracks the satellite across the sky. Gruneisen *et al.*[19] simulated B_λ for two typical LEO satellite passes. In the first case, B_λ varied between 15 and 23 $\mathrm{Wm^{-2}sr^{-1}\mu m^{-1}}$ throughout the pass, while in the second case, it varied roughly between 3 and 16 $\mathrm{Wm^{-2}sr^{-1}\mu m^{-1}}$. While including a dynamical simulation of B_λ in the present model would certainly be interesting, it is beyond the scope of this work. In our simulations, we kept a fixed B_λ for the entire path, and the values for Alice and Bob were the same.

We performed simulations for 4 different sky brightness scenarios. The first scenario, in which we set the background noise to zero, served as a benchmark. Then we defined three daylight scenarios: dark day, bright day, very bright day. Under cloud-free conditions, sky spectral radiance from less than 1 to more than 100 $\mathrm{Wm^{-2}sr^{-1}\mu m^{-1}}$ can be expected during daytime.[19] A MODTRAN simulation with the Sun being at $\alpha = 45°$ and the observer being at sea level and looking towards $\alpha = 50°$ estimates sky spectral radiance to be in the order of 100 $\mathrm{Wm^{-2}sr^{-1}\mu m^{-1}}$ at ∼800 nm and an order of magnitude smaller at 1550 nm.[9] Based on these arguments, we define the sky spectral brightness for the three daylight scenarios as shown in Tab. 5.

For atmospheric transmittance at zenith η_{zen}, we used the MODTRAN online tool[‡], arriving at values of 0.78 for 800 nm and 0.91 for 1550 nm. For calculating Fried parameters at each satellite position, the standard H-$V_5/7$[11] model was used.

Table 5. Sky spectral radiance used for simulations.

Sky spectral radiance [$\mathrm{Wm^{-2}sr^{-1}\mu m^{-1}}$]	dark day	bright day	very bright day
@ 800 nm	1	10	100
@ 1550 nm	0.1	1	10

3.4 Fibre Coupling and the Level of Wavefront Correction

It has often been argued in the community that full AO, together with some form of strong spatial filtering such as single-mode-fibre coupling, is the only way to go for daylight QKD. Full AO, however, incurs high additional costs and complexity to the receiver system. For this reason, we investigated whether a much simpler and affordable tip-tilt-only correction would, at least in principle, lead to acceptable amounts of secure key per satellite pass. Moreover, since tip-tilt correction usually suffices for efficient multi-mode fibre coupling, we investigated also coupling a MM fibre. We assumed a typical MM fibre, with its core and numerical aperture of 50 µm and 0.22, respectively. With the present model and for the parameters above, we observed no considerable improvement of MM fibre coupling efficiency by adding higher mode AO correction to the basic tip-tilt correction. And if full AO correction is available, going for MM fibre coupling does not seem to make much sense. For these reasons, we excluded simulations of MM fibre coupling with full AO.

4. RESULTS

Using the model described in Sec. 2 and parameters defined in Sec. 3, we first observed the QKD performance for a typical pass. The results for 800 nm signal, SPAD detectors, SM fibre coupling, and full AO correction are shown in Fig. 4. Note, that the link geometry corresponds to the one shown previously in Fig. 3). We can see that even if there was no noise, the expected secure key rates would be within the 10-100 bps range throughout the pass. This clearly shows the impact of enormous channel losses. Adding noise corresponding to a dark day scenario, the performance reduces only slightly, but on a bright day, the key rates would reduce roughly by half. On a very bright day, the QBER is beyond the permissible threshold, thus no key can be generated throughout the pass. By integrating the secure key rate over the pass, we arrive at the total secret key per pass. For the pass in Fig. 4, this results in 9.5 kb, 9.1 kb, 4.9 kb, and 0 kb for no noise, dark day, bright day, and very bright day scenario, respectively.

We then calculated the total key per pass in a similar way for all the passes in the sample and for various combinations of parameters. We observed how often a total key size of a certain order of magnitude can be generated. Results for 800 nm signal and SPAD detectors are shown in Fig. 5. We can clearly see that with MM fibre coupling, no key can be generated during daytime. SM fibre coupling is therefore necessary. As for correction level, tip-tilt correction would suffice only for dark days. Full AO is obviously required to generate key on bright days, and the key per pass would mostly be in the range between 1 kb and 100 kb. QKD on a very bright day is not possible with this wavelength-detector combination.

[‡] http://modtran.spectral.com/modtran_home

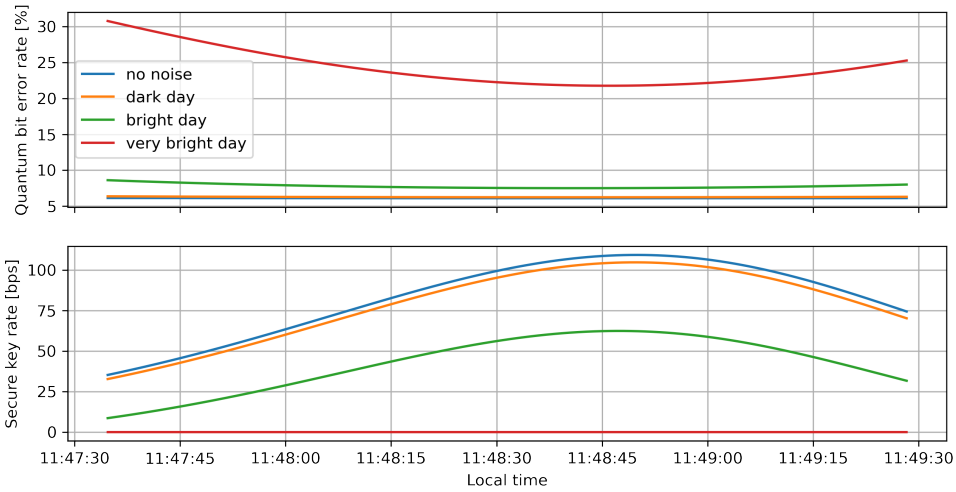


Figure 4. Quantum key distribution performance for a typical Micius pass over Berlin and Munich under different levels of sky brightness. Signal wavelength of 800 nm, SPAD detection technology, SM fibre coupling, and full AO correction is assumed.

Figure 5. Distribution of key per pass for 800 nm signal and SPAD detectors.

Next, we show how the situation changes, if SNSPDs are used instead of SPADs, see Fig. 6. While MM coupling remains infeasible for anything but nights and dark days, SM fibre coupling with tip-tilt correction would produce more than 1 kb of key per pass in about 80% of bright days and about 40% of very bright days. Further adding full AO to the system, even keys as high as 100 kb - 1 Mb may be expected. This demonstrates a clear advantage of SNSPD technology for daylight QKD.

We also investigated the combination of 1550 nm signal and SPADs. It turned out that this is by far the least feasible choice. Even without noise and full AO, we could barely simulate any key, and even then it was mostly below 10 b per pass. The situation greatly improves by introducing SNSPDs, as can be seen in Fig. 7. Again, MM fibre coupling doesn't seem to be a reasonable option. SM coupling with tip-tilt correction, on the other hand, would work for bright days, with keys mostly in the range of 1-10 kb. For very bright days, however, full AO is again required for daylight QKD on very bright days and would result in keys mostly in the 100 kb - 1 Mb range.

Figure 6. Distribution of key per pass for 800 nm signal and SNSPD detectors.

Figure 7. Distribution of key per pass for 1550 nm signal and SNSPD detectors.

5. CONCLUSION

We presented a complete approach for simulating daylight QKD in a dual-downlink configuration. It is based on the BBM92 protocol and incorporates well established models for link geometry, channel loss, and secure key calculations. In addition, we derived models for fibre coupling of signal and noise, both for the case of single- as well as multi-mode fibres. While based on several approximations and assumptions that should be carefully considered for more extensive and in-depth studies, the overall approach should nevertheless be suitable for a quick investigation of bounds and basic system requirements, and provide a solid initial guess for achievable secure keys under various conditions.

We demonstrated the use of the developed approach in a hypothetical but realistic scenario of daylight QKD between Berlin and Munich with a LEO satellite. Based on our results, we may conclude that multi-mode fibre coupling is not a feasible choice for daylight QKD, at least not with 50 micron or larger fibres. Furthermore, the results clearly show that the SNSPD detection technology will play a key role in achieving practical amounts of secure keys in daytime. The advantage of SNSPDs over SPADs seems even more substantial than the advantage of full AO over tip-tilt-only correction. While the combination of SNSPD and 800 nm might allow for reasonable amounts of secure keys with tip-tilt-only correction even for the brightest of days, both SNSPD and full AO seem to be required in other wavelength-detector combinations. With regards to the wavelength choice, our results also demonstrate a notable advantage of the 800 nm wavelength with the state-of-the-art technology. With SPADs, daylight QKD is not even possible at 1550 nm, and with SNSPDs, 800 nm promises substantially higher amounts of key. The higher downlink throughput and better spatial filtering due to a smaller SM fibre therefore seem to outweigh the order of magnitude larger spectral brightness.

There are several possible further improvements and extensions of the present approach on the horizon. A

better single-mode coupling model, such as the experimentally verified model in Ref. 20, would provide more reliable estimates for fibre coupling efficiency and in turn for overall QKD performance. Furthermore, since relatively small blocks of key can be expected per pass, as we have shown, it would make sense to include finite key effects.[21] Implementing dynamic modelling of the sky spectral radiance throughout the satellite pass would further improve the reliability of results, and more advanced atmosphere models would make the overall approach applicable also to lower satellite altitude angles. Finally, adding a more sophisticated AO model that would allow for a realistic partial correction might be necessary for more elaborate studies.

APPENDIX A. DOWNLINK EFFICIENCY

The downlink efficiency, which characterizes the loss that the light experiences from the moment it leaves the satellite until right after it enters the receiver, can be calculated using Eq. (12) and the following relations:[9,11]

$$G_{\mathrm{Tx}}^{\mathrm{i}} = 8\left(\frac{\pi w_0^{\mathrm{i}}}{\lambda^{\mathrm{i}}}\right)^2, \tag{20}$$

$$L_{\mathrm{p}}^{\mathrm{i}} = \frac{1}{\left(\frac{2\pi w_0^{\mathrm{i}}\sigma_{\mathrm{p}}^{\mathrm{i}}}{\lambda^{\mathrm{i}}}\right)^2 + 1}, \tag{21}$$

$$L_{\mathrm{FS}}^{\mathrm{i}} = \left(\frac{\lambda^{\mathrm{i}}}{4\pi z^{\mathrm{i}}}\right)^2, \tag{22}$$

$$L_{\mathrm{atm}}^{\mathrm{i}} = 10^{\log\left(\eta_{\mathrm{zen}}^{\mathrm{i}}\right)\csc\left(\alpha^{\mathrm{i}}\right)}, \tag{23}$$

$$L_{\mathrm{BS}}^{\mathrm{i}} = \frac{1}{1+T^{\mathrm{i}}}, \tag{24}$$

$$T^{\mathrm{i}} = 4.35{\Lambda^{\mathrm{i}}}^{5/6}{k^{\mathrm{i}}}^{7/6}\left(H-h_0^{\mathrm{i}}\right)^{5/6}\csc^{11/6}(\alpha^{\mathrm{i}})\int_{h_0^{\mathrm{i}}}^{H} C_n^2(h)\left(\frac{h-h_0^{\mathrm{i}}}{H-h_0^{\mathrm{i}}}\right)^{5/3}\mathrm{d}h, \tag{25}$$

$$z_{\mathrm{R}}^{\mathrm{i}} = \frac{\pi {w_0^{\mathrm{i}}}^2}{\lambda^{\mathrm{i}}}, \tag{26}$$

$$w_{\mathrm{vac}}^{\mathrm{i}} = w_0^{\mathrm{i}}\sqrt{1+\left(\frac{z^{\mathrm{i}}}{z_{\mathrm{R}}}\right)^2}, \tag{27}$$

$$\Lambda^{\mathrm{i}} = \frac{2z^{\mathrm{i}}}{k{w_{\mathrm{vac}}^{\mathrm{i}}}^2}, \tag{28}$$

and

$$G_{\mathrm{Rx}}^{\mathrm{i}} = \left(\frac{\pi D_{\mathrm{Rx}}^{\mathrm{i}}}{\lambda^{\mathrm{i}}}\right)^2. \tag{29}$$

Here, $k^{\mathrm{i}} = 2\pi/\lambda^{\mathrm{i}}$ is the wavenumber, λ^{i} is the wavelength, w_0^{i} is the transmitted beam waist, $\sigma_{\mathrm{p}}^{\mathrm{i}}$ is the total pointing jitter, z^{i} is the downlink path length, $D_{\mathrm{Rx}}^{\mathrm{i}}$ is the receiver primary aperture diameter, $\eta_{\mathrm{zen}}^{\mathrm{i}}$ is the atmospheric transmittance at zenith, and α^{i} is the satellite altitude angle, as seen from the ground station i.

APPENDIX B. MULTI-MODE FIBRE COUPLING EFFICIENCY

Receiver focal plane intensity distribution in the presence of atmospheric turbulence in the link can be approximated with a Gaussian function of the form[11]

$$I_{\mathrm{PSF}}(r) = \frac{\pi^2 D_{\mathrm{Rx}}^4}{64\lambda^2 f_c^2 \left[1+\gamma(D_{\mathrm{Rx}}/r_0)^{5/3}\right]} \exp\left[-\frac{\pi^2 D_{\mathrm{Rx}}^2 r^2}{4\lambda^2 f_c^2 \left[1+\gamma(D_{\mathrm{Rx}}/r_0)^{5/3}\right]}\right], \tag{30}$$

where f_c is the focal length of the coupling optics, r_0 is the Fried parameter that characterizes the strength of turbulence, and the AO correction factor is given by Eq. (14).

A MM fibre is characterized by numerical aperture $\mathrm{NA}_{\mathrm{MM}}$, which defines its acceptance cone, its core diameter d_{MM}. For efficient coupling, numerical aperture of the coupling optics $\mathrm{NA}_{\mathrm{opt}}$ should not exceed the angle of the MM acceptance cone, which is given by $\mathrm{NA}_{\mathrm{MM}}$. For the sake of simplicity, we remove the explicit dependence of $I_{\mathrm{PSF}}(r)$ on f_c by assuming an optical system where both numerical apertures are matched, therefore

$$\mathrm{NA}_{\mathrm{MM}} = \mathrm{NA}_{\mathrm{opt}} \approx \frac{D_{\mathrm{Rx}}}{2f_c}, \tag{31}$$

Integrating $I_{\mathrm{PSF}}(r)$ over the MM core area yields the coupled intensity

$$I_c = \int_0^{2\pi} \mathrm{d}\varphi \int_0^{\frac{d_{\mathrm{MM}}}{2}} I_{\mathrm{PSF}}(r) r \,\mathrm{d}r = I_0 \left(1 - \exp\left[-\frac{d_{\mathrm{MM}}^2}{8\sigma_{\mathrm{PSF}}^2}\right]\right), \tag{32}$$

where I_0 is the intensity of light before coupling and σ_{PSF}^2 is given by Eq. (16). Finally, we arrive at the MM coupling efficiency

$$\eta_{\mathrm{MM}} = \frac{I_c}{I_0} = 1 - \exp\left[-\frac{d_{\mathrm{MM}}^2}{8\sigma_{\mathrm{PSF}}^2}\right]. \tag{33}$$

ACKNOWLEDGMENTS

The authors thank Sakshi Sharma and Uday Chandrashekara for helpful discussions about entanglement photon sources. This work is funded by the Federal Ministry for Economic Affairs and Climate Action (BMWK, Funding Reference Number 50YH2205B). A.K. is part of the Max Planck School of Photonics supported by the German Federal Ministry of Education and Research (BMBF), the Max Planck Society, and the Fraunhofer Society. A.K. is co-sponsored by the European Space Agency (ESA) through the Networking Partnering Initiative (NPI) Contract No. 4000125842/18/NL/MH/mg (Project DIFFRACT).

REFERENCES

[1] Krenn, M., Malik, M., Scheidl, T., Ursin, R., and Zeilinger, A., "Quantum communication with photons," in [*Optics in Our Time*], Al-Amri, M. D., El-Gomati, M., and Zubairy, M. S., eds., **84**, 455–482, Springer International Publishing, Cham (2016).

[2] Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M.-J., Nolan, D., Martin, A., and Zbinden, H., "Secure quantum key distribution over 421 km of optical fiber," *Physical review letters* **121**(19), 190502 (2018).

[3] Liao, S.-K., Yong, H.-L., Liu, C., Shentu, G.-L., Li, D.-D., Lin, J., Dai, H., Zhao, S.-Q., Li, B., Guan, J.-Y., Chen, W., Gong, Y.-H., Li, Y., Lin, Z.-H., Pan, G.-S., Pelc, J. S., Fejer, M. M., Zhang, W.-Z., Liu, W.-Y., Yin, J., Ren, J.-G., Wang, X.-B., Zhang, Q., Peng, C.-Z., and Pan, J.-W., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics* **11**(8), 509–513 (2017).

[4] Gruneisen, M. T., Eickhoff, M. L., Newey, S. C., Stoltenberg, K. E., Morris, J. F., Bareian, M., Harris, M. A., Oesch, D. W., Oliker, M. D., Flanagan, M. B., Kay, B. T., Schiller, J. D., and Lanning, R. N., "Adaptive-optics-enabled quantum communication: A technique for daytime space-to-earth links," *Physical Review Applied* **16**(1), 126111 (2021).

[5] Kržič, A., Sharma, S., Spiess, C., Chandrashekara, U., Töpfer, S., Sauer, G., Campo, L. J. G.-M. d., Kopf, T., Petscharnig, S., Grafenauer, T., Lieger, R., Ömer, B., Pacher, C., Berlich, R., Peschel, T., Damm, C., Risse, S., Goy, M., Rieländer, D., Tünnermann, A., and Steinlechner, F., "Metropolitan free-space quantum networks."

[6] Bennett, Brassard, and Mermin, "Quantum cryptography without bell's theorem," *Physical review letters* **68**(5), 557–559 (1992).

[7] Neumann, S. P., Scheidl, T., Selimovic, M., Pivoluska, M., Liu, B., Bohmann, M., and Ursin, R., "Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources," *Physical Review A* **104**(2), 226 (2021).

[8] Waks, E., Zeevi, A., and Yamamoto, Y., "Security of quantum key distribution with entangled photons against individual attacks," *Physical Review A* **65**(5), 3121 (2002).

[9] Hemmati, H., [*Near-Earth Laser Communications*], vol. 143 of *Optical science and engineering*, CRC Press, Boca Raton (2009).

[10] Ruilier, C., "Degraded light coupling into single-mode fibers," *SPIE Proceedings*, 319, SPIE (1998).

[11] Andrews, L. C. and Phillips, R. L., [*Laser Beam Propagation Through Random Media*], SPIE Press, Bellingham, Wash., 2nd ed. ed. (2005).

[12] Marcuse, D., "Gaussian approximation of the fundamental modes of graded-index fibers," *Journal of the Optical Society of America* **68**(1), 103 (1978).

[13] Dikmelik, Y. and Davidson, F. M., "Fiber-coupling efficiency for free-space optical communication through atmospheric turbulence," *Applied optics* **44**(23), 4946–4952 (2005).

[14] Neumann, E.-G., [*Single-mode fibers: Fundamentals*], vol. 57 of *Springer series in optical sciences*, Springer, Berlin and New York (1988).

[15] Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., Li, M., Huang, Y.-M., Deng, L., Li, L., Zhang, Q., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W., "Satellite-to-ground entanglement-based quantum key distribution," *Physical review letters* **119**(20), 200501 (2017).

[16] Zhang, L., Dai, J., Li, C., Wu, J., Jia, J., and Wang, J., "Design and in-orbit test of a high accuracy pointing method in satellite-to-ground quantum communication," *Optics express* **28**(6), 8291–8307 (2020).

[17] Steinlechner, F., Gilaberte, M., Jofre, M., Scheidl, T., Torres, J. P., Pruneri, V., and Ursin, R., "Efficient heralding of polarization-entangled photons from type-0 and type-ii spontaneous parametric downconversion in periodically poled ktiopo_4," *Journal of the Optical Society of America B* **31**(9), 2068 (2014).

[18] Meyer-Scott, E., Prasannan, N., Eigner, C., Quiring, V., Donohue, J. M., Barkhofen, S., and Silberhorn, C., "High-performance source of spectrally pure, polarization entangled photon pairs based on hybrid integrated-bulk optics," *Optics express* **26**(25), 32475–32490 (2018).

[19] Gruneisen, M. T., Flanagan, M. B., Sickmiller, B. A., Black, J. P., Stoltenberg, K. E., and Duchane, A. W., "Modeling daytime sky access for a satellite quantum key distribution downlink," *Optics express* **23**(18), 23924 (2015).

[20] Takenaka, H., Toyoshima, M., and Takayama, Y., "Experimental verification of fiber-coupling efficiency for satellite-to-ground atmospheric laser downlinks," *Optics express* **20**(14), 15301–15308 (2012).

[21] Tomamichel, M. and Leverrier, A., "A largely self-contained and complete security proof for quantum key distribution," *Quantum* **1**, 14 (2017).