

International Conference on Space Optics—ICSO 2020

Virtual Conference

30 March–2 April 2021

Edited by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas



Optical front-end for a quantum key distribution cubesat



Optical Front-End for a Quantum Key Distribution Cubesat

Paul Serra^a, Ondrej Čierny^a, William Kammerer^a, Ewan S. Douglas^b, Dae Wook Kim^{b,c}, Jaren N. Ashcraft^{b,c}, George Smith^{b,c}, Charlotte Guthery^{b,c}, Tom Vergoossen^d, Alex Lohrmann^d, Robert Bedington^d, Chithrabhanu Perumangatt^e, Alexander Ling^e, and Kerri Cahoy^a

^aDepartment of Aeronautics and Astronautics, MIT, Cambridge, MA, USA

^bDepartment of Astronomy and Steward Observatory, University of Arizona, Tucson, AZ, USA

^cWyant College of Optical Sciences, University of Arizona, Tucson, AZ, USA

^dSpeQtral Pte. Ltd., 73 Science Park Drive, Cintech 1, 118254, Singapore

^eCentre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore

ABSTRACT

Recent advances in pointing and tracking capabilities of small satellite platforms have enabled adoption of capabilities such as high-resolution Earth Observation (EO), inter-satellite laser communications and, more recently, quantum communications. Quantum communications requires unusually narrow optical beams and tight pointing performance (on the order of ten microradians) to close an inherently brightness-limited quantum link. This limit is due to quantum communication protocols such as quantum key distribution and teleportation requiring individual quantum states to be transmitted with photon number restrictions. We examine an opportunity to combine quantum communications with laser communications in sharing an optical link. We discuss a combined quantum and laser communication terminal capable of performing space-to-ground entanglement-distribution and high data rate communications on a 12U CubeSat with a 95 mm beam expander and an 60 cm aperture optical ground telescope. Photon pairs produced by the quantum terminal are entangled in polarization so the polarization must be maintained throughout the optical link. We discuss active and passive compensation methods in space and polarization reference frame correction using a polarized reference beacon at the ground station. The combined quantum and laser communication terminal approach enables secure communications over an optical channel with rates of 100 Mbps and sub-nanosecond time transfer.

Keywords: CubeSat, Quantum key distribution, Optical communication, Telescope, Link budget

1. INTRODUCTION

Small satellites now offer capabilities previously only associated with larger satellite platforms, particularly high-accuracy pointing and tracking.¹ This has enabled their use for high-resolution Earth imaging, laser communication between satellites and ground stations^{2,3} and between satellites,^{4,5} as well as for quantum communications.⁶

Quantum light sources are inherently brightness-limited because quantum communication protocols require individual quantum states to be transmitted with photon number restrictions.⁷ This translates to strict pointing and tracking requirements, with beam divergences and pointing errors on the order of ten microradians and a few microradians, respectively.

On the ground, due to high losses in optical fibers on long distances, quantum communication links are typically limited to distances on the order of 100 km. Free-space links have atmospheric absorption and line-of-sight limitations. If links are established among satellites, e.g. in Low Earth Orbit (LEO), the satellites can act

Further author information:

P.S.: E-mail: pserra@mit.edu

D.W.K.: E-mail: dkim@optics.arizona.edu

E.S.D.: E-mail: douglase@arizona.edu

T.V.: E-mail: tom@speqtral.space

A.L.: E-mail: cqtalej@nus.edu.sg

as nodes in a quantum network, exchanging single photon level signals as quantum bits, or qubits, to perform quantum communication protocols with the ground stations they pass over.

A near-term application of quantum communications is quantum key distribution, a method to establish encryption keys between two points that betrays the presence (or at least can certify the absence) of eavesdroppers in the communication channel. This is an attractive method to distribute symmetric encryption keys to enable highly secure communications. In contrast to the present-day next-best alternative, the trusted courier, the quantum key distribution method can be automated and offers stronger security guarantees. However, this is typically at the expense of low data rates, in the hundreds of bits by seconds, due to the inherent brightness limits.

Quantum communication from satellites is analogous to laser communications in that both technologies use light that is transmitted via a telescope over an optical channel and captured by a receiving telescope. This suggests it may be possible to have a combined system that offers the capability to establish encryption keys as well as securely communicate at high data rates. In addition, transmission and detection of quantum signals, such as entangled photon pairs or carefully encoded single photons, can be used for clock synchronization with security characteristics not available to a classical optical signal. In particular, the synchronization process can be shown to be unspoofable.^{8,9}

This work presents a preliminary design of an optical terminal that takes as input a quantum and synchronization signal from a quantum payload and transmits this from a nanosatellite in Low Earth Orbit to a ground station on Earth. At the same time, it will perform space-to-ground laser communication over the same channel at a rate of 100 Mbps. The synchronization signal is used to synchronize clocks between the two points to within 1 nanosecond.

2. CONCEPT OF OPERATIONS

The optical terminal is intended for use on a 12U CubeSat in Low Earth Orbit. The pointing and tracking system includes two stages: body-pointing of the satellite and fine beam-steering adjustments made within the optical terminal. Both the quantum signal and the laser communication signal make use of the same telescope and thus the same optical channel, but the pointing and tracking beacons may be transmitted separately. Prior to a pass, ground support will assess if conditions are favourable for quantum communications with the satellite. This assessment must take into account local background light and weather conditions. Typically, cloudless night-time passes with good seeing conditions are required. During a pass, the optical terminal establishes and maintains a high-gain optical channel while the quantum payload transmits both quantum and synchronization signals to the ground station.

2.1 Quantum Key Distribution Source and Protocol

During the pass, the QKD source generates entangled photon pairs, which by convention are said to each contain one signal photon and one idler photon. It transmits the signal photon to the optical terminal and locally performs a polarization measurement of the idler photon using polarizing beam splitters and single photon detecting avalanche photodiodes in geiger-mode. It randomly measures in either the horizontal-vertical, or diagonal-antidiagonal basis. The time of each detection event is time-stamped and the data is stored in compressed form. On the ground, the telescope receives the quantum signal from the satellite and routes it to a detector where the same polarization measurement is performed. The synchronization signal, also transmitted by the quantum payload, is detected and time-stamped on both ends.

On a subsequent ground station pass, the quantum payload transmits the timestamps and which of the two polarization tests were made for each timestamp (but not the result of that polarization measurement!) via the laser communications channel to the ground station. This information contains the timing signal which is used to synchronize detection events recorded on the satellite to those on the ground with an accuracy of less than 1 nanosecond (limited by detector jitter). This enables the time windows where there was a coincident detection event of signal and idler photons to be identified, this also enables identification of which of those the same polarization test was made on both the satellite and ground station. This information is sent up to the quantum payload via the telemetry and telecommand link and detection events for which the signal photon did not make

it to the ground station are discarded. The end result is a shared list of coincident signal and idler detections tested in the same basis. If quantum entanglement has been maintained then the results of the polarization tests will be correlated for signal and idler allowing the results to be used as a string of private, random, ones and zeros. This process is called 'sifting', or basis reconciliation, and the string is called the 'raw key'.

Because of the losses in the space-to-ground channel there are fewer detection events on the ground (by a factor equal to the link loss) so it would naively seem most economical to upload detection events to the satellite and perform the processing steps for sifting there, instead. However, this process is computationally intensive and best performed where computational resources are not limited. Furthermore, the necessity of the optical channel for transmission of the quantum channel provides an opportunity to download the data via laser communication. This also enables simultaneous transmission of the quantum signal and data transmission for basis reconciliation, another advantage of this configuration.

After the sifting step, additional communication rounds over the telemetry link are required to compare samples of the raw key to perform error correction and verify the entanglement. Privacy amplification processing is then performed to ensure that only a minimal fraction of information could be determined by an eavesdropper (typically 1E-10 or smaller). Errors appear in the quantum signal due to dark counts, background light, and from imperfect entanglement quality of the quantum signal, which manifest as noise. If an eavesdropper is attempting to perform a man-in-the-middle attack then the entanglement is lost on the intercepted photons and these will create errors in processing. With no eavesdropper, the final result, after privacy amplification, is a shared string of random bits, which can be used as an encryption key with very strong security guarantees as to its privacy. If an eavesdropper is present the error correction and privacy amplification steps fail and there is no key. For an open-source QKD software stack see qcrypto.¹⁰

2.2 Optical Communication Transmitter

Since the entangled photon link relies on single-photon detection on the ground and necessitates a very high-gain spacecraft optical antenna to close successfully, it is possible to take advantage of this high-gain optical frontend and use it simultaneously for traditional laser communications. Such an approach allows not only quantum key exchange, but potentially also encrypted high-bandwidth optical downlinks using the same front end. An additional advantage of this architecture is that both the entangled photon (QKD) link and the data link can share the same internal fine-pointing system.

A simple solution to combine the two channels is by wavelength multiplexing. Adding a seed laser along the internal optical train with a different wavelength allows for easy routing of the channels both on the spacecraft and when received on ground using dichroic optics. Since the data seed laser can have significantly higher output power in comparison with the QKD source, detection on ground can be simplified by using a direct-detect chain with a single avalanche photodiode (APD). Similarly, for the beacon uplink channel that is used as feedback for pointing and tracking, a different wavelength will be used and routed onto a tracking sensor onboard the spacecraft. The uplink channel and the approach for pointing, acquisition, and tracking are further described in the *Uplink Beacon* section.

The lasercom transmitter is based on directly modulated laser diode at 915 nm. The modulator maximum data rate is 100 Mbps, using On/Off Keying (OOK) modulation. It reuses some of the electronics developed for the CLICK-BC mission.⁵ The optical communication link is further discussed in the *Data Downlink* section.

3. OPTICAL DESIGN

3.1 Optical Configuration

The optical design is targeting low complexity and the fewest number of surfaces necessary to accomplish signal routing, beacon tracking, and the highest possible transmit optical gain given the CubeSat size constraints. On the spacecraft transmit side, both the QKD and the data sources are assumed to be fiber-coupled and multiplexed using a wavelength division multiplexer (WDM). The WDM output will be collimated to fit onto a MEMS fast steering mirror (FSM), which will perform fine pointing adjustments to compensate for the residual spacecraft body pointing error. The multi-wavelength high-gain architecture favors a reflective telescope for beam expansion to avoid aberrations that come with a large refractive beam expander design. Consequently, the collimated beam

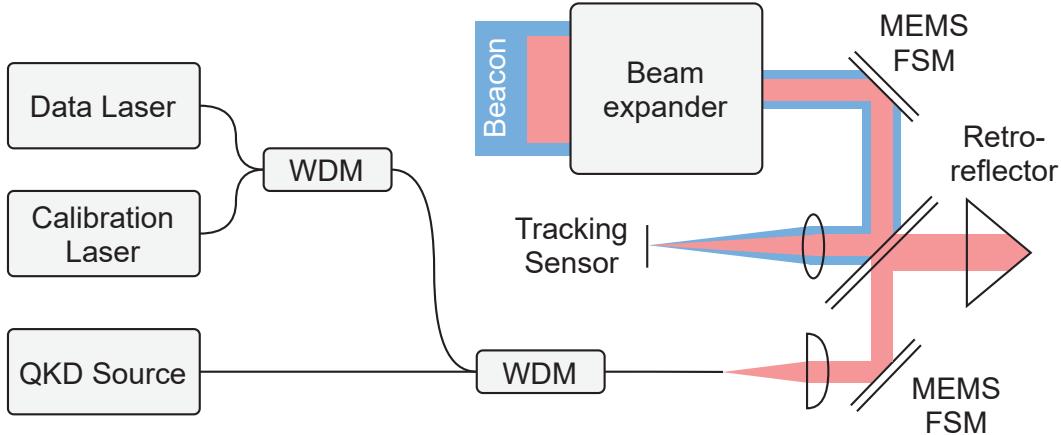


Figure 1: High-level optical layout diagram for a hybrid QKD/lasercom front end. Note the retroreflector for self calibration

corrected by the FSM will be magnified using an on-axis folded telescope to achieve the necessary optical gain. On the receive side, the same telescope will be used to collect light from the ground beacon, and route it onto a tracking sensor using a dichroic mirror.

Since the transmit beams are much narrower ($12\text{-}15 \mu\text{rad}$) than the expected maximum LEO point-ahead angle ($54 \mu\text{rad}$), the point-ahead has to be accounted for. In order to compensate for point-ahead, the FSM has to maintain an additional pointing offset between the received beacon and the transmit beams, using the instantaneous point-ahead angle between the spacecraft and the ground station. To account for potential mechanical misalignment and thermal drift, a calibration path is added by retro-reflecting a small fraction of the seed laser output onto the beacon tracking sensor. This enables tracking of the transmit beam simultaneously with the beacon, which in turn allows maintaining the point-ahead offset even if the alignment between the transmit fiber and the sensor drifts post-launch. A high-level diagram of this architecture is depicted in fig. 1.

3.2 Beam Expander Requirements

A critical element of the optical frontend is the beam expander which will provide the high optical gain necessary to close the QKD link. To meet our requirements, the expander needs to resize the transmit Gaussian beam waist from roughly 1-2 millimeters (constrained by the FSM surface area) such that the output beam at the QKD wavelength has a Gaussian full-width half maximum (FWHM) divergence of $12 \mu\text{rad}$.

Since the expanded beam might experience truncation and obstruction within the telescope, it is more convenient to convert the requirement into an optical transmit gain for analysis. For an assumed $12 \mu\text{rad}$ free-space Gaussian beam, the corresponding far-field on-axis transmit gain can be calculated as follows:¹¹

$$G_{\text{Tx}} = \frac{8}{\theta^2} = \frac{16 \ln 2}{\theta_{\text{FWHM}}^2} \approx 108.8 \text{ dB} \quad (1)$$

where θ is the $\frac{1}{e^2}$ half-width beam divergence. As discussed previously, for low aberration and high gain, a reflective beam expander is preferred. In terms of volume and ease of alignment, a traditional on-axis folded telescope is likely the best solution. Given the volume constraints of CubeSats, we set a 95 mm upper limit on the telescope primary mirror diameter, so the aperture is limited to a single CubeSat unit face, of $10 \times 10 \text{ cm}$. However, a potential problem with a traditional on-axis telescope is the central obstruction present due to the secondary mirror. For a Gaussian beam impinging on a centrally-obstructed telescope, the on-axis far-field gain can be calculated as:¹²

$$G_{\text{Tx}} = \left(\frac{2\pi R_1}{\lambda} \right)^2 \frac{2}{\alpha^2} \left[e^{-\alpha^2} - e^{-\gamma^2 \alpha^2} \right]^2 \quad (2)$$

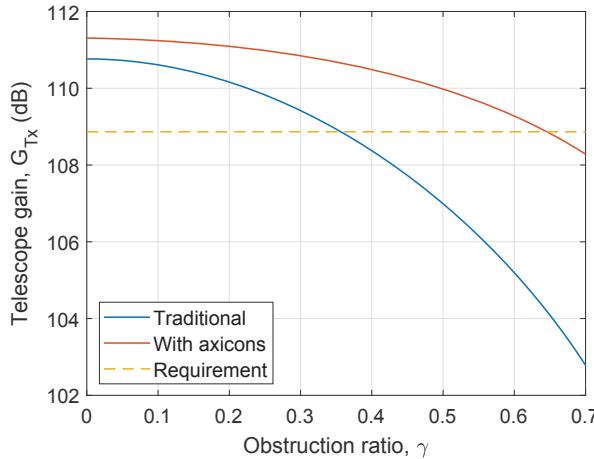


Figure 2: Theoretical maximum far-field on-axis transmit gain for a 95 mm centrally-obstructed telescope at 780 nm.

where R_1 is the radius of the primary mirror, $\alpha = \frac{R_1}{\omega}$ is the ratio of the primary mirror to the Gaussian beam waist radius, and $\gamma = \frac{R_2}{R_1}$ is the ratio of the secondary mirror radius to the primary mirror radius – the obstruction ratio. Unsurprisingly, it can be seen that an increasing obstruction ratio will degrade the gain of the telescope. Additionally, for each γ , there is an optimal α , or beam waist, that will maximize the transmit gain by minimizing the power lost due to truncation of the Gaussian beam. For high obstruction ratios, it has been shown that redistributing the power from a Gaussian to a ring or doughnut-shaped distribution can yield significant improvement in terms of transmit gain.¹³ The simplest way to accomplish such redistribution is by using optical axicons. However, using the axicons comes with additional challenges, especially in terms of alignment and precise manufacturing.

To find a suitable γ and α for our system, we analyze the maximum achievable telescope gain for a 95 mm diameter primary mirror at the QKD wavelength (780 nm) in terms of γ and compare it with our 108.8 dB requirement. The result of this analysis can be seen in fig. 2. It can be seen that a traditional design with a 95 mm primary mirror can meet the gain requirement as long as the obstruction ratio is below roughly 35%, which is not a very difficult requirement to meet. If axicons are used to optimally redistribute power, the 95 mm telescope could theoretically meet the gain requirement all the way up to a γ of about 65%. However, due to the difficulties when dealing with axicons, this approach is not preferred since the gain improvement for smaller γ becomes negligible. Consequently, a traditional approach with a Gaussian input beam and a smaller γ is preferred.

To leave margin for additional telescope implementation loss, such as obstruction loss due to spider vanes for mounting of the secondary mirror or transmitted wavefront error, a γ lower than 35% is desired. A γ of 25% leaves exactly a 1 dB margin in terms of the telescope gain, and will be considered as a baseline in the following calculations.

By maximizing eq. (2) as a function of α , the optimal Gaussian beam waist for a given γ can be found. Using a 95 mm diameter and $\gamma = 0.25$ yields $\alpha = 1.0522$, which corresponds to an expanded beam waist $\omega = 45.14$ mm. Finally, we can use ω to determine the necessary telescope magnification such that the beam fits onto the FSM with minimal truncation. The magnification calculation is summarized in Table 1 below for a few commercially available MEMS FSMs.¹⁴

3.3 Optical Modeling

As part of the preliminary optical design, a sequential Zemax optical model was developed to help guide the placement of the optics in the available volume. Given the primary mirror diameter limit (95 mm) and the determined magnification (18.3 \times for a 6.4 mm FSM with 1 mm margin) an on-axis all-reflective two-mirror telescope was modeled to fit within a roughly 150 \times 100 \times 100 mm³ (1.5U) with additional 100 \times 100 \times 100 mm³

Table 1: Calculation of the necessary beam expander magnification.

FSM diameter (mm)	4.6	5	6.4
Mirror fold angle		15°	
Projected diameter (mm)	4.44	4.83	6.18
$\omega_{\text{in,max}}$ (mm, T=99%)	1.41	1.54	1.97
Desired ω_{out} (mm)		45.14	
Magnification needed	31.9	29.4	22.9

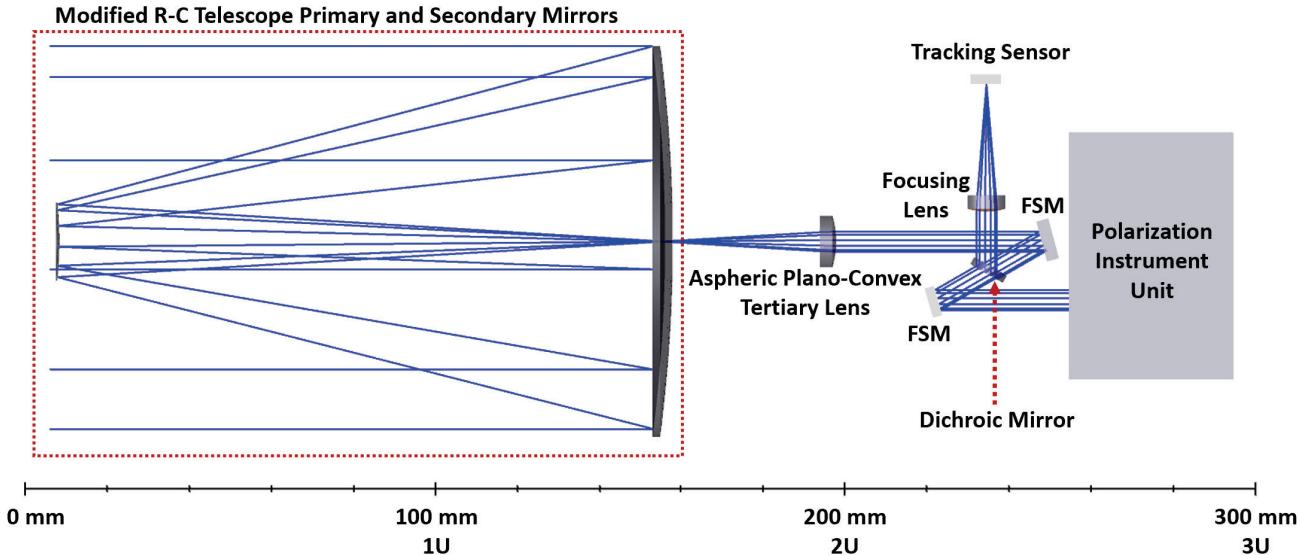


Figure 3: Side view of a ray-trace of the preliminary optical model. The whole structure fits in $300 \times 100 \times 100$ mm 3 (i.e., 3U). The telescope backend includes the FSM and fold mirrors routing the signals behind the primary mirror. Also, the dichroic mirror splits the received light onto a tracking sensor, and the transmit signal coming out of a polarization unit.

(1U) available for the frontend optics. This preliminary 2U optical design leaves plenty of space for other support hardware, such as polarization calibration unit, electronic boards, fiber components, or extensions of the optical chain planned in future iterations. The overall optical configuration and layout is shown in Fig. 3 with the on-axis ray tracing overlay.

The telescope, as shown in fig. 3, is of a modified Ritchey–Chrétien (R-C) configuration, which is a variant of the traditional Cassegrain telescope design, with a concave elliptical 95 mm primary mirror (easier to perform an interferometric null test compared to a hyperbolic mirror) and a convex hyperbolic secondary mirror, yielding a 20% obstruction ratio. The Ritchey–Chrétien design is chosen as it provides a wide Field of View (FoV) performance relaxing the satellite pointing jitter requirement significantly. The preliminary design has a superb on-axis performance of 0.99 Strehl ratio (Fig. 5 (top)), which is of most significance for the optical frontend. In the meantime, the off-axis performance (+/- 0.2 degree) also reaches 0.94 Strehl ratio (Fig. 5 (bottom)) as the R-C telescope optical design (combined with the tertiary collimating lens) controls the off-axis aberrations (e.g., coma). Commercially available CubeSat attitude control systems support precision pointing to within a few hundredths of a degree,¹⁵ and the wide FoV performance will enable a robust optical system with good safety margin and tolerances. The telescope has an intermediate focus near the location of the primary mirror, after which the aspheric tertiary lens (higher order plano-convex asphere) is placed to collimate and correct the beam, completing the afocal telescope configuration. All the ray incidence angles are minimized in order to preserve the polarization state across the pupil throughout the afocal system. Also, the on-axis design provides an axially symmetric polarization aberration, which is already minimized, so any residual effect can be more

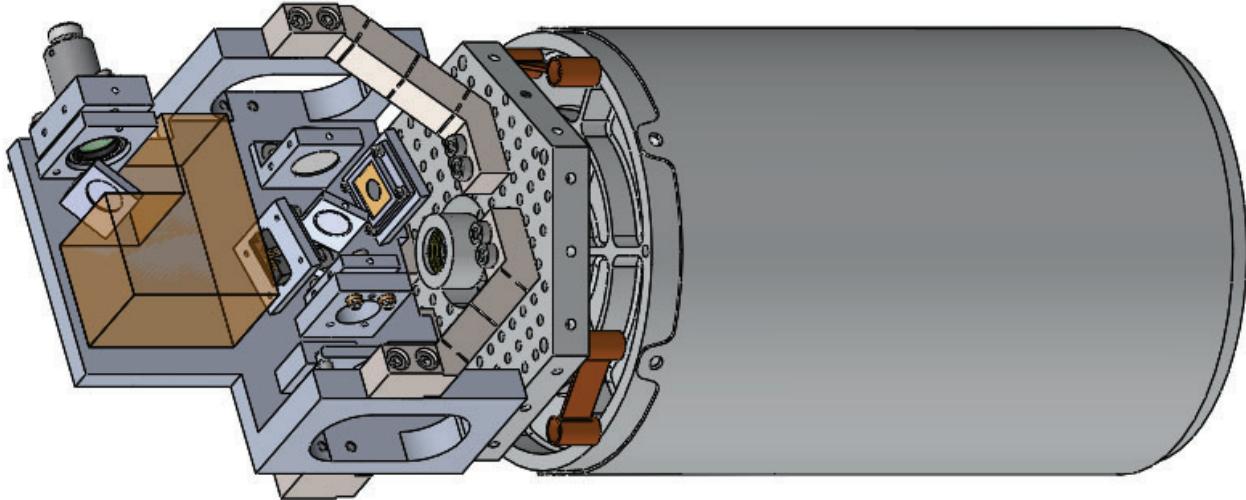


Figure 4: Computer Aided Design rendering of the telescope and the optical bench.

simply calibrated.

The 6.4 mm Mirrorcle MEMS FSM is placed at the exit pupil of the afocal telescope at a fold angle of 15° in order to maximize the projected surface area and its angular steering range. An additional FSM is placed after the polarization unit to route the signals upward behind the primary mirror so that the 0.5U volume can be utilized efficiently. Next, the dichroic mirror is placed to reflect received light onto a tracking sensor and transmit the collimated transmit beam through. The dichroic and fold mirrors are angled such that the two chains continue diagonally to the corners of the structure, maximizing the available optical path length. This allows using a focusing lens with a longer focal length for the sensor, decreasing its field of view and increasing its angular sensitivity/resolution for more precise beacon tracking using FSM. The design utilizes higher order aspheric lenses for collimation, focusing onto the sensor, as well as for the telescope tertiary. The retro-reflector, as well as any filtering optics were omitted from this preliminary design.

Using the Zemax model, the angular transfer function (effective focal length) of the tracking sensor was determined to be roughly 775 mm/rad, taking the angular telescope magnification into account. Several Huygens point-spread functions with different spot diameters were also exported for various telescope incidence angle, to be used in analysis of the tracking sensor noise sensitivity described in the following sections.

4. LINK BUDGETS

In this section, we will first describe the models assumed for the payload optical links, including the range loss as well as atmospheric effects, including both scintillation and radiative transfer. We will then discuss three links: (1) the uplink laser beacon, (2) the downlink beacon and data, and (3) the downlink entangled photon link.

4.1 Range Loss

We are considering a satellite at an altitude h . The Earth radius is noted R_E , and we assume $R_E = 6378$ km. The elevation ξ for a given angle of incidence from nadir at the payload θ_{inc} is given by the following equation:

$$\xi = \arccos \left(\frac{R_E + h}{R_E} \sin(\theta_{inc}) \right) \quad (3)$$

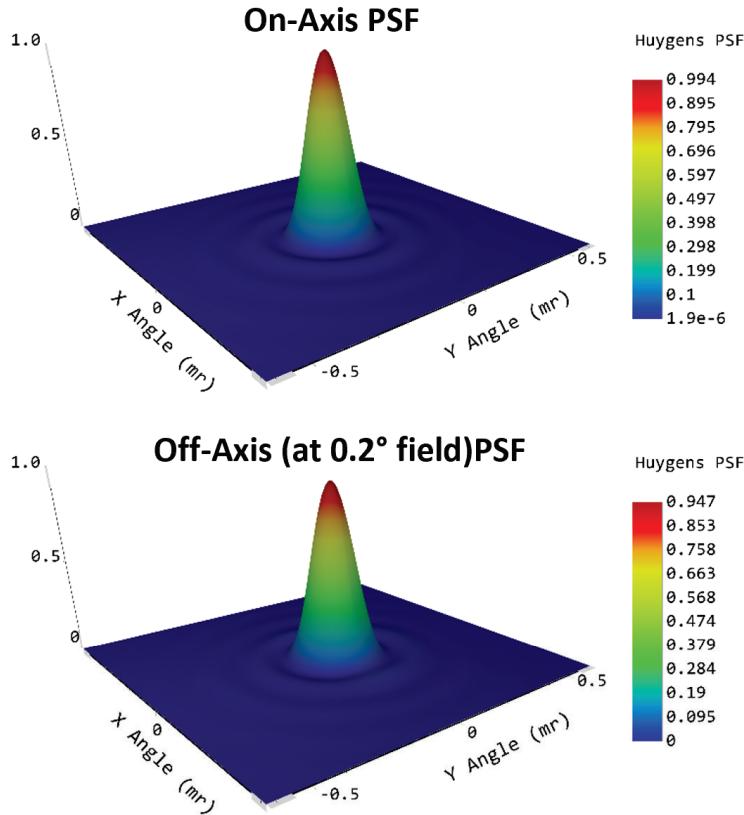


Figure 5: Huygens Point Spread Function (PSF) showing high Strehl ratio of 0.99 for on-axis (top) and 0.94 for 0.2 degree off-axis field of view (bottom).

The slant range L is then^{*}:

$$L = \sqrt{R_E^2 + (R_E + h)^2 - 2R_E(R_E + h)\sin(\theta_{inc} + \xi)} \quad (4)$$

This can be simplified to:

$$L = \sqrt{R_E^2 \sin^2(\xi) + (R_E + h)^2 - R_E^2} - R_E \sin(\xi) \quad (5)$$

Assuming a transmitter with FWHM divergence of θ_{TX} , the $1/e^2$ transmitter beam radius W_0 is

$$W_0 = \lambda \frac{\sqrt{2 \cdot \log(2)}}{\pi \cdot \theta_{TX}} \quad (6)$$

With a pointing error θ_{PT} , and assuming a Gaussian beam, the range loss G_{range} is:

$$r = L \cdot \tan(\theta_{PT}) \quad W = W_0 \cdot \sqrt{1 + \left(\frac{\lambda \cdot L}{\pi \cdot W_0^2} \right)^2} \quad G_{range} = \frac{d_{RX}^2}{2 \cdot W^2} \exp \left(\frac{-2r^2}{W^2} \right) \quad (7)$$

Scintillation

Atmospheric turbulence has an impact on the laser beams, for both uplink and downlink. Turbulence creates variations in the received power, called scintillation, and for uplink in particular, it introduces beam wander.

^{*}Law of cosines on a triangle with the spacecraft, a ground station and the Earth center.

Our link budget is based on the model of Ref. 16. First, we define the atmospheric turbulence strength, using the Hufnagel-Valley 5/7 model:¹⁶

$$C_n^2(h) = 3.6 \times 10^{-3} (10^{-5} h)^{10} \exp(-h/1000) + 2.7 \times 10^{-16} \exp(-h/1500) + 1.7 \times 10^{-14} \exp(-h/100) \quad (8)$$

For both uplink and downlink, the model includes a small scale and a large scale variance of the received irradiance noted $\sigma_{x,up}$, $\sigma_{y,up}$ and $\sigma_{x,down}$, $\sigma_{y,down}$. The calculations for the scintillation variances are detailed in appendix B and appendix C.

For each link, the resulting variances $\sigma_x^2 = 1/a$ and $\sigma_y^2 = 1/b$ can be plugged to a Gamma-Gamma distribution:¹⁶

$$f_{\Gamma-\Gamma}(I) = \frac{2(ab)^{(a+b)/2}}{\Gamma(a)\Gamma(b)I} \left(\frac{I}{I_e(r,L)} \right)^{(a+b)/2} K_{a-b} \left(2\sqrt{\frac{abI}{I_e(r,L)}} \right) \quad (9)$$

The Gamma-Gamma Cumulative Density Function (CDF) is difficult to compute. One can either integrate the Probability Density Function (PDF) of the distribution, or fit another distribution whose CDF can be directly computed. We chose to fit another using the α - μ distribution:

$$f_{\alpha\mu}(I) = \frac{\alpha\mu^\mu I^{\alpha\mu-1}}{(rI_0)^{\alpha\mu}\Gamma(\mu)} \exp\left(-\mu\left(\frac{I}{rI_0}\right)^\alpha\right) \quad (10)$$

$$P_{\alpha\mu}(I > I_t) = F_I(I_t) = 1 - \frac{\Gamma(\mu, \mu(I_t/rI_0)^\alpha)}{\Gamma(\mu)} = 1 - Q(\mu, \mu(I_t/rI_0)^\alpha) \quad (11)$$

$$I(P_{\alpha\mu} > P_t) = rI_0 \left(\frac{1}{\mu} \Gamma^{-1}(\mu, (1 - P_t)\Gamma(\mu)) \right)^{1/\alpha} = \frac{rI_0}{\mu^{1/\alpha}} (Q^{-1}(\mu, P_t))^{1/\alpha} \quad (12)$$

In eq. (11) and eq. (12), Q is the regularized upper incomplete gamma function, and Q^{-1} is its inverse such that $y = Q(\mu, x)$, $x = Q^{-1}(\mu, y)$. The two distributions are fitted by matching the expected value and two other moments.^{17,18}

$$\mathbb{E}\{X^n\} = r^n \frac{\Gamma(\mu + n/\alpha)}{\mu^{n/\alpha}\Gamma(\mu)} = \frac{\Gamma(a+n)\Gamma(b+n)}{\Gamma(a)\Gamma(b)(ab)^n} \quad \text{for } n \in \mathbb{N} \quad (13)$$

In particular, since $\Gamma(z+1) = z\Gamma(z)$,

$$\mathbb{E}\{X\} = 1 \quad r = \frac{\mu^{1/\alpha}\Gamma(\mu)}{\Gamma(\mu + 1/\alpha)} \quad \mathbb{E}\{X^n\} = \frac{1}{(ab)^{n-1}} \prod_{i=1}^{n-1} (a+i)(b+i) \quad \text{for } n \geq 2 \quad (14)$$

We can get a system of 2 equations with logarithmic scaling, which helps with the large range of values due to the Gamma function. For $n \geq 2$:

$$M_n = (n-1) \log \Gamma(\mu) + \log \Gamma\left(\mu + \frac{n}{\alpha}\right) - n \log \Gamma\left(\mu + \frac{1}{\alpha}\right) - \log\left(\frac{1}{(ab)^{n-1}} \prod_{i=1}^{n-1} (a+i)(b+i)\right) = 0 \quad (15)$$

A closed-form equation exists for the Jacobian, again with a logarithmic scale, and with ψ as the digamma function:

$$\begin{aligned} \frac{\partial M_n}{\partial \alpha} &= \frac{n}{\alpha^2} \left(\psi\left(\mu + \frac{1}{\alpha}\right) - \psi\left(\mu + \frac{n}{\alpha}\right) \right) \\ \frac{\partial M_n}{\partial \mu} &= (n-1)\psi(\mu) + \psi\left(\mu + \frac{n}{\alpha}\right) - n\psi\left(\mu + \frac{1}{\alpha}\right) \end{aligned} \quad (16)$$

The system can be solved by using an iterative least-squares algorithm. The α - μ distribution can be computed efficiently for a large array, and its inverse is also well-behaved. Thanks to the inverse distribution function, we can specify a desired fractional fade time and obtain a derated optical power satisfying this condition.

Table 2: Link Budget Parameters

Case	Beacon Uplink	Data Downlink	Key Downlink
Altitude	500 km		
Wavelength	978 nm	915 nm	760 nm to 790 nm
Transmitter divergence	500 μrad FWHM	20 μrad FWHM	12 μrad FWHM
Transmitter power	2.5 W	100 mW	25×10^6 photon/s
Transmitter optical loss	3 dB	3 dB	3 dB
Pointing error	5 μrad		
Receiver aperture	95 mm	600 mm	600 mm
Aperture obstruction (area)	5%	40%	40%
Receiver optical loss	3 dB	3 dB	1 dB
Minimum elevation	20 deg		
Turbulence	HV 5/7, 95%	$10 \times$ HV 5/7	None
Atmospheric absorption	MODTRAN Urban	MODTRAN Urban	Urban, Maritime
Detector bandwidth	200 Hz	10 MHz to 1 GHz	Single photon

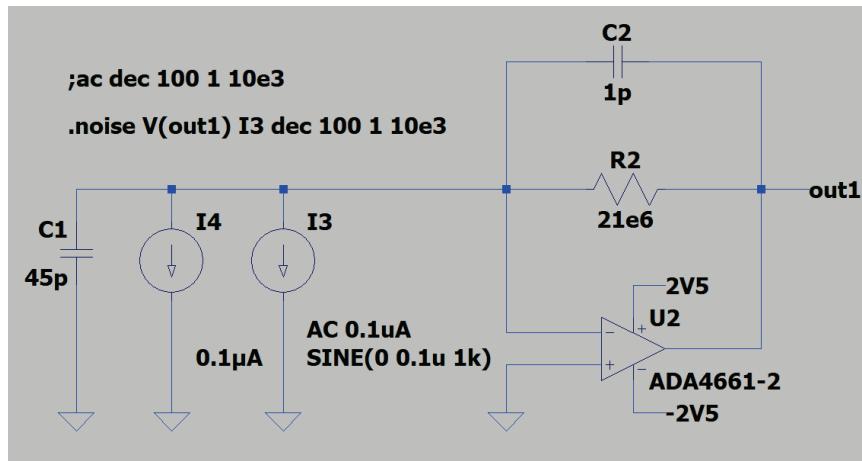


Figure 6: Circuit for the quadcell transimpedance amplifier.

Uplink Beacon

Several design options are available for the pointing detector in closed-loop tracking. The most common ones are image sensors and four quadrant detectors or “quadcells”. Image sensors have several advantages: the readout circuit is integrated and offers performances close to the shot noise floor with little integration effort. Also, the estimated spot position is a function of the pixel pitch, which is well known, contrary to quadcells where a transfer function needs to be estimated in order to find the spot position. On the other end, quadcells allow more flexible implementations, with a wider wavelength range available and the opportunity to customize filtering. This is the reason why a quadcell-based detector has been selected for this project. The payload is intended to be used with a ground station at night in an urban environment. Frequency filtering along with a modulated beacon source allow the tracking system to effectively remove background light from both the Earth and the Sun. It also enables the simultaneous tracking of the distant beacon source and of the internal position of the payload transmitter, so that continuous alignment calibration is performed.

The detector electronics for this payload are identical to the one in the CLICK-BC payload.⁵ It is composed of a silicon quadcell, four Transimpedance Amplifiers (TIAs), a frequency filtering stage and a 24 bit four-channel Analog to Digital Converter (ADC). The model for the detector and the TIA is shown in fig. 6. The digital signal processing section is similar to Ref. 5, however, two signals at two different frequencies are extracted in parallel in order to track the distant and the local source on the same detector. Contrary to the CLICK-BC payload, the transmit beam for this optical front-end is tight enough to require the introduction of a point-ahead angle between the received and the transmitted beam. If a single FSM is used for both pointing error

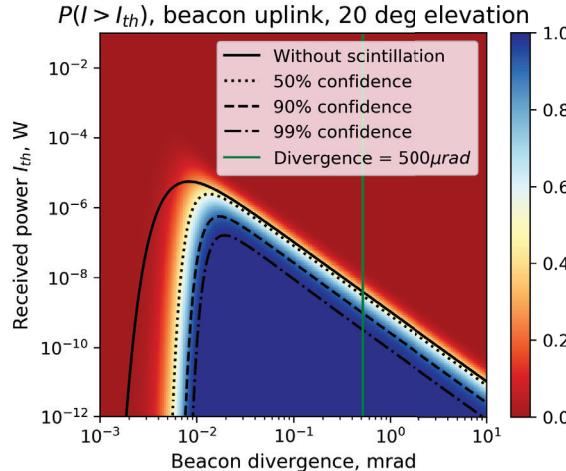


Figure 7: Received power probability distribution at the payload quadcell versus transmitter divergence. The selected divergence for the uplink beacon is shown in green. The color indicates the probability that the measured power is higher than y axis power threshold I_{th} .

correction and point-ahead, the spot on the quadcell must be defocused in order to maintain a good enough pointing estimation error, unlike CLICK-BC, where a spot as small as possible was desired. For this reason, we first modeled the spot as a generic 2D Gaussian Point Spread Function (PSF) in order to get a rough estimate of the desired pointing parameters, such as the spot size and the quadcell effective focal length (EFL).

The free-space link parameters are listed in table 2. The resulting power distribution at the quadcell is plotted in fig. 7 against beacon divergence with a constant pointing error of 5 μ rad, which is the ground station 3σ pointing requirement. A divergence of 500 μ rad is selected as it offers sufficient link margin and is consistent with the optical ground station hardware and pointing capabilities. In these conditions, the power at the quadcell is $P_0 = 668$ pW. With a spot radius of W , we assume the PSF has form:

$$\text{PSF}_G(r) = \frac{2}{\pi W^2} \exp\left(-\frac{2r^2}{W^2}\right) \quad (17)$$

The PSF integrated over a square window is then:

$$\begin{aligned} P_{G,x_1,x_2,y_1,y_2} &= P_0 \int_{x_1}^{x_2} \int_{y_1}^{y_2} \text{PSF}_G\left(\sqrt{x^2 + y^2}\right) dx dy \\ &= \frac{P_0}{4} \left(\operatorname{erf}\left(\sqrt{2} \frac{x_2}{W}\right) - \operatorname{erf}\left(\sqrt{2} \frac{x_1}{W}\right) \right) \left(\operatorname{erf}\left(\sqrt{2} \frac{y_2}{W}\right) - \operatorname{erf}\left(\sqrt{2} \frac{y_1}{W}\right) \right) \end{aligned} \quad (18)$$

The offset of the spot on the detector, noted x_{spot} and y_{spot} for its component on each axis, depends on the EFL, f_{PT} , and the pointing error, θ_{err} , with $\sqrt{x_{spot}^2 + y_{spot}^2} = f_{PT} \tan \theta_{err}$. The spot offset as well as the geometry of the quadcell detector are used to get the integration bounds x_1 , x_2 , y_1 , and y_2 relative to the spot center, assumed to be 0 in eq. (18). The voltage signal for each quadrant of the quadcell after the TIA, as well as its noise, is calculated:

$$\begin{aligned} V_{PD} &= R_{TIA} I_{PD} & I_{PD} &= R_{PD} P_{G,x_1,x_2,y_1,y_2} \\ \sigma_{shot} &= R_{TIA} \sqrt{2q_e I_{PD} \Delta F} & \sigma_{PD} &= \sqrt{\sigma_{shot}^2 + \sigma_{TIA}^2 \Delta F} \end{aligned} \quad (19)$$

The voltage noise of the signal σ_{PD} is assumed to be composed of shot noise σ_{shot} and amplifier noise σ_{TIA} . I_{PD} is the current of an individual quadrant, R_{PD} is the quadcell responsivity, R_{TIA} is the transimpedance of the amplifier and ΔF is the detector bandwidth. The amplifier noise is found by simulating the circuit in fig. 6.

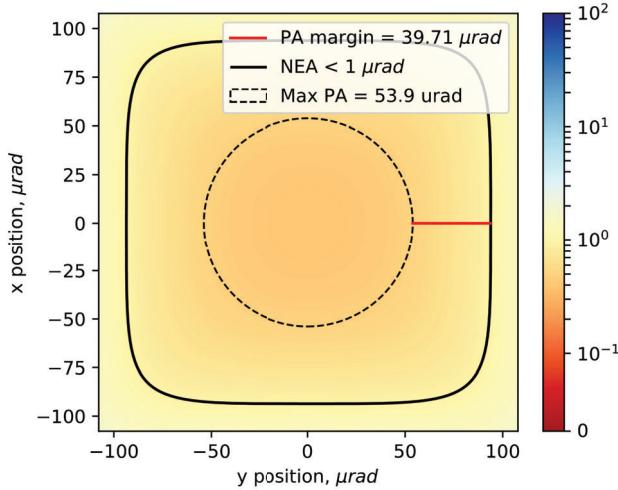


Figure 8: Noise Equivalent Angle (NEA) in μrad with a Gaussian PSF, plotted as a function of pointing error at the aperture of the payload. The largest expected Point-Ahead (PA) angle is shown as a dotted line, and the contour where NEA is better than the required $1 \mu\text{rad}$ is shown in solid black. The point-ahead margin, between the two, is $39.71 \mu\text{rad}$.

The quadcell position signal is a combination of the four quadrants:¹¹

$$\begin{aligned} x_{quad}(\theta_x, \theta_y) &= -\frac{(V_A + V_B) - (V_C + V_D)}{V_A + V_B + V_C + V_D} \\ y_{quad}(\theta_x, \theta_y) &= -\frac{(V_A + V_D) - (V_B + V_C)}{V_A + V_B + V_C + V_D} \\ SNR(\theta_x, \theta_y) &= \frac{V_A + V_B + V_C + V_D}{\sqrt{\sigma_A^2 + \sigma_B^2 + \sigma_C^2 + \sigma_D^2}} \end{aligned} \quad (20)$$

The signal-to-noise ratio (SNR) is estimated for each spot position. The estimated spot position is numerically differentiated to find the signal slope on each axis.

$$s_x(\theta_x, \theta_y) = \frac{\partial x_{quad}}{\partial \theta_x} \quad s_y(\theta_x, \theta_y) = \frac{\partial y_{quad}}{\partial \theta_y} \quad NEA(\theta_x, \theta_y) = \frac{1}{f_{PT} SNR} \sqrt{\frac{1}{s_x^2} + \frac{1}{s_y^2}} \quad (21)$$

With the local slope, we can convert the quadcell position error back to angular error at the payload telescope, called the Noise Equivalent Angle (NEA). The NEA for a $W = 90 \mu\text{m}$ spot and a focal length of $f_{PT} = 700 \text{ mm}$ is shown in fig. 8.

Once an initial estimate for the spot size and EFL have been found, we can perform a new NEA analysis using the PSF obtained by ray-tracing from Zemax. The PSF is exported as a cross-section. This cross-section is linearly interpolated to form a 2D image of the spot with a resolution of 1000 by 1000 points. The cumulative sum of this array is then taken against each axis and normalized, to obtain the 2D integral of the PSF over a rectangular section. This rectangular section emulates the corner of one of the active elements of the quadcell. Unlike eq. (18), this calculation does not take into account the other two edges of the active element, however since the PSF is assumed to be of finite dimension and always smaller than the size of the active elements ($1.5 \times 1.5 \text{ mm}^2$), there is no impact from the quadcell active elements far edges for spots near the center.

The NEA for an in-focus spot is plotted in fig. 9a, and in fig. 9b for a wider defocused spot. The NEA is improved close to the quadcell center for the small spot, however, a wider spot enables larger pointing deviations with a small NEA, which is necessary to maintain the point-ahead offset. Figure 11a shows margins for both the point-ahead angle and the noise equivalent angle. As the spot widens, so does the margin for the maximum deviation angle, until the NEA drops below the required value over the entirety of the quadcell. The impact of

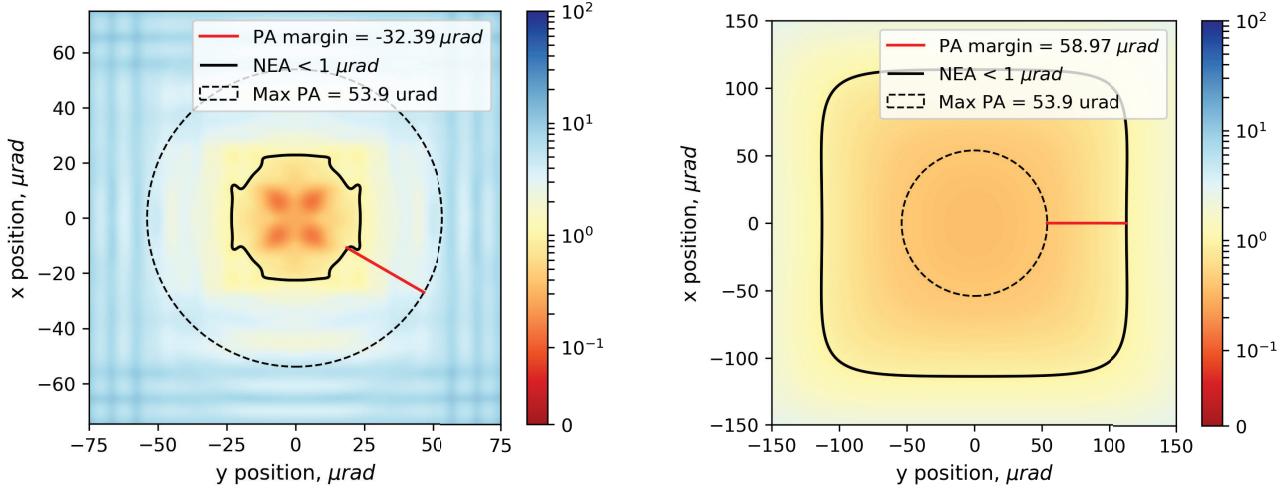
(a) Spot size of 5.7 μm (in focus).(b) Spot size of 114 μm (defocused).

Figure 9: Noise Equivalent Angle (NEA) in μrad with a Zemax-simulated PSF. The Point-Ahead (PA) margin is in red.

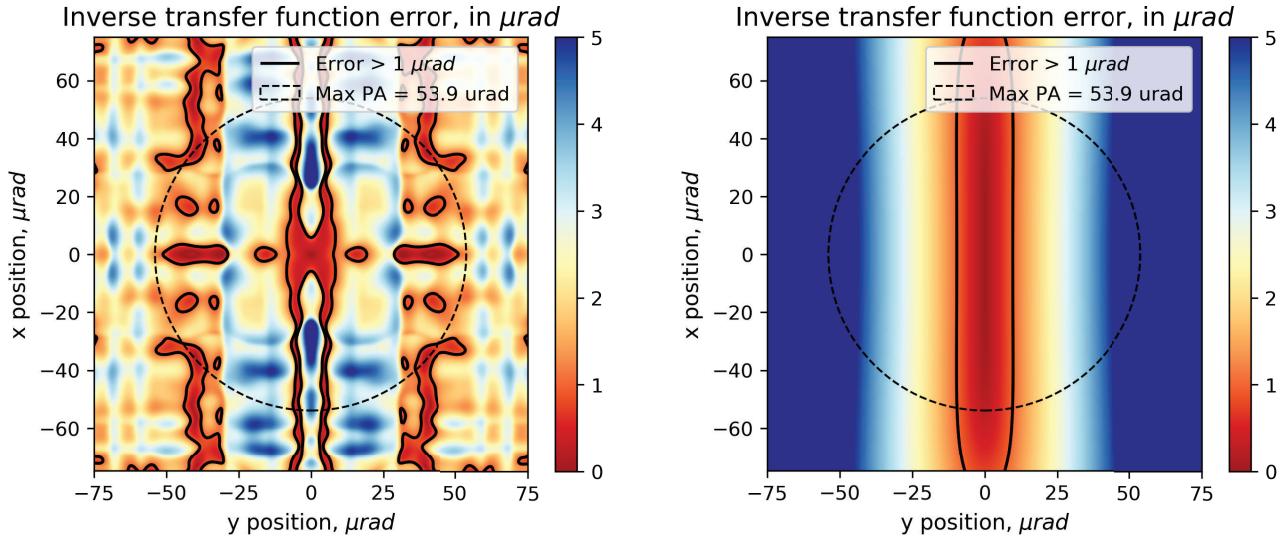
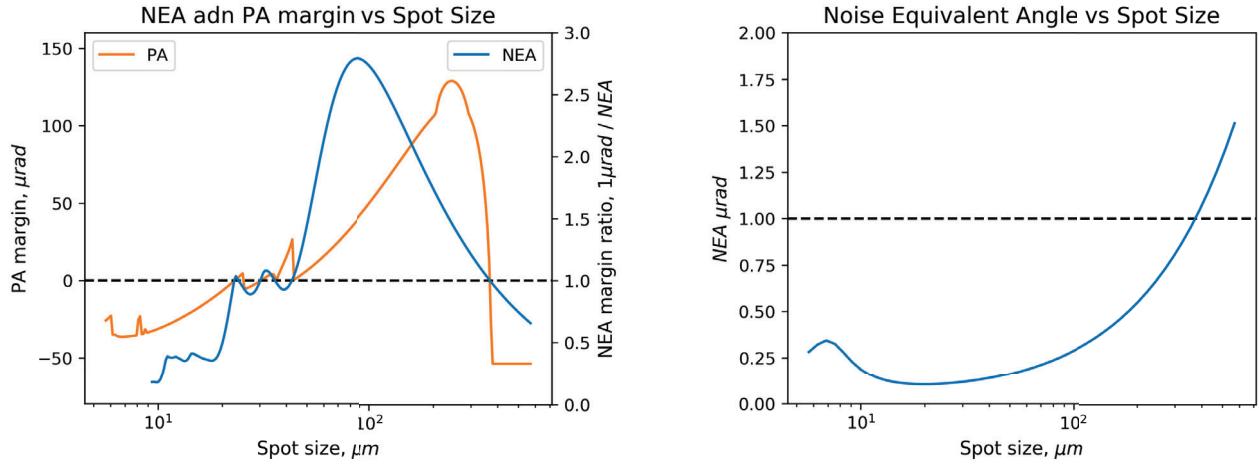
(a) Spot size of 5.7 μm (in focus).(b) Spot size of 114 μm (defocused).

Figure 10: Error in pointing angle estimation due to the PSF change at different telescope angles of incidence.

the secondary mirror obstruction is limited, primarily degrading the link budget by reduction of the collection area, rather than having a negative impact on the PSF itself. Based on the results of fig. 11a, a spot size of around 100 μm is desired, with an acceptable deviation of 20 μm . The performance of the detector predicted by this analysis is compatible with the results of a similar design; Ref. 19 reports a NEA better than 0.1 μrad at a power of 200 pW, with a focal length of 4 m.

Unlike an imaging detector, we are evaluating the position of the beam relatively far away from a fixed position feature, like the boundaries of a pixel. Therefore, if using a single FSM, it is critical that the quadcell transfer function is well-known. A source of a variation of the PSF is the change in angle of incidence on the telescope, as seen in fig. 5. In order to estimate the error due to PSF changes, we evaluate the quadcell response with a 0.2 deg angle of incidence, and then use interpolation to inverse the quadcell transfer function at an



(a) Point ahead angle margin and NEA margin as a function of the spot size for a single FSM.

(b) Noise equivalent angle as a function of the spot size for 2 FSMs.

Figure 11: Poiting performance for a single FSM and a 2 FSMs optical layout. The dashed line is the requirement for all quantities.

incidence of 0 deg. The resulting error $\Delta\theta$ is then:

$$\begin{aligned} \Delta\theta_x &= \theta_x - x_{quad}^{-1}|_{0^\circ}(x_{quad}|_{0.2^\circ}(\theta_x, \theta_y)) & \Delta\theta_y &= \theta_y - y_{quad}^{-1}|_{0^\circ}(y_{quad}|_{0.2^\circ}(\theta_x, \theta_y)) \\ \Delta\theta &= \sqrt{\Delta\theta_x^2 + \Delta\theta_y^2} \end{aligned} \quad (22)$$

fig. 10 shows $\Delta\theta$ for two different spot size. With any amount of defocus, the error due to PSF varaitons are too large. To solve this issue, a second FSM is used to introduce the point-ahead angle. The quadcell must now track to the uplink beacon spot on its center, a well-defined location. In that configuration, the NEA is only relevant near the center of the quadcell plan, within an area defined by the FSM actuation noise. The FSM closed-loop control residual has been measured at 0.137 μrad. We selected a region of interest with a radius of 1 μrad. The resultin NEA is ploted in fig. 11b. In a two FSM configuration, spot sizes of 10 μm to 100 μm are optimal, with a wide acceptable range.

4.2 Data Downlink

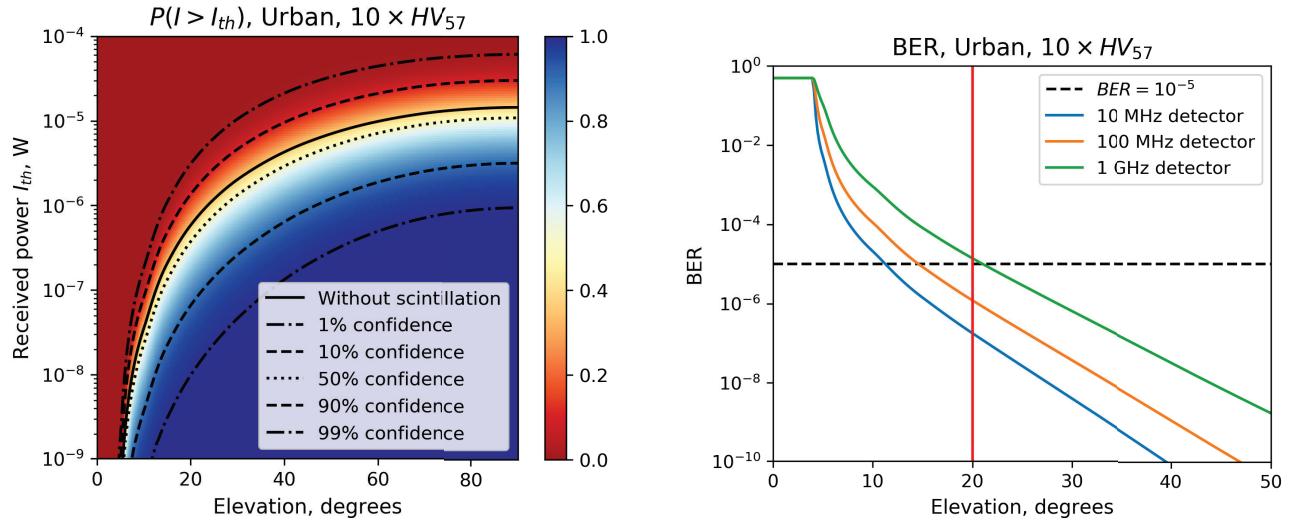
The payload lasercom transmitter uses the same telescope as the key distribution link, with a higher divergence to account for chromatic aberrations in the optics. Data is modulated at 100 Mbps, with a 100 mW average power. The power is limited to 100 mW to avoid over-heating of the fast steering mirrors. The link parameters are listed in table 2.

Figure 12a shows the distribution of the optical power at the ground detector, for elevations ranging from 0 to 90 deg. Once the received power is known, we can compute the Bit Error Ratio (BER). First, we need to find the SNR. On the ground, an APD is used to receive the signal, with a responsivity of $R_{APD} = 50$ A/W and an excess noise factor of $F_{APD} = 3.2$. The APD dark current is 1.5 nA. For an avalanche photodetector, the SNR can be expressed as:

$$SNR(P) = \frac{R_{APD}^2 P^2}{2q_e F_{APD} (R_{APD} P + i_{dark}) \Delta F} \quad (23)$$

ΔF is the bandwidth of the detector. For a data rate of 100 Mbps, a bandwidth of 100 MHz is sufficient. The BER is obtained with eq. (24), and is plotted in fig. 12b for three different bandwidth values.

$$BER = \frac{1}{2} \int_0^\infty f_{\alpha\mu}(p) \operatorname{erfc} \left(\frac{SNR(p)}{2\sqrt{2}} \right) dp \quad (24)$$



(a) Received power distribution at the ground communication detector.

(b) Bit Error Rate for three detector bandwidths.

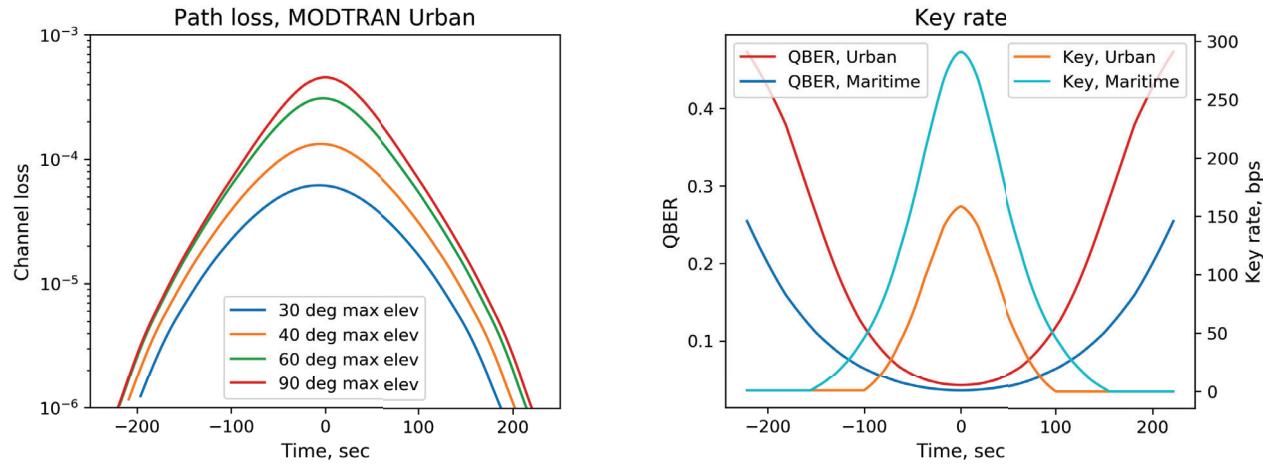
Figure 12: Data downlink results for worst case scintillation, $C_n^2 = 10 \times HV_{57}$, with parameters summarized in table 2. The vertical red line indicates the elevation angle for which the link budgets must close.

With a 100 MHz bandwidth at the detector output, the BER is better than 1×10^{-5} once the elevation is higher than 15 deg. The relatively low range loss of the free-space optical channel could support higher data rates, for example 1 Gbps for elevations higher than 22 deg. The APD would also support the higher bandwidth required, however the data rate is limited by the modulator design, to 200 to 400Mbps. Higher rates would limit the laser diode options and require a more complex modulation circuit, or a change of modulation scheme.

4.3 Key Downlink

The quantum key distribution link is driving the optical front-end divergence and pointing requirements, and because of that, the optics are optimized to obtain the lowest divergence for this beam – 12 μ rad FWHM at a center wavelength of 780 nm. For this analysis, we assume that the entangled photon source generates photon pairs at a rate comparable to the Micius mission.²⁰ Other link parameters are listed in table 2.

The overall loss of the optical channel, from the photon source to the ground single photon detector, is shown in fig. 13a. The loss is plotted for a direct-overhead pass, with the time axis centered on the highest elevation at the ground station, when the satellite is directly above the ground telescope. The link is limited to elevations above 20 deg. There is currently no maximum elevation, but it is possible that the optical ground station telescope mount may have limitations. Also, at low elevation the Quantum Bit Error Rate (QBER) is too low to ensure privacy. With the free-space channel losses, and the specifications of the ground detectors, the Quantum Bit Error Rate can be computed.²¹ The single photon detectors and polarization controllers characteristics are listed in table 3. With the QBER, the asymptotic key rate, as well as the asymptotic key size for a single pass are obtained. The resulting key rate and QBER are shown in fig. 13b, for either a maritime or an urban aerosol model. For the urban case, the asymptotic key size is 16 603 bit, and for the maritime case, it is 39 572 bit long. The asymptotic key rate provides an estimate of the secret key that can be extracted assuming that the raw key is of infinite length. Claiming information theoretic security requires considering the finite size of the raw key and involves integration over the satellite pass and then optimization over the error correction parameters.²² The parameters are ϵ_{cor} , the probability that the key contains an error after error correction, and ϵ_{sec} , the probability that an attacker knows any part of the key without being detected. The finite key size are 1862 bit for the urban model, and 17 677 bit for maritime. The urban case is marginal for single pass key exchange, but can still support QKD demonstrations. The maritime case is sufficient for a single pass secure key exchange.



(a) Optical channel loss over time for various pass maximum elevations.

(b) Quantum Bit Error Rate, and asymptotic key rate for a direct overhead pass. The two cases are for the MODTRAN Urban and Maritime aerosol models.

Figure 13: Key downlink results

Table 3: Quantum detection and privacy amplification and parameters

Parameter name	Value
Mean number of photons	0.025 / 1 ns coincidence window
Visibility	98%
Dark counts in space	100 kcps
Dark counts on the ground	500 cps
Jitter	320 ps
Detector dead time	50 ns
After-pulsing probability	5%
Error correction efficiency	1.1
Basis reconciliation efficiency	50%
Key error probability ϵ_{cor}	10^{-10}
Insecure key probability ϵ_{sec}	10^{-10}

Table 4: Single pass key exchange performances

Model	Urban	Maritime
Asymptotic key size	16 603 bit	39 572 bit
Finite key size	1862 bit	17 677 bit

5. CONCLUSIONS AND FUTURE WORK

Based on the optical design and the link analysis presented in this work, quantum key distribution (QKD) is feasible within the volume and power envelope of a CubeSat. QKD can be achieved with a 100 mm class space telescope. Specifically, based on our analysis, a 95 mm telescope with a 20% obstruction ratio is capable of reaching our gain requirement of 108.8 dB with a margin of 1 dB. A 12U CubeSat would have enough volume to include the spacecraft bus components, including a high performance ADCS system, the entangled photon source and the optical front-end. A suitable optical train, with a low volume (less than 1U) and power (less than 30 W) has been designed, supporting both precision pointing and laser communication at 100 Mbps or more. Future work on this project includes the detailed mechanical design of the optical bench, a thermal analysis for the optical components, and verification of the pointing sensor performance using the CLICK-BC hardware.

APPENDIX A. GAUSSIAN BEAM PROPAGATION

Gaussian beam parameters, where $k = 2\pi/\lambda$ is the wave number:

$$\Lambda_0 = \frac{2L}{kW_0^2} = \frac{\lambda L}{\pi W_0^2} \quad \Theta_0 = 1 - \frac{L}{F_0} = 1 \quad \Lambda = \frac{\Lambda_0}{\Theta_0^2 + \Lambda_0^2} \quad \overline{\Theta} = 1 - \Theta = 1 - \frac{\Theta_0}{\Theta_0^2 + \Lambda_0^2} \quad (25)$$

APPENDIX B. DOWNLINK SCINTILLATION VARIANCE

See 16, chap. 12, eq. (68)

$$\sigma_{x,down}^2 = \exp \left[\frac{0.49\sigma_R^2}{\left(1 + 1.11\sigma_R^{12/5}\right)^{7/6}} \right] - 1 \quad \sigma_{y,down}^2 = \exp \left[\frac{0.51\sigma_R^2}{\left(1 + 0.69\sigma_R^{12/5}\right)^{5/6}} \right] - 1 \quad (26)$$

APPENDIX C. UPLINK SCINTILLATION VARIANCE

Scintillation index with tracking under weak fluctuation:

$$\sigma_{Bu}^2 = 8.70\mu_{3u}k^{7/6}(H - h_0)^{5/6}\sec^{11/6}(\zeta) \quad (27)$$

$$\mu_{3u} = \operatorname{Re} \int_{h_0}^H C_n^2(h) \left(\xi^{5/6} [\Lambda\xi + i(1 - \overline{\Theta}\xi)]^{5/6} - \Lambda^{5/6}\xi^{5/3} \right) dh \quad (28)$$

Equation (28) is integrated over 1000 points equally spaced from 0 to 20 km.

Scintillation index with tracking, see 16, chap. 12, eq. (60):

$$\sigma_{x,tracked} = \exp \left[\frac{0.49\sigma_{Bu}^2}{\left(1 + (1 + \Theta)0.56\sigma_{Bu}^{12/5}\right)^{7/6}} \right] - 1 \quad \sigma_{y,tracked} = \exp \left[\frac{0.51\sigma_{Bu}^2}{\left(1 + 0.69\sigma_{Bu}^{12/5}\right)^{5/6}} \right] - 1 \quad (29)$$

Pointing error variance, see 16, chap. 12, eq. (53):

$$\sigma_{pe}^2 = 0.54(H - h_0)^2 \sec^2(\zeta) \left(\frac{\pi}{kW_0} \right)^2 \left(\frac{2W_0}{r_0} \right)^{5/3} \left[1 - \left(\frac{C_r^2 W_0^2 / r_0^2}{1 + C_r^2 W_0^2 / r_0^2} \right)^{1/6} \right] \quad (30)$$

Scintillation index without tracking, see 16, chap. 12, eq. (80) and (81):

$$\sigma_{x,up}^2 = 5.95(H - h_0)^2 \sec^2(\zeta) \left(\frac{2W_0}{r_0} \right)^{5/3} \left[\left(\frac{r - \sigma_{pe}}{LW} \right)^2 \operatorname{U} \left(\frac{r - \sigma_{pe}}{L} \right) + \left(\frac{\sigma_{pe}}{LW} \right)^2 \right] + \sigma_{x,tracked} \quad (31)$$

$$\sigma_{y,up}^2 = \sigma_{y,tracked}$$

$\operatorname{U}(x)$ is the unit step function.

ACKNOWLEDGMENTS

This work is supported by the Singapore-MIT Alliance for Research and Technology (SMART) and SpeQtral Pte Ltd.

REFERENCES

- [1] Shields, J., Pong, C., Lo, K., Jones, L., Mohan, S., Marom, C., Mckinley, I., Wilson, W., and Andrade, L., "Characterization of CubeSat Reaction Wheel Assemblies," *Journal of Small Satellites* **6**(1), 565–580 (2017).
- [2] Kingsbury, R., *Optical Communications for Small Satellites*, PhD thesis, Massachusetts Institute of Technology (2015).
- [3] Clements, E., Aniceto, R., Barnes, D., Caplan, D., Clark, J., del Portillo, I., Haughwout, C., Khatsenko, M., Kingsbury, R., Lee, M., Morgan, R., Twichell, J., Riesing, K., Yoon, H., Ziegler, C., and Cahoy, K., "Nanosatellite optical downlink experiment: design, simulation, and prototyping," *Optical Engineering* **55**, 111610 (Sept. 2016).
- [4] Yenchesky, L., Cierny, O., Grenfell, P., Kammerer, W., Do, P., Periera, V., Sevigny, T., and Cahoy, K., "Optomechanical Design and Analysis for Nanosatellite Laser Communications," in [*Proceedings of the 33rd AIAA/USU Conference on Small Satellites*], (2019).
- [5] Serra, P., Cierny, O., Diez, R., Grenfell, P., Gunnison, G., Kammerer, W., Kusters, J., Payne, C., Murphy, J., Sevigny, T., do Vale Pereira, P., Yenchesky, L., Cahoy, K., Clark, M., Ritz, T., Coogan, D., Conklin, J., Mayer, D., Hanson, J., and Stupl, J., "Optical Communications Crosslink Payload Prototype Development for theCubesat Laser Infrared CrosslinkK (CLICK) Mission," in [*Proceedings of the AIAA/USU Conference on Small Satellites, SSC20-VI-04.*], (2019).
- [6] Oi, D. K. L., Ling, A., Grieve, J. A., Jennewein, T., Dinkelaker, A. N., and Krutzik, M., "Nanosatellites for quantum science and technology," *Contemporary Physics* **58**(1), 25–52 (2017).
- [7] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of Modern Physics* **74**(1), 145–195 (2002).
- [8] Lee, J., Shen, L., Cerè, A., Troupe, J., Lamas-linares, A., and Kurtsiefer, C., "Symmetrical clock synchronization with time-correlated photon pairs," *Applied Physics Letters* **114** (2019).
- [9] Dai, H., Shen, Q., and Wang, C. e. a., " Towards satellite-based quantum-secure time transfer," *Nature Physics* (2020).
- [10] Kurtsiefer, C., "Qcrypto; open-source QKD software stack."
- [11] Lambert, S. G. and Casey, W. L., *[Laser communications in space]*, Artech House (1995).
- [12] Klein, B. J. and Degnan, J. J., "Optical Antenna Gain 1: Transmitting Antennas," *Applied Optics* **13**, 2134 (sep 1974).
- [13] Peters, W. N. and Ledger, A. M., "Techniques for Matching Laser TEM_00 Mode to Obscured Circular Aperture," *Applied Optics* **9**, 1435 (jun 1970).
- [14] Mirracle Technologies Inc., "Bonded Mirror Devices."
- [15] Blue Canyon Technologies, "ATTITUDE CONTROL SYSTEMS," tech. rep.
- [16] Andrews, L. C. and Phillips, R. L., *[Laser beam propagation through random media]*, SPIE Press, Bellingham, Wash, 2nd ed ed. (2005).
- [17] Yang, G., Khalighi, M.-A., Bourennane, S., and Ghassemlooy, Z., "Approximation to the sum of two correlated gamma-gamma variates and its applications in free-space optical communications," *IEEE Wireless Communications Letters* **1**, 621–624 (Dec. 2012).
- [18] Peppas, K. P., "A simple, accurate approximation to the sum of gamma-gamma variates and applications in MIMO free-space optical systems," *IEEE Photonics Technology Letters* **23**, 839–841 (July 2011).
- [19] Toyoda, M., "Measurement of the characteristics of a quadrant avalanche photodiode and its application to a laser tracking system," *Optical Engineering* **41**, 145 (Jan. 2002).
- [20] Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., Li, G.-B., Lu, Q.-M., Gong, Y.-H., Xu, Y., Li, S.-L., Li, F.-Z., Yin, Y.-Y., Jiang, Z.-Q., Li, M., Jia, J.-J., Ren, G., He, D., Zhou, Y.-L., Zhang, X.-X., Wang, N., Chang, X., Zhu, Z.-C., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W., "Satellite-based entanglement distribution over 1200 kilometers," *Science* **356**, 1140–1144 (June 2017).
- [21] Ma, X., Fung, C.-H. F., and Lo, H.-K., "Quantum key distribution with entangled photon sources," *Physical Review A* **76** (July 2007).
- [22] Chapman, J. C., Lim, C. C. W., and Kwiat, P. G., "Hyperentangled Time-bin and Polarization Quantum Key Distribution," *arXiv e-prints* , arXiv:1908.09018 (Aug. 2019).