

PROCEEDINGS OF SPIE

SPIDigitalLibrary.org/conference-proceedings-of-spie

QKD optical ground terminal developments

Klop, Wimar, Saathof, Rudolf, Doelman, Niek, Gruber, Michael, Moens, Thijs, et al.

Wimar Klop, Rudolf Saathof, Niek Doelman, Michael Gruber, Thijs Moens, Clara I. Osorio Tamayo, Cristina Duque, "QKD optical ground terminal developments," Proc. SPIE 11852, International Conference on Space Optics — ICSO 2020, 118520Y (11 June 2021); doi: 10.1117/12.2599217

SPIE.

Event: International Conference on Space Optics — ICSO 2021, 2021, Online Only

International Conference on Space Optics—ICSO 2020

Virtual Conference

30 March–2 April 2021

Edited by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas



QKD optical ground terminal developments



International Conference on Space Optics — ICSO 2020, edited by Bruno Cugny, Zoran Sodnik, Nikos Karafolas, Proc. of SPIE Vol. 11852, 118520Y · © 2021 ESA and CNES
CCC code: 0277-786X/21/\$21 · doi: 10.1117/12.2599217

Proc. of SPIE Vol. 11852 118520Y-1

QKD optical ground terminal developments

Wimar Klop^{*a}, Rudolf Saathof^a, Niek Doelman^{a,b}, Michael Gruber^a, Thijs Moens^a, Clara I. Osorio Tamayo^a, Cristina Duque^a

^aTNO Technical sciences, Delft the Netherlands; ^bLeiden Observatory, Leiden University, the Netherlands

ABSTRACT

Free space optical (FSO) satellite communications has very attractive properties for Quantum Key Distribution (QKD). The quantum channel loss and noise are major factors in setting the maximum achievable secure key rate of QKD systems. Primarily for a LEO satellite node and the BB84 protocol a number of technologies are proposed to reduce the quantum channel loss and noise. These technologies apply to the receiver side of the QKD link, the Optical Ground Terminal. It is shown that an optical beam shaper to optimize fiber mode matching, dedicated thermo-mechanical design to reduce misalignment induced by temperature gradients and an Adaptive Optics (AO) system to counteract optical turbulence effects can result in a significant reduction of loss and background noise. A breadboard verification experiment shows that using an medium-size AO system can maintain a fiber coupling efficiency up to 40%. The developed technologies have a general applicability with respect to satellite orbit and QKD protocol used.

Keywords: Quantum Key Distribution, Free Space Optics, Optical Ground Stations, Opto-mechanics, Adaptive Optics

1. INTRODUCTION

Quantum Key Distribution involves the generation and sharing of private keys between two parties, known as Alice and Bob, to transfer encrypted data over a public channel. As its security is based on quantum physical principles rather than computational hardness, QKD has evolved quickly since the first concept proposal in 1984 [1]. Furthermore, QKD is mainly an optical technology, and therefore it fits nicely into the recent advances in data communication over optical links, either in fiber or in free space.

QKD over a terrestrial link in fiber faces distance limitations as a result of the channel transmittance. For an ultra-low loss fiber, with a fiber transmittance loss of in the order of 0.15 dB/km, the distribution of quantum keys at a decent rate is limited to a few 100's km [2]. To enlarge the range, while preserving the attractive security properties of QKD, requires the use of quantum repeaters with performance properties yet to be demonstrated.

Using satellite-based QKD nodes is an alternative and more mature way to distribute quantum keys between two distant parties. In free space, optical beam diffraction and limited transmitter (Tx) and receiver (Rx) aperture sizes are the main factors that determine the channel loss. The effective channel loss can be significantly lower than for the terrestrial QKD counterpart for various configurations of satellite links with distant Alices and Bobs. Several studies and experiments have been performed on satellite-based QKD links; see, for instance [3, 4] and the Micius mission [5, 6]. And, given the need to build a global secure communication infra-structure, satellite-based quantum key distribution is currently drawing significant attention from research institutes, technology development parties, large system integrators, and communication service providers; (see, for instance, the EU initiative of a quantum communication infrastructure ref. EU QCI; [7]).

In this paper, we will address QKD from LEO-orbit satellites and describe technology advances that enable a high secret key rate. In a companion paper, the GEO-stationary satellite case is described [8]. For a QKD link, the channel loss and noise are crucial factors defining the performance. Next to the free space path loss, environmental effects such as atmospheric turbulence, absorption, and background radiation affect channel loss and noise. Also, instrumental effects such as pointing precision and accuracy and optical terminal wave front errors play a role.

^{*} *wimar.klop@tno.nl; phone +31 (0)64 641 73 62; www.tno.nl*

TNO has a long-standing track record in space instrumentation. In the field of free space optical communication, we work on both space and ground optical terminals. We have several space terminal developments [9, 10], including optical telescopes, coarse pointing assemblies, and fast steering mirrors [11, 12] to limit pointing errors. For ground terminal developments, adaptive optics systems are being developed to improve the fiber coupling in downlinks and to pre-correct turbulence effects in uplinks [13, 14]. High power beam multiplexers are being developed for the very high throughput Earth-GEO satellite cases [15].

A major objective of TNO Space is to design and develop optical, mechanical and mechatronic technologies that enable very high secure key-rate QKD links through free space. Minimizing quantum channel loss and noise plays a central role in the designs, next to keeping complexity, cost and SWaP (Size, Weight and Power use) of the communication terminals low. This requires a thorough understanding of the behaviour and performance of QKD protocols in order to make the right trade-off's during the technologies developments. The ESA ScyLight project Quantum Cryptography Telecommunication System (QUARTZ), led by SES, aims to define, design, and develop a satellite-based Quantum Key Distribution (QKD) system and service architecture. TNO is designing an optical ground terminal (OGT) for this LEO-satellite-based QKD service within this project. The main design driver of our OGT is the reduction of loss in the quantum channel. This has resulted in a combination of technology approaches, being: a low wave front error optical terminal, an optical beam shaper to optimize fiber mode matching, dedicated thermo-mechanical design to reduce misalignment induced by temperature gradients, adaptive optics to improve fiber-coupling and to enable severe rejection of background radiation.

The organization of the paper is as follows. First, we describe a generic analysis for a LEO to ground QKD link in Section 2, which provides the theoretical context and conceptual link for QKD with day-time operation. Then Section 3 presents the architecture of an OGS suitable for a QKD link. In Section 4, the adaptive optics system and analysis is worked out. The latter two sections relate to the QUARTZ project. Using an experimental laboratory environment, we study the relationship between this adaptive optics performance and the fiber coupling efficiency. Using the findings from Sections 2-5, Section 6 draws the perspective of QKD technology, and Section 7 describes our conclusions.

2. SECURE KEY RATE ANALYSIS

There are two fundamental performance indicators for Quantum Key Distribution (QKD), security and secure key rate. This paper focuses on the secure key rate, i.e., the number of secure bits per second that Alice and Bob can share while performing a QKD protocol. The key rate is generically determined by the protocol choice, the channel behaviour, and the noise or error sources. In this section, we consider a (theoretical) LEO-to-ground satellite link.

2.1 QKD protocol and key-rate

The vast and growing set of QKD protocols differ mainly on the degree of freedom encoding information and how this information is transmitted and processed. In this paper, we consider BB84 as the baseline protocol [16]. It is the quintessential QKD protocol, i.e., it is not overly exotic and forms a reference case to existing literature.

In particular, we consider a 'vacuum plus weak decoy-state' BB84 implementation using polarization for encoding [17]. In this implementation, Alice randomly chooses to transmit vacuum, a signal or a decoy-state, with a mean photon number per pulse μ and ν photons[†], respectively. For each signal pulse, Alice chooses a bit ('0' or '1') and one of two bases to encode this bit (e.g., Horizontal / Vertical or 45 / -45 polarization bases). She then sends the encoded bit to Bob, who randomly chooses a basis, measures, and records the results. Once quantum communication has finished, Bob announces the position of the bits he detected and the basis used. Alice then announces her basis choices. Alice and Bob retain the bits for which the basis employed in the encoding and the decoding processes coincide and discard the rest. This subset is called the sifted key.

Using a segment of the sifted key, Alice and Bob estimate the quantum bit or QBER. When the estimated QBER is below a predefined threshold (e.g., 11%), the protocol continues with error correction. If the QBER is above the threshold, they

[†] For optimal performance of the protocol, the mean photon number per pulse for the signal and decoy-state must be optimized for the channel loss. Here, we have set the signal state, and the decoy states to $\mu = 0.45$ and $\nu = 0.05$ for simplicity, which are close to the optimal for the protocol and values considered [18].

abort that run of the protocol. The QBER is defined as the ratio of erroneous bits over the total number of transmitted bits. For the protocol that we are considering, the QBER of the signal states (E_μ) can be estimated using [18]:

$$E_\mu = \frac{0.5 * Y_0 + e_{det}(1 - e^{-\eta\mu})}{Y_0 + 1 - e^{-\eta\mu}}$$

in which Y_0 is the background detection probability consisting of noise, e_{det} is the probability of an erroneous detection due to cross talk (e.g., detecting as 'vertical' a 'horizontal' polarized photon), $\eta = \eta_{channel} + \eta_{detector}$ is the channel and detector loss. Using the QBER it is also possible to estimate a lower bound on the secure key rate:

$$R \geq \frac{1}{2} \{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_l [1 - H_2(e_1)]\}$$

With the gain of the signal states Q_μ (i.e., the ratio of signal detections by Bob to signal pulses sent by Alice) given by $Q_\mu = Y_0 + 1 - e^{-\eta\mu}$, $f(e)$ is the efficiency of error correction, here we consider $f(e) = 1.22$, the binary entropy function is $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$, Q_l is a lower bound for the gain of single-photon states given by $Q_l = \mu^2 e^{-\mu} / (\mu\nu - \nu^2) (Q_\nu e^\nu - Q_\mu e^\mu \nu^2 / \mu^2 - (\mu^2 - \nu^2) / \nu^2 Y_0)$, Q_ν is the gain of the weak decoy state; e_1 is the error rate of single-photon states, which has an upper bound given by $e_1 = (E_\nu Q_\nu e^\nu - e_0 Y_0) / (Y_1 \nu)$ with $Y_1 = \mu / (\mu\nu - \nu^2) (Q_\nu e^\nu - Q_\mu e^\mu \nu^2 / \mu^2 - (\mu^2 - \nu^2) / \nu^2 Y_0)$. For additional details, we refer the reader to Reference [18].

The following sections describe our estimations for the channel loss $\eta_{channel}$ and noise required to estimate the secret key.

2.2 Channel loss

To estimate the LEO-to-ground channel's losses $\eta_{channel}$, we define the link budget, as presented in Source, with both generic items and specific items. The transmit antenna gain G_{Tx} , the receive antenna gain G_{Rx} and the free space losses L_{FS} together are also known as geometric losses and are defined as:

$$G_{Tx} = \frac{8}{\theta_{div}^2}, G_{Rx} = \left(\frac{\pi D_R}{\lambda}\right)^2, L_{FS} = \left(\frac{\lambda}{4\pi L}\right)^2$$

In which θ_{div} is the divergence angle of the transmit beam. D_R the diameter of the receiver, λ the used wavelength, and L the propagation length. The transmittance of the satellite and optical ground station results from the analysis of the optical systems, e.g., the summation of the optics' transmission losses and the clipping losses.

The link budget has different items. The transmit channel consists of the transmit antenna gain, the transmittance, and additional divergence losses. These are caused by residual wave front errors of the optical system.

The propagation losses consist of free space loss and atmospheric loss. These losses are modelled, according to [3]:

$$\chi_{ext} = \exp \left[- \int_{H_{OGS}}^{L_{Path}} \beta_{ext}(L) dL \right], \beta_{ext} = \beta_{ext}^0 \exp \left(- \frac{L_{Path}}{\mathcal{H}_0 \sec \zeta} \right),$$

In which χ_{ext} is the atmospheric extinction, β_{ext} is the extinction coefficient, and β_{ext}^0 the extinction coefficient on the ground level, H_{OGS} the altitude of the ground station, L_{Path} the path length, \mathcal{H}_0 the scale parameter and ζ the zenith angle.

The atmospheric turbulence related losses relevant for QKD are the systematic pointing loss, the average pointing jitter loss, and the wave front error loss. Optical power fluctuations (scintillation) do not play a role for QKD since it is about the average power received [19]. In addition, the beam spread loss is negligible for a downlink since most turbulence is located at the ground layer, which is at the end of the downlink path. Static pointing loss is quantified by the deviation from the Gaussian center, i.e. $L_p = \exp(-2\theta_p^2/\theta_{div}^2)$. Pointing jitter is characterized by the beta distribution [20], and its average can be quantified by: $\bar{I} = \beta/(\beta + 1)$ with $\beta = w_0^2/4\sigma_p^2$. This formula only holds for a system without systematic error, and the model is adopted to take the dependence on the systematic error into account. The wave front error loss is due to atmospheric distortion. In this term, the correction is already included and is described in Section 4.

Source focusses on what is in technical context required to establish an QKD channel during day-time conditions. As can be observed the apertures on both satellite and ground terminal side have reasonably large sizes. For a commercial

application the technical complexity should be traded-off towards operation range. The operational properties to compromise on could be for instance day-time support or elevation angle range. Night-time conditions would allow for significantly higher link losses.

Table 1. Link budget for a LEO to ground QKD link for an elevation angle of 20 degrees and a wavelength of 1550 nm and daytime conditions.

Source	Gain / Loss	Background
Transmitter	Tx Antenna	Divergence: 4.9 μ rad, waist radius ($1/e^2$): 101 mm
	Satellite transmission	Transmission: 0.90 including clipping losses
	Additional divergence	WFE Tx: 100 nm RMS
Propagation	Free space	Slant path length: 1192.8 km
	Atmospheric	Visibility = 20 km, Scale parameter = 4 km. cirrus clouds = 1.00 km
Atmospheric turbulence & pointing	Systematic pointing	Static pointing error: 1 μ rad (max)
	Average pointing jitter	Pointing jitter: 1 μ rad (rms)
	Wave front error	Residual WFE after AO correction: 225 nm (rms), $r_0 = 10.3$ cm, nominal coupling loss = 0.85
Receiver	Rx Antenna	Diameter receiver = 1.2 m
	Rx transmission	Transmission = 0.75, excluding fiber coupling loss
Total	Channel loss $\eta_{channel}$	-27.2 [dB]

2.3 Noise Analysis

For day-time operation of QKD, the two dominant noise sources for quantum key distribution are detector noise ξ_{det} and background noise ξ_{BG} [4]. These noise contributions relate to the background detection probability $Y_0 = 4\xi_{det} + \xi_{BG}$. The error sources are assumed to be randomly polarized, so the detection error rate $e_{det} = 0.5$.

Detector noise can be modelled as units of electrons:

$$\xi_{det} = f_n/f_d$$

with f_n the noise count in Hz and f_d the effective detector rate. Background radiation N_{BG} is quantified by the power per solid angle Ω , collecting area A and the wavelength band $\Delta\lambda$. For 1550 nm, we assume 10 W/m²/sr/ μ m. The amount of background radiation can be computed by:

$$\xi_{BG} = N_{BG}A\Omega\Delta\lambda\tau/E_p$$

With $E_p = hf$ is the photon energy, in which h is Planck's constant, $f = c/\lambda$ the frequency of the optical beam and τ is the gate time. The solid angle is dependent on the field of view of the telescope $\theta_{FOV} = 2\pi(1 - \cos \theta_{FOV})$. The field of view can be reduced to the size of a single-mode fiber when using adaptive optics, without significantly losing link margin. By using a focal length of the telescope of $f_T = d_T/2\theta_{NA}$, with a single-mode fiber diameter $d_{SMF} = 10 \mu$ m and numeric aperture of $\theta_{NA} = 0.15$, the field of view is $\theta_{FOV} = d/2f_T$. In addition, we assume a spectral filter characteristic of 1 pm bandwidth to do significant background suppression.

2.4 Total channel performance

The turbulence and link budget modelling have been integrated into a software tool developed at TNO, which can assess a free space optical link's feasibility. Figure 1 presents the results of integrating the case, as described, into this tool. Figure 1 (a) depicts the relation between the elevation angle and the link loss. As expected, the distance is longer at low elevation angles, leading to increasing free space losses. The effective path through the atmosphere is longer, and turbulence related losses increase. Figure 1 (b) presents the loss versus key-rate curve for a source rate of 10 GHz, background radiation of $10 \text{ W}/(\text{m}^2\text{sr } \mu\text{m})$ and 100 Hz detector noise. From this figure, we conclude that a key can still be distilled with a loss of 28 dB. Using a detector efficiency of 85%, which accounts for 0.7 dB, a maximum channel loss of 27.3 dB is required. This holds for an elevation angle of 20 degrees and in day-time conditions.

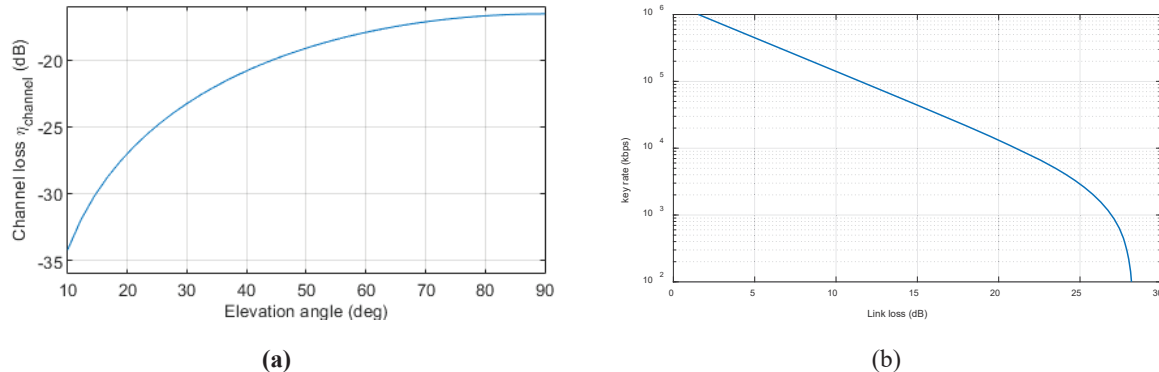


Figure 1. FSO channel performance: (a) link loss as a function of elevation angle and (b) the key rate as a function of channel loss.

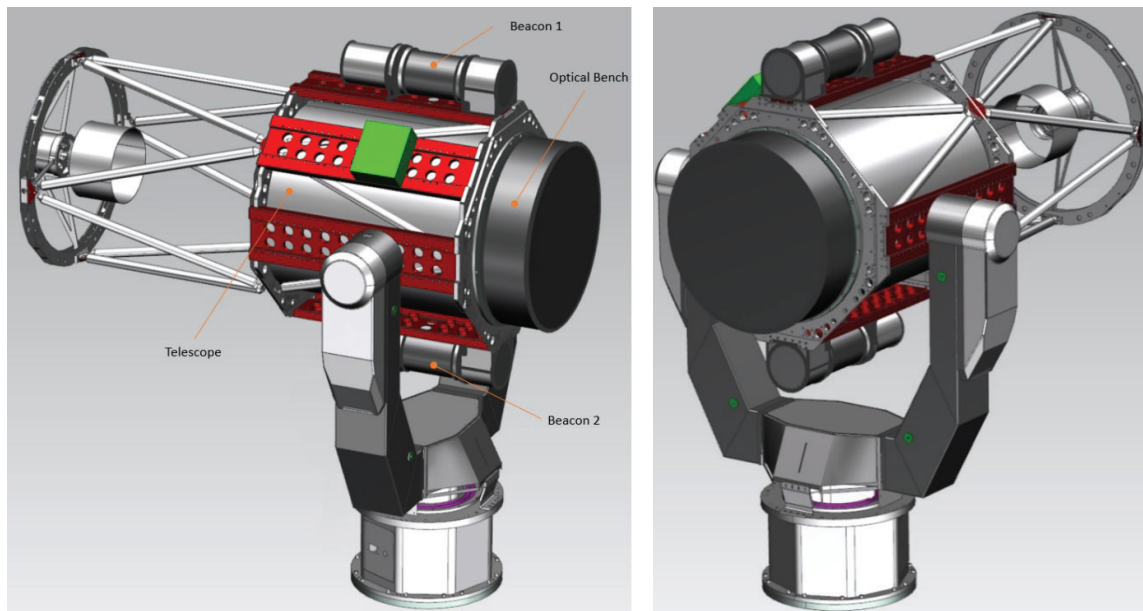


Figure 2. CAD rendering of the telescope, including mounted beacon and optical bench. The left and right images show the telescope from different orientations.

3. OPTICAL GROUND TERMINAL DESIGN

QKD drives the Optical Ground Terminal (OGT) design in multiple ways, of which high photon efficiency and background suppression are key design drivers. The subsequent section shall describe how these design drivers are translated to the design developed in the scope of the QUANTum cRyptography Telecommunication [Z]system (QUARTZ) program. SES leads the QUARTZ program. The goal is to develop a satellite-based QKD service based on BB84. QUARTZ is a typical design example for a low Earth orbit (LEO) satellite-based QKD service. TNO being part of the QUARTZ consortium, is responsible for the development and the design of the Optical Ground Terminal.

3.1 Optical ground terminal Architecture

The OGT's primary objective is to capture as much of the QKD signal into a single-mode fiber as possible while limiting the noise contribution. This is apart from its secondary objectives. For QUARTZ these objectives also involve classical downlink and uplink communication. For the OGT the process starts at the telescope aperture. This is a key aspect, as the aperture determines the light collection capabilities of the telescope. However, it also defines a lot in terms of its dimensions, mass, and system complexity. Consider QUARTZ is a LEO based service. The larger the telescope, the more challenging or complex the tracking of the satellite shall be. In addition, the higher the number of modes needs to be corrected for, by the adaptive optics system. For the QUARTZ design, an 800 mm classical Cassegrain telescope was selected with the optical bench on the telescope's back. The classical Cassegrain configuration was chosen as this has, per definition, the least amount of optical elements and thus the highest transmission. The aperture diameter is on the edge, in terms of diameter, what is commercially available as a semi-standard product and thus maximizes the light collection area. The telescope is based on an a-focal design that reduces central obscuration and minimizes optical elements in the overall design. Due to the a-focal design, the FSM can be the first optical bench element, folding the optical beams immediately to the correct plane. The telescope's transmission is optimized with customized coatings, achieving a 94% transmission in the applicable wavelength band. Figure 2 presents a mechanical view of the assembled telescope, including the beacons and the optical bench.

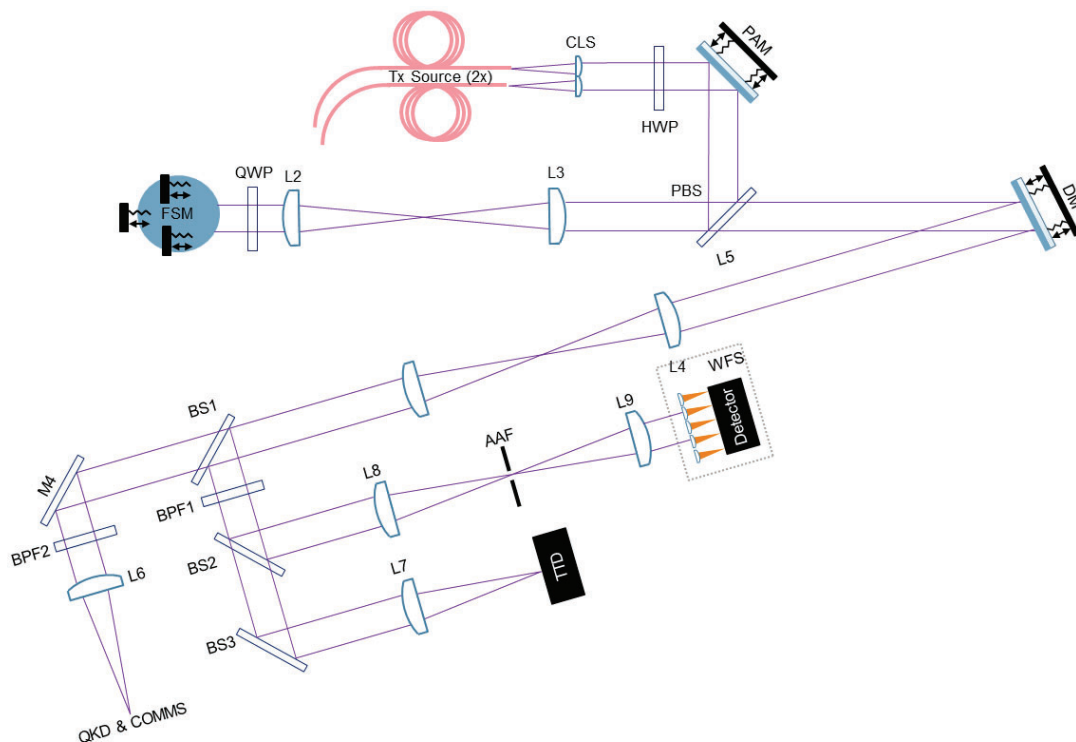


Figure 3. (a) Adaptive Optics System consisting of a fast steering mirror (FSM), a deformable mirror (DM) a Tip/Tilt Detector (TTD), a wave front sensor (WFS), a point ahead mirror (PAM) and a single-mode fiber (SMF).

As mentioned before, the QKD detector is coupled to a single-mode fiber. To efficiently couple info, a single-mode fiber unperturbed wave fronts are required. In the use case, the wave front is being distorted by atmospheric turbulence, a potential mitigation technology for this is adaptive optics. Figure 3 presents a high-level schematically overview of the optical bench design, including adaptive optics. The fast steering mirror (FSM) is defined as the interface plane between the Telescope and the optical bench and corrects tip/tilt errors based on the tip/tilt detector's measurements. After a relay, the two Tx beams are coupled into the common path using a polarization beam splitter. The beam combining or isolation is based on a combination of polarization and wavelength splitting to maximize the suppression of the Tx light straylight which is back reflected toward the Rx channel. Consider that the possibility of using polarization isolation is dependent of the QKD protocol encoding principle used. The Point Ahead Mirror allows to apply an offset with respect to the Rx pointing and accommodate the point ahead angle induced by the satellite's relative velocity. The deformable mirror corrects the wave front phase errors of the Rx beam. The correction of the 192 actuator deformable mirror is based on the measurements performed by the 17 x 17 sub-aperture wave front sensor and calculated by a real-time control platform. After a secondary relay, part of the beam is split off for the OGT Optical Bench sensors using a dichroic beam splitter, only affecting the signal level in the communication wavelength. The light (both QKD and communication wavelengths) passed by the beam splitter is now coupled into a fiber.

3.2 Beam shaper

The limited aperture of the OGS with the central obscuration causes the Gaussian beam transmitted by the satellite to become a top-hat, donut shaped beam at the receiver. Coupling a top-hat profile would result in an ideal coupling efficiency of 81% as an result of the overlap integral between airy disk on gaussian mode field of single mode fiber. Coupling a donut shaped top-hat intensity profile into a single-mode induces additional losses due to the larger mode mismatch and drops down to 64% fiber coupling efficiency. A beam shaper is introduced that fits the intensity profile into a Gaussian profile. It consists of two plano-convex aspheric lenses. The first lens maps the homogenous top-hat intensity profile of the collimated beam into a diverging Gaussian intensity distribution at the second lens location. The second aspheric lens collimates this diverging beam while maintaining a near flat wave front with minimal errors. The resulting Gaussian beam profile is then focused into a polarization maintaining single-mode fiber. The beam shaper and corresponding ray mapping is shown in Figure 4 (a), and the intensity before and after shaping the beam profile is illustrated in Figure 4 (b, c). The introduction of beam shaper provides an increase of fiber coupling efficiency from about 64% to 85%, assuming an unperturbed wave front at the telescope entrance.

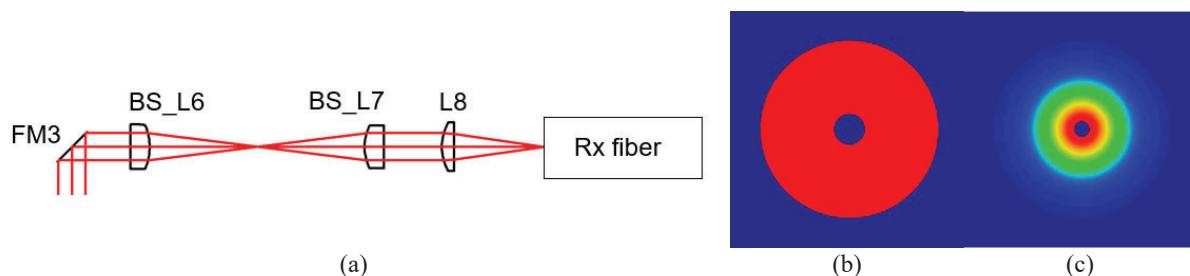


Figure 4. (a) Layout of the Rx fiber coupling, WFS and PAT beam paths including beam shaper. (b) Intensity beam profiles before and (b) after the beam shaper. The top-hat profile (with obscuration) shown on the left. The $1/e^2$ diameter of the Gaussian fit of the resulting beam shown on the right.

3.3 Thermal mechanical design

The OGS will be located on various sites globally and have to operate over the different seasons of the year. Posing some challenging environmental conditions on the system to maximize operational availability. To address this, the system was subdivided into zones. Each zone has a set of environmental conditions to cope with and implement the measures to uphold the zonal conditions. E.g., the most unfavourable environmental survival conditions are for the zone outside for which the telescope dome has to cope with. The dome slit reduces to the operational range applicable to the telescope. The most sensitive to environmental disturbances is the optical bench. Temperature variations can introduce misalignments between the different optical paths. Tracking is based on the PAT sensor, but performance is determined at the Rx fiber-coupling path, As such mechanical stability directly affects fiber coupling efficiency. On top of this condensation shall degrade the components inside. For this reason the optical bench is fully enclosed and thermally controlled at a temperature of $20^\circ\text{C} \pm 1^\circ\text{C}$. Apart from an optical-mechanical stable design this is achieved in three ways:

- Thermal insulated enclosure made of a sandwich structure to reduce conduction effects. The enclosure is at the outside foreseen of reflective coating to reduce solar radiation effects.
- A double optical window as interface as depicted in Figure 5 as optical interface between the telescope and optical bench. Again to limit conduction, but also to avoid condensation effects and reduce thermal boundary layer effects which could occur with a single window. Mechanically the optical bench is mounted using three ball-v-groove mounts to minimize thermal heat transfer.
- Active thermal control with Peltier elements directly mounted to the back of the baseplate to maintain its temperature at the setpoint of $20^{\circ}\text{C} \pm 1^{\circ}\text{C}$. Due to the precautions described in the previous two points the required power is limited and due to the active components inside the optical bench, mainly cooling power is anticipated.

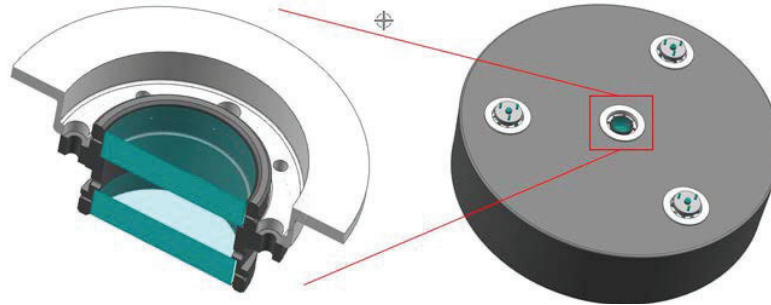


Figure 5. Double optical windows as interface between the telescope subsystem (left). Mounted into the optical bench enclosure (right)

4. FIBER COUPLING IMPROVEMENT BY ADAPTIVE OPTICS

This section will describe the Adaptive Optics (AO) system to reduce the channel loss in the QKD link. The main objective of AO is to improve the coupling of the optical beam into a single mode fiber. Several authors have reported on the fiber coupling efficiency in the presence of an AO system; see for instance [21, 22, 23]. References [21, 23] evaluate the fiber coupling efficiency using a Zernike modes description [24]. Reference [21] also describes an experiment which verifies the fiber coupling model. Alternatively, reference [22] presents a method for fiber coupling with AO without wave front sensor. This approach however requires a lot of iterations to converge to its optimal value given a single phase screen.

This section provides the approach TNO has taken to verify the various hardware components. First, the fiber coupling model is presented that are used to estimate the coupling efficiency of an AO system (Section 4.1). In Section 4.2 we experimentally demonstrate that the AO system is able to perform according to generic models [25]. The laboratory set-up of this experiment, will deviate from the final AO system architecture required for the application. The purpose of the demonstration is to show that the laboratory set-up behaves in accordance to the relations indicated by the models (e.g. bandwidth vs. FCE and number of corrected modes vs. FCE). The models can then be used to design the AO system architecture to meet the FCE requirement.

4.1 Fiber coupling efficiency

Due to the atmospheric turbulence-induced wave front aberrations, the efficiency of coupling a free space optical beam into a single mode fiber can be reduced severely. The essence of coupling an optical beam into a focal-plane single mode fiber is given by the spatial match between the PSF and the fundamental mode shape of the fiber (often approximated by a Gaussian). In the nominal case of a flat wave front, the coupling efficiency depends on the match of the Airy disk and the fiber mode. Typical values for the nominal Fiber Coupling Efficiency (FCE) η_{nom} range from 0.7 to 0.8, with 0.81 being the maximum for an unobstructed pupil; see for instance [26].

Coupling a distorted optical beam into a single mode fiber again depends on the match of the distorted PSF and the SMF mode. Ignoring amplitude aberrations, Ruilier [27] has derived an approximation which relates the effective FCE η_{FCE} to the variance σ_M^2 of the pupil-plane phase φ matched to the fundamental SMF mode:

$$\eta_{\text{FCE}}(\varphi) = \eta_{\text{nom}} \exp(-\sigma_M^2(\varphi)) \quad (1)$$

Generally this approximation leads to an under-estimation of the FCE. Furthermore, when decomposing the wavefront phase into Zernike's modes for instance, the true FCE exhibits a clear dependency on the specific Zernike mode shape. This property has gone lost in eq. (1).

4.2 Laboratory experiments on fiber coupling

In order to find a practical guideline for the design of the AO system, we have conducted a set of laboratory experiments on fiber coupling efficiency. For this purpose TNO's optical feeder link adaptive optics (OFELIA) breadboard has been used. This experimental set-up has been built to test and verify the performance of Adaptive Optics pre-correction for optical feeder links [13, 14]; see also Figure 6. It consists of an AO system, a Tx and Rx channel, and a focus camera to verify beam quality. For the experiments the breadboard was modified to assess the fiber coupling efficiency (FCE) of optical beams under partial AO correction of atmospheric-turbulence-induced aberrations.

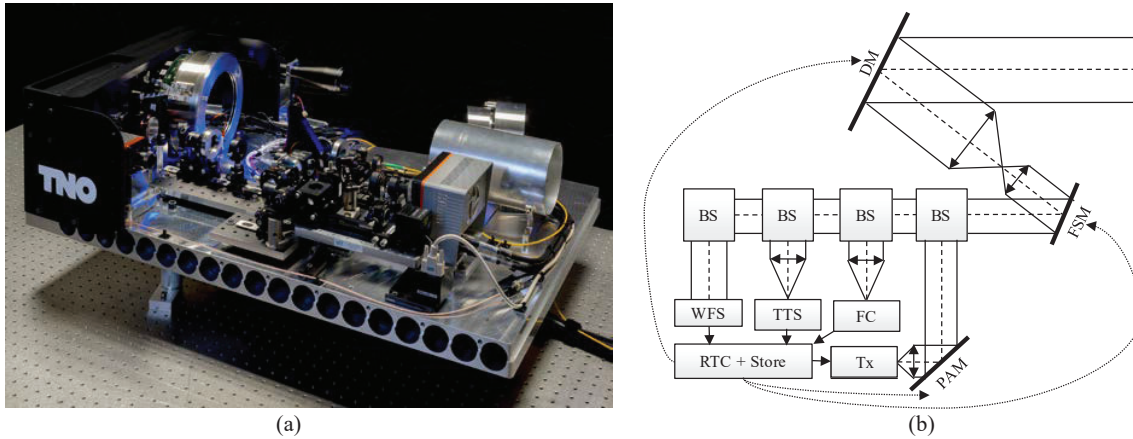


Figure 6. OFELIA breadboard (a) fully integrated breadboard (b) schematic overview of the breadboard with several beam splitters (BS), a focus camera (FC), a tip-tilt sensor (TTS), a wave front sensor (WFS), a real time computer (RTC), the transmitter (Tx), the point ahead mirror (PAM), the fast steering mirror (FSM) and deformable mirror (DM).

A collimator is used to generate a receiving laser beam. This laser beam runs over a deformable mirror (DM) and is split towards a wave front sensor and a single mode fiber. The single mode fiber has a nominal coupling efficiency of 0.74, which is mainly caused by alignment error. Residual wave front errors, that cannot be eliminated by the AO system, further limit the coupling efficiency.

The control scheme of the AO can be represented by the block diagram in Figure 7.

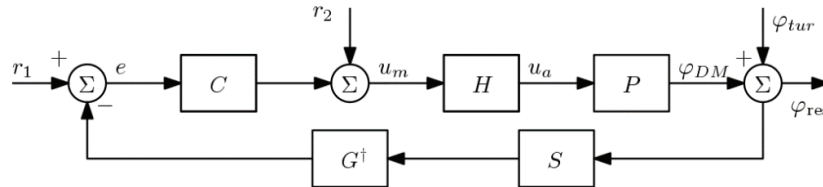


Figure 7. Control architecture with C the controller, H the modal decoupling matrix, P the DM and electronics, S the WFS and G^\dagger the decoupling matrix. In addition the signals are r the reference, e the error signal u_m the modal actuation signal, u_a the actuator signals and φ_{DM} the output, which is the deformation of the DM. The distorted wave front is represented by φ_{tur} and the residual wave front error by φ_{res} .

The deformable mirror and its electronics (P) actively correct for the wave front aberrations. In order to do so, the wave front is measured by the wave front sensor S . For the adaptive optics system architecture, we have chosen a modal correction scheme. Decoupling the modes from the wave front sensor measurement is done via the decoupling matrix G^\dagger . The matrix H is the modal coupling matrix, which couples the modal control signals u_m into the actuator control signals u_a . Hence, a reference signal r_2 corresponds to a disturbance signal of the modal shapes (e.g. Zernike shapes) at the DM, i.e. $G^\dagger S P H \approx I$ for low spatial frequencies.

In order to simulate turbulence-induced wave front errors in the experiments, the DM has been used. Individual Zernike modes with various amplitudes have been imposed on the DM, both as static and dynamic aberrations. Although using reference, r_1 would yield the modal shapes with higher accuracy, reference r_2 yields more flexibility. Adding a signal to r_2 is equivalent to a disturbing signal φ_{tur} , so the effect of the AO feedback loop can be verified.

The coupling results for the static Zernike modes are shown in Figure 8 (a). The individual Zernike modes have been imposed on the DM through reference r_2 , in open loop (i.e. without the use of the feedback loop over the controller C). The graphs show that the minimum WFE equals 90 nm RMS and consequently the FCE in these tests has a maximum value of 0.68.

The measured FCE values are fitted on the exponential function in Eq. 1. To further reduce the complexity of the approach, the SMF mode matching operation has been left out and the plain wave front phase variance is used instead. In this way, effectively the Strehl ratio (under the extended Marechal approximation) now determines the reduction of the nominal FCE. From Figure 8 (a), it can be clearly observed that the analytic model and the least-squares fit correspond well. Also, the analytical model has a slightly lower FCE than the least-squares fit. Still, the variance of the measured FCE values around the least-squares fit is relatively high. A possible explanation of this phenomenon can be found in the specific behaviour of the FCE as a function of the Zernike modal shapes. This corresponds to the analysis in [27].

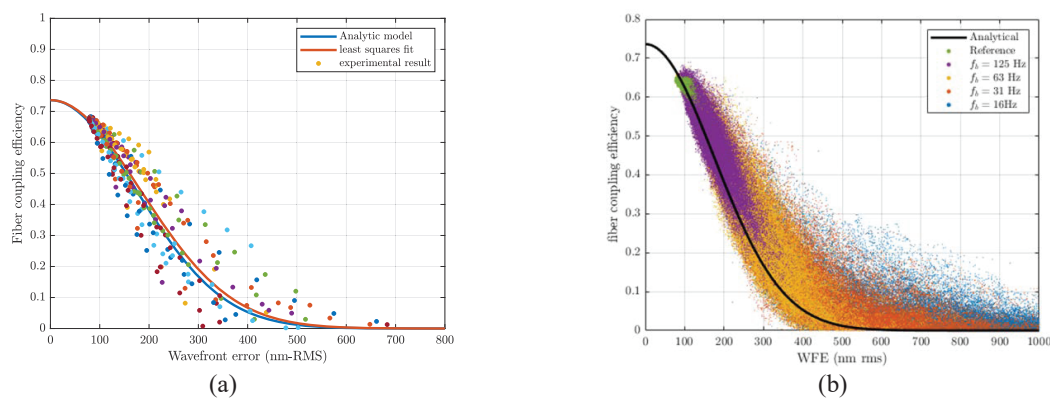


Figure 8. Fiber coupling results in the lab (a) measurements with static, individual wave front aberrations (b) measurements with dynamic aberrations following a Kolmogorov spectrum.

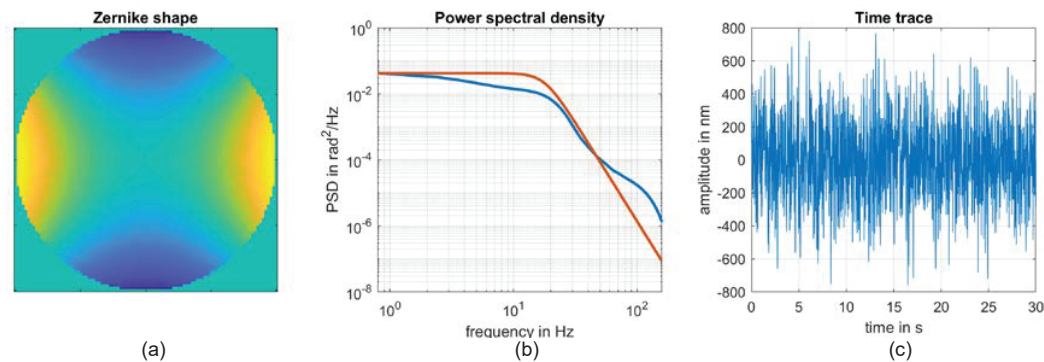


Figure 9. Dynamic response of astigmatism. (a) the spatial shape, (b) the power spectrum, the blue line is the computed spectrum, the red line is a filter approximation, (c) a time trace with the spectrum of (b).

Next to static Zernike mode aberrations, also dynamic tests, following the Kolmogorov spectrum have been done, which results are shown in Figure 8 (b). This approach is based on the Kolmogorov spectrum and the assumption of frozen flow (Taylor's hypothesis). The spatial power spectrum per mode follows from the filter expressions presented in [28]. This can be converted to a temporal spectrum by inserting the transverse wind speed model, e.g. using the Bufton model. An

example of this approach is depicted in Figure 9, where the spatial mode, the power spectrum and an amplitude time trace are shown. Time traces have been obtained for 40 Zernike modes, and have been superimposed using reference r_2 .

The FCE measurements for the dynamic Zernike test show a similar behaviour as for the static modes. It can be concluded that the basic approximation of Eq. (1) has a slight conservatism, hence it is a safe approach to use for analysis and design of the AO system. In conclusion, the basic approximation of FCE leads to the design of a regular AO system in which the wave front phase variance is to be minimized.

Besides this relation between WFE and FCE, also the ability of the AO system to follow the relation for spatial correction and temporal correction are verified. For the spatial error, turbulence signals for all Zernike modes have been injected at r_2 again. Now the controller has been switched on for a limited range of modes up to all available modes (see Figure 10 (a)). As is shown in the graph, the AO system is clearly able to follow the trend predicted by the model. For the temporal behaviour, the disturbance signal for all Zernike modes has been injected on r_2 again, and now the bandwidth has been varied from 16 to 125 Hz. Also here, this plot shows good resemblance with theory. To gain additional insight, in Figure 10 (b), the different colours represent the different bandwidths. For higher bandwidths, the resulting FCE is higher and more confined around the fitted curve. Hence, it is concluded that the AO system performs according to the known relation between wave front error and spatial and temporal correction.

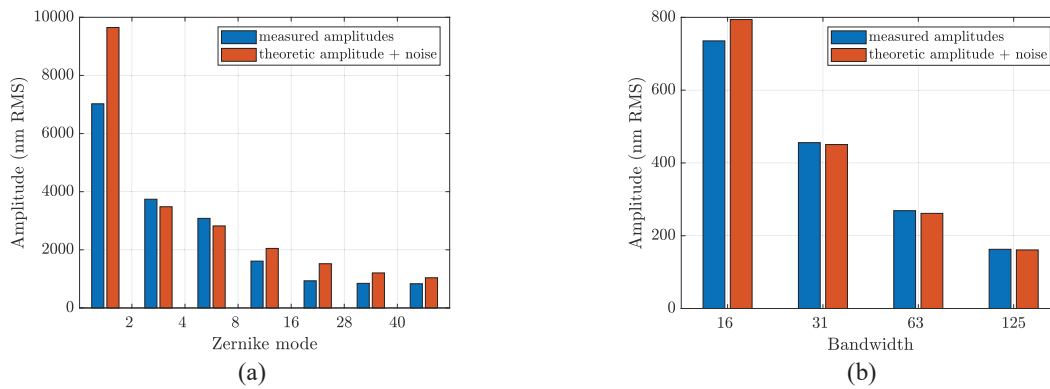


Figure 10. Experimental results for model verification. (a) relation between corrected Zernike modes and WFE. (b) relation between bandwidth and wave front error.

4.3 Adaptive Optics system design

The link budget in Table 1 aims at a wave front error loss of 4.3 dB, assuming a nominal FCE of 0.81. This implies that the AO system will have to reduce the variance of the wave front phase fluctuations down to a value of roughly 220 nm (RMS). This is similar to the requirements in QUARTZ requirements, in which the link budget allows 6 dB for the combination of optical transmission loss and fiber coupling loss. Based on the design about -1.4 dB is induced by transmission losses. Since the telescope aperture impacts the dimensioning of the AO system, it should be emphasized that the analysis below is performed in the context of the QUARTZ project.

To estimate the uncorrected beam distortion by atmospheric turbulence, a Hufnagel-Valley Cn²-profile has been assumed. A ground layer strength of $1.7 \cdot 10^{-14}$ and a pseudo-wind of 21 m/s leads to the common HV5/7 model. Furthermore, the wind speed at ground level is set to 13.9 m/s using the Bufton wind profile. With a satellite Tx diameter of \varnothing 60 mm and a Ground station Rx diameter of \varnothing 800 mm, the following beam distortion parameters can be derived as a function of elevation angle; based on expressions in [28].

The underlying expressions for computing turbulence parameters are given below. The Fried coherence length r_0 , for plane wave can be evaluated as:

$$r_0 = \left[0.423 \sec(\zeta) k^2 \int_{h_{\text{OGS}}}^{h_{\text{Sat}}} C_n^2(h) dh \right]^{-3/5},$$

in which ζ is the zenith angle, $k = \frac{2\pi}{\lambda}$ is the wave number, h_{OGS} and h_{Sat} are the altitude of the OGS and the satellite respectively, C_n^2 indicates the refractive-index structure function as a function of h , the altitude along the path. The Greenwood frequency, relevant for the required bandwidth of the AO system is:

$$f_G = 2.31\lambda^{-6/5} \left[\sec(\zeta) \int_{h_{\text{OGS}}}^{h_{\text{Sat}}} C_n^2(h) v_{\text{wind}}^{5/3}(h) dh \right]^{3/5}$$

Here $v_{\text{wind}}(h)$ is the (transverse) wind speed as a function of height. Specifically for the Z tip-tilt mode, the Greenwood frequency reads:

$$f_{G,TT} = 0.368 D^{1/6} \lambda^{-1} \sec^{1/2}(\zeta) \left[\int_{h_{\text{OGS}}}^{h_{\text{Sat}}} C_n^2(h) v_{\text{wind}}^2(h) dh \right]^{1/2}$$

To estimate the amplitude of the tip-tilt mode the angle of arrival (AoA) is relevant. Its variance is:

$$\sigma_{\text{AoA}}^2 = 2.91 \sec(\zeta) D^{-1/3} \int_{h_{\text{OGS}}}^{h_{\text{Sat}}} C_n^2(h) dh,$$

with D the aperture diameter. Evaluation of the these distortion properties for several elevation angles leads to the numbers in Table 2.

Table 2. Beam distortion parameters.

		Elevation angle ϵ				
		10	20	30	90	°
Fried coherence length	r_0	7.0	10	13	19	cm
Wave front phase error (RMS)	σ_{WFE}	1.9	1.4	1.2	0.81	μm
Greenwood frequency	f_G	122	95	91	122	Hz
Greenwood frequency Z-Tilt	$f_{G,TT}$	18	15	16	25	Hz
Angle of Arrival fluctuations (RMS)	σ_{AoA}	6.1	4.5	3.7	2.6	μrad

Clearly, these beam parameters show a strong dependence on the elevation angle. A first conclusion from this analysis is that the wave front error is relatively large ($1.4 \mu\text{m}$ at 20 degrees elevation) and hence feeding the uncorrected beam to the fiber is not an option at all. Adaptive Optics is a prerequisite to arrive at acceptable values of FCE.

The focus in designing the AO system has been put on the case of 20 degrees elevation angle. Specific design choices for the AO system are:

Table 3. Main parameters of the AO system

AO system parameter	value
Number of DM actuators	192
Number of WFS sub-apertures	17 x 17 grid
Detector frame-rate	5000 Hz
AO loop latency	0.3 ms
Closed-loop bandwidth	600 Hz
TT stage closed-loop bandwidth	400 Hz

In the selection of AO system parameters, the spatial error and the temporal error have been balanced. Next to the fitting error and the latency error, the vibrations-induced tip-tilt error (which are the non-turbulence induced errors, like alignment errors, vibration induced tip/tilt errors, drift and stability) is a major source of residual phase error. The typical use case pre-scribes that the OGT is able to be placed on high-rise buildings. These buildings come with significant vibrations induced by wind and ground vibrations, tilting the full OGT. These vibration not only affect the telescope pointing and tracking directly, but also indirectly by introducing vibration in the telescope structure itself. Analysis has shown significant tip/tilt errors, and although being suppressed by the AO system a considerable residual could remain. Given the AO system parameters and the description of the individual error sources in for instance [25], we arrive at the budget given in Table 4. All error sources have been verified using an end-to-end AO system simulation.

Table 4. System errors determining the residual WFE at 20 degrees elevation angle

AO system errors	value (RMS)	Other	value (RMS)
Fitting Error	84 nm	Alignment and Vibrations-induced tip-tilt errors	158 nm
Wave front sensor precision	21 nm	Margin	100 nm
Calibration and chromatic Error	14 nm		
Bandwidth error	53 nm		
Latency error	68 nm	Total WFE	224 nm
Tip-tilt error (atmospheric)	10 nm		

In conclusion, the residual of 224 nm (RMS) wave front error would lead to a reduced fiber coupling efficiency by a factor of 0.43 and hence an additional loss of 3.6 dB above the nominal fiber coupling loss in the case of a flat incident wave front. Having a nominal loss of 0.85 (as created by the beam shaper), the total fiber coupling loss using a dedicated AO system then arrives at 4.3 dB.

5. PERSPECTIVE ON GROUND STATION TECHNOLOGIES FOR QKD

5.1 Perspective on QKD-node Earth Orbit

The presented OGT design is primarily driven by the BB84 protocol with a satellite service node orbiting at LEO. The BB84 approach is relatively mature, for which subsystems have been demonstrated in laboratories or in relevant environments and even a comparable full end-to-end system has already been demonstrated [14, 15]. With an overpass time of (only) a few minutes, a LEO satellite based service could offer near global coverage. Altogether, this makes it a logical step for a first product line and QKD service.

Several alternatives for both satellite orbit and QKD protocol exist. For instance a QKD service from a GEO-satellite system would not be limited by the overpass time of a LEO-node and the link can be preserved for a long time. On the other hand, a GEO satellite link will encounter a much higher link loss, which inevitably leads to a lower key rate. Technologies – such as discussed in the previous sections - that will lead to a reduction of the link loss very much apply to the GEO-node case as well.

A relatively large region – say the size of a continent - could be serviced by a single GEO-satellite continuously. This makes it an attractive node for entanglement-based QKD, sharing keys between 2 (very) remote users; from a LEO orbit the distance between Alice and Bob would be restricted. Entanglement based QKD is a very attractive protocol from a security perspective [8]. This makes it suitable for users demanding ultimate security such as governments and MOD's. For now however, trusted-node LEO systems based on BB84 for instance are regarded as a more mature and cost effective solution, which offer an acceptable security level for the majority of users .

5.2 Perspective on ground stations applications for QKD

The distribution of quantum keys over FSO channels offers several benefits. First of all, it overcomes the distance limit of fiber-based QKD, which is caused by the higher transmission loss. Second, naturally occurring obstructions, such as oceans or mountains can make it rather complex and expensive to deploy a fiber network. Then, an FSO link can be an attractive, alternative channel to distribute quantum keys. This FSO link could be a direct ground-to-ground connection or via a satellite node.

Achieving a sufficiently high secure key rate for a satellite-based QKD protocol requires advanced technologies to restrict the quantum channel loss and noise levels. Reduction of the OGS cost will therefore remain to be a critical design driver for this generation of QKD systems. For the specific OGT design discussed in this paper, there are two sub-systems that play a significant role in the overall cost: the telescope and the AO system. In this QUARTZ design, a main driver is the need for a single-mode fiber based detector. Therefore, optical imaging quality of the receiver was required, leading to the demand of a very low wave front phase error and hence an AO system and a high optical quality telescope. Future developments in for instance multi-mode fiber coupled or free space detectors with large detector areas may be beneficial to effectively lead to a cost reduction for OGS's in satellite-based QKD.

6. CONCLUSIONS

Satellite-based QKD has the potential to cover larger distances than optical fiber based QKD, due to lower transmission loss of the channel. By evaluating the BB84 protocol it is shown that it is possible to reach a 20 degrees elevation angle link with a LEO satellite and still be able to distil a key. In this evaluation it is shown that background radiation is dominant over the detector noise during day-time conditions.

To enable a high key rate QKD, a design study has been presented for the optical ground station. The optical bench is placed in the Cassegrain focus to avoid complexity related to the rotation of the telescope and minimize optical elements. To reduce the effect of the donut shaped top-hat irradiance profile sampled by the OGT on the fiber coupling, a beam shaper is proposed. This beam shaper improves the nominal fiber coupling efficiency from 64% to 85%. To cope with a large range of environmental conditions, the optical bench has a dedicated thermo-mechanical design. The optical bench is put in an enclosed compartment to reduce thermal convection, and the interface with the telescope is devised by a double glass window. Furthermore, the optical ground station has been equipped with an adaptive optics system to compensate for atmospheric turbulence. It consists of a DM with 197 actuators and a Shack-Hartmann wave-front sensor with 17x17 sub-apertures and a real-time controller with a (closed-loop) bandwidth of 600 Hz. In this way, a high-performance adaptive optics architecture is achieved by balancing and strongly limiting the spatial and temporal errors.

In order to verify the design guidelines used for the adaptive optics system for reaching high fiber coupling efficiency, experiments on a laboratory setup have been performed on a comparable breadboard. To this end, wave front errors have been applied by the DM having a representative amplitude and temporal behaviour for turbulence induced perturbations. The pragmatic approach by modelling fiber coupling efficiency through the Strehl ratio is proven to be an effective first order estimate.

Using the proposed technology channel loss can be reduced to 27.2 dB for an elevation angle of 20 degrees. This enables the use of QKD from a low earth orbit to earth during day-time conditions. These conclusions can be extrapolated to other protocols than BB84, e.g. channel losses are generic for QKD applications. In addition, cost effective OGS with large apertures are a common need to support QKD links, regardless of the QKD protocol. From these findings, it is concluded that an additional step has been made to come to the realization of QKD services around the globe.

7. REFERENCES

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: public-key distribution, and coin-tossing," in *International Conference on Computers, Systems & Signal Processing*, Bangalore, 1984.
- [2] H. Yin, T. Chen, Z. Yu, H. Liu, L. You, Y. Zhou, S. Chen, Y. Mao, M. Huang, W. Zhang and H. Chen, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.
- [3] D. Vasylyev, W. Vogel and F. Moll, "Satellite-mediated quantum atmospheric links," *Physical review*, vol. 99, no. 5, 2019.
- [4] F. Laudenbach, C. Pacher, C. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations," *Advanced quantum technologies*, vol. 1, no. 1, 2018.
- [5] S. Liao, C. W. W. Liu, L. Zhang, Y. Li, J. Ren, J. Yin, Q. Shen, Y. Cao, Z. Li and F. Li, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43-47, 2017.
- [6] R. Bedington, J. M. Arrazola and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, pp. 1-12, 2017.
- [7] "The future is quantum: EU countries plan ultra-secure communication network," European Union, 13 06 2019. [Online]. Available: <https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>. [Accessed 7 01 2021].
- [8] B. Dirks, I. Ferrario, A. Le Pera, D. Vito Finocchiaro, D. de Lange, H. de Man, A. Meskers, J. Morits, N. Neumann, R. Saathof and G. Witvoet, "GEOQKD: Quantum Key Distribution from a geostationary satellite," in *ICSO Proceedings*, 2021.

- [9] M. Dresscher, W. Korevaar, N. v. d. Valk, D. d. Lange, R. Saathof and N. Doelman, "Key Challenges and Results in the Design of cubesat laser terminals, optical heads and coarse pointing assemblies," in *IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2019.
- [10] R. Saathof, W. Crowcombe, S. Kuiper, N. v. d. Valk, F. Pettazzi and D. d. Lange, "Optical satellite communication space terminal technology at TNO," in *Proc. SPIE*, 2019.
- [11] S. Kuiper, W. Crowcombe, J. Human, B. Dekker, E. Nieuwkoop, A. Meskers and W. v. d. Hoogt, "Kuiper, Stefan, et al. "Hight bandwidth and compact fine steering mirror development for laser communications," in *ESMATS*, 2017.
- [12] G. Witvoet, S. Kuiper and A. Meskers, "Performance validation of a high-bandwidth fine steering mirror for optical communications.," in *ICSO*, 2018.
- [13] R. Saathof, R. d. Breeje, W. Klop, S. Kuiper and N. Doelman, "Optical technologies for terabit/s-throughput feeder link," in *ICSOS*, 2017.
- [14] R. Saathof, R. den Breeje, W. Klop, N. Doelman and T. Moens, "Pre-correction adaptive optics performance for a 10 km laser link," in *Proc. SPIE*, 2019.
- [15] F. Silvestri, F. Pettazzi, M. Eschen, J. J. Boschma, J. B. Lutgerink, G. F. Kramer, W. C. Korevaar, R. d. Breeje, C. M. Duque and N. J. Doelman, "Beam multiplexing for satellite communication optical feeder links," in *SPIE*, 2020.
- [16] H. B.-P. Valerio Scarani, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.* , vol. 81, p. 1301 , 2009.
- [17] X. Ma, B. Qi, Y. Zhao and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physics Review A*, vol. 72, p. 012326, 2005.
- [18] M. T. Gruneisen, M. B. Flanagan, B. A. Sickmiller, J. P. Black, K. E. Stoltenberg and A. W. Duchane, "Modeling daytime sky access for a satellite quantum key distribution link," *Optics Express*, vol. 23, no. 18, p. 23924, 2015.
- [19] J. H. Shapiro, "Scintillation has minimal impact on far-field Bennett-Brassard 1984 protocol quantum key distribution," *Physical review*, vol. 84, no. 3, 2011.
- [20] M. Toyoshima, T. Jono, K. Nakagawa and A. Yamamoto, "Optimum divergence angle of a Gaussian beam wave in the presence of random jitter in free-space laser communication systems," *JOSA*, vol. 19, no. 3, pp. 567-571, 2002.
- [21] M. Chen, C. Liu and H. Xian, "Experimental demonstration of single-mode fiber coupling over relatively strong turbulence with adaptive optics," *Applied Optics*, vol. 42, no. 29, pp. 8722-8726, 2015.
- [22] Y. Li, D. Zheng and J. Wu, "Free space to single mode fiber coupling efficiency improvement using wave-front sensorless adaptive optics," *Asia communications and photonics*, 2016.
- [23] H. Wu, H. Yan and L. X., "Modal correction for fiber-coupling efficiency in free-space optical communication systems through atmospheric turbulence," *Optik*, pp. 1789-1793, 2010.
- [24] R. J. Noll, "Zernike polynomials and atmospheric turbulence," *JOSA*, vol. 66, no. 3, pp. 207-211, 1976.
- [25] J. Hardy, *Adaptive Optics for Astronomical Telescopes*, Oxford University Press, 1998.
- [26] C. Ruilier, "A study of degraded light coupling into single-mode fibers," in *Proc. SPIE 3350, Astronomical Interferometry*, (24 July 1998); doi: 10.1117/12.317094, 1998.
- [27] C. Ruilier and F. Cassaing, "Coupling of large telescopes and single-mode waveguides: application to stellar interferometry," *J. Opt. Soc. Am. A*, vol. Vol. 18, no. No. 1, pp. 143-149, 2001.
- [28] L. Andrews and R. Philips, *Laser beam propagation through random media*, Bellingham, Washtington USA: SPIE Press, 2005.