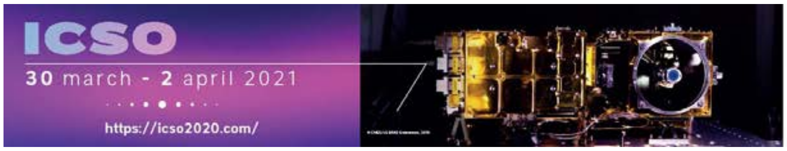
International Conference on Space Optics—ICSO 2020

Virtual Conference

30 March–2 April 2021

Edited by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas



GEOQKD: quantum key distribution from a geostationary satellite

International Conference on Space Optics — ICSO 2020, edited by Bruno Cugny, Zoran Sodnik,
Nikos Karafolas, Proc. of SPIE Vol. 11852, 118520J · © 2021 ESA and CNES
CCC code: 0277-786X/21/$21 · doi: 10.1117/12.2599164

GEOQKD: Quantum Key Distribution from a geostationary satellite

Bob P.F. Dirks*[a], Ivan Ferrario[a], Alessandro Le Pera[b], Daniele Vito Finocchiaro[b], Marine Desmons[a], Dorus de Lange[a], Harry de Man[a], Arjan J.H. Meskers[a], Jaco Morits[a], Niels M.P. Neumann[a], Rudolf Saathof[a], Gert Witvoet[a]

[a]Netherlands Organisation for Applied Scientific Research (TNO), Stieltjesweg 1, 2628 CK, Delft, The Netherlands;
[b]Eutelsat SA, 32 Boulevard Gallieni, 92130 Issy-les-Moulineaux, France

ABSTRACT

Due to the distance limitation of quantum communication via ground-based fibre networks, space-based quantum key distribution (QKD) is a viable solution to extend such networks over continental and, ultimately, over global distances. Compared to Low Earth Orbits (LEO), QKD from a Geostationary Orbit (GEO) offers substantial advantages, such as large coverage, continuous link to ground stations (cloud cover limited), 24/7 operation (background limited), and no tracking required. As a downside, QKD from GEO comes with large link losses due to the space-ground distance, lowering the achievable key rates. From our feasibility and conceptual design study it is concluded that although link losses are high, QKD from GEO is technically feasible, and a favourable solution if the satellite needs to act as an untrusted node (that is, no security assumptions required for the space segment). However, the optimal solution, generating a higher value-for-money, is to have the possibility to operate it in trusted mode as well, as higher key rates can be obtained. But this will be at the cost of security as key material needs to be (temporarily) stored on board of the satellite. In order to arrive at a minimum required secure bit rate of ~1 bit/s in untrusted mode, two ~0.5m diameter telescopes in the space segment are required with <0.65μrad pointing accuracy each, a >1GHz entangled photon pair generation rate, in combination with ~2.5m diameter telescopes on ground, operating at 810nm wavelength. In trusted mode, with the same optical system but only using one telescope in the space segment, a factor of ~300 to ~10000 more key can be obtained. Details on our assumptions and results and drawings of the high level system design are presented, as well as a description of the required technology improvements and building blocks needed, which is applicable to non-GEO applications as well.

Keywords: Quantum Key Distribution, QKD, geostationary, optical satellite communication, quantum communication, cryptography

1. INTRODUCTION

Quantum communication, and Quantum Key Distribution (QKD) in particular, is an increasingly accepted means for future secure communications thanks to its capability to securely distribute symmetric keys, which can serve as input to quantum-safe encryption protocols such AES and the information theoretically secure one-time pad. There is a growing interest in QKD as a technique to safeguard communications from future quantum-based attacks. Based on quantum mechanical principles (superposition, entanglement, and no-cloning) QKD allows to detect any eavesdropping in the transmission channel.

Due to the distance limitation of quantum communication via ground-based fibre networks, space-based QKD is a viable solution to extend these networks over continental and, ultimately, over global distances. QKD from a Low Earth Orbit (LEO) has been demonstrated by Chinese researchers using the Micius satellite[1,2,3], and commercial QKD solutions for LEO could become available over the next few years[19]. QKD from a geostationary orbit (GEO) would offer substantial advantages[4] over LEO. GEO satellites have a circular geosynchronous orbit 35,786 km above Earth's equator where it appears at a fixed position in the sky to ground observers. Ground stations that communicate with these satellites have to apply only very limited tracking, GEO satellites are still slightly moving, and can be pointed permanently at nearly the same position in the sky where the satellite is located. In comparison, satellites in LEO with an altitude of 2,000 km or

*bob.dirks@tno.nl; phone +31 652803623; www.tno.nl

less pass with at least ten orbits per day (with a different ground track per pass). Also, when providing a QKD service from space, GEO satellites offer a distinct benefit over LEO satellites due to the high link availability (weather permitting) and large coverage over relevant locations on ground.

These advantages have also been identified by TNO's partners Eutelsat and CGI-NL. Eutelsat's vision is that secure communication needs are dramatically evolving over the last years, pushed by quantum computing evolutions but also by perceived needs of security in several layers of today's Information Society. The continuously increasing quantity of data exchanged requires stronger security practices and a differentiation of means. QKD could become one of the future solutions to fulfil these needs. By focusing on QKD from a geostationary orbit, the company distinguishes itself from other space based QKD initiatives[7,8] which are mainly directed towards LEO satellites.

For both Eutelsat and CGI-NL it is important that feasibility of GEOQKD is investigated using commercially viable needs and requirements such as realistic key rates, number of ground stations, size limitation of ground and space segment, etc. In the most secure setting the satellite acts as an untrusted node, therefore requiring no additional security assumptions. In practice this means that there is no way that a potential eavesdropper could obtain information on the key even if it has full control over the satellite. However, to be more flexible with respect to user requirements, less secure settings, where satellite becomes a "trusted" element of the system, should be investigated as well.

In this paper we will present the results of our feasibility and high level system design study on GEOQKD which is split into two phases: Phase 1 focuses on investigating the technical feasibility of QKD from GEO with the satellite preferably acting as an untrusted node, as illustrated by the left part of Figure 1. As an alternative to an untrusted node, a trusted node concept is considered as well, also from GEO. Here, secure bits are (temporarily) stored on board of the satellite as illustrated by the right part of Figure 1. This requires strict security measures to prevent key material leaking to an eavesdropper (either intentionally or unintentionally). Phase 1 also includes an investigation of key parameters and constraints, as well as secure rate estimations and a detailed characterization of the space-ground link.

In Phase 2 the focus is on the high-level system design of the space and ground segment, with an emphasis on the space terminal, including several detailed analyses to confirm feasibility. Here we build on TNO's knowledge and expertise gained in different optical satellite communication projects[16,18]. A technology roadmap is compiled with key technologies required for GEOQKD.

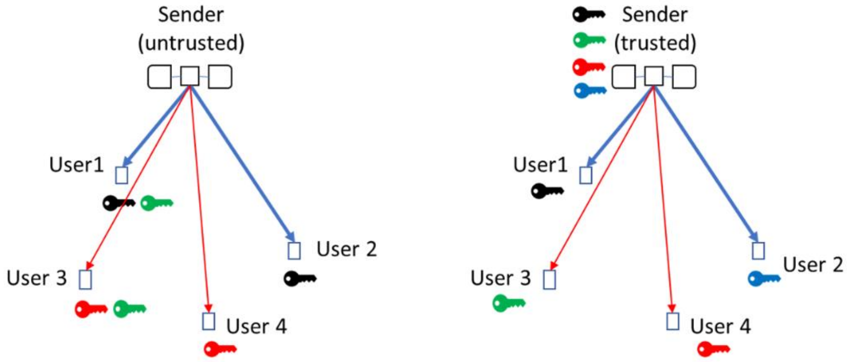


Figure 1. Two concepts studied in GEOQKD. Left: the satellite acts as an untrusted node, allowing to generate secure bits between different users on ground. Right: the satellite acts as a trusted node, creating keys between satellite and users on ground.

2. PHASE 1 FEASIBILITY

2.1 Use case, user requirements and constraints

For the study a realistic use case of a financial company was used, which requires the distribution of symmetric keys (type AES256 at minimum) to clients on ground who wish to securely communicate. Clients are located in the main European financial centres, these cities often separated by hundreds of kilometres. The number of clients varies between 10 to 100. The use case focuses on Europe but a worldwide coverage is desired. The key distribution protocol shall be information theoretically secure. The shared part of the system, here the space segment, shall be untrusted. The security parameter (relevant for the key distillation) shall be $\varepsilon = 10^{-12}$. Using these and additional requirements on key type, lifetime and storage time, a minimum required secure key rate of 1 bit/s is obtained during key exchange. Due to company confidentiality reasons no specifications on these other requirements can be given.

2.2 Concept

Untrusted mode. With the use case as input, as a baseline concept, a system implementing the BBM92 QKD protocol[5] is used; it allows to have the space segment acting as an untrusted node. It is equipped with a high rate, polarization entangled photon pair source. Each of the photons of a pair shall be guided via an optical system to two optical transmitters which shall send the photons to two ground receivers (called Alice and Bob). The receivers shall be capable to receive the photons, to analyse their polarization state, and to detect them individually. Both a free space and fibre-based connection to the detectors is considered, but the free space concept is taken as the baseline given the lower link loss which can be achieved and its simpler implementation.

The system shall further allow for precise time synchronization and time-stamping of the photon detections at Alice and Bob in order to synchronize their measurement outcomes, and correctly correlate them. The system shall be able to authenticate Alice and Bob and to allow for classical communication between both receivers so that the BBM92 protocol, including error correction and privacy amplification, can be executed, eventually leading to an identical string of random bits at Alice and Bob. The ground segments are considered fixed locations in or near financial centres on the European continent.

As an alternative to BBM92, Measurement Device Independent (MDI-)QKD[12] is also considered as a protocol, as it also allows for an untrusted node in space. However, it requires two uplink channels to a central receiver in the satellite which leads to significantly more link loss compared to a downlink scenario (due to influence of turbulence)[18]. Moreover, it has very challenging spectral, spatial, temporal, and polarization-related requirements (e.g. photons sent by the two users on ground must arrive simultaneously and shall be indistinguishable in the beforementioned degrees of freedom) which makes this protocol less suited for a GEOQKD mission. Although developments in Continuous Variable (CV-)QKD protocols advance, their Technology Readiness Level (TRL)[9] seems to be too low to be suited for GEOQKD applications.

Trusted mode. As an alternative concept, an implementation of prepare-and-measure QKD from GEO is considered as well, as it is expected to achieve higher key rates. Here the space segment will act as a trusted node, as key material will be (temporarily) stored on board of the satellite, thus requiring additional security assumptions. It shall contain a source able to emit qubits (either true single photons or weak coherent pulses) over a single link to a ground-based receiver, polarization encoded,. Similar to the baseline concept, the receiver shall be able to collect, analyse and detect the individual photons. Here, a proper time synchronization will be needed between the space and ground segment in order to correlate the photon information of sender and receiver. Also, a classical communication channel is required for authentication and exchanging classical information for the key distillation part of the QKD protocol. In this way, an identical key is created in the space and ground segment. When users on ground want to share a key using this concept, the protocol shall be executed twice, first with User 1, generating key K1, and then with User 2, generating K2. The space segment contains both keys. Combining both keys via and XOR operation and publicly sending this string via classical means to one of the two users will allow the latter to obtain the other key.

For the prepare-and-measure QKD protocols, we consider BB84 with decoy states[6] and BBM92 in trusted mode. For BBM92 in trusted mode one of the photons of an entangled pair is directly measured on board of the spacecraft, while the other one is sent to a user on ground. The standard BBM92 protocol can be applied except that key material will now be generated on board of the satellite and on ground. The satellite, more precisely the payload, containing information on the key, must therefore act as a trusted node, similar to the case of BB84 with decoy states. This particular implementation of BBM92 has already been demonstrated by Chinese researchers using the Micius satelllite[3].

2.3 Key rate estimations

In order to compare the different QKD protocol implementations, secure key rate estimations have been made for BBM92 in untrusted mode (both photons sent to ground), BB84 with decoy states, and BBM92 in trusted mode. In addition, a high level assessment has been made of the complexity of implementation and the expected security of the protocols. The security aspect scores ‘high’ for the untrusted node in the space segment, whereas the trusted node in the space segment scores ‘low’ for the security aspect. For the key rate estimations, a source rate of 10GHz is used, defined as the inverse of the coincidence window at the receiver side, which is again determined by the total jitter of the detection system, which for the used system is 100ps. The optimized mean pair generation probability of the source is μ=~0.1 per detection window. Background counts, which are all detection events not attributed to the quantum signal, are set to ~1,000Hz. The polarization error is set to 1%, and the security parameter of the protocol ε is set to 10^{-12}. The model incorporates finite size effects.

The key rate model for BBM92 untrusted mode shows that a ~1 bit/s secure bit rate can be achieved at a maximum link loss of ~41dB per link (so ~82dB for both links – see next section for link loss computation). The key rate for the other two protocols is also estimated at this link loss. The results are summarized below in Table 1.

Table 1. Assessment of selected QKD protocols.

Protocol	Total link loss	Estimated key per day (based on 3-6h link time)	Security	Complexity
BB84 decoy	~41dB	**~100Mbit**	**Low**	**High**
BBM92 untrusted	~82dB (2x41dB)	**~10kbit**	**High**	**Low**
BBM92 trusted	~41dB	**~3–10Mbit**	**Low**	**Medium**

It is important to mention that for every classical communication round in the protocol, secure bits are required for authentication. While for the first authentication rounds a pre-shared secret must be used, for subsequent rounds secure bits from the generated QKD key can be used, resulting in less key material available for data encryption. The number of authentication bits per round and the number of classical communication rounds depend on the chosen security parameter; in our case ε=10^{-12}. Figure 2 shows the estimated usable bits as a function of link time for the BBM92 protocol in untrusted mode.

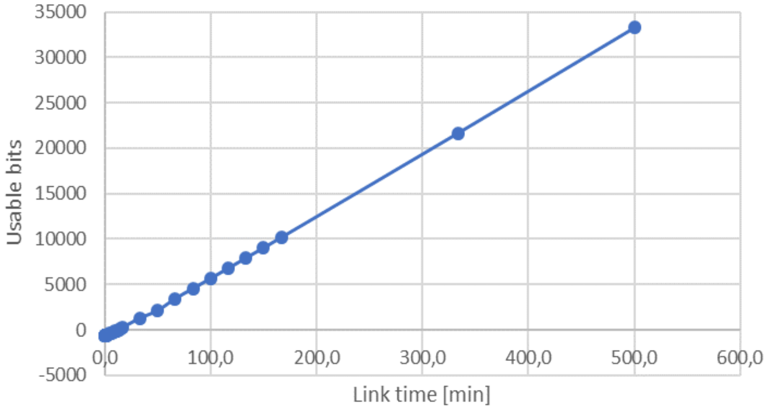


Figure 2. Simulated number of usable bits as a function of link time for the BBM92 protocol in untrusted mode, assuming a security parameter of 10^{-12}, dark count of 1000Hz, a source rate of 10GHz, 2x41dB link loss and an error correction efficiency of 1.22.

The choice of protocol will strongly depend on the specific use-case and corresponding user requirements. If it is acceptable to put a certain trust into the satellite, the payload manufacturer or the service provider, then the BB84 protocol with decoy states will be most suited given its high achievable key rates. However, it comes with high complexity because it must guarantee indistinguishability of signal and decoy states in all degrees of freedom (or at least exactly quantified). Also, pulse intensities need to be monitored in real time. Moreover the modulation of the intensities as well as the polarizations in the ~10GHz regime and the storage and handling of this information at that rate, is extremely challenging and comes with an important operational complexity. On the other hand, no single photon detectors will be required in space.

If the use case requires ultimate security in combination with moderate key rates, then BBM92 in untrusted mode provides the best solution. Additional advantage is that it also allows for a trusted mode implementation using the same system with which >~300x more key material can be generated, but which is simpler to realize than the BB84 with decoy states implementation at these high rates. A disadvantage is however, that single photon detectors are required in the space segment.

2.4 Link budget

From the key rate estimates it is concluded that a maximum loss of 41dB per link is allowed. Using TNO's link budget tool, a detailed analysis is performed on the expected losses as a function of relevant system and link parameters, resulting in a set of system characteristics required to achieve the 41dB link loss. Below in Table 2 the used input parameters are given and explained.

Table 2. Input parameters used for the link loss analysis.

Input parameter	Value	Remarks
Source repetition rate	10 GHz	Corresponds to maximum detection rate as determined by system jitter (=100ps)
Background rate	1000 Hz	This includes false counts coming from stars, atmosphere, Moon, reflection spacecraft, etc., as well as the detector dark counts.
Wavelength (λ)	810 nm	Of the quantum signal (see Section 2.5)
Wavefront error (WFE) (≤λ/10)	81 nm RMS	Summed WFE of all optical components in transmitter telescope; challenging due to quality optical components, stability, alignment.
Block size (number of successful coincidences)	1e5 bits 1e7 bits	For BBM92 For BB84 decoy (larger block size possible thanks to lower loss)
Obscuration ratio (linear)	30%	Of the ground telescope; space telescope is not obscured.
Optical bench transmission loss	-1 dB	Space segment
Optical bench transmission loss	-1 dB	Ground segment
Atmospheric absorption and scattering	-1.5 dB	Including a 0.25dB margin
Cirrus clouds	-1 dB	~1 km of Cirrus clouds considered (matching good weather conditions)
Detector efficiency	~85%	Valid for existing SNSPDs.
Ground station latitude	52.37º	For the Netherlands (line-of-sight distance to satellite: ~38,598,331km)
Coupling to detector	Free-space	Currently not yet compatible with SNSPDs as these are fibre-coupled.
Adaptive Optics (AO)	No	Not needed for free space coupled detectors.

Besides these fixed input parameters, variable system parameters are used to obtain the total link loss. The most relevant are the transmitter and receiver telescope aperture diameters and the pointing accuracy of the space segment (split into a static and dynamic component). Below in Table 3 four configurations are presented. The highlighted configuration is used as input to the high level system design of Phase 2, and has a 0.5m diameter space telescope diameter, a 2.5m ground receiver diameter and a 0.65µrad static and dynamic pointing accuracy. First assessments based on low-order dynamic analyses on the expected vibrations on the satellite and sensor noise propagation shows that a pointing accuracy down to 0.25µrad seems possible as well. This would allow for a smaller ground telescope of ~2m diameter. The secure bit rates for BBM92 in untrusted and trusted mode and BB84 decoy are also shown in the same table. For BBM92 in trusted mode, two scenarios are analysed: one with a maximum on-board detection rate of ~10MHz (current detector performance) and one with ~600MHz detection rate. The latter would require a specific detector multiplexing scheme in which the incoming photons are divided over multiple detectors. It has to be emphasized that the average pair generation rate of the source, and therefore the laser power, must be lowered in order not to saturate the on-board detectors. In fact, laser power must be tuned to the given maximum on-board detection rate. Taking the case of 41dB loss per channel, a ~1.1bit/s key-rate for BBM92 in untrusted mode can be achieved; for trusted mode key-rates of ~330bit/s to almost ~10kbit/s are possible; and for BB84 decoy state a ~86kbit/s key-rate is achievable. Clearly, achievable key rates increase if losses can be reduced, but this will have direct consequences on other system parameters. For example, in order to lower the loss to 36dB per link while keeping the size of the space segment the same, a receiver diameter of at least ~4.1m will be required. This makes practical implementations significantly more difficult. It must be noted that we keep the transmitter diameter in the space segment fixed to 0.5m, which is considered as an optimal size in terms of telescope gain, pointing loss, but also still realistic to manufacture and affordable.

Table 3. Link loss scenarios for 810nm wavelength.

Link loss:	**41**	**41**	**39.5**	**36**
Transmitter diameter	0.5m	0.5m	0.5m	0.5m
Bit rate BMM92 untrusted	1.1bit/s	1.1bit/s	2.3bit/s	11.5bit/s
Bit rate BBM92 trusted	~330bit/s @10MHz ~9.5kbit/s @600MHz	~330bit/s @10MHz ~9.5kbit/s @600MHz	Not simulated	Not simulated
Bit rate BB84 decoy	85.9kbit/s	85.9kbit/s	123.1kbit/s	282.0kbit/s
Receiver diameter	2.5m	2m	2.9m	4.1m
Pointing accuracy	0.65µrad	0.25µrad	0.65µrad	0.6µrad

2.5 Wavelength choice

The QKD signal wavelength is an important parameter, as it directly influences the atmospheric and optical fibre transmissions, diffraction, detection efficiency, laser availability etc. We considered two wavelengths: 810nm and 1550nm. The former, 810nm, is typically used in spontaneous parametric down-conversion (SPDC) sources[2,10] whereas 1550nm is the standard telecom wavelength. The advantage of using 810nm wavelength is that it has less diffraction, and is compatible with efficient and relatively cheap single photon detectors (e.g. SiAPDs). The advantage of using 1550nm wavelength is that it has lower atmospheric absorption and is compatible with standard telecom fibres, but this comes at the cost of higher diffraction and less efficient detectors, such as those based on InGaAs.

The corresponding link budgets at these wavelengths have been compared, using the same optical system for the space and ground terminal. In case of a free space coupling to detectors, the link loss turns out to be similar for both wavelengths (the advantages and disadvantages cancel out). However, the 1550nm wavelength is favourable in terms of link loss in cases where the QKD signals are first coupled into and transported via a single mode fibre, before being analysed and detected. Here we assume the use of adaptive optics (AO) for both wavelengths to limit coupling losses to the fibre. Yet even with 1550nm, link losses are still significantly higher (+~5dB) than those resulting from free space coupling; this limits the achievable secure key rate to <0.1 bit/s using fibre. In order to still achieve a ~1 bit/s key-rate in this fibre-coupled configuration, the ground telescope diameter must be increased to ~5m.

As for the current baseline there is a strong preference for a relatively simple and less expensive system (so without implementation of a complex AO system), 810nm is chosen for the baseline system design. However, it must be emphasized that for a future Quantum Communication Infrastructure (QCI), where space- and ground-based fibre networks will be integrated, 1550nm may be more suitable. Also, it would allow to share the large and expensive optical ground terminal with multiple users, each connected to it via a fibre, as illustrated below in Figure 3. The measurement device, which must be ‘trusted’ can be located at a protected site at the user’s premises, while the shared ground receiver, can remain ‘untrusted’.

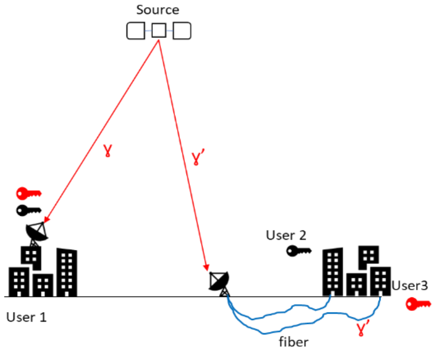


Figure 3. Sketch illustrating the two possible configurations of a free space and fibre coupling to detectors. Left: User 1 receives photons from the satellite containing the entangled photon source. These are directly measured near the telescope using a free-space link to the detectors. Right: photons are collected using a shared telescope, ideally outside an urban area; photons are coupled into an optical fibre leading the photons, via optical switches, to different users.

2.6 Cloud coverage

Another important parameter is cloud coverage. Clouds limit the QKD link availability and therefore have a strong impact on the overall feasibility of the QKD system, both on the technical level (too high a loss) and on the commercial level (insufficient key material to fulfil the use case). Especially for an entanglement-based concept, in which two simultaneous free line-of-sights are needed, this can significantly limit link time. Seeing the high risk and impact, an in-depth analysis was performed to estimate link availability to relevant (financial) centres in Europe. Both single and double links have been investigated based on geostationary satellite data[11] from MVIRI/SEVIRI radiometers on board the geostationary Meteosat satellites.

Using historical data on cloud coverage, a good indication is obtained on average total cloud free periods. This is important for receiver site selection and/or to get an average link availability on a yearly, monthly, or even daily basis. When using these data in combination with cloud cover predictions, one can efficiently make use of the available cloud free periods. During these periods it is assumed that the link loss is limited to 41dB per link.

The analysis resulted in plots showing the available link time for single and dual links to different cities in Europe. In Figure 4 the cumulative number of days/nights is shown which have more than a certain number of available dual-link minutes over the years 2012 to 2015, between Amsterdam and Budapest. It shows for example that in 2015 at least 50 nights were available with in total more than 240min of dual-link time. Beside this specific city-pair, other dual links have been analysed as well, resulting in similar plots. For all dual links considered it is concluded that during at least 10 nights per year a total link time of 400min/night can be achieved. We only consider night-time operation because of the achievable ~1000Hz of background count rate. For daytime operation, significantly higher backgrounds rates are to be expected, which, without additional filtering, will significantly limit the maximal allowable loss and achievable key rate.

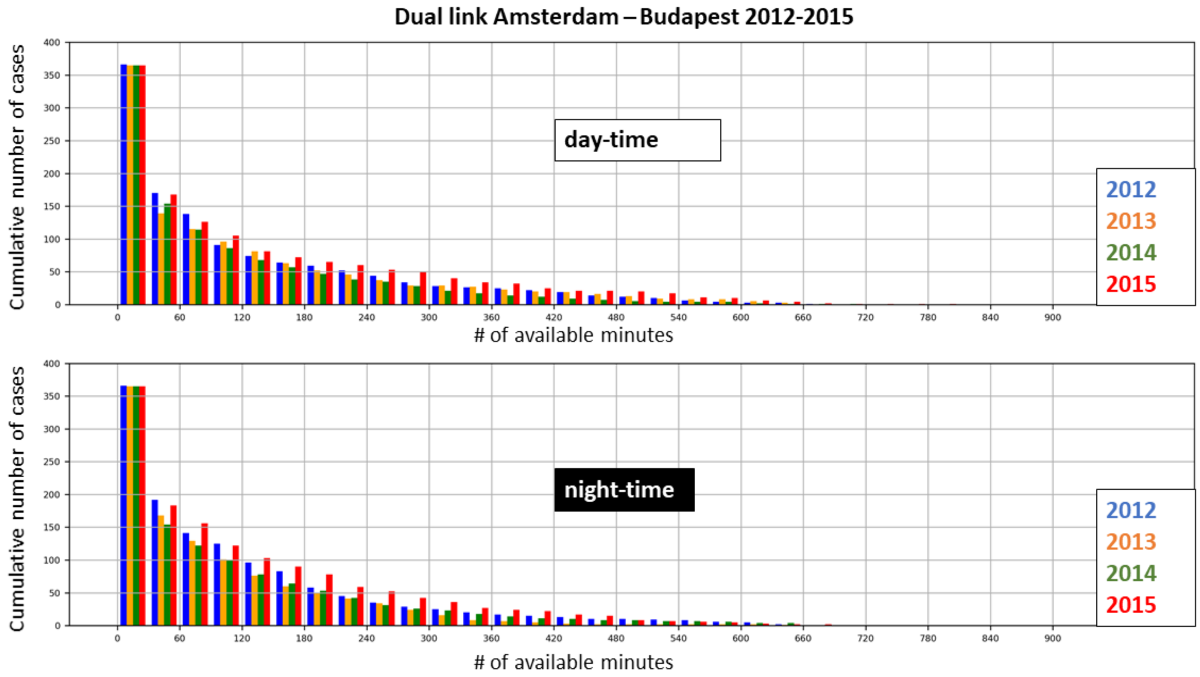


Figure 4. Plots showing the cumulative number of cases having more than a certain number of available dual link time minutes (in 30min interval) for day- and night-time over the years 2012 to 2015 between Amsterdam and Budapest.

In order to estimate the service feasibility, it is considered that, with a sufficient number of users, there will (almost) always be a couple of users that can be served (i.e., both users are in clear sky conditions) so that the GEO satellite is continuously used, with no wasted time. Also note that from the point of view of the users, the useful duration of the night, is the period during which *both* sites of a pair are in night conditions. However, from the point of view of the satellite, the useful duration is all the time when *at least* a pair of sites is in night conditions.

In an actual QKD service an optimization shall be made based on the required number of bits per unit time for the client, the available link time, the number of services per night, the number of clients, etc. For example, for clients in ten different cities, there will be 45 city-pairs. In the case of a single service of ~6h per city-pair per night, there will be only 365 day per year divided by 45 pairs is ~8 nights available per city-pair per year. Based on the curve of Figure 2, the number of usable bits per 6h service will be ~23.5kbits. So in this example, each of the city pairs can generate a maximum of 8x23.5= 188kbits per year in untrusted mode. Here the limitation does not come from cloud coverage, but from the number of sites to be served.

2.7 Phase 1 conclusions

From the analyses performed in Phase 1 it is concluded that QKD from an untrusted geostationary satellite is technically feasible. A ~1.1 secure bit/s key rate can be obtained with a maximum link loss of ~41dB per channel. This can be achieved using a polarization entangled photon source of ~10GHz source rate, a space segment with two telescopes of ~0.5m diameter each, ~0.65 µrad pointing accuracy for static and dynamic pointing, and a ground telescope of ~2.5m diameter, free-space coupled to highly sensitive single photon detectors (>85% detection efficiency). Background counts must be limited to at most 1000Hz. Given the low key rate in untrusted mode, a trade-off has to be made between the number of clients which can be served, the frequency of service and the number of secure key generated per service.

In order to increase the key rate, a hybrid configuration using BBM92 in untrusted (double link) and trusted mode (single link) can be used. The same photon source can be used for both implementations. In trusted mode a factor of ~300x higher secure bit rate can be obtained compared to untrusted mode only. Yet, this comes at the cost of security, since in trusted mode key material will be temporarily stored on-board of the satellite.

3. PHASE 2 HIGH LEVEL SYSTEM DESIGN

Using the beforementioned results as an input, Phase 2 focuses on a high-level system design of the space and ground segment, with a special emphasis on the space terminal, given its relevance to confirm feasibility.

3.1 Optical design space segment

A possible optical design for the space segment is shown below in Figure 5. The design consists of a large Coarse Pointing Mirror (CPA1) followed by a 3-mirror telescope. In the exit pupil of the first telescope a second CPA is placed (CPA2). After the CPA2s, two LEOCAT optical heads are placed containing the QKD, data and tracking channels.

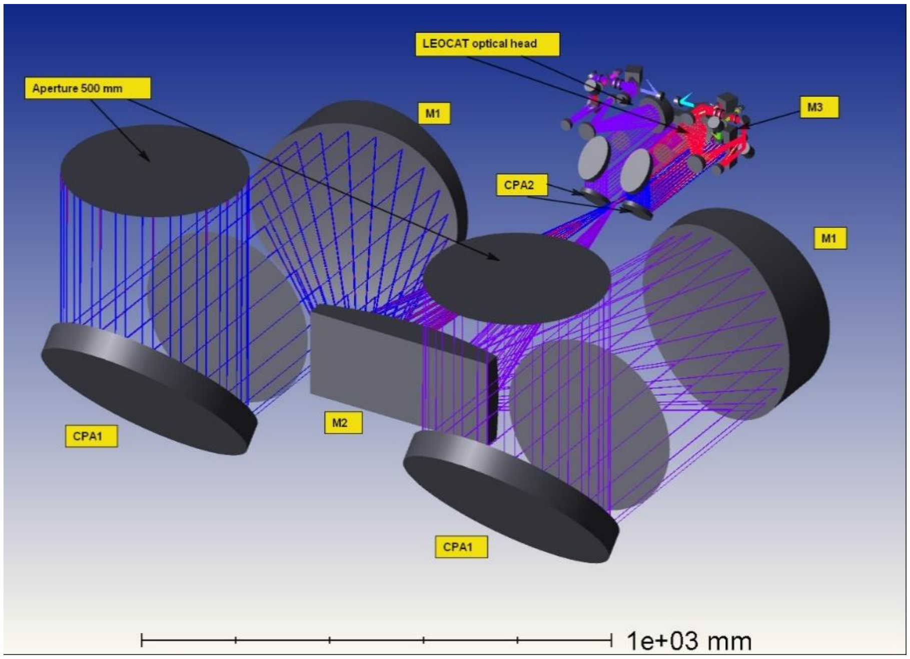


Figure 5. Proposed optical system layout of the QKD system in the space segment in isometric view. CPA: coarse pointing assembly, M: mirror. Colours of rays refer to transmission, receiving and tracking paths.

CPA1. Each optical path starts with a large coarse pointing mirror (CPA1) with a few degrees of range. With these CPA1s, two ground stations on the European continent can be chosen. After pointing to the ground stations of interest, the relatively large mirrors will be 'fixed' to these ground stations, without any active control during the link time. The absolute pointing accuracy of these mirrors shall therefore be better than 0.1°.

500 mm diameter telescopes and CPA2. The CPA1s are followed by a three mirror telescope with a magnification of 1/8.5 to reduce the beam diameter. To make the design more compact and for ease of manufacturing, the M2 and M3 mirrors are made on one mirror body. The absolute pointing accuracy of the CPA1s shall be better than 0.1°, to keep the maximum WFE contribution of the optical design of the first telescope below 18 nm Root-Mean-Square (RMS). (Remark: in Table 2, a total WFE of ≤81nm RMS was used. The difference between the 18nm and 81nm will be used for tolerances, alignment and manufacturing).

The entrance pupil of these telescopes is imaged (exit pupil) on a second coarse pointing mirror (CPA2). The CPA2s are still relatively large and the control bandwidth on this mechanism is limited and certainly not high enough to provide the required <0.65μrad, or even 0.25μrad pointing accuracy. The main function of the CPA2s is to 'offload' the Fast Steering Mirrors (FSMs)[17] in terms of required range, which is placed in the third optical module.

LEOCAT optical head. The third optical module is based on an earlier developed LEOCAT optical head (as part of the development of an intersatellite link terminal[16]). The LEOCAT optical head has a second telescope with a magnification of 1/8x to further reduce the beam size. The FSM is placed in the exit pupil plane of this telescope. The LEOCAT optical head contains several fiber interfaces, a tracking channel and a pointing calibration path. The FSM in combination with the tracking channel will provide the required pointing accuracy of <0.65µrad.

3.2 Mechanical design space segment

Based on the optical design, a suitable preliminary mechanical design for the space terminal has been made as shown below in Figure 6. The overall dimensions of the terminal will be in the order of ~2.4m x 2.2m x 0.8m, with an estimated mass of ~570kg. The aluminium housing ensures a good thermal conduction, thus reducing thermal gradients and thereby reducing thermal pointing errors. The Ti6Al4V struts ensure a high strength support to survive the launch loads as well as thermal isolation from the satellite platform. The LEOCAT optical head is an already developed system that uses a similar design philosophy (aluminium housing, Ti6Al4V struts).

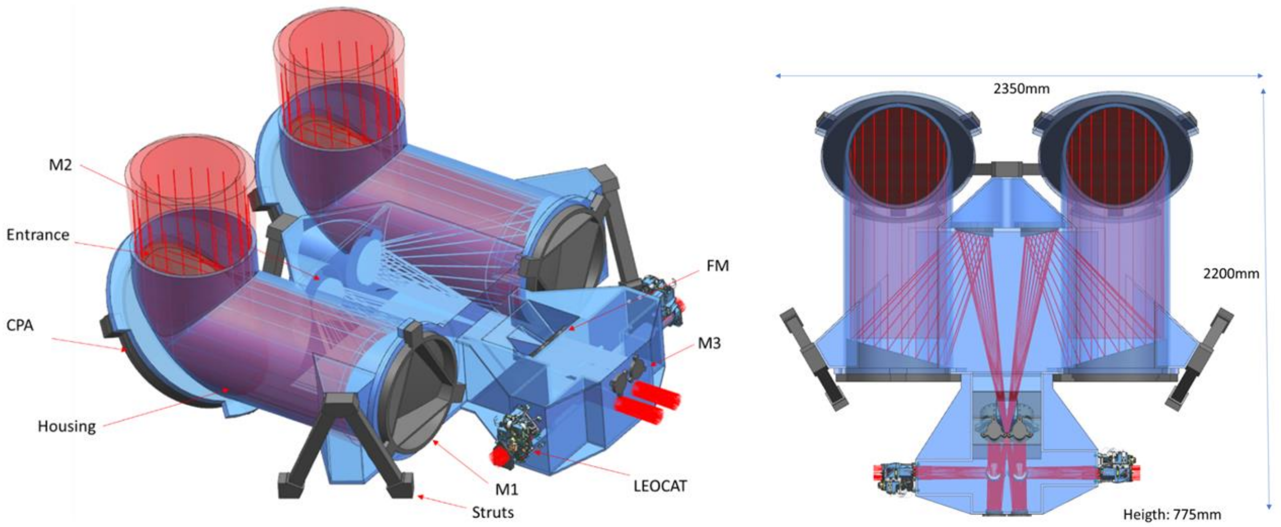


Figure 6. Mechanical design of the QKD payload in the space segment.

A first modal vibration analysis has been carried out on this concept, indicating that the first modes will be in the region of 80Hz. This is estimated to be a potential issue in terms of coupling with the satellite and launcher, that needs to be addressed in a follow-up conceptual design phase together with the platform provider. Additionally, preliminary dynamics analysis concludes that this initial 80Hz support should be reduced to ~10Hz in order to minimize the impact of micro-vibrations on the critical pointing accuracy requirements for the system, by means of passive vibration isolation. This would mean that a soft support would be needed, where probably a launch lock should be foreseen.

The pointing stability of the system is identified as one of the main design drivers for the mechanical design. Slow deformations of the large telescope (for example due to thermal gradients) are not so critical since they influence the optical components that are in the common path for both the outgoing QKD beam as well as in the incoming beacon, and this will be corrected by the active mirrors. Micro-vibrations are likely to be the most critical aspect of the mechanical design. It will probably drive the design to place certain eigenfrequencies at a specific region, in such a way that, together with the active mirrors, the influence of satellite vibration on the pointing of the outgoing QKD beam is minimized.

3.3 Quantum system space segment

The QKD system in the space segment shall be capable of implementing the BBM92 protocol in untrusted and trusted mode.

Untrusted mode. In untrusted mode the entangled photon pairs coming from the source are routed to the two on-board optical transmitters, and emitted towards their respective ground receiver. After the ground receivers have measured a significant amount of pairs, key distillation can start between both, eventually leading to the final secure key. No active elements for basis or decoy state choice are needed in the space segment. In both untrusted and trusted mode, a small percentage of the pairs is sent to an on-board testing and calibration system to guarantee proper functioning of the source.

Trusted mode. In trusted mode one of the photons of the entangled pair is sent to the telescope and emitted towards one of the ground receivers. The other photon is routed to an on-board measurement module as shown below in Figure 7. It shows a sketch of the on-board system, equivalent to the measurement modules in the ground stations. The quantum receiver contains a 50/50% beam splitter for passive basis choice. In one arm the photon is measured in the standard (H/V) basis while in the other a half-wave plate is placed in order to measure in the Hadamard (45°/-45°) basis. Photons are detected by the on-board single photon detectors. By applying detector multiplexing, key rates in trusted mode can be increased. Using N times more detectors leads to N times higher detection rate and thus N times higher key rate. Classical communication will take place by modulating the beacon laser.

Although a more in-depth design has been made for the quantum system, this cannot be shared in the current paper.

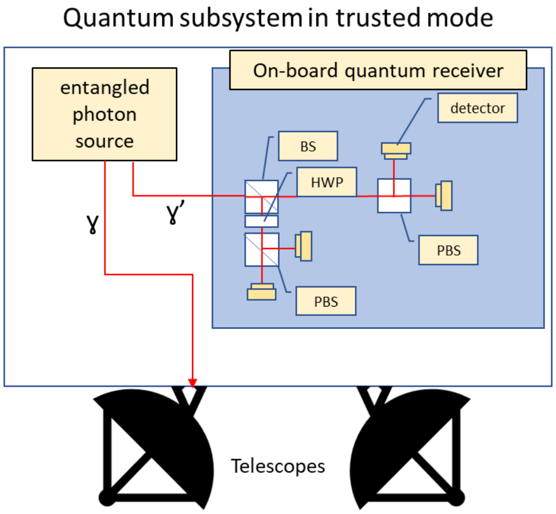


Figure 7. Sketch of the quantum subsystem in the space segment used for operation in trusted mode. BS=beam splitter, PBS=polarization beam splitter, HWP=half wave plate.

3.4 Optical and mechanical system ground segment

The link budget calculations from Phase 1 showed that for the ground segment telescope an aperture diameter of ~2.5 m is required (in combination with 0.65µrad pointing accuracy). For the quantum detector we assume a circular active detection area of ~200µm diameter. To limit cost and complexity the ground segment will operate without AO, using tip/tilt correction only. This means that the average point spread function (PSF) on the focal plane of the optical system is completely captured by the detector surface (otherwise there will be too much signal loss). Assuming an atmospheric seeing of ~10µrad (FWHM of average PSF), which corresponds to a realistic Fried parameter of ~8cm at 810nm, the required Field-of-View (FoV) shall be ~20urad (full angle). The focal length matching this system will be ~10m. With these specifications, the average PSF of a point-like object (here the source is the satellite) affected by turbulence, can still be captured by the detector surface. The result is a F/4 telescope for the ground segment. The pointing accuracy of the system shall be such that the average tilt of the wavefront is compensated. This means that the tip/tilt sensor shall be able to compensate tilts down to 1-2 µrad so that most of the PSF is captured on the detector.

In order to check feasibility, a European manufacturer of ground telescopes was contacted. It confirmed that F/4 telescopes with 2m to 2.5m diameter primary mirrors don't pose any risk, confirming feasibility.

3.5 Quantum system ground segment

The quantum system in the ground segment is similar to what is shown in Figure 7. Important is the addition of a polarization control before entering the polarization state analysis subsystem as the satellite may be oriented differently with respect to the ground station. Photon polarization states are again passively analysed and detected by four single photon detectors, one for every polarization state (H/V/-45°/45°).

3.6 Other critical (sub-)systems

Besides these main (sub-)systems, we also looked at the beacon in space- and ground-segment as well as time-synchronization. Given the limited scope of the study, these topics have not been analysed in detail. We therefore limit ourselves to the following conclusions:

Beacon. The beacons on space and ground segment shall have several functionalities: 1) to realize and maintain a proper alignment between space and ground system, 2) to provide the classical communication required as part of the QKD protocol, and possibly 3) to provide a clock signal for time synchronization. An on-board modulator allows to encode the classical information onto the beacon for which a 850nm wavelength is chosen, which is sent via the same optical path as the QKD signal to Earth. The space segment must also able to receive an 850nm wavelength modulated beacon signal from Earth which is split from the QKD signal (operating at 810nm) and detected with a tracking and data-acquisition sensor. For the ground segment a separate beacon using its own (smaller) telescope is foreseen – i.e. not using the 2.5m telescope – to prevent blinding the receivers by backscatter. Because of eye safety regulations, the beacon power going to the satellite must be limited. Two implementations are proposed: 1) a simple system requiring a 450mm diameter transmitting beacon telescope with 70W optical power (passively covering the foreseen uncertainty cone upon acquisition), or 2) a more complex system with a 150mm diameter telescope, fine-steering mirror and 8W optical beacon power (actively covering the uncertainty cone upon acquisition). A further and more detailed investigation is needed to determine which solution is best.

Time synchronization. Another important functionality is the proper time synchronization between Alice and Bob so that detected events can be properly correlated. A first assessment shows that time synchronization at a 10GHz source rate seems to be technically feasible given the low jitter of current state of art detectors, time-taggers and clocks. In order to synchronize clocks at both receivers (either on ground or between satellite and ground), continuous modulation of the beacon received by both receivers seems to be the best option but this requires a more in-depth analysis.

4. CRITICAL TECHNOLOGIES

From the high level system design, critical technologies have been identified which are required for a successful implementation of GEOQKD. These are summarized below in Table 4.

Table 4. Critical technologies required for GEOQKD with estimated current TRL.

Key Technologies	Required	Current TRL, other information
Space segment		
Mechanical pointing technology	0.25 µrad static and dynamic (RMS)	Two main technologies are foreseen: - TRL: ≤4. Vibration isolation in space, possibly active, for large structures. TNO has experience with passive and active systems for ground-based systems[20] - TRL: 6-7. Low-noise, large field of view tracking detectors; technology is most likely available (e.g. CMOS, quadrant detectors, etc), but specific hardware and software designs might be required for this application.
Large optics	2x 0.5m diameter telescope apertures	TRL: 9. On itself no critical technology; it is however advised to first build an Engineering Model (EM) to test feasibility and manufacturability.
Wavefront error on optical elements	~81nm (RMS)	TRL: 5. From fiber to exit telescope there are several optical surfaces. The total WFE budget is ~81 nm RMS which has to divided over all optical surfaces including the deformation due to mounting which makes this very challenging.
Entangled photon source	>1GHz average pair generation rate	TRL 1-4: although GHz rates have been demonstrated in a laboratory environment[13], a space-qualified source at these rates needs to be developed. Recently, an ESA Artes 4S project within SAGA has started on this topic.
Single photon detectors	>10 MHz detection rate, > 85% detection efficiency, low dark counts, small jitter.	TRL≤4 for space applications. For short mission durations COTS components have already been used (such as SAP-500 Geiger-Mode APDs during the Spooky mission of NUS[14]. However, for long duration missions (>10yrs), space-qualified detector will be needed.

Secure key storage	At a minimum fulfilling FIPS 140-3 requirements[15]	TRL: 9. In trusted mode, secure keys need to be temporarily stored on board of the satellite. A sufficiently safe and space qualified storage is needed, which needs, at a minimum, to fulfil the security requirements as set by the given FIPS certification. Similar systems exist in military satellites. Commercially they are not available (yet) as far as we know. Therefore TRL may be considered lower.
Ground Segment		
Single photon detectors	>85% detection efficiency, total jitter<100ps (FWHM), dark counts<~100Hz, free space coupled	Although these values can be achieved with cryogenic detectors (such as those of Single Quantum or IDQ), they require single mode fibre coupling and are therefore not compatible with the current baseline which is a free space coupling. Developments towards free space coupled detectors with similar performance is therefore needed. TRL: 9 for fibre coupled detectors. TRL: <3 for free space coupled detectors with similar performance.
Large optics	2- 2.5m diameter telescope apertures	TRL 9. Although these systems can be built and even commercially available, they must be tailored for QKD purposes.
Key storage	At a minimum fulfilling FIPS 140-3 requirements[15]	TRL~7-9 Systems exist but need to be integrated and tailored for QKD use.
Adaptive Optics		Only applicable for fibre coupled configuration, which is not the current baseline.
Time synchronization system	Matching 10GHz source rate (<100ps jitter)	TRL: 6-7. Requires a more in-depth analysis of possibilities. Currently beacon modulation from the satellite seems to be a suitable option.

5. CONCLUSIONS

From the study we conclude that GEOQKD is technically feasible and that a hybrid system combining untrusted and trusted mode BBM92 seems to be the most promising concept, leading to a higher value for money. With a maximum tolerable loss of 41dB per channel, a ~1.1bit/s key rate in untrusted and ~300bit/s key rate in trusted mode can be achieved, which can be increased to 10kbit/s when detector multiplexing is applied. A realistic, high level optical and mechanical design has been made for the space segment which can fulfil the required functionalities and main system characteristics. A system architecture for the space based quantum system is provided as well, which allows the GEOQKD system to operate in untrusted and trusted mode. Pointing accuracies down to 0.25 µrad (static and dynamic) seem to be feasible for which on-board vibration disturbances are the most dominant performance limiting factors. For the ground segment a F/4 telescope will be required, with a 2.5m diameter aperture and a 10m focal length in combination with 200µm diameter single photon detectors which are free-space coupled. The proposed quantum system in the ground segment is proven feasible and is already used within practical experiments with the Micius satellite. A list of critical technologies has been provided which serves as a technology roadmap to an actual GEOQKD space mission.
Based on this study, we believe that a GEOQKD implementation must be considered as a serious addition to the design of a space-based quantum communication network (e.g. as part of the EuroQCI).

REFERENCES

[1] Liao, S., et al, "Satellite-to-ground quantum key distribution," Nature 549(7670), 43-47 (2017).
[2] Yin, J., et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature 582, 501-505 (2020).
[3] Yin, J. et al., "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," Phys. Rev. Lett. 119, 200501 (2017).
[4] Miao, E., Han, Z., Zhang, T. and Guo, G., "The feasibility of geostationary satellite-to-ground quantum key distribution," Physics Letters A 361(1-2), 29-32 (2007).

[5] Bennet, C.H., Brassard, G. and Mermin, D.N., "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. 68, 557 (1992).

[6] Hwang, W., "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. 91, 057901 (2003).

[7] ESA, "Space photons bring a new dimension to cryptography," ESA, 3 May 2018, <https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Space_photons_bring_a_new_dimension_to_cryptography> (21 January 2021)

[8] ESA, "A-QKD-S - Augmented Quantum Key Distribution Services," ESA 24 June 2020, <https://business.esa.int/projects/a-qkd-s> (21-1-2021)

[9] Dequal, D., et al., "Feasibility of satellite-to-ground continuous-variable quantum key distribution," npj Quantum Inf. 7, 3 (2021).

[10] Fraunhofer IOF, "Quantum Communication Technologies at Fraunhofer IOF," Fraunhofer IOF, 2021, <https://www.iof.fraunhofer.de/en/competences/emerging-technologies/quantum-technologies/Quantum-communication-technologies.html> (28-1-2021)

[11] EUMETSAT CM SAF, "CM SAF – Product Navigator," 2010-2020 DWD | 2010-2020 CM SAF, <https://wui.cmsaf.eu/safira/action/viewProduktSearch> (2020)

[12] Lo, H.-K., Curty, M. and Qi B., "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. 108, 130503 (2012).

[13] Cao, Y., et al., "Bell Test over Extremely High-Loss Channels: Towards Distributing Entangled Photon Pairs between Earth and the Moon," Phys. Rev. Lett. 120(14), 140405 (2018).

[14] Villar, A., et al., "Entanglement demonstration on board a nano-satellite," Optica, 7(7). 734-737 (2020).

[15] NIST CSRC, "Security Requirements for Cryptographic Modules", NIST, 22 March 2019, <https://csrc.nist.gov/publications/detail/fips/140/3/final> (3-2-2020)

[16] Saathof, R., et al. "Optical satellite communication space terminal technology at TNO," ICSO 2018, Vol. 11180, International Society for Optics and Photonics (2019).

[17] Witvoet, G., S. Kuiper, and A. Meskers, "Performance validation of a high-bandwidth fine steering mirror for optical communications," ICSO 2018, Vol. 11180, International Society for Optics and Photonics (2019).

[18] Saathof, R., et al., "Optical technologies for terabit/s-throughput feeder link," 2017 IEEE International Conference on Space Optical Systems and Applications (ICSOS), IEEE, 2017.

[19] Saathof, R., et al., "QKD optical ground terminal developments, " ICSO 2021.

[20] Rijnveld, N., et al., "Low-frequency vibration isolation in six degrees of freedom: The Hummingbird," Proc. 10th Inter. Conf. EUSPEN, 1, 275-278 (2010).