

International Conference on Space Optics—ICSO 2018

Chania, Greece

9–12 October 2018

Edited by Zoran Sodnik, Nikos Karafolas, and Bruno Cugny



Tracking challenges of QKD over relay satellite

S. Sharma

N. Perlot

J. Rödiger

R. Freund



icso proceedings



Tracking challenges of QKD over relay satellite

S. Sharma*, N. Perlot, J. Rödiger, R. Freund

Fraunhofer Heinrich-Hertz Institute, Einsteinufer 37, 10587 Berlin, Germany
*sakshi.sharma@hhi.fraunhofer.de; phone +49 30 31002 514; www.hhi.fraunhofer.de

ABSTRACT

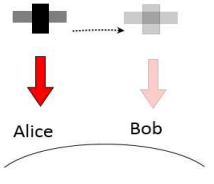
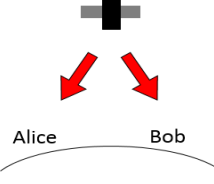
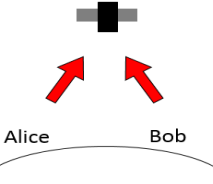
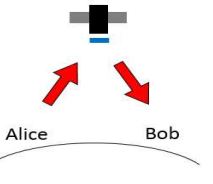
We investigate a quantum key distribution (QKD) system with relay satellite for communication between two distant Earth-based parties, Alice and Bob. The satellite acts as a relay station which simply redirects the QKD signal. It has several advantages that can be decisive. The optical relay provides a high transparency to protocols and wavelengths. The relay node does not have to be trusted. Like entanglement-based or measurement-device-independent satellite QKD, relay-assisted QKD suffers from a higher propagation loss than trusted-node scenarios. Challenges are expected when pointing the relay mirror precisely between Alice and Bob and dealing with significant point-ahead angles that result from the satellite velocity. We start our analysis by evaluating the point ahead angles (PAA) of Alice and Bob for scenarios of interest. The difference between the two PAA vectors tells us whether the relay mirror will be able to maintain a bidirectional transmission with beams sent from the ground. Considering a satellite altitude of 500 km and an Alice-Bob separation of 1000 km, observation of large PAA vector difference enjoins us to place additional beacon sources on the satellite. A conceptual design of the relay-tracking system is drafted. Onboard measurements of the beacons from Alice and Bob provide feedback to the relay-mirror positioning control loop. With a typical relay-mirror size of 0.2 m, propagation losses are calculated for different ground antennas. We conclude on the attractiveness and feasibility of satellite relay QKD.

Keywords: QKD, satellite, relay, tracking, point-ahead angle, quantum communication.

1. INTRODUCTION

Quantum Key Distribution (QKD) is a method of generating secure keys usually between two remote parties (Alice and Bob) who then use the key for encryption and decryption of messages. The security of QKD in combination with one-time pad encryption relies on the postulates of quantum mechanics with the crucial property that the two communication partners can detect the presence of any third party trying to intercept i.e. trying to gain knowledge of the key. Despite many tempting features, QKD faces some challenges to be eligible for the implementation on a commercial-scale. One important limitation of long-scale commercial realization of QKD is the distance over which QKD-aided communication can take place. Space-based quantum communication using a satellite extends the range of QKD, which is otherwise limited with the current fiber-based technology^[1]. However, present level of technology uses satellite as an intermediate trusted node, compromising the security of the distributed key. QKD over an untrusted node could be achieved using an entangled-photon source on the satellite^[2]. Measurement-device-independent (MDI) QKD is another form of QKD with an untrusted node^[3]. Alice and Bob both send quantum signals to an untrusted intermediary (which could be on a satellite). However, the two uplinks required for MDI-QKD cause higher propagation losses and the synchronization of the quantum signals is challenging. While various attempts to extend the quantum communication distance by using satellites can be found in the literature^{[2][4][5]}, no such attempt have used satellite merely as a untrusted relay node. To our knowledge, we report here the first theoretical analysis on the feasibility of using an untrusted satellite as a relay node for QKD without any onboard entanglement source or Bell-state measurement. Possible satellite QKD scenarios are depicted in Table 1.

Table 1. Four QKD scenarios involving a satellite. The present work focuses on a satellite with a relay mirror (last scenario).

Must satellite be trusted?	Yes	No		
Satellite role	One-way distributor	Entangled photon source	Bell-measurement station	Relay mirror
Depiction				
QKD principle	Prepare and measure	Entanglement based	MDI	Prepare and measure

In relay-satellite QKD a relay mirror is positioned on the satellite and redirects the QKD transmission from Alice to Bob. Hence, a high transparency to protocols and wavelength is accomplished. Thus, photon emission rates can be higher if restricted to entanglement sources. In addition, with relay-satellite QKD no quantum device needs to be in space. However, there are some limitations of relay-satellite QKD. First, the propagation losses are higher than the trusted node scenario (See §4 for more details). Moreover, a possible disadvantage of the relay-mirror scenario, compared to an entangled-photon source with two downlinks, is the uplink that in terms of turbulence suffers more impairments. In this regard, the MDI scenario with its two uplinks has the biggest weakness. Advantages and disadvantages of relay-satellite QKD scenario are summarized in Table 2.

Table 2. Advantages and disadvantages of relay satellite QKD system.

Advantages	Disadvantages
<ul style="list-style-type: none"> No need to trust the satellite. Protocol- and wavelength-transparent satellite. System complexity is shifted to ground (Alice and Bob). High photon rate (e.g. 10 Gbit/s) compared to entanglement sources (e.g. 10 Mbit/s) transmitted by Alice. 	<ul style="list-style-type: none"> Higher propagation loss than the trusted node scenario. Atmospheric turbulence is difficult to correct in uplink. Alice and Bob must be simultaneously visible to the satellite (unlike trusted node situation). Challenging onboard optical tracking system.

The outline of the paper is as follows: §2 contains the theoretical analysis of the relay satellite QKD system, investigating the point-ahead angles of the ground stations for different situations of interest. In §3 the design for relay-satellite assisted QKD is introduced along with the onboard fine tracking system design. Examples of link power budget are presented in §4 where we particularly examine the expected loss and compare it to other QKD scenarios. Finally, results are summarized and discussed in §5.

2. POINT-AHEAD ANGLES

Using a satellite to transmit the quantum beam from Alice to Bob involves high velocities and significant point-ahead angles (PAA). The PAA θ is a three-dimensional (x, y, z) vector transverse to the beam. When the PAAs of the two ground stations are different, the relay-mirror position needed to maintain the link from Alice to Bob is different from the positioning required to maintain the link from Bob to Alice. The difference between the two PAA vectors (of Alice's link and Bob's link), the differential PAA $\Delta\theta$, tells us whether the relay-mirror will be able to maintain a bidirectional transmission with beacons sent from ground. A simplified scenario is depicted in Figure 1 where at time t_2 the mirror needs to point in two different directions to maintain the bidirectional link.

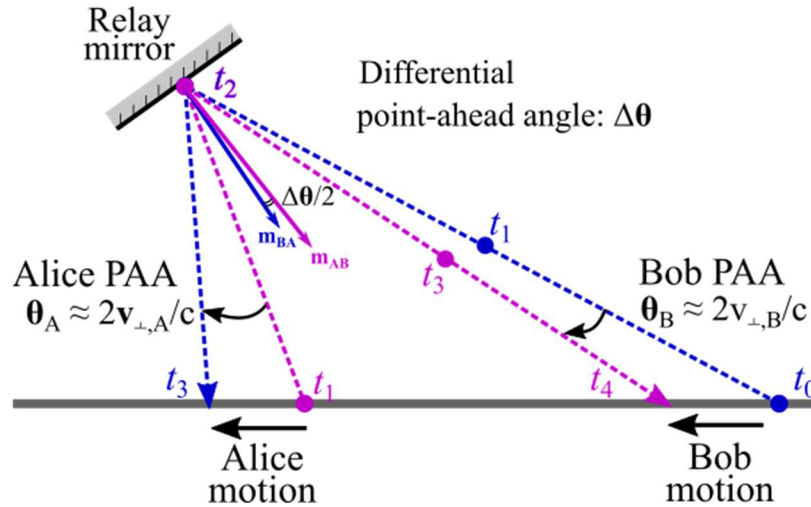


Figure 1. Illustration of the rays sent and received by Alice and Bob from the viewpoint of the flying mirror. Positions of the two travelling signals are marked at different times t_N . The point-ahead angle θ_A (resp. θ_B) on Alice's side (resp. Bob's side) depends on the beam-transverse velocity $v_{\perp,A}$ (resp. $v_{\perp,B}$) of Alice (resp. Bob) and on the light velocity c . Generally, $\theta_A \neq \theta_B$. Vectors \mathbf{m}_{AB} and \mathbf{m}_{BA} are the mirror vectors required to satisfy Alice-mirror-Bob link and Bob-mirror-Alice link respectively.

In this report, we analyze $\Delta\theta$ for different cases. The differential PAA ($\Delta\theta$) is calculated as follows. To compare Alice's PAA (θ_A) with Bob's PAA (θ_B), we first flip θ_A over the relay mirror axis

$$\theta_{A,\text{flipped}} = 2(\theta_A \cdot \mathbf{m})\mathbf{m} - \theta_A \quad (1)$$

with \mathbf{m} being the mirror's unitary pointing vector defined by

$$\mathbf{m} = \frac{\mathbf{b} + \mathbf{a}}{\|\mathbf{b} + \mathbf{a}\|} \quad (2)$$

where \mathbf{a} and \mathbf{b} are the unitary vectors from the mirror to Alice and Bob respectively. The differential PAA $\Delta\theta$ is given by,

$$\begin{aligned} \Delta\theta &= \theta_{A,\text{flipped}} + \theta_B \\ &= 2(\theta_A \cdot \mathbf{m})\mathbf{m} - \theta_A + \theta_B \end{aligned} \quad (3)$$

We consider a relay satellite at an altitude of 500 km and moving at 7.6 km/s whilst Alice and Bob, the two ground-based communicating stations, are 1000 km apart from each other. Although a GEO satellite will provide a smaller $\Delta\theta$, we consider LEO in our analysis to limit the propagation loss. We analyze the variation of the $\Delta\theta$ of the two ground stations for, Case 1: when the satellite motion is parallel to AB (Alice-Bob) separation, and Case 2: when the satellite motion is orthogonal to AB separation. For link elevation angle of 5° , the investigated cases are illustrated in Figure 2 where Alice-Bob1 depicts Case 1 while Alice-Bob2 depicts Case 2.

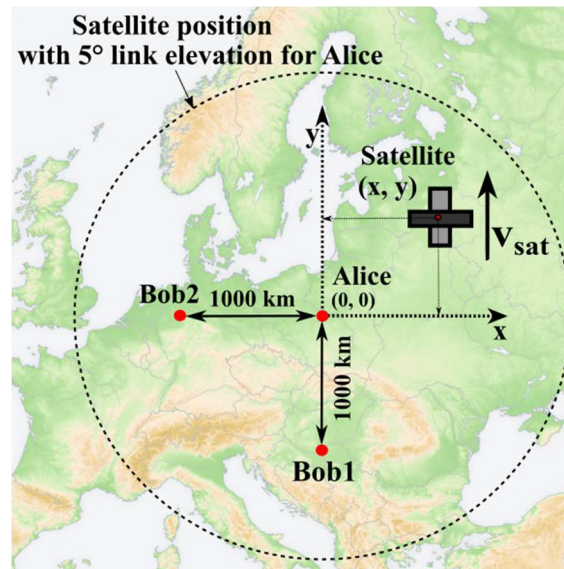


Figure 2. Considered geometry of Alice, Bob and the satellite. The circle indicates the approximate satellite position when Alice sees the satellite at 5° elevation. Satellite altitude is 500 km. The chosen geographical map is only an illustrative example.

The variation of the magnitude θ_A of Alice’s PAA is shown in Figure 3 for link elevations down to 5°. Symmetrical pattern is observed around the coordinates of Alice (0, 0). The pattern for θ_B around Bob’s position is identical to θ_A .

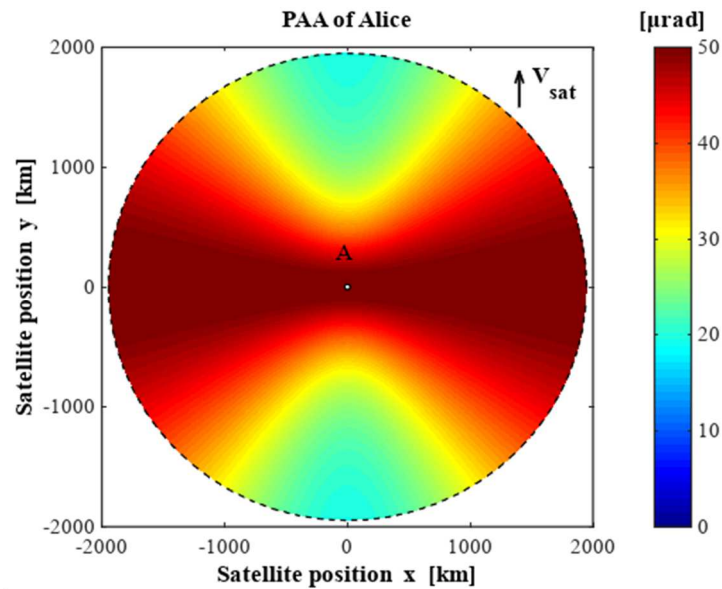


Figure 3. Point-ahead angle (PAA) θ_A of the Alice-satellite link along the Earth-surface coordinates of the satellite (x, y) with respect to Alice at (0, 0). The satellite is assumed to move over the y-axis, e.g. from south to north.

Next, variations of differential PAA ($\Delta\theta$) as calculated from Eq. (3) are shown in Figure 4.

2.1 Case 1: Satellite motion is parallel to Alice-Bob axis

The first case of consideration is when AB is parallel to \mathbf{V}_{sat} (see Figure 4, left). We observe $\Delta\theta = 0 \mu\text{rad}$ when the satellite is equidistant to Alice and Bob1 (in Figure 2), i.e. when the satellite is at $y = -500 \text{ km}$. A maximum value of $\Delta\theta \sim 30 \mu\text{rad}$ is observed when the satellite is exactly above a ground station.

2.2 Case 2: Satellite motion is orthogonal to Alice-Bob axis

The next case we consider is the orthogonal configuration i.e. when AB is orthogonal to V_{sat} (see Figure 4, right). This case presents higher differential PAA values as compared to the parallel case, with a maximum around $40 \mu\text{rad}$. When the satellite is aligned with the Alice-Bob axis (i.e. when $y = 0$), both beams are transverse to V_{sat} and $\Delta\theta = 0 \mu\text{rad}$.

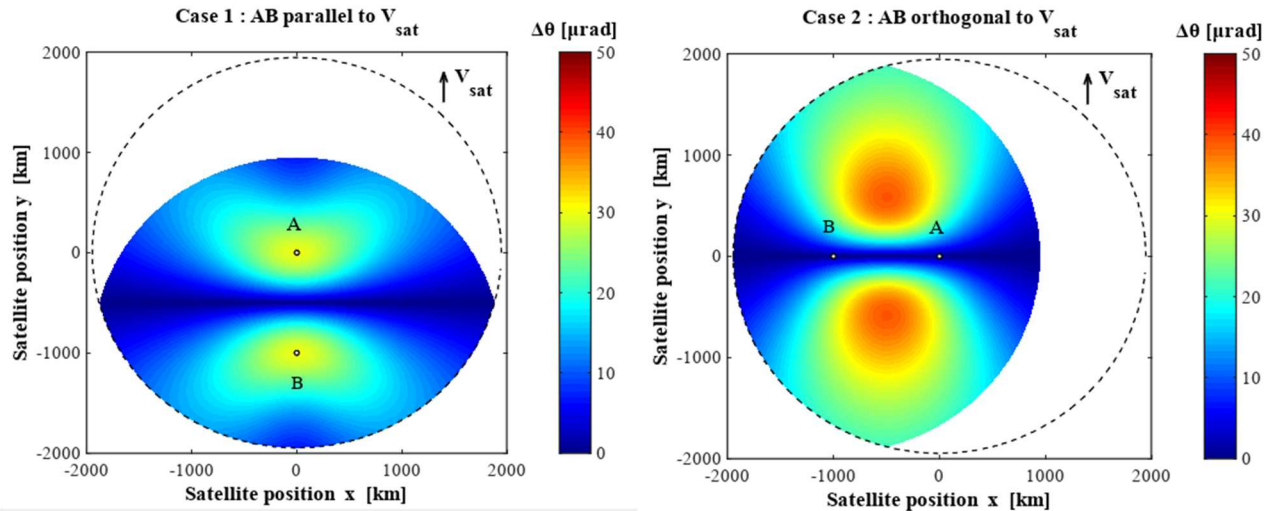


Figure 4. Variation of the difference in PAA of Alice and Bob along the coordinates of the satellite (x, y) with Alice as the origin when AB parallel to V_{sat} (left) and when AB orthogonal to V_{sat} (right).

Values of the differential PAA (e.g. $30 \mu\text{rad}$) are generally larger than considered diffraction-limited beam divergence angles (e.g. $5 \mu\text{rad}$). This differential PAA will thus have to be taken into account in the relay-mirror tracking system. Furthermore, whereas Alice's beam can be pointed correctly towards Bob over the relay, Bob's beam after the relay reflection will wander on ground up to some tens of meters away from Alice's position. Although considered too complex, the following implementation would maintain a bidirectional link: At one node (Alice, relay mirror or Bob), the bidirectional beams would go through separate optics. For example, Alice's receiver is separated from her transmitter and is made mobile over some tens of meters to track for the changing differential PAA. Similarly, the satellite could accommodate two relay mirrors, one mirror for each direction.

3. CONCEPTUAL TRACKING DESIGN

The considered onboard design consists of a motorized 20 cm planar mirror, typically elliptical, responsible for pointing the incoming signal from one ground station towards the other ground station without performing any measurements on the QKD beam. Coarse pointing is expected to be done by the satellite. As shown in Figure 5, the satellite needs one beam from Alice (Beacon a) and one from Bob (Beacon b) to point precisely the relay mirror. Although both beacons, from Alice and from Bob, are measured, only the beam from Alice shall be correctly redirected by the mirror. The relay mirror shall point between the two received beams and add a deterministic angular offset as a result of the PAA and differential PAA.

The optical system for the acquisition of Beacons a and b must deal with large incidence angles on the mirror, hence with a large field of view (FoV). Our approach is to divide the FoV into regions with dedicated acquisition optics and detectors. The design presented in Figure 6 is acceptable for incidence (half) angle down to about 25° . For small incidence angles, acquisition can be done according to the method of Figure 7. Acquisition optics shall be attached to and move with the relay mirror. Although Figure 6 and Figure 7 show the acquisition optics behind the relay mirror, the relay mirror does not have to be partially transparent (or act as a beam splitter): the acquisition optics can have an aperture aside of the relay mirror or the relay mirror can have a central opening/hole for the acquisition optics.

Alice and Bob also need to receive a beacon beam in order to point to the satellite. Because the relay mirror will maintain the link from Alice to Bob (but not necessarily from Bob to Alice), Bob may use Beacon a, i.e. the beacon sent by Alice.

However, since high propagation loss is expected for Beacon a to reach Bob, it is safer to add an onboard beacon towards Bob (depicted in Figure 5 as Beacon d). On the other hand, Alice cannot rely on Beacon b (the beacon sent by Bob), so the satellite must provide a beacon (Beacon c in Figure 5) towards Alice. For the QKD receiver at Bob, beacon light is regarded as noise and must be optically filtered. The optical isolation of the QKD signal will be greatly simplified if Bob couples the QKD beam into standard single mode fiber. In this way, angular and spectral filtering can be optimized.^[6]

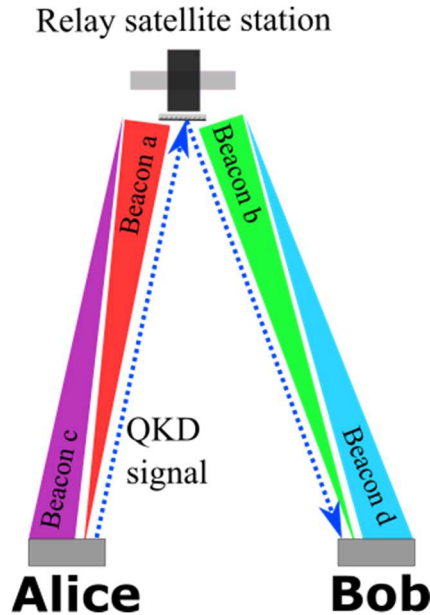


Figure 5. Considered beacon beams and relay QKD beam.

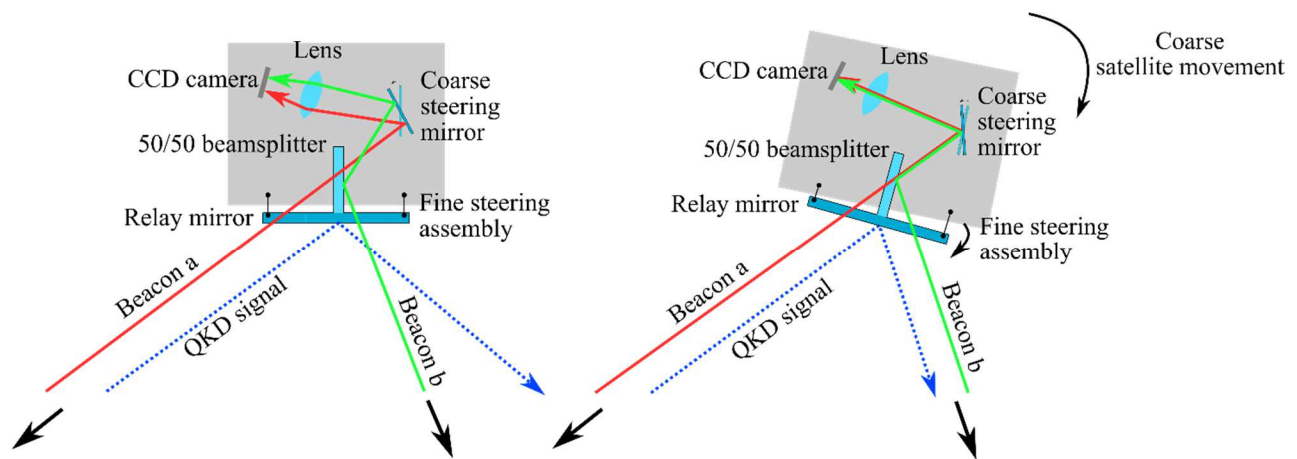


Figure 6. Example of fine tracking system of the relay-satellite station for the case of large incident angles where, the beam splitter and relay mirror constitute a monolithic assembly. Assuming negligible PAA, correct pointing is achieved when the two spots of Beacon a and Beacon b superpose on the CCD camera. A coarse steering mirror keeps the two beams on a CCD camera. With a significant differential PAA, the two spots should no longer superpose, but be dissociated with respect to the differential-PAA vector $\Delta\theta$.

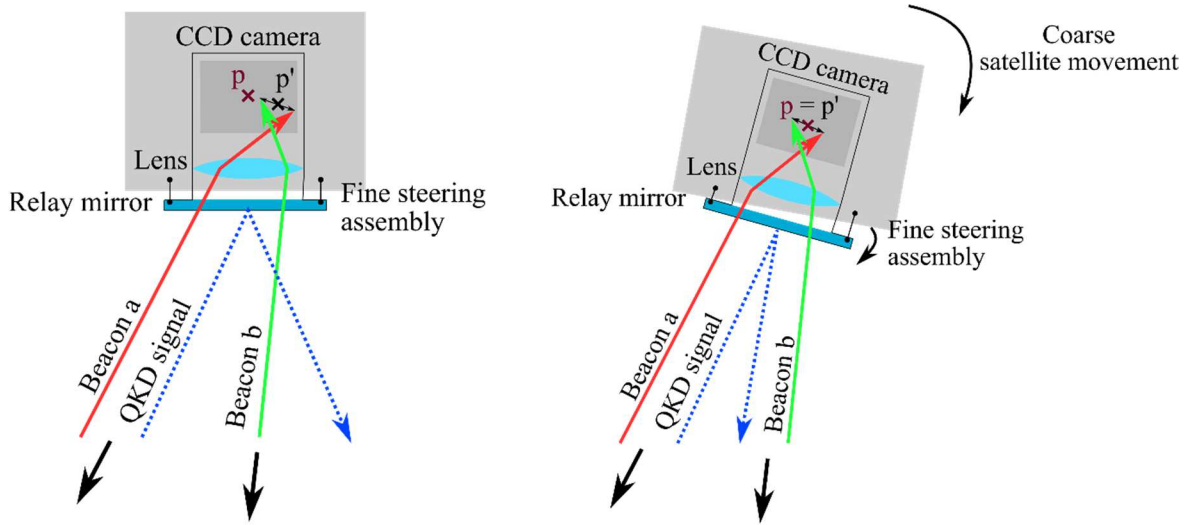


Figure 7. Example of fine tracking system of the relay-satellite station for the case of small incident angles. p is the point of reference and p' is the center between Beacon a and Beacon b. p' should be moved to p (relay mirror's direction corrected by PAA offset) for accurate pointing of the signal.

4. LINK POWER BUDGET

In a first iteration of the link budget calculation, atmospheric losses (turbulence, cloud, background light) can be ignored and diffraction-limited beam propagation formulas can be applied^[7]. With a symmetric up and down propagation path, we obtain a rough and optimistic link loss of

$$\left[\frac{D_{\text{sat}} D_{\text{Alice}}}{\lambda L} \right]^2 \left[\frac{D_{\text{sat}} D_{\text{Bob}}}{\lambda L} \right]^2 \sim -40 \text{ dB} \quad (4)$$

where, D_{sat} is the relay mirror diameter of the LEO satellite (~ 0.1 m),

D_{Alice} is the telescope diameter of Alice ground station (~ 1 m),

D_{Bob} is the telescope diameter of Bob ground station (~ 1 m),

λ is the wavelength used ($\sim 1e-6$ m),

L is the link distance ($\sim 1e6$ m).

This propagation loss in dB is double of what we expect from a trusted node scenario. The doubling of the loss in dB through double propagation is characteristic of untrusted-node scenarios such as QKD with entangled photons or measurement-device-independent QKD.

The relay scenario involves an uplink from Alice to the satellite, which is more challenging than the downlink because of the atmospheric turbulence, which cannot be fully compensated. Turbulence compensation with adaptive optics for an uplink is still an active research topic.^[8] With significant uncompensated turbulence, a non-symmetrical relay link is expected with $D_{\text{Alice}} < D_{\text{Bob}}$. Considering $D_{\text{Alice}} \approx 0.3\text{m}$, we obtain

$$\left[\frac{D_{\text{sat}} D_{\text{Alice}}}{\lambda L} \right]^2 \left[\frac{D_{\text{sat}} D_{\text{Bob}}}{\lambda L} \right]^2 \sim -30 \text{ dB} - 20\text{dB} \quad (5)$$

$$\sim -50 \text{ dB.}$$

Despite the uplink turbulence loss, relay QKD has the potential to provide higher key rates because the emission rate of qubits by Alice can be much higher than e.g. with an entangled-photon source. With Alice sending $1e10$ photons/s and a total link loss of 50 dB, one could hope reaching a secret key rate of 10 kbit/s. To calculate the key length per satellite overflight, one should integrate the varying link attenuation over the overflight duration.^[9]

5. CONCLUSIONS

We presented a novel analysis of relay satellite QKD. The simple idea of beam forwarding with a mirror is contrasted with the complexity of keeping the mirror in the correct direction. The investigation shows that the difference in the point-ahead angle of the two communicating ground stations cannot be neglected and have a strong impact on the relay-mirror tracking. A satellite at higher altitude would provide lower differential PAA values but with the compromise of higher propagation losses. We sketched a conceptual tracking design with two different beam acquisition systems that would cover two different ranges of beam incidence angles: for larger incidence angles (typ., $> 25^\circ$) and smaller incidence angles (typ., $< 25^\circ$). The relay satellite scenario faces higher propagation losses than the trusted node scenario but maintains the security level promised by QKD. The relay satellite makes one-way QKD possible with both Alice and Bob on ground, separated by large distances. A simple loss and key rate calculation shows that relay QKD can provide higher key rates than the entanglement-based or MDI QKD with the flexibility to choose any protocol and wavelength.

REFERENCES

- [1] Yin, H.L. et al, "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber," *Phys. Rev. Lett.* 117, 190501 (2016).
- [2] Yin, J. et al, "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," *Phys. Rev. Lett.* 119, 200501 (2017).
- [3] Lo, H.K., Curty, M. and Qi, B., "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.* 108, 130503 (2012).
- [4] Liao, S.K. et al, "Satellite-Relayed Intercontinental Quantum Network," *Phys. Rev. Lett.* 120, 030501 (2018).
- [5] Villoresi, P. et al, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New J. Phys.* 10, 033038 (2008).
- [6] Perlot, N., Rödiger, J. and Freund, R., "Single-mode optical antenna for high-speed and quantum communications," *ITG-Fachbericht 279: Photonische Netze 11*, 66-69 (2018).
- [7] Perlot, N. and Rohde, M., "Transmission loss between single-mode Gaussian antennas," *Opt. Express* 24, 19491-19496 (2016).
- [8] N. Leonhard, R. Berlich, S. Minardi, A. Barth, S. Mauch, J. Mocchi, M. Goy, M. Appelfelder, E. Beckert, and C. Reinlein, "Real-time adaptive optics testbed to investigate point-ahead angle in pre-compensation of Earth-to-GEO optical communication," *Opt. Express* 24, 13157-13172 (2016).
- [9] Liao, S.K. et al, "Satellite-to-ground quantum key distribution," *Nature* 549, 43-47 (2017).