Evaluation of integration concepts of Optical Ground Stations for satellite-based Quantum Key Distribution into a quantum network

Stefanie Häusler
Institute of Comm. and Nav.
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany
stefanie.haeusler@dlr.de

Davide Orsucci
Institute of Comm. and Nav.
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany
davide.orsucci@dlr.de

Andrew Reeves
Institute of Comm. and Nav.
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany
andrew.reeves@dlr.de

Florian Moll
Institute of Comm. and Nav.
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany
florian.moll@dlr.de

2023 IEEE International Conference on Space Optical Systems and Applications (ICSOS) | 979-8-3503-0790-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSOS59710.2023.10491230

Abstract— **Quantum Key Distribution (QKD) is a promising method to guarantee future-proof, information theoretic security. Since optical fibers have an exponential loss with distance, satellite-based QKD solutions are being developed in order to realize long-distance links. Therefore, Optical Ground Stations for QKD (QKD-OGS) need to be designed to enable quantum communication with satellites. Different link configurations will result in different integration options of the QKD-OGS in the terrestrial fiber network and therefore impact its performance. Applicable integration options must be identified and trade-off analysis conducted at the architecture, system and sub-system level. The reference scenario is a Low Earth Orbit (LEO) downlink configuration employing a decoy-state BB84 protocol with polarization encoded qubits at 1550 nm wavelength. The satellite acts as trusted node for implementation of the key distribution between two parties on ground. Furthermore, only direct connections from the satellite to the end-users are considered, i.e. the QKD-OGS does not serve as a trusted-node relay. This results in the selection of three main integration concepts: first, a free-space, end-user QKD-OGS which is located directly at the end-user where the quantum signal is measured directly behind the receiver telescope in free-space; second, a fiber-coupled, end-user QKD-OGS where the quantum signal is coupled into a single-mode fiber and guided to a co-located server room hosting the QKD Receiver system; third, a fiber-coupled, provider QKD-OGS, which reaches several end-users by using a local fiber network. In order to evaluate these three concepts, the comparison parameter is defined to be an estimated factor of suppliable end-users. The estimated comparison factor shows that the fiber-coupled, end-user QKD-OGS can supply 6.7 times more end users than the free-space, end-user QKD-OGS. The fiber-coupled, end-user QKD-OGS can supply 129.7 times more end-users than the free-space, end-user QKD-OGS.**

Keywords—Optical Ground Station, Quantum Key Distribution, secure communication, quantum network

I. INTRODUCTION

The security of current encryption methods is based on mathematical problems that are supposed to be exponentially hard to solve. Quantum algorithms can efficiently solve some of these problems, such as integer factoring and discrete logarithms. The development of quantum computer would result in the breakdown of the security of the encryption methods that rely on these. Quantum Key Distribution (QKD) is a method to secure communication without relying on these computational assumptions. As a quantum signal is used to exchange the key, the laws of quantum physics apply which means that the information gained by an eavesdropper results in an increased noise of the received quantum signal. With suitable post-processing, there is an arbitrarily low probability that an eavesdropper which does have any information about the key is not detected. [1], [2]

The overall goal of current developments in this field is to be able to establish quantum networks where quantum keys can be exchanged worldwide. To reach this, a quantum channel must be provided to transmit the quantum signal. Optical fibers are feasible for short distances, but cannot be used for long distance due to exponential transmission loss of the fiber. Satellite-based QKD can bridge this as free-space channel loss is quadratic with distance and atmospheric extinction loss is not the dominant factor. On the other hand, other aspects that are specific to free-space optical (FSO) channels need to be considered, like link availability, general weather conditions, signal fluctuations due to turbulence and background light. Furthermore, the satellite must be a trusted node, since the secure key of the end-users is always accessible to the satellite as well [3].

Current developments concentrate to achieve a QKD satellite with small size, weight and power (SWaP) profile. The development in this field is currently pushed forward in satellite missions like the QUBE and QUBE2 mission. [4], [5] This reduces the cost and complexity in space. On the other hand, a small QKD satellite can only be equipped with a laser communication terminal (LCT) having a small aperture, forcing the Optical Ground Station for QKD (QKD-OGS) to have an aperture of about 80 cm in order to close the link budget. This increases the form factor and weight of the QKD-OGS. Another possibility is to launch satellites with a larger LCT aperture and therefore allowing a reduction of the aperture of the QKD-OGS leading to a smaller, less expensive QKD-OGS.

In general, several integration concepts of a QKD-OGS into a quantum network arise, which are shown in Fig. 2. Integration concept #1 features a free-space quantum measurement and is stand-alone. Therefore, this is referred to as free-space, end-user QKD-OGS. Integration concept #2, called fiber-coupled, end-user QKD-OGS, is also stand-alone

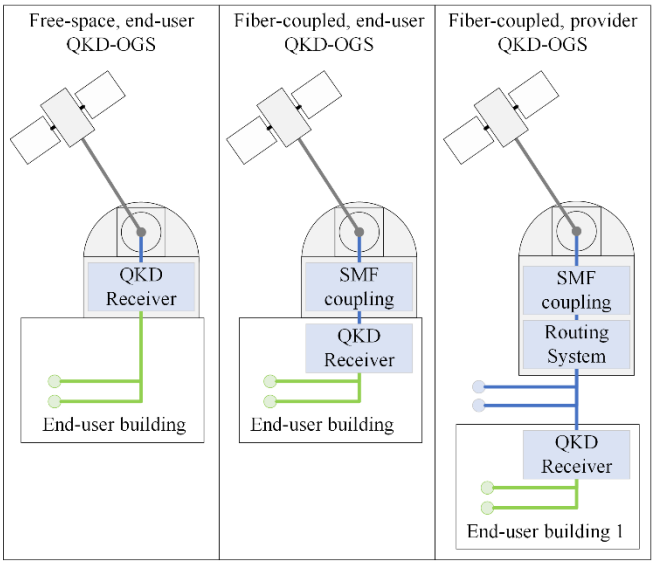

Fig. 2. Overview of the integration concepts (SMF: Single Mode Fiber)

with the difference that the quantum state is measured using a fiber interface. Integration concept #3 is a fiber-coupled, provider QKD-OGS, which is integrated into a fiber network and therefore reaches multiple end users via direct forwarding and optical switching of the quantum signal through the fiber. For a first comparison of the QKD-OGS resulting from the integration concepts, the LCT aperture of the satellite is kept the same for all QKD-OGS to be compared to allow for an evaluation on equal footing. A method to compare the integration concepts of the QKD-OGS is provided and the evaluation by using estimates of influencing parameters is carried out.

A reference scenario is selected in Sec. II to limit the amount of integration concepts and QKD-OGS system designs to be considered. An overview of the three integration options is given, which shows the differences between the three concepts. The method chosen to evaluate the integration concepts is described in Sec. III, starting with a method to design the QKD-OGS for the different integration concepts and afterwards defining the evaluation parameter. In Sec. IV the estimation of the evaluation parameter is carried out. In Sec. V the result of the evaluation is discussed and further actions required to obtain a more precise estimation of the evaluation parameter and to evaluate the overall quantum network architecture are outlined. A conclusion is given in Sec. VI.

II. Optical Ground Station for Satellite-based QKD

A. Reference scenario

To realize satellite-based QKD technically in the viewpoint of the QKD-OGS, several reference scenario options are possible. To evaluate the different integration concepts of a QKD-OGS a reference scenario is defined.

For the evaluation of the integration concepts of the QKD-OGS a downlink configuration is chosen. The disadvantages of an uplink configuration are higher transmission loss [3], higher background light [6] and higher dark counts of the detector due to radiation exposure in orbit [7].

The connection from the satellite to the QKD-OGS to the end-user could be established in a direct way, meaning the quantum signal or quantum key is forwarded directly to the end-user. The QKD-OGS could also serve as a trusted node relay, so that the QKD-OGS detects the quantum signal from the satellite and provides a new quantum signal to the end-user. Another option could be to use a measurement-device-independent protocol. The disadvantage of a measurement-device-independent protocol is that it requires synchronisation of laser pulses originating from the satellite and from the end-user with high accuracy. This is technologically challenging and not yet experimentally demonstrated. Measurement-device-independent protocols are therefore excluded in this evaluation. Furthermore, only the direct connection between QKD-OGS and end-user is considered, because it is assumed that the number of trusted node relays should be kept to an absolute minimum as they present a potential security risk. Moreover, this assumption results in a simplified system architecture for this evaluation of the QKD-OGS integration concepts.

A satellite in Low Earth Orbit (LEO) is chosen since these are characterised by the shortest link distances and thus the highest quantum signal collection efficiency. Furthermore, 1550 nm is selected as a wavelength to allow high compatibility with existing fiber components. It is further defined that decoy-state BB84 protocol with polarization-encoded qubits is used. This protocol is chosen as several proof-of-concept experiments have already been successful [3].

The choice to focus on a downlink scenario and a direct connection to the end-user results in the architecture shown in Fig. 1. The QKD-OGS consists of an OGS and a QKD Receiver, which includes the post-processing systems. Therefore, the QKD Receiver generates the final key by using a bi-directional classical channel to the satellite and delivers the quantum key to the Key Management System (KMS) of the end-user. As the quantum state is measured in the QKD-OGS in the reference scenario, the QKD Receiver, the KMS and the end-user need to be within a private area.

The specifications of the QKD satellite shown in Tab. I shall be considered as a reference scenario.

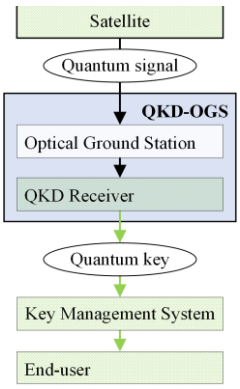

Fig. 1. System architecture of a QKD satellite-to-ground scenario (in green: private area)

Table I. Relevant specification of the QKD satellite

Parameter	Specification
Aperture diameter	25 cm (central obscuration: 8 cm)
M^2	1.2
Transmitter altitude	500 km
Pulse rate R_{Alice}	1 GHz

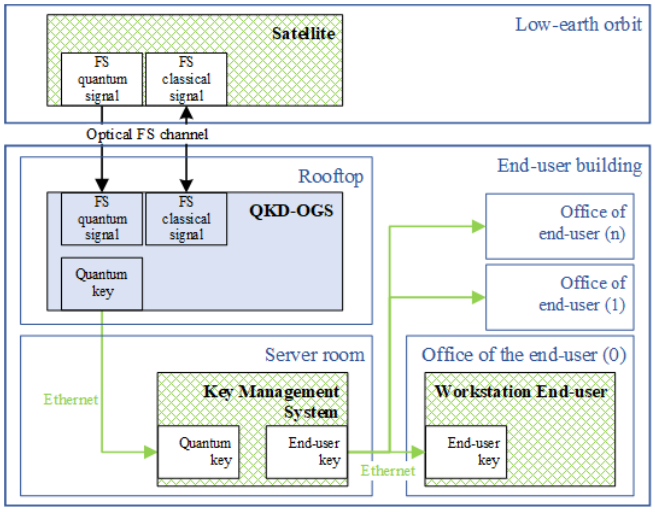

Fig. 3. Integration concept #1: free-space, end-user QKD-OGS (FS: free-space; FC: fiber-coupled; in green: private area)

B. Integration concepts of an QKD-OGS into a quantum network

1) Integration concept #1: Free-space, end-user QKD-OGS

The integration concept of the free-space, end-user QKD-OGS is shown in Fig. 3. The satellite transmits the quantum signal via the optical free-space channel. The QKD-OGS is located at the rooftop of the end-user and the QKD Receiver module is placed directly behind the OGS telescope. The quantum signal is measured on the rooftop of the end-user by means of a free-space detector. The post-processing happens in the QKD Receiver on the rooftop using the bi-directional classical link to the satellite. The final quantum key is guided via ethernet to a sever room where the KMS of the end-user is located. From there, the quantum key can be delivered to multiple end-users within the end-user building. As the QKD Receiver is located behind the OGS telescope, the quantum signal is measured there, concluding that the data line to transmit the final key to the end-user is classical from the QKD Receiver on. Therefore, in this integration concept the QKD-OGS, the connection to the server room, the KMS and the connection from KMS to the workstation of the end-user must be within a defined private area, because data privacy is not enforced via quantum key distribution in this area.

2) Integration concept #2: Fiber-coupled, end-user QKD-OGS

The fiber-coupled, end-user QKD-OGS, shown in Fig. 4, is also located on the rooftop of the end-user location. The OGS includes an integrated fiber-coupling module. The quantum signal is guided from the OGS to the QKD Receiver via fiber. The QKD Receiver is placed in a server room where the KMS is located as well. This decreases the private area compared to integration concept #1. After generating the quantum key in the post-processing, the quantum key is sent to the KMS placed in the server room and then transmitted to the end-user.

3) Integration concept #3: Fiber coupled, provider QKD-OGS

The integration concept of a fiber-coupled, provider QKD-OGS for the defined reference scenario is shown in Fig. 5. Here, the OGS is hosted by a dedicated provider building. The

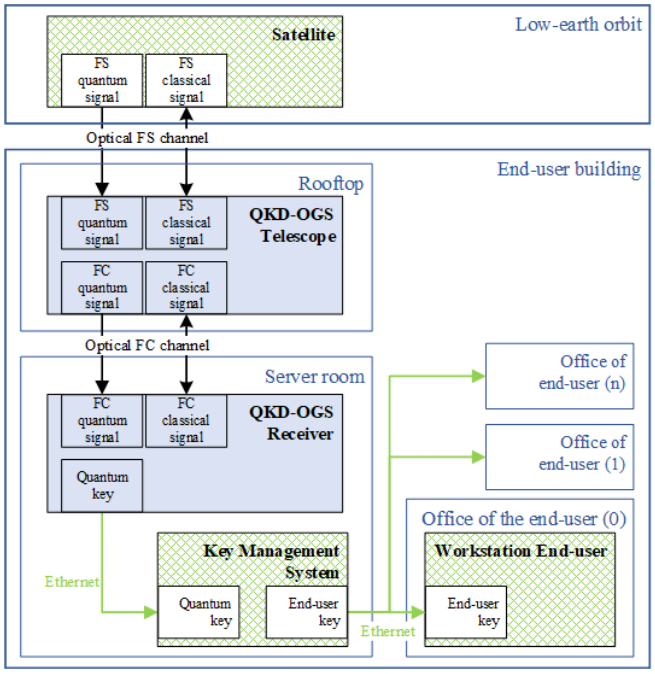

Fig. 4. The integration concept #2: fiber-coupled, end-user QKD-OGS (FS: free-space; FC: fiber-coupled; in green: private area)

quantum signal is received by the OGS telescope, is coupled to single-mode fiber and forwarded to a server room that hosts a routing system. This routing system connects the end-user to its data line. This can happen via wavelength separation, meaning the routing is via wavelength division multiplexing, or by time, meaning the quantum signal for different end-users is separated in time and thus the end-user is selected by an optical switch.

In the case chosen, the end-user is directly connected to the OGS in a star topology. In practice it is likely that in between the server room and the end-user more routing systems, e.g. optical switches, will exists and therefore a more complex routing topology will arise. Additionally, the routing system can also be hosted by a different provider than the QKD-OGS' provider and can also be located in another building. The routing system must provide a quantum channel and a bi-directional classical channel to the end-user.

In the building of the end-user the QKD Receiver, KMS and workstation of the end-user is located and the key is distributed to the end-user as shown in the other integration concepts.

III. Method of Evaluation

A. Method of designing the QKD-OGS for the different integration concepts

A comparison of the concepts includes the process of designing the OGS. Primarily the aperture size is important, as this significantly influences the end-to-end transmission loss and thus the performance. Here, both end-user QKD-OGS are assumed to have the same aperture size. The end-user QKD-OGS should have a small form factor and be easy to deploy. The Optical Ground Station Oberpfaffenhofen (OGSOP) with 40 cm aperture diameter, has shown easy deployment in the past and therefore is categorized to meet these requirements [8]. Therefore, 40 cm aperture diameter with 12 cm central obscuration is chosen here as reference system for the end-user QKD-OGS. The fiber-coupled, provider QKD-OGS should have a much larger aperture size

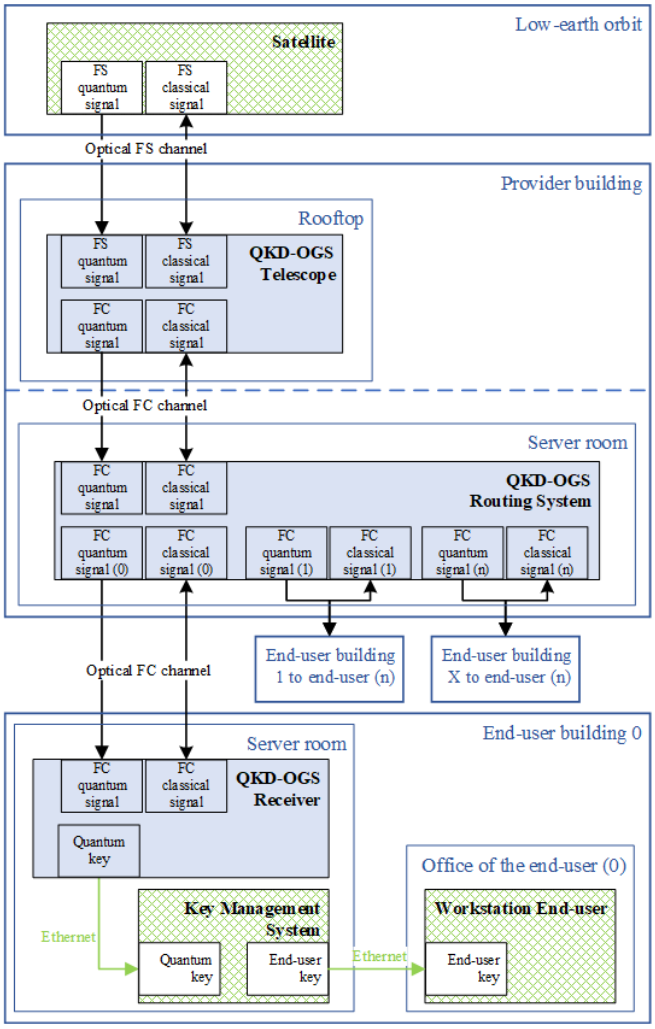

Fig. 5. Integration concept #3: fiber-coupled, provider QKD-OGS (FS: free-space; FC: fiber-coupled; in green: private area)

to be able to distribute the quantum signal to several end-users. Satellite-based entanglement distribution has been demonstrated with a 1.8 m telescope in China [9]. 2 m telescopes used in observatories can be found, e.g. the Wendelstein observatory [10]. Therefore, a 2 m aperture diameter with 60 cm central obscuration is chosen for the fiber-coupled, provider QKD-OGS.

B. Definition of the evaluation parameter

The evaluation parameter that is important for the end-user is the Secure Key Length (SKL) that can be delivered in a certain time frame. To provide this value several parameters need to be considered. First, the number of satellite passes above a given QKD-OGS location for a specific orbit within a given time frame need to be identified. Then, the range of elevation angles in which QKD is possible need to be identified. This is influenced by the acquisition time and the blind spot at the zenith of the OGS, which is present in two-axes mounted telescopes. From this, the passes will be further reduced by the downtime of the individual systems, namely the satellite, the OGS, the QKD Receiver, if necessary, the SMF coupling module and the channel influenced by environmental conditions. For the remaining passes the finite key for each pass can be calculated and added up to get the SKL for the selected time frame.

For now, this comparison can be simplified as the comparison of the integration concepts is prioritized. For this, the comparison factor representing the number of end-users that can be supplied with a quantum key $f_{\#end-user}$ is introduced here. This factor is defined to be the Secure Key Rate (SKR) of the free-space, end-user QKD-OGS divided by the SKR of the QKD-OGS to be evaluated. For the purpose of simplification the SKR is only calculated at 30° elevation.

$$f_{\#\mathrm{end-user}} = \frac{\mathrm{SKR}_{\mathrm{QKD-OGS}}(\mathrm{El.}=30°)}{\mathrm{SKR}_{\mathrm{free-space,end-user\ QKD-OGS}}(\mathrm{El.}=30°)} \quad (1)$$

On the example of decoy-state BB84 protocol with polarization encoded qubits with passive choice of measurement basis, the SKR is derived for each of the QKD-OGS as shown as in Appendix A.

Summarizing, the QBER and SKR can be calculated for a specific system setup. The QKD-OGS can influence the QBER by controlling the following parameters: misalignment angle, received background light (wavelength, effective filter bandwidth, transmittivity of the optical system, receiver aperture and FOV), gating time of the detector, end-to-end transmittivity (antenna gain and internal losses), polarization dependent loss, dark count rate of the detector, efficiency of the detector. The parameters are estimated for each of the integration concepts by using literature, existing experimental data and simulation tools. The QBER, SKR and $f_{\#\mathrm{end-user}}$ are calculated for each of the presented QKD-OGS concepts.

IV. Estimation of the Comparison Factor

The comparison factor introduced in (1) in Sec. III.B. to evaluate the integration concepts of the QKD-OGS is now derived for the three different QKD-OGS concepts. Therefore, all influencing factors need to be estimated first.

A link budget for each of the three integration concepts is provided in Tab. II. The SMF coupling loss is set to be -5 dB at 30° elevation for all QKD-OGS concepts. The Adaptive Optics (AO) as a sub-system of the SMF coupling module corrects the wavefront distortion across the aperture. With a larger aperture diameter larger variation of the wavefront distortion needs to be corrected by the AO. Therefore, an AO for a larger aperture diameter telescope needs to be equipped with high performance wavefront sensor, deformable mirror and control software. Being aware of this, it is still evaluated to be realistic to design an SMF coupling module that can reach -5 dB coupling loss at 30° elevation for both the 40 cm and 2 m aperture diameter telescope. For the Rx optical and splitting loss -1 dB and -1.5 dB is assumed for the free-space and the fiber-coupled QKD-OGS respectively. For the fiber-connection loss -3 dB is assumed for the fiber-coupled, end-user QKD-OGS and the fiber-coupled, provider QKD-OGS. It is the fiber connection to the end-user and shall include the routing system and the fiber length to the end-user.

Starting at the transmitter the specification is taken from Tab. I. The misalignment angle δ of the system is set to be 5° [11]. Misalignment angle fluctuations in fiber are technological challenging to compensate. For simplification purposes, it is assumed that δ does not increase when using fibers.

For the QKD Receiver a detector must be chosen. The state-of-the art, commercially available detectors that can be found at the time of publication are the ID Qube NIR, IDQ fitting the need of a free-space detector and a superconducting-nanowire single photon detector (SNSPD) for the fiber-coupled detector. Here, an SNSPD from IDQ is

taken as a reference. The specifications can be found in Tab. III.

The dark count rate of the detector is suppressed by the gating time Δt=400 ps for the free-space, end-user QKD-OGS and Δt =100 ps for the fiber-coupled QKD-OGS. The difference is due to the chosen detector systems having different timing jitter. Night time operations are assumed and thus the rate of background light photons coupled in the QKD Receiver is assumed to be negligible for this analysis.

The resulting QBER, SKR and $f_{\#end-user}$ calculated with the assumptions made and the method described in Sec. III. is shown in Tab. IV. Thus, the evaluation shows that with the estimations made the fiber-coupled, end-user QKD-OGS can supply 6.7 times more end-users than the free-space, end-user QKD-OGS. The fiber-coupled, provider QKD-OGS can supply 129.7 times more end-users than the free-space, end-user QKD-OGS.

TABLE II. LINK BUDGET

	Free-space, end-user QKD-OGS	**Fiber-coupled, end-user QKD-OGS**	**Fiber-coupled, provider QKD-OGS**
Tx antenna gain [dB]	109.2	109.2	109.2
Tx pointing loss [dB]	-3.0	-3.0	-3.0
Free-space loss at 30° elevation [dB]	-257.3	-257.3	-257.3
Atmospheric loss at 30° elevation [dB]	-0.5	-0.5	-0.5
Rx antenna gain [dB]	117.8	117.8	131.7
Rx optical and splitting loss [dB]	-1.0	-1.5	-1.5
SMF coupling loss at 30° elevation [dB]	0	-5.0	-5.0
Fiber connection loss [dB]	0	-3.0	-3.0
Total channel loss at 30° elevation η_{Ch} [dB]	-37.7	-42.3	-29.4

TABLE III. DETECTOR CHARACTERISTICS OF COMMERCIALLY AVAILABLE DETECTORS AT 1550NM [12], [13]

Detector	**ID Qube NIR, IDQ**	**SNSPD ID281, IDQ**
Quantum efficiency η_{detector}	0.20	0.90
Dark count rate R_{DCR}	3 kHz	90 Hz
Dead time T_{d}	100 ns	30 ns
Jitter	200 ps	30 ps

TABLE IV. GLOBAL QBER, SKR AND $f_{\#\mathrm{END-USER}}$ AT 30° ELEVATION

	Free-space, end-user QKD-OGS	**Fiber-coupled, end-user QKD-OGS**	**Fiber-coupled, provider QKD-OGS**
Global QBER [%]	6.3	0.9	0.8
SKR [bits/sec]	1056	7050	137012
$f_{\#\mathrm{end-user}}$	1	6.7	129.7

V. DISCUSSION

The presented evaluation is of interest for the lower level design of the sub-systems of the QKD-OGS, the conceptualization of the QKD-OGS itself and the higher-level impact on the quantum network including the QKD satellite and the user needs.

Whilst a provider QKD-OGS can be operated by a provider which sells the quantum key distribution as a service to the end-user, the end-user QKD-OGS holds the possibility of operating the device on its own which might be required in some cases. The end-user QKD-OGS allows lower weight and form factor.

The fiber-coupled QKD-OGS need a fiber connection to the end-user. Furthermore, the design of an optical routing system needs to be taken care of which meets the security requirements. Both the fiber-coupled, end-user QKD-OGS and the fiber-coupled, provider QKD-OGS require a decreased private area which can be located completely inside the end-user building. A free-space, end-user QKD-OGS cannot provide this and the overall operation concept needs to ensure that the private area starts behind the telescope and further covers the connection from QKD Receiver module to the KMS and the end-user. However, this concept has the advantage of less complexity and higher maturity compared to the other concepts.

The results in Tab. IV show that the fiber-coupled, end-user QKD-OGS can provide a higher performance due to the ability to choose a SNSPD with higher detection efficiency, lower dark count rate and lower possible gating time due to the lower jitter. The provider QKD-OGS can supply even more end-users by a factor of $f_{\#\mathrm{end-user}}$=129.7 compared to the free-space, end-user QKD-OGS due to the large receiver aperture of 2 m.

For the end-user and providers, the costs of a quantum key to be generated is crucial. The costs per secure quantum key bit is not only dependent on the QKD-OGS but on the overall quantum network design which will result in the SKR over a certain time span and an overall cost. Therefore, and to get a more accurate performance estimation of a QKD-OGS, it is specifically interesting to simulate the SKL over a certain time span for different scenarios. To come to a valid comparison in the end several parameters need to be considered like possible passes, QKD relevant elevation range determined by acquisition phase and zenith pass problem, uptime of the sub-systems namely the transmitter, the OGS, the receiver, the SMF coupling module and the channel itself. Furthermore, the expected background light at the time of the satellite pass need to be included in these simulations.

Considering the uptime of the sub-systems this will not only result in a SKL in a certain time span, but also in the key availability. Here, it is crucial to know from the user how long a key is allowed to be stored and what amount of data needs to be encrypted in order to evaluate the reachable key availability. Furthermore, the uptime of the satellite for a specific QKD-OGS must include the link availability between satellite and QKD-OGS. The link availability of one single satellite for one QKD-OGS will decrease when increasing the overall number of QKD-OGS. Number of satellites and QKD-OGS and their quantum key throughput must be matched to come to an efficient constellation. To further optimize the

evaluation, all influencing parameters should be estimated more precisely.

From a lower system level point of view, the sub-system developers must be provided with specific requirements that each of the sub-systems must reach to allow for a certain performance of the QKD-OGS. At the same time, to evaluate the QKD-OGS integration concepts realistically it must be ensured that the sub-systems are well-known and performance boundaries are understood.

VI. Conclusion

Three integration concepts, namely the free-space, end-user QKD-OGS, the fiber-coupled, end-user QKD-OGS and the fiber-coupled, provider QKD-OGS, have been presented. The end-user QKD-OGS allows for an easy installation at the end-user's rooftop. It is outlined that the private area is substantially different for free-space coupled and fibre-coupled systems. A fiber-coupled QKD-OGS allows for an implementation where the private area is limited to the QKD Receiver and the connection to the end-user. A comparison of the SKR at an elevation of 30° of the three integrations concepts, shows that a fiber-coupled QKD-OGS can supply 6.7 times more end-users and a fiber-coupled, provider QKD-OGS 129.7 times more end-users.

This evaluation gives an estimation on performance for the different QKD-OGS integration concepts. At the same time, it is crucial to develop further simulation tools to get more accurate estimations. The evaluation of these parameters will ultimately be driven by a holistic assessment of the whole quantum network setup, of which the QKD-OGS is only a sub-system.

The evaluation shows the importance of carefully evaluating the different link concepts considering the entire system architecture in order to realise a quantum network which sub-systems are holistically and not only unilaterally low-cost, small size, low weight and high performant. The three presented QKD-OGS integration options are likely to be successful in different environments but the overall quantum network must match the needs of the end users.

Acknowledgment

The project on which this report is based was funded by the German Federal Ministry of Education and Research under the funding code 16KIS1265. The authors are responsible for the content of this publication.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, 'Quantum cryptography', *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, 'The security of practical quantum key distribution', *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/RevModPhys.81.1301.

[3] R. Bedington, J. M. Arrazola, and A. Ling, 'Progress in satellite quantum key distribution', *Npj Quantum Inf.*, vol. 3, no. 1, p. 30, Dec. 2017, doi: 10.1038/s41534-017-0031-5.

[4] Knips, Lukas, Auer, Michael, Adomas, Baliuka, and Ömer Bayraktar, 'QUBE–Towards Quantum Key Distribution with Small Satellites'.

[5] M. Hutterer *et al.*, 'QUBE-II - Quantum Key Distribution with a CubeSat', in *73rd International Astronautical Congress, IAC 2022*, Paris, Frankreich, Sep. 2022. Accessed: Sep. 04, 2023. [Online]. Available: https://iafastro.us4.list-manage.com/track/click?u=8a03d3b7f15ba5be6f8125bf9&id=eb6e251842&e=868c55cbf9

[6] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, and P. Villoresi, 'Link budget and background noise for satellite quantum key distribution', *Adv. Space Res.*, vol. 47, no. 5, pp. 802–810, Mar. 2011, doi: 10.1016/j.asr.2010.11.009.

[7] M. A. Krainak, A. W. Yu, G. Yang, S. X. Li, and X. Sun, 'Photon-counting detectors for space-based laser receivers', in *Quantum Sensing and Nanophotonic Devices VII*, SPIE, Jan. 2010, pp. 676–684. doi: 10.1117/12.846983.

[8] F. Moll, S. Nauerth, C. Fuchs, J. Horwath, M. Rau, and H. Weinfurter, 'Communication system technology for demonstration of BB84 quantum key distribution in optical aircraft downlinks', in *Laser Communication and Propagation through the Atmosphere and Oceans*, SPIE, Oct. 2012, pp. 9–16. doi: 10.1117/12.929739.

[9] D. He, Y.-M. Huang, Q. Wang, B. Qi, W.-S. Liu, and D.-J. Zhong, 'An acquisition technology of optical ground station in satellite-ground QKD', in *Astronomical Optics: Design, Manufacture, and Test of Space and Ground Systems*, SPIE, Sep. 2017, pp. 197–207. doi: 10.1117/12.2272920.

[10] U. Hopp *et al.*, 'Improving the Wendelstein Observatory for a 2m-class telescope', in *Observatory Operations: Strategies, Processes, and Systems II*, SPIE, Jul. 2008, pp. 565–573. doi: 10.1117/12.787071.

[11] S.-K. Liao *et al.*, 'Satellite-to-ground quantum key distribution', *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017, doi: 10.1038/nature23655.

[12] 'ID Qube NIR Free-Running', *ID Quantique*. https://www.idquantique.com/quantum-sensing/products/id-qube-nir-free-running/ (accessed Aug. 16, 2023).

[13] 'ID281 Superconducting Nanowire Series', *ID Quantique*. https://www.idquantique.com/quantum-sensing/products/id281-snspd-series/ (accessed Aug. 16, 2023).

[14] A. Scriminich *et al.*, 'Optimal design and performance evaluation of free-space quantum key distribution systems', *Quantum Sci. Technol.*, vol. 7, no. 4, p. 045029, Oct. 2022, doi: 10.1088/2058-9565/ac8760.

[15] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, 'Squashing model for detectors and applications to quantum-key-distribution protocols', *Phys. Rev. A*, vol. 89, no. 1, p. 012325, Jan. 2014, doi: 10.1103/PhysRevA.89.012325.

[16] 'Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD - IOPscience'. https://iopscience.iop.org/article/10.1088/1367-2630/ac7f4e/meta (accessed Aug. 16, 2023).

Appendix A

In this appendix, the SKR is derived for a decoy-state BB84 protocol with polarization encoded qubits with passive choice of measurement basis, see Fig. 6. The QBER needs to be calculated and the optimised parameters of the decoy-state protocol have to be obtained numerically.

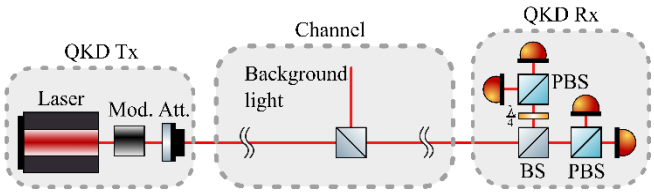

Fig. 6. Schematic drawing of a decoy-state version of the BB84 protocol with polarization encoded qubits with passive choice of measurement basis (Mod.: Modulator; Att.: Attenuator; PBS: Polarization beam splitter; BS: 50:50 Beam splitter)

A. Description of state preparation for decoy-state BB84

The polarization $P \in \{\mathrm{H}, \mathrm{V}, \mathrm{D}, \mathrm{A}\}$ can encode a qubit via the mapping $|\mathrm{H}\rangle \equiv |0\rangle$, $|\mathrm{V}\rangle \equiv |1\rangle$, $|\mathrm{D}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\mathrm{A}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Ideally, Alice would choose a polarization angle

$$\theta \in \left\{0, \frac{\pi}{2}, \frac{\pi}{4}, -\frac{\pi}{4}\right\} \tag{2}$$

to select a polarization state. The prepared polarization state will be misaligned by the misalignment angle δ due to imperfections in the system, including birefringence in the channel and the relative misalignment of Alice's and Bob's setups. For a moving transmitter or receiver, the polarization reference frame rotates and must be compensated, which will introduce a residual misalignment angle. Here, the misalignment angle of the whole system is projected onto Alice's setup and thus Alice prepares a state with polarisation

$$\bar{\theta} = \theta + \delta. \tag{3}$$

where Bob's setup, by assumption, defines the reference polarisation. He measures the state either in the rectilinear basis $\{|\mathrm{H}\rangle, |\mathrm{V}\rangle\}$ or in the diagonal basis $\{|\mathrm{D}\rangle, |\mathrm{A}\rangle\}$.

Three values for the signal intensity prepared by Alice are considered here in order to implement the decoy-state method. These are $\mu \in \{\mu_0, \mu_1, \mu_2\}$, where μ_0 denotes the vacuum pulse $(\mu_0 = 0)$, μ_1 denotes the weak decoy pulse and μ_2 denotes the signal pulse, with$(0 < \mu_1 < \mu_2 < 1)$.

B. Model of a QKD receiver with passive choice of measurement basis and threshold detectors

Considering the prepared polarization state and the misalignment angle, the intensity for each polarization direction are given with respect to the QKD receiver:

$$\begin{cases} \mu_H = \mu \cdot \cos^2(\bar{\theta}) \\ \mu_V = \mu \cdot \sin^2(\bar{\theta}) \end{cases} \begin{cases} \mu_D = \mu \cdot \cos^2(\bar{\theta} - \pi/4) \\ \mu_A = \mu \cdot \sin^2(\bar{\theta} - \pi/4) \end{cases} \tag{4}$$

In the channel the quantum signal will be attenuated by the channel transmittivity η_{Ch} including all losses up to the 50:50 BS of the QKD Receiver module. Furthermore, in the free-space channel an average amount of background light photons will couple into the detector. The rate of background light photons coupled in front of the QKD Receiver I will depend on the chosen wavelength, effective filter bandwidth, transmittivity of the receiving optical system and, in case no SMF coupling is included in the system, on the field of view (FOV) and receiver area [14]. Within the gating time Δt an average amount of background light photons of $\upsilon = \frac{1}{2}\mathrm{I}\Delta\mathrm{t}$ is detected in front of each of the four detectors, where the factor $\frac{1}{2}$ stems from the fact that the background light is assumed to be unpolarised. The effect of the 50:50 BS will be considered later in η_{receiver}.

The overall average amount of photons collected by each of the four detectors is given by:

$$\begin{cases} \tau_{\mathrm{H}} = \eta_{\mathrm{Ch}}\mu_{\mathrm{H}} + \frac{1}{2}I\Delta t \\ \tau_{\mathrm{V}} = \eta_{\mathrm{Ch}}\mu_{\mathrm{V}} + \frac{1}{2}I\Delta t \end{cases} \begin{cases} \tau_{\mathrm{D}} = \eta_{\mathrm{Ch}}\mu_{\mathrm{D}} + \frac{1}{2}I\Delta t \\ \tau_{\mathrm{A}} = \eta_{\mathrm{Ch}}\,\mu_{\mathrm{A}} + \frac{1}{2}I\Delta t \end{cases} \tag{5}$$

The single-photon detectors are modelled as threshold detectors which cannot distinguish between single-photon states and multi-photon states. The probabilities for each detector to register a click depend on the received signal intensity, including the background light contributions, as well as on the Dark Count Rate (DCR) R_{DCR} within the gating time Δt. Assuming that the photon number distribution is Possonian, these probabilities are given by:

$$\begin{cases} p_{\mathrm{H}} = 1 - \exp\left(-\tau_{\mathrm{H}}\eta_{\mathrm{receiver,H}} - R_{\mathrm{DCR}}\Delta t\right) \\ p_{\mathrm{V}} = 1 - \exp\left(-\tau_{\mathrm{V}}\eta_{\mathrm{receiver,V}} - R_{\mathrm{DCR}}\Delta t\right) \\ p_{\mathrm{D}} = 1 - \exp\left(-\tau_{\mathrm{D}}\eta_{\mathrm{receiver,D}} - R_{\mathrm{DCR}}\Delta t\right) \\ p_{\mathrm{A}} = 1 - \exp\left(-\tau_{\mathrm{A}}\eta_{\mathrm{receiver,A}} - R_{\mathrm{DCR}}\Delta t\right) \end{cases} \tag{6}$$

where η_{receiver} is the efficiency to detect a signal with the receiver setup for each polarisation, including both the quantum efficiency of the detector η_{detector} and the transmission η_{BS} or reflection $1 - \eta_{\mathrm{BS}}$ of the beam splitter for this path, so that $\eta_{\mathrm{receiver,H}} = \eta_{\mathrm{receiver,V}} = \eta_{\mathrm{detector}}\eta_{\mathrm{BS}}$ and that $\eta_{\mathrm{receiver,H}} = \eta_{\mathrm{receiver,V}} = \eta_{\mathrm{detector}}(1 - \eta_{\mathrm{BS}})$. It is assumed that the beam splitter is balanced, $\eta_{\mathrm{BS}} = 1 - \eta_{\mathrm{BS}} = 1/2$, so that the rectilinear basis and the diagonal basis measurements are performed by Bob's setup with equal probability.

The observed click pattern is mapped to one of the 5 possible outcomes $O \in \{\emptyset, \mathrm{H}, \mathrm{V}, \mathrm{D}, \mathrm{A}\}$ using the squashing model approach [15] in order to map the outcomes of the four threshold detectors to a single equivalent outcome $\widetilde{\mathrm{O}} \in \{\emptyset, \mathrm{H}, \mathrm{V}, \mathrm{D}, \mathrm{A}\}$ of an ideal, photon-number-resolving detector. No-click events have to be mapped to no-click events of the ideal detector. If there are one or more clicks in two different bases, it is also mapped to a no-click event. If there are two clicks in the same basis, the click will be mapped randomly to one of the detectors. If there is only one click in one basis, the click will be mapped to the detector that clicked. [15]

Following this prescription, the probability $\tilde{p}_{\mathrm{O}}$ of each outcome $\tilde{O}$ can be computed to be

$$\tilde{p}_{\emptyset} = (1 - p_{\mathrm{H}})(1 - p_{\mathrm{V}})(1 - p_{\mathrm{D}})(1 - p_{\mathrm{A}}) + p_{+}p_{\times} \tag{7}$$

$$\tilde{p}_{\mathrm{H}} = \left(p_{\mathrm{H}} - \frac{p_{\mathrm{H}}p_{\mathrm{V}}}{2}\right)(1 - p_{\times}) \tag{8}$$

$$\tilde{p}_{\mathrm{V}} = \left(p_{\mathrm{V}} - \frac{p_{\mathrm{H}}p_{\mathrm{V}}}{2}\right)(1 - p_{\times}) \tag{9}$$

$$\tilde{p}_{\mathrm{D}} = \left(p_{\mathrm{D}} - \frac{p_{\mathrm{D}}p_{\mathrm{A}}}{2}\right)(1 - p_{+}) \tag{10}$$

$$\tilde{p}_{\mathrm{A}} = \left(p_{\mathrm{A}} - \frac{p_{\mathrm{D}}p_{\mathrm{A}}}{2}\right)(1 - p_{+}) \tag{11}$$

where

$$p_{+} = p_{\mathrm{H}} + p_{\mathrm{V}} - p_{\mathrm{H}}p_{\mathrm{V}} \tag{12}$$

and

$$p_{\times} = p_{\mathrm{D}} + p_{\mathrm{A}} - p_{\mathrm{D}}p_{\mathrm{A}} \tag{13}$$

are respectively the probabilities of at least one click in the rectilinear and in the diagonal basis.

C. Calculation of the signal detection rate

The signal detection rate R_{Bob} can be computed from Alice's setup pulse repetition rate R_{Alice}, from Bob's setup click probability per pulse and from the detector dead time, i.e. the time required for a detector to recover after a photon detection.

The probability per transmitted pulse that the QKD receiver clicks, including post-processing, is given by

$$\tilde{p}_{\mathrm{click}} = 1 - \tilde{p}_{\emptyset}. \tag{14}$$

The click probability per pulse implicitly depends on the pulse intensity $\mu \in \{\mu_0, \mu_1, \mu_2\}$ employed by Alice, $\tilde{p}_{\mathrm{click}} = \tilde{p}_{\mathrm{click}}(\mu)$. The global click probability is given by the average

of these click probabilities, weighted by the probability p_μ of choosing each of the three intensities

$$\tilde{p}_{\text{click,avg}} = \sum_\mu p_\mu \cdot \tilde{p}_{\text{click}}(\mu). \quad (15)$$

The signal detection rate is then

$$R_{\text{Bob}} = R_{\text{Alice}} \cdot \tilde{p}_{\text{click,avg}} \cdot r_{\text{uptime}} \quad (16)$$

where R_{Alice} is the repetition rate of Alice's transmitter and the uptime ratio r_{uptime} is the fraction of the time the receiver is not in dead time T_{d}. This is computed as

$$r_{\text{uptime}} = \frac{\Delta t_{\text{click}}}{\Delta t_{\text{click}} + T_{\text{d}}} \quad (17)$$

where Δt_{click} is the expected time difference between two consecutive clicks, excluding the effect of the dead time:

$$\Delta t_{\text{click}} = \frac{1}{\tilde{p}_{\text{click,avg}} \cdot R_{\text{Alice}}}. \quad (18)$$

It is assumed that the signal photons always arrive at the detector within the gate time window and thus the signal detection rate is not affected by the gating time [14]. This assumption is justified by the choice of a gating time which is much larger than the standard deviation of the signal time of arrival. Furthermore, polarization-dependent mode dispersion is considered to be negligible.

D. Calculation of the Quantum Bit Error Rate

In general, the QBER is given by

$$\text{QBER} = \frac{\text{noise clicks}}{\text{total clicks}} \quad (19)$$

The QBER can then be computed in the following manner for each angle θ that Alice can choose. First, the basis sifting dictates that Alice and Bob discard all events in which Bob's basis doesn't match Alice's. This then defines the entire set of valid events. Then, the QBER is the proportion in which Alice and Bob bits are different. This results in:

$$\text{QBER}(\theta = 0) = \frac{\tilde{p}_{\text{V}}}{\tilde{p}_{\text{H}} + \tilde{p}_{\text{V}}} \quad (20)$$

$$\text{QBER}\left(\theta = \frac{\pi}{2}\right) = \frac{\tilde{p}_{\text{H}}}{\tilde{p}_{\text{H}} + \tilde{p}_{\text{V}}} \quad (21)$$

$$\text{QBER}\left(\theta = \frac{\pi}{4}\right) = \frac{\tilde{p}_{\text{A}}}{\tilde{p}_{\text{D}} + \tilde{p}_{\text{A}}} \quad (22)$$

$$\text{QBER}\left(\theta = -\frac{\pi}{4}\right) = \frac{\tilde{p}_{\text{D}}}{\tilde{p}_{\text{D}} + \tilde{p}_{\text{A}}} \quad (23)$$

The QBER in the rectilinear basis, QBER_+, is the average of the QBER for $\theta = 0$ and for $\theta = \frac{\pi}{2}$, and the QBER in the diagonal basis $\text{QBER}_\times$ is analogously defined. The average QBER ($\text{QBER}_{\text{global}}$) is given by the weighted average of the QBERs as it is assumed that the probability of Alice choosing a value θ for the polarization setting is equal.

E. Calculation of the Secret Key Rate

The secure key generation rate is calculated according to the analysis presented in [16]. Only the pulses that are prepared and measured in the rectilinear (+) basis are used to generate the final secure key, while the pulses prepared and measured in the diagonal (×) basis are only used for parameter estimation. It is then advantageous to bias the basis choice increasing the probability of employing the Z basis to increase the key generation rate.

Preliminarily, it is necessary to compute several auxiliary quantities. The average number of signals $N_{\text{Bob},\mu}$ detected by Bob for each signal intensity μ during the total QKD link time t_{link} is given by

$$N_{\text{Bob},\mu} = R_{\text{Bob}} \cdot t_{\text{link}} \cdot p_\mu. \quad (24)$$

The average number of received signals sifted in the rectilinear basis $N_{\text{Bob},\mu,+}$ and in diagonal basis $N_{\text{Bob},\mu,\times}$ are

$$N_{\text{sifted},\mu,+} = N_{\text{Bob},\mu} \cdot p_{\text{Alice},\mu,+} \cdot \tilde{p}_+(\mu) \quad (25)$$

$$N_{\text{sifted},\mu,\times} = N_{\text{Bob},\mu} \cdot p_{\text{Alice},\mu,\times} \cdot \tilde{p}_\times(\mu) \quad (26)$$

where $\tilde{p}_+ \approx \tilde{p}_\times \approx 0.5$ are the probabilities that Bob measures a click in the rectilinear and diagonal basis, which are mainly determined by the BS transmission and reflection coefficients, while $p_{\text{Alice},\mu,+} = p_\mu p_{\text{Alice},+}$ and $p_{\text{Alice},\mu,\times} = p_\mu p_{\text{Alice},\times}$ are the probabilities of the sending a pulse with intensity μ in the rectilinear and diagonal basis (with $p_{\text{Alice},\times} = 1 - p_{\text{Alice},+}$), which Alice is free to choose. The average number of erroneous detections at Bob's receiver are

$$N_{\text{err},\mu,+} = N_{\text{sifted},\mu,+} \cdot \text{QBER}_+ \quad (27)$$

$$N_{\text{err},\mu,\times} = N_{\text{sifted},\mu,\times} \cdot \text{QBER}_\times \quad (28)$$

The Secret Key Length (SKL) is then calculated using $\text{QBER}_{\text{global}}$, $N_{\text{sifted},\mu,+}$, $N_{\text{sifted},\mu,\times}$ and $N_{\text{err},\mu,\times}$ according to decoy state equations, as presented in [16] and in the references therein. The secrecy parameter and the correctness parameters have been fixed to $\varepsilon_{\text{sec}} = 10^{-9}$ and $\varepsilon_{\text{corr}} = 10^{-15}$, respectively, while the error correction efficiency factor to $f_{\text{e.c.}} = 1.22$. The free parameters $\{\mu_1, \mu_2, p_{\mu_1}, p_{\mu_2}, p_{\text{Alice},+}\}$ are then numerically optimised to obtained the largest possible SKL. The expected SKL is an increasing function of the total link time and the asymptotic secret key generation rate is then defined as

$$\text{SKR} = \lim_{t_{\text{link}} \to \infty} \frac{\text{SKL}(t_{\text{link}})}{t_{\text{link}}}. \quad (29)$$

It is observed that in the asymptotic regime almost all pulses are prepared in the rectilinear basis and almost all in the signal state, as should be expected from the fact that asymptotically a vanishing fraction of the sent qubits is required for accurate parameter estimation.