Best Paper Award

Measurements of atmospheric background light in the urban area Waterloo and its impact on satellite QKD system performance

Stefanie Häusler[a], Florian Schümann[a], Leonard Vollmann[a], Davide Orsucci[a], Paul Godin[b], Katanya Kuntz[b], Nouralhoda Bayat[b], Thomas Jennewein[b], and Florian Moll[a]

[a]Institute of Communications and Navigation, German Aerospace Center (DLR), Wessling, Germany
[b]Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

ABSTRACT

Quantum Key Distribution (QKD) allows sharing encryption keys with information theoretic security. Satellite-based QKD can establish long distance links due to the quadratic transmission loss in free-space instead of the exponential transmission loss in optical fibers. Atmospheric background light plays an important role in the QKD scheme as it may significantly contribute to the system Quantum Bit Error Rate (QBER). Therefore, background light needs to be examined closely. Due to the high variability of atmospheric conditions, direct measurements of the background light under different meteorological conditions are the best option to properly characterize the effect. Current considerations are mainly limited to the analysis of cloud-free scenarios by simulation and by experiment. Links can also take place when the environment differs from this ideal condition. Measurement data was recorded in C-band at the campus of the University of Waterloo, Canada, during the day with clear sky and during sunset with clear sky and partly-clouded sky conditions. The measurement data is shown and compared to simulation results and to the measurement data taken in Oberpfaffenhofen, Germany. The impact of background light is discussed on a chosen reference scenario outlining the importance of detector gating time and end-to-end transmission loss when wanting to realize daylight QKD.

Keywords: light pollution, background noise, sky brightness, daylight

1. INTRODUCTION

Methods of cryptography are used to ensure that sensitive information is kept confidential, is protected from manipulation and parties are authenticated correctly. Asymmetric and symmetric key encryption methods are used to ensure this. Asymmetric key encryption, like Rivest–Shamir–Adleman (RSA), is based on a hard-to-solve mathematical problem, like the integer factorization problem. This security assumption could be broken in the future since there is a quantum algorithm, namely the Shor's algorithm, that is capable to solve the integer factorization problem with exponential speedup compared to a classical system. Symmetric key encryption, like Advanced Encryption Standard (AES), can be seen as relatively secure from a quantum resistant perspective. A quantum algorithm called Grover's algorithm does indeed speed up against symmetric ciphers, but only quadratically compared to a classical system. This results in the fact that by doubling the key length the security can be restored. However, the principle security of AES relies on the fact, that no algorithm is known to efficiently solve the mathematical problem and not by proving that it is not possible in general. Furthermore, in symmetric key encryption a secure key needs to be shared first which is implemented by sharing a hard drive in the beginning or by using asymmetric key encryption.[1,2]

Quantum Key Distribution (QKD) relies not on mathematical assumptions but on the laws of quantum physics. The key is generated via the distribution of a quantum state and given the information-disturbance trade-off an eavesdropper will be detected because it will increase the Quantum Bit Error Rate (QBER). Therefore, QKD is a valuable option to ensure that the goals of cryptography are met even in a post-quantum era.[2,3] In

Send correspondence to Stefanie Häusler (stefanie.haeusler@dlr.de)

Environmental Effects on Light Propagation and Adaptive Systems VII, edited by Karin Stein, Szymon Gladysz, Proc. of SPIE Vol. 13194, 131940R
 · 0277-786X · doi: 10.1117/12.3033670

QKD the quantum state, a weak optical signal, must be transferred between two parties via a quantum channel. The quantum channel can be provided by using optical fibers. However, due to the exponential loss in fiber, long-distance connections cannot be implemented directly. Satellite-based QKD can implement long-distance links with a quadratic loss with distance and technology which can be developed now. When realising free-space QKD links, background light is additional noise source compared to fiber links. Current QKD satellite missions focus on night operation when background light conditions are relaxed. However, when wanting to implement QKD as a service, daylight QKD will enhance the service capacity. The question arises how background light can to be predicted and how accurate the prediction needs to be. The prediction of background light can be used for the system design of satellite and QKD-OGS, site characterization of the Optical Ground Station (OGS) and link scheduling when several OGS can be selected by one satellite and the overall key throughput should be optimized. Here, focus lies on the prediction of background light.

The presence of background light depends on the location, time, environmental conditions and the link setting, like up- or downlink. Sources of background light can arise from the communication system itself, namely channel crosstalk, or from light scattered in the atmosphere originating from the sun, the moon, stars and planets or a anthropogenic cause. Atmospheric background light has been analysed by astronomy in rural environments and at broad bandwidths.[4] A background light measurement shown in Fig. 1 carried out at the rooftop of the Institute of Communications and Navigation (KN) building at the campus of the German Aerospace Center (DLR) in Oberpfaffenhofen, Germany, which shows that ideal clear daylight sky conditions can be simulated using tools like library for radiative transfer (libRadtran) or MODerate resolution atmospheric TRANsmission (MODTRAN) and default aerosol models when knowning visibilty and albedo. For the estimation of visibility and alebedo background light measurements were used.[5] It is practical to carry out more measurements at different locations and time of the year to verify this.

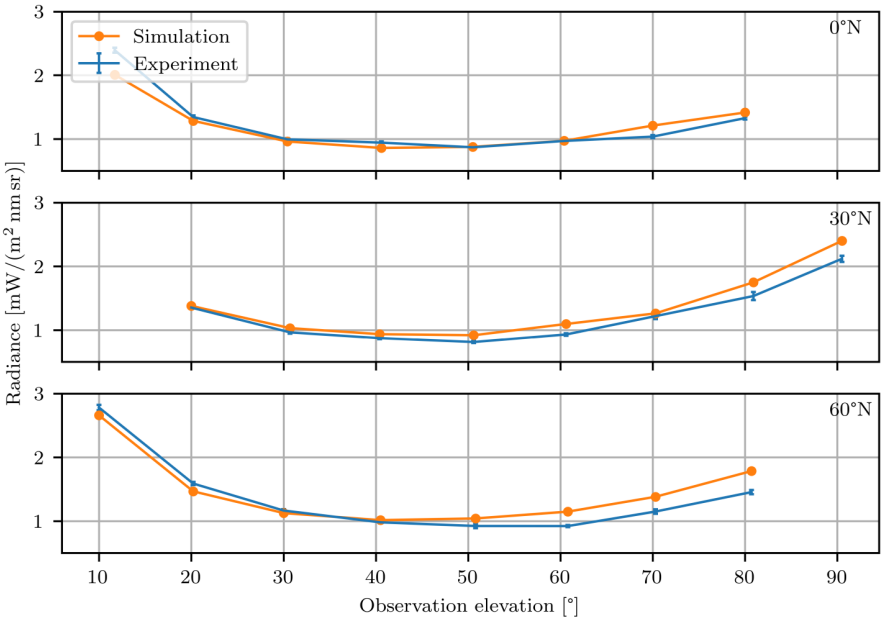

Figure 1. Background light measurement during daylight with clear sky conditions on the KN rooftop at the campus of DLR in Oberpfaffenhofen, Germany, on 2022-04-22 compared to libRadtran simulation results (settings: one-dimensional DISORT solver, default aerosol model with rural type aerosol boundary layer, background aerosol above 2 km, spring-summer conditions, albedo of 0.15 and visibility of 30 km)[5]

Several environmental conditions can influence the presence of background light, like smog, smoke of forest fire, clouds, fog and antrophogenic light. E.g. bright clouds can be as bright as 240 $\frac{\mathrm{mW}}{\mathrm{m^2\,nm\,sr}}$[4] compared to brightest daylight with clear sky having about 60 $\frac{\mathrm{mW}}{\mathrm{m^2\,nm\,sr}}$.[5] Simulation tools like libRadtran do have the possibility to optimize the aerosol model for different conditions. To actually model it in practice is however complicated as

the exact formation of clouds, fog, forest fire smoke, etc. is unknown. Therefore, sky radiance for these scenarios cannot be predicted by simulation at the moment and a difference between measured and simulation results would exist.

Here, the method of measuring background light is shown and measurement data at an additional location to Oberpfaffenhofen, Germany, and time of the year is shared to further verify simulation results with libRadtran. Measurement data was recorded during the day with clear sky conditions and during sunset with clear sky and partly-clouded sky conditions. In order to analyse the impact of background light in QKD a reference scenario is defined and a method to show the impact on this reference scenario is presented. The results of the measurement and the impact on QKD are outlined and discussed.

2. METHOD OF INVESTIGATING BACKGROUND LIGHT IN QKD SCENARIOS

2.1 Measurement- and simulation-based method of determining background light

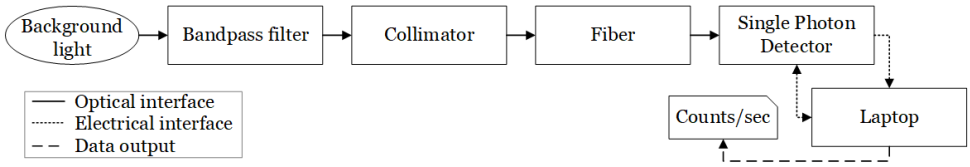

Figure 2. Background light measurement setup with a Single Photon Detector

The concept of measuring background light is visualized in Fig. 2. To receive background light a collimator is used. A bandpass filter which is mounted in front of the collimator filters the light for the wavelength to be characterized. Afterwards, the light is coupled into an Single Mode Fiber (SMF) where it is guided towards the Single Photon Avalanche Diode (SPAD). The counts/sec are logged and are later converted to radiance as described in App. A. The components used are listed in Tab. 1. The optical setup has a transmission loss $\eta_{\text{optical}} = 0.51$.

Table 1. Measurement setup

	Used component	Details
Collimator	F230APC-1550	Alignment wavelength λ: 1550 nm
Bandpass filter	FB1550-12	Wavelength: 1550 nm, B_{eff}=7.8 nm
SPAD	PDM-IR, MPD	Hold off time T_{Holdoff}: 100 µs Dark Count Rate (DCR) $R_{\text{D,meas}}$: 2000 Hz Quantum efficiency η_{detector}: 0.22

The background light was measured at 1550 nm during daytime in clear sky conditions at different days and times. One measurement row consists of a fixed azimuth direction and a scan in elevation from about 20° to 70°. Each position was measured for 10 minutes, the measured counts are converted to radiance and the mean value of the radiance is calculated. The measurement results are then compared to simulation results stemming from libRadtran by calculating the average sun position for each observation position and using the one-dimensional Radiative Transfer Equation (RTE) solver called DIScrete ORdinate Radiative Transfer (DISORT) by Stamnes.[6,7] Furthermore, the integrated default aerosol model by Shettle[8] is used with the settings urban type aerosol boundary layer, background aerosol above 2 km, fall-winter conditions and visibility and albedo tuned according to the experimental results.[8,9]

In addition, to the daylight measurements, measurements have been carried out during sunset in clear sky and partly-clouded sky conditions. Counts are converted to radiance, plotted in time and compared to simulation results. For the simulation libRadtran is used again with the same aerosol model as used for the daylight simulation. In addition, to using the one-dimensional DISORT solver, the three-dimensional RTE solver called

"Monte Carlo for the physically correct tracing of photons in cloudy atmosphere" (MYSTIC) by Mayer[10] is used to allow simulating the afterglow of the sunlight after sunset. The simulation is set to trace 1e6 total number of photons by MYSTIC and to use the 1D spherical atmosphere model which assumes a plane-parallel atmosphere.[9]

2.2 Method of analysing the impact on QKD

The measured radiance will be analyzed in a QKD reference scenario. A downlink and decoy-state BB84 with polarization-encoded qubits and active choice of measurement basis is examined. The QBER is chosen as a performance parameter. The protocol and calculation of the QBER is described in App. B. The misalignment angle between polarization state of preparation and detection is set to 0° as only the impact on background light shall be investigated here. Two cases of end-to-end transmission loss meaning the loss from satellite ex-aperture to the interface of the detector are analysed which are derived from reasonable, future satellite and QKD-OGS setups at 30° elevation.[11] The two end-to-end transmission losses to be considered are therefore set to -30dB and -40dB. The optical loss of the OGS η_{OGS} attenuating the background light is assumed to be -1.5 dB. As a detector a Superconducting Nanowire Single Photon Detector (SNSPD) is used with a detection efficiency $\eta_{\mathrm{detector}} = 0.9$ and DCR $R_{\mathrm{D}} = 90\,\mathrm{Hz}$. Reasonable spatial and spectral filtering is chosen and temporal filtering will be investigated. SMF-coupling is used and an effective filter bandwidth B_{eff} of 0.5 nm. Temporal filtering will be investigated from 100 ps to 1 ns. Summarizing, the input parameters for the impact analysis are listed in Tab. 2. As a threshold QBER, three different thresholds are outlined:

- 0.1% as a threshold for a desirable QBER contribution from background light
- 5% as a practical limit according to a reference experimental realization[12]
- 11% as a theoretical limit according to the ideal single-qubit version of the BB84 protocol[13]

Table 2. Input parameters for the impact analysis on QKD

QKD signal intensity μ	0.7
Detector efficiency η_{detector}	0.9
Detector DCR R_{D}	90 Hz
Detector gating time Δt	100 ps to 1 ns
Polarization misalignment angle δ	0°
End-to-end transmittivity η	-30 dB and -40 dB
Optical loss of the OGS η_{OGS}	-1.5 dB
Effective filter bandwidth B_{eff}	0.5 nm

3. RESULTS AND DISCUSSION

3.1 Measurement- and simulation-based results of background light

The measurements were carried out on the rooftop of the Research Advancement Center (RAC) at the campus of the University of Waterloo where the OGS is located. The coordinates are 43.479°N, 80.555°W. The RAC building is in the North-West corner of the campus and the city. Lawn, forest and a lake are present to the West (azimuth direction of about 260° to 315°). In all other directions the RAC building is separated from the city or the campus by about 20 to 500 m nature consisting of lawn and lakes.

Background light was measured during daylight with clear sky conditions at the 2023-10-02, 2023-10-03 and 2023-02-04 in different azimuth directions and elevation of about 20° to 70° as can be seen in Fig. 3. To fit the experimental and simulated radiance as good as possible the albedo and visibility is adjusted manually for each measurement row. Results of this best-fit of the simulation are summarized in Tab. 3.

A reasonable visibility from 18 km to 26 km can be determined for measurements carried out from the 2023-10-02 to 2023-10-04. The albedo which is determined by the best-fit of the simulation to the experiment is

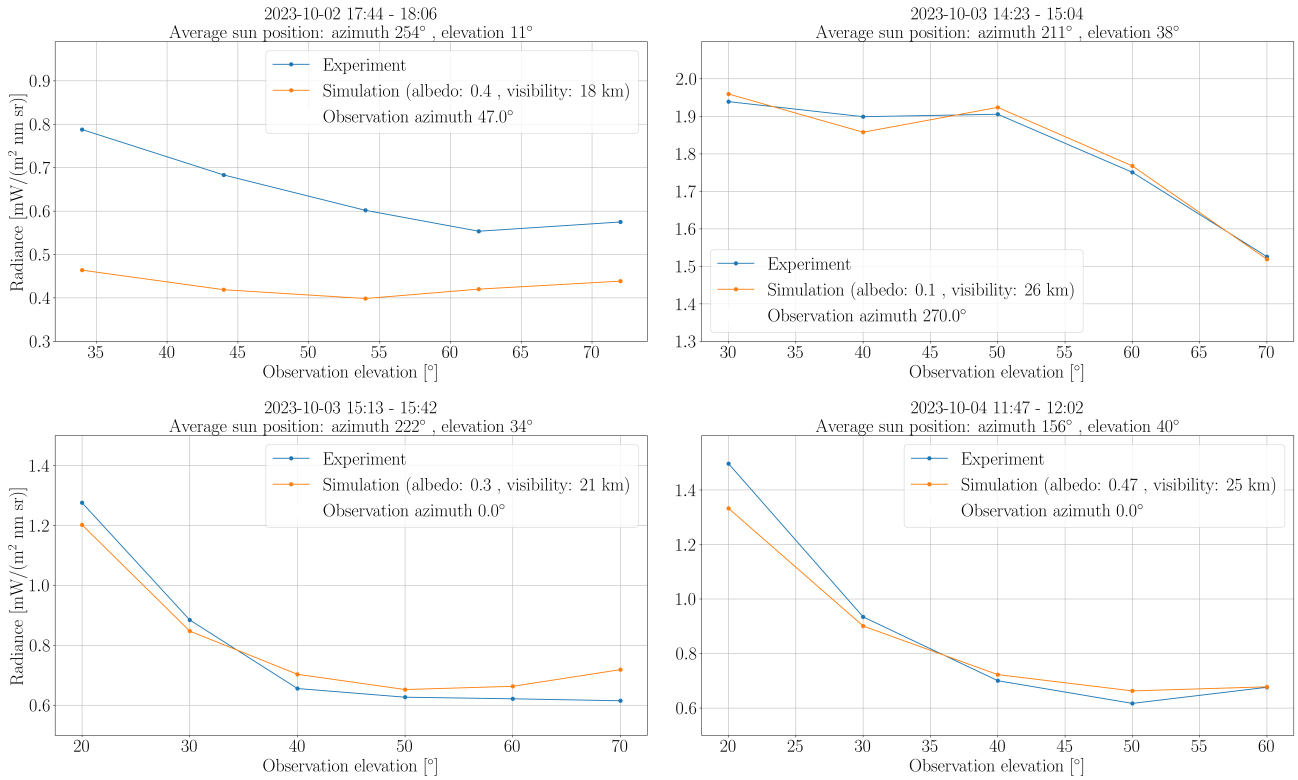

Figure 3. Background light measurement during daylight with clear sky conditions on the RAC rooftop at the campus of the University of Waterloo, Canada, compared to libRadtran simulation results (settings: one-dimensional DISORT solver, default aerosol model with urban type aerosol boundary layer, background aerosol above 2 km and fall-winter conditions)

Table 3. Values for visibility and albedo used in the simulation to match to experimental results

Azimuth	Visibility	Date	Albedo	Ground conditions in azimuth direction
0°	21 to 25 km	2023-10-03, 2023-10-04	0.3 to 0.47	500 m lawn, then city
47°	18 km	2023-10-02	0.4	600 m lawn and asphaltic parking slots, then city
270°	26 km	2023-10-03	0.1	1 km lawn and forest, then lake

different depending on azimuth direction. The albedo is between 0.3 and 0.5 in the direction of the city. At an azimuth of 270° the ground conditions are different as in this direction there are lawns, forest and a lake. This can be noticed by a lower determined albedo of 0.1. A similar albedo of 0.15 was determined by the experiment carried out in Oberpfaffenhofen, Germany, where the ground conditions in the surroundings is also shaped by lawn, fields, forest and lakes.

In general it is shown that libRadtran simulation results can be matched to experimental results when fitting the albedo and visibility. In this way libRadtran can be used to get best- and worst-case prediction of the background light conditions on site. Albedo and visibility must be known from independent measurement results to verify the validity of the simulation results completely. For the purpose of QKD, a background light site characterization tool could also be used to estimate the albedo using libRadtran and to map different visibility to different weather conditions. Afterwards, the visibility might be able to be predicted by weather data, allowing to get an estimate of the background light. This information could then be used for link scheduling.

Furthermore, Fig. 4 shows the background light measurement during sunset in clear sky and partly-clouded sky conditions. The impact of clouds can clearly be seen as the measured radiance is up to four times higher. The measurement shows random fluctuations of the sky radiance because of the cloud movement. The cloud formation during the measurement was not measured and thus, it cannot be stated when the channel would have been blocked or free for satellite QKD. However, it can be outlined that the presence of bright clouds do increase the sky radiance even when the channel is not blocked by clouds. Furthermore, in air-to-ground QKD the channel will not be blocked due to clouds, but bright clouds will increase the present background light.

The simulation is carried out using the one-dimensional DISORT solver and the three-dimensional MYSTIC solver. When using the DISORT solver, a one-dimensional gemoetry is used, resulting in a simulated radiance of zero at the point when the sun sets. The three-dimensional MYSTIC solver with the assumption of a plane-parallel atmosphere allows simulating the afterglow after the sun sets. Minor fluctuations in MYSTIC simulation results can be seen. The severity of the fluctuations depends on the number of photons for which the Monte Carlo simulation is carried out. Here, 1e6 photons are used as an input parameter. In general, the simulation is underestimating the radiance by about 0.5 $\frac{\mathrm{mW}}{\mathrm{m^2\,nm\,sr}}$ at the start of the measurement and experimental and simulated results converge during the sunset.

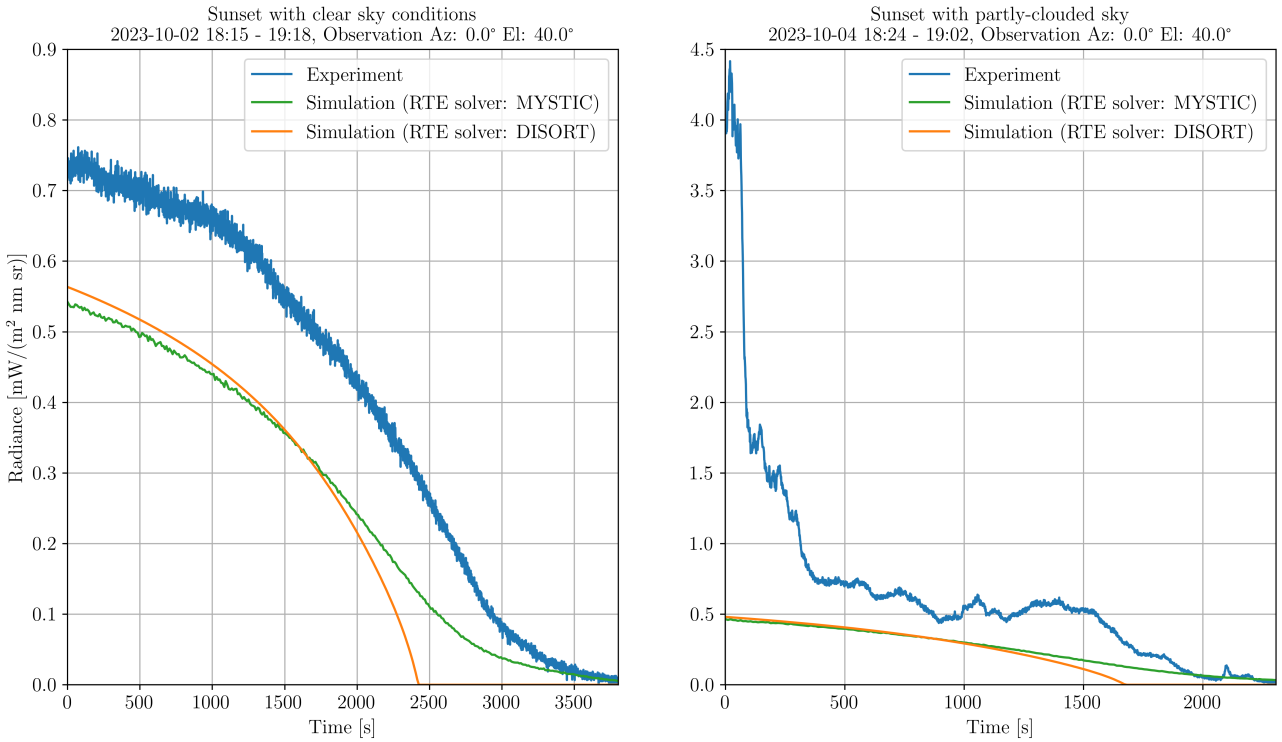

Figure 4. Background light measurement during sunset with clear sky and partly-cloudy sky conditions on the RAC rooftop at the campus of the University of Waterloo, Canada, compared to libRadtran simulation results (settings: default aerosol model with albedo of 0.4, visibility of 18 km, urban type aerosol boundary layer, background aerosol above 2 km and fall-winter conditions)

3.2 Analysis of the impact of background light on satellite QKD performance

It is evaluated under which temporal filtering conditions daylight QKD is possible for the two end-to-end transmission losses of -30 dB and -40 dB and the defined reference scenario in Sec. 2.2. In Fig. 5, QBER depending on gating time is shown. -40dB is challenging when not taking daylight into account because of the high attenuation. However, for chosen satellite paths where the sky radiance is not expected to be more than 1 $\frac{\mathrm{mW}}{\mathrm{m^2\,nm\,sr}}$ the practical QBER threshold of 5% is not reached for a gating time almost up to 1 ns. By increasing the

end-to-end transmittivity to -30 dB and limiting the gating time to 100 ps the practical limit of the QBER is not reached even for the highest expected radiance in a clear sky condition which is estimated to be 60 $\frac{\mathrm{mW}}{\mathrm{m^2\,nm\,sr}}$. It can be concluded that when wanting to establish daylight QKD, end-to-end transmittivity and the feasibility to establish a gating time of about 100 ps or better are key. The end-to-end transmittivity can be increased by increasing transmitter or receiver aperture. The feasibility of a 100 ps gating time or better depends on the jitter of the signal laser pulse, detector, time tagger and time synchronisation signal.

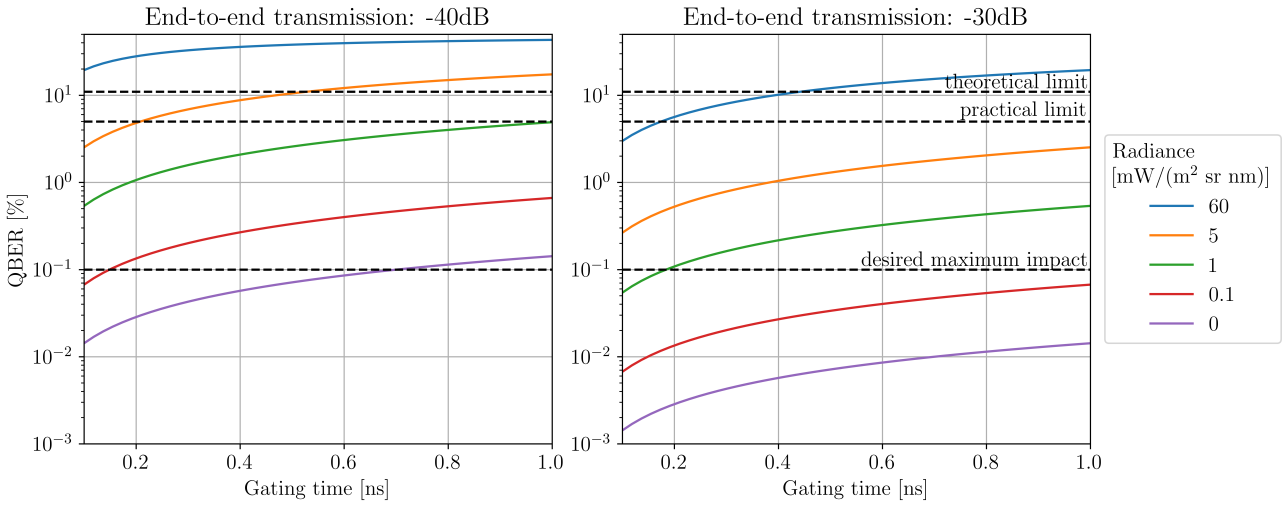

Figure 5. Dependency of QBER and gating time of the detector for the defined reference scenario being a polarization-encoded, decoy-state BB84 protocol with active choice of measurement basis and system settings described in Tab. 2

4. CONCLUSION

Background light in QKD scenarios is analysed to provide information for the system design of satellite and QKD-OGS. Furthermore, in the attempt to establish a world-wide quantum network, locations for QKD-OGS must be found which are both close to the end-user and do have conditions for acceptable background light. When a satellite QKD network is established it might be of interest to predict background light in different locations in order to chose link sequences to different QKD-OGS for highest key throughput.

An experimental method to measure background light is presented and the data sets taken during daylight in clear sky conditions and sun set during clear sky and partly-clouded sky conditions at the campus of the Universtiy of Waterloo are shared. The results show that simulation tools can be used when knowing visibility and albedo of the location. Realistic values for albedo and visibility at a particular location can be determined by using a background light measurement setup as presented. The impact of daylight on satellite QKD is shown on a reference scenario. Based on this example the importance of the end-to-end transmission loss in regard to enabling daylight QKD is shown. Furthermore, it is concluded that being able to establish high temporal filtering is of importance. This results in the need of low jitter of the involved instruments, like laser, detector, time tagger and the time synchronisation system.

APPENDIX A. CONVERSION FROM COUNT RATE TO RADIANCE

The measured count rate of the detector is converted to radiance $L_\lambda[\frac{\mathrm{mW}}{\mathrm{m^2\,nm\,sr}}]$. First, the count rate is converted to photon rate. Therefore, the hold off time $T_{\mathrm{Holdoff}}[\mathrm{s}]$ is taken into account for the measured count rate $R_{\mathrm{P,meas}}[\mathrm{Hz}]$ and the measured dark count rate $R_{\mathrm{D,meas}}$ for the selected T_{Holdoff}:

$$R_{\mathrm{E}} = \frac{R_{\mathrm{P,meas}}}{1 - R_{\mathrm{P,meas}} \cdot T_{\mathrm{Holdoff}}} \tag{1}$$

$$R_{\mathrm{D}} = \frac{R_{\mathrm{D,meas}}}{1 - R_{\mathrm{D,meas}} \cdot T_{\mathrm{Holdoff}}} \tag{2}$$

The photon rate R_{P} [Hz] is calculated by considering the R_{E} [Hz] and R_{D} [Hz] as well as the quantum efficiency η_{detector} [−]:

$$R_{\mathrm{P}} = \frac{R_{\mathrm{E}} - R_{\mathrm{D}}}{\eta_{\mathrm{detector}}} \tag{3}$$

The photon rate can be converted to power P [mW]:

$$P = \frac{R_{\mathrm{P}} \cdot \mathrm{hc}}{\lambda} \cdot 1000 \tag{4}$$

with the central wavelength λ [m], Planck's constant h [Js], speed of light c $[\frac{\mathrm{m}}{\mathrm{s}}]$ and furthermore, to radiance $L_\lambda[\frac{\mathrm{mW}}{\mathrm{m^2 nm sr}}]$:

$$L_\lambda = \frac{P_{\mathrm{SMF}}}{B_{\mathrm{eff}} \cdot \beta^2 \cdot \lambda^2 \cdot \eta_{\mathrm{optical}}} \tag{5}$$

for SMF coupled systems only and with the transmittivity of the opical system η_{optical} [−], effective filter bandwidth B_{eff} [nm] and $\beta = 1.12$ for unobscured apertures.[5,14]

APPENDIX B. CALCULATION OF THE QBER

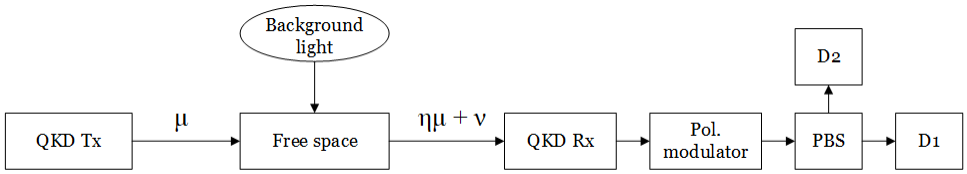

Figure 6. Decoy-state, polarization encoded BB84 QKD setup with active choice of measurement basis in a free-space scenario (μ: signal intensity of the laser pulse, QKD Tx: transmitting telescope, η: transmittivity, ν: average number of background light, QKD Rx: receiver telescope, PBS: polarizing beamsplitter, D1 and D2: detectors[5]

In the decoy-state, polarization-encoded BB84 protocol[15] as represented in Fig. 6, a quantum signal is produced by Alice. The quantum state is encoded in the polarization $P \in \{\leftrightarrow, \updownarrow, \swarrow, \nwarrow\}$ by mapping it $|\leftrightarrow\rangle \equiv |0\rangle, |\updownarrow\rangle \equiv |1\rangle$ and $|\swarrow\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |\nwarrow\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Each quantum state has a different pulse intensity μ. The intensity is either the vacuum decoy pulse ($\mu_0 = 0$), μ_1, the weak decoy pulse or the μ_2 signal pulse with $(0 < \mu_1 < \mu_2 < 1)$.

The quantum signal is then transmitted to Bob over the free-sapce channel with an end-to-end transmittivity η to Bob. Bob is receiving this signal as well as an average amount of background light photons ν within the gating time Δt of the detector which coupled into the channel. Resulting in the received average number of photons $\tau = \eta\mu + \nu$. As an active choice of measurement basis takes place at Bob, two detectors are sufficient.[2]

The approximate probability of the wrong detector to click $p_\swarrow$ and the approximate probability of the right detector to click $p_\mathcal{X}$ clicks for $\tau_\swarrow \eta_{\mathrm{detector}} + R_{\mathrm{D}}\Delta t \ll 1$ is

$$\begin{cases} p_\swarrow &= 1 - e^{-\tau_\swarrow \eta_{\mathrm{detector}} - R_{\mathrm{D}} \cdot \Delta t} \approx \tau_\swarrow \eta_{\mathrm{detector}} + R_{\mathrm{D}} \cdot \Delta t \\ p_\mathcal{X} &= 1 - e^{-\tau_\mathcal{X} \eta_{\mathrm{detector}} - R_{\mathrm{D}} \cdot \Delta t} \approx \tau_\mathcal{X} \eta_{\mathrm{detector}} + R_{\mathrm{D}} \cdot \Delta t \end{cases} \tag{6}$$

with the present light intensity $\tau_\mathcal{X}$ or $\tau_\swarrow$, the detector efficiency η_{detector}, the detector dark count rate R_{D} and its gating time Δt.

The pulse intensities at Bob's receiver in the two orthogonal states ($\tau_\checkmark$ or $\tau_\mathcal{X}$) are

$$\begin{cases} p_\checkmark: & \tau_\checkmark \equiv \eta\,\mu\,\cos^2\delta + \frac{1}{2}\,\nu \\ p_\mathcal{X}: & \tau_\mathcal{X} \equiv \eta\,\mu\,\sin^2\delta + \frac{1}{2}\,\nu\,. \end{cases} \tag{7}$$

with end-to-end transmittivity of the channel η, the mean photon number send by Alice μ, misalignment between the state of preparation basis and the state of measurement basis (δ) and the average photon number of background light ν into account. The average photon number of background light ν is derived from the radiance $L_\lambda[\frac{\mathrm{mW}}{\mathrm{m^2nmsr}}]$ is

$$\nu = \frac{\frac{L_\lambda}{1000}\cdot B_{\mathrm{eff}}\cdot\beta^2\cdot\lambda^3\cdot\eta_{\mathrm{OGS}\cdot\Delta t}}{\mathrm{hc}}. \tag{8}$$

with the effective filter bandwidth B_{eff}, $\beta = 1.12$ for unobscured apertures, wavelength λ, OGS optical loss η_{OGS}, gating time Δt, Planck's constant h and speed of light c.

The QBER is given by

$$\mathrm{QBER} = \frac{p_\mathcal{X}(1-p_\checkmark) + \frac{1}{2}p_\checkmark p_\mathcal{X}}{p_\checkmark(1-p_\mathcal{X}) + p_\mathcal{X}(1-p_\checkmark) + p_\checkmark p_\mathcal{X}} = \frac{p_\mathcal{X} - \frac{1}{2}p_\checkmark p_\mathcal{X}}{p_\checkmark + p_\mathcal{X} - p_\checkmark p_\mathcal{X}}\,. \tag{9}$$

with the probability ($p_\checkmark(1-p_\mathcal{X})$) that only the right detector clicks ($p_\checkmark(1-p_\mathcal{X})$), the probability ($p_\mathcal{X}(1-p_\checkmark)$) that only the wrong detector clicks ($p_\mathcal{X}(1-p_\checkmark)$) and with the probability ($p_\checkmark p_\mathcal{X}$) that both detector click and the click is located randomly to one of the detectors.[5,16]

ACKNOWLEDGMENTS

This report is based on projects funded by the German Federal Ministry of Education and Research (BMBF) under the funding code 16KIS1265 and the Short Term Scientific Missions (STSMs) by the European Network on Future Generation Optical Wireless Communication Technologies (NEWFOCUS), CA19111, as part of the European Cooperation in Science and Technology (COST) and supported by the project Establishing German-Canadian Quantum Communication Satellite Interfaces (GCQuSAT) as part of the High-Throughput & Secure Challenge Program by the National Research Council Canada (NRC). The authors are responsible for the content of this publication.

GLOSSARY OF TERMS

AES Advanced Encryption Standard
DCR Dark Count Rate
DISORT DIScrete ORdinate Radiative Transfer
DLR German Aerospace Center
KN Institute of Communications and Navigation
libRadtran library for radiative transfer
MODTRAN MODerate resolution atmospheric TRANsmission
MYSTIC "Monte Carlo for the physically correct tracing of photons in cloudy atmosphere"
OGS Optical Ground Station
QBER Quantum Bit Error Rate
QKD Quantum Key Distribution
RAC Research Advancement Center
RSA Rivest–Shamir–Adleman
RTE Radiative Transfer Equation
SMF Single Mode Fiber
SNSPD Superconducting Nanowire Single Photon Detector
SPAD Single Photon Avalanche Diode

REFERENCES

[1] Bernstein, D. J. and Lange, T., "Post-quantum cryptography," *Nature* **549**(7671), 188–194 (2017).

[2] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–195 (Mar. 2002). Publisher: American Physical Society.

[3] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Reviews of Modern Physics* **81**, 1301–1350 (Sept. 2009). Publisher: American Physical Society.

[4] Er-long, M., Zheng-fu, H., Shun-sheng, G., Tao, Z., Da-sheng, D., and Guang-can, G., "Background noise of satellite-to-ground quantum key distribution," *New Journal of Physics* **7**, 215–215 (Oct. 2005).

[5] Häusler, S., Orsucci, D., Vollmann, L., Peev, E., and Moll, F., "Measurement-based characterization of atmospheric background light in satellite-to-ground quantum key distribution scenarios," *Optical Engineering* **63**, 041211 (Feb. 2024). Publisher: SPIE.

[6] Stamnes, K., Tsay, S.-C., Wiscombe, W., and Jayaweera, K., "Numerically stable algorithm for discrete-ordinate-method radiative transfer in multiple scattering and emitting layered media," *Applied optics* **27**(12), 2502–2509 (1988).

[7] Stamnes, K., Tsay, S.-C., Wiscombe, W., and Laszlo, I., "Disort, a general-purpose fortran program for discrete-ordinate-method radiative transfer in scattering and emitting layered media: documentation of methodology," (2000).

[8] Shettle, E. P., "Models of aerosols, clouds, and precipitation for atmospheric propagation studies," *In AGARD* (Mar. 1990). ADS Bibcode: 1990apuv.agar.....S.

[9] Mayer, B., Kylling, A., Emde, C., Hamann, U., Buras, R., Gasteiger, J., and Richter, B., "libRadtran User's Guide," (2012).

[10] Mayer, B., "Radiative transfer in the cloudy atmosphere," *EPJ Web of Conferences* **1**, 75–99 (2009). Publisher: EDP Sciences.

[11] Häusler, S., Orsucci, D., Reeves, A., and Moll, F., "Evaluation of integration concepts of Optical Ground Stations for satellite-based Quantum Key Distribution into a quantum network," in [*2023 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*], 209–216 (Oct. 2023).

[12] Marco, I. D., Woodward, R. I., Roberts, G. L., Paraïso, T. K., Roger, T., Sanzaro, M., Lucamarini, M., Yuan, Z., and Shields, A. J., "Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter," *Optica* **8**, 911–915 (Jun 2021).

[13] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., and Wallden, P., "Advances in quantum cryptography," *Adv. Opt. Photon.* **12**, 1012–1236 (Dec 2020).

[14] Scriminich, A., Foletto, G., Picciariello, F., Stanco, A., Vallone, G., Villoresi, P., and Vedovato, F., "Optimal design and performance evaluation of free-space quantum key distribution systems," *Quantum Science and Technology* **7**, 045029 (Oct. 2022).

[15] Lo, H.-K., Ma, X., and Chen, K., "Decoy State Quantum Key Distribution," *Physical Review Letters* **94**, 230504 (June 2005).

[16] Gottesman, D., Lo, H.-K., Lutkenhaus, N., and Preskill, J., "Security of quantum key distribution with imperfect devices," in [*International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*], 136, IEEE (2004).