Journal of Physics Communications

OPEN ACCESS

RECEIVED
19 December 2025

REVISED
5 March 2026

ACCEPTED FOR PUBLICATION
26 March 2026

PUBLISHED
9 April 2026

PAPER

Satellite-based quantum key distribution in the Arctic: a case study of Finnish Lapland

Sara Nikula[1,*] **and Kokkatil Gopalkrishnan**[2]

[1] VTT Technical Research Centre of Finland Ltd, Oulu, Finland
[2] Aalto University, Espoo, Finland
[*] Author to whom any correspondence should be addressed.

E-mail: sara.nikula@vtt.fi and gopalkrishnan.v.kokkatil@aalto.fi

Keywords: quantum key distribution, satellite QKD, post-quantum cryptography, security, free-space optical links, cloud cover, polar regions

Supplementary material for this article is available online

Abstract

The advent of quantum computing necessitates the transition from conventional encryption systems to quantum-resistant alternatives. Quantum key distribution (QKD) represents one such approach. Nevertheless, fibre-based QKD is constrained by severe limitations in transmission distance. A promising solution is satellite-based QKD, wherein a satellite establishes secure communication with a ground station. However, daylight presents a considerable challenge for QKD devices, which are highly sensitive to ambient light. Implementing satellite-based QKD in Arctic regions is particularly compelling due to their distinctive annual cycle and prolonged periods of darkness; yet, this possibility has received limited attention in the existing literature. This study assessed the feasibility of satellite-based QKD in regions above the Arctic Circle by simulating a satellite QKD link to three ground stations located in Finnish Lapland: Rovaniemi, Sodankylä, and Utsjoki. The simulation tool comprised MATLAB code for modelling the quantum link, satellite orbital data generated using the Python Skyfield library, and local weather data collected for the year 2024, including cloud cover, rain, snow, ice crystals, and fog. Our findings suggest that while the polar night provides favourable conditions for wintertime quantum communication, continuous daylight during summer and high cloud-cover probabilities may lead to extended service interruptions, severely limiting the achievable secret key material. Optimizing satellite overpass timing substantially reduces outage periods caused by background light; however, this optimization becomes ineffective during summer months due to the persistently high ambient light levels. These constraints underscore the need for robust key-storage mechanisms and careful evaluation of potential use cases. It is recommended that advanced filtering techniques be investigated as a potential means to mitigate summer outage periods caused by excessive ambient light.

1. Introduction

Modern society is profoundly dependent on telecommunications. In numerous contexts, it is essential that communication remains confidential between the sender and the recipient. A common example involves sensitive information pertaining to banking or healthcare, which should be accessible solely to the customer and the corresponding institution. At present, the confidentiality of such exchanges is maintained through efficient symmetric encryption schemes. A fundamental challenge, however, lies in the secure distribution of the encryption key from sender to recipient. Traditionally, this has been addressed through public-key encryption, which provides an effective and scalable mechanism for key exchange. Yet, with the emergence of quantum computing in the 21st century, these cryptographic methods have come under significant scrutiny. Peter Shor's algorithm, introduced in the 1990s, demonstrates the capability to compromise public-key cryptographic schemes when executed on a sufficiently powerful quantum computer [1]. Consequently, both the European Commission and the National Institute of

Standards and Technology (NIST) advocate for a transition to post-quantum cryptography (PQC), which is based on mathematical problems that, according to current knowledge, remain intractable even for quantum computers [2, 3].

An alternative approach to encryption key delivery is quantum key distribution (QKD), the most widely recognized protocol of which was introduced in 1984 [4]. In contrast to computational cryptography, QKD is grounded in the no-cloning theorem of quantum mechanics and exploits Heisenberg's uncertainty principle to guarantee the secrecy of the distributed key. Crucially, QKD facilitates key exchange without reliance on computational hardness assumptions, a property unattainable by classical cryptographic algorithms. Consequently, an encryption key delivered via QKD remains secure irrespective of future advancements in algorithms or computing technologies.

One of the principal challenges in QKD is scalability, which arises directly from the physical principles underpinning the protocol's security. Due to the inherently weak nature of quantum signals, the communication distance achievable through optical fibre is typically restricted to a few hundred kilometres [5–7], even though the distance can be extended with so-called twin-field QKD [8]. Another promising alternative for extending these distances is satellite-based QKD, where communication occurs via free-space links rather than fibre. This concept has already been validated experimentally [9], and the European Space Agency (ESA) is scheduled to launch a satellite designed for QKD operations in 2026 [10]. The effectiveness of satellite-based communication can be attributed to the near-vacuum conditions of space, which allow signals to propagate with substantially lower attenuation compared to terrestrial media or optical fibre. While signal degradation does occur upon entering the atmosphere due to scattering by atmospheric particles and potential turbulence, this segment constitutes only a relatively short portion of the overall transmission path.

Satellite-based QKD can be implemented through several configurations. The primary distinction lies between uplink and downlink modes: in an uplink configuration, the ground station serves as the transmitter while the satellite functions as the receiver; conversely, in a downlink configuration, the satellite acts as the transmitter and the ground station as the receiver. Downlink is generally considered more efficient, as the signal traverses most of its path through vacuum and encounters atmospheric disturbances only near the end of its trajectory. This reduces the cumulative effects of atmospheric disturbances, such as turbulence, before the signal reaches the transceiver [11].

Another distinction exists between prepare-and-measure (PM) and entanglement-based (EB) protocols. PM protocols involve a single sender, a single receiver, and one quantum link through which photons are transmitted. In contrast, EB protocols employ a satellite that simultaneously distributes entangled photon pairs to two ground stations, enabling the formation of a shared secret key by exploiting quantum entanglement. However, EB protocols require both ground stations to be simultaneously visible to the satellite, which imposes additional constraints. In this study, we focus on the downlink decoy-state BB84 protocol, which falls within the PM category. This choice is motivated by prior work showing that decoy-state BB84 is among the most efficient protocols for satellite-based QKD [11] and is widely used both in satellite-QKD simulations [12–16] and in real-world demonstrations [9]. Further details on BB84, its decoy-state variant, and optimal parameter selection can be found in sources such as [4, 17–20].

1.1. Scope of the paper

The potential and challenges of satellite-based QKD have been examined in numerous studies [9, 11, 12, 21–23]. Nevertheless, one aspect that remains largely unexplored in the existing literature is the applicability of satellite-based QKD in Arctic regions, including areas at or beyond the Arctic Circle. High-latitude environments introduce unique considerations for QKD, stemming from pronounced seasonal variations in daylight and constraints imposed by satellite orbital dynamics. At the same time, the strategic importance of northern regions is considerable. Owing to these distinctive characteristics, Finnish Lapland represents an especially compelling area for investigating satellite-based QKD. This paper seeks to address this research gap by evaluating the feasibility of QKD in Arctic conditions. As a case study, we analyse three locations in Finnish Lapland—Rovaniemi, Sodankylä, and Utsjoki—and assess QKD link performance under two satellite orbital configurations. The primary contribution of this work is to extend the existing body of satellite-QKD simulation studies by focusing on northern locations.

The free-space BB84 link is modelled using an approach adapted from [12]; however, we improve the statistical robustness by incorporating finite-size effects into the key rate calculation and accounting for weather phenomena, including cloud cover, precipitation, and fog. Since clouds are pervasive across many regions of the Earth, simulations based solely on clear-sky conditions fail to provide a realistic assessment of link performance. By integrating weather data, our analysis offers a more accurate estimation of daily achievable key rates for the selected locations.

The structure of this paper is as follows: section 2 presents the methodology, outlining the specific characteristics and challenges associated with implementing QKD in northern regions, along with a description of the simulation software and data employed. Section 3 reports the simulation outcomes. Section 4 interprets these findings and examines potential limitations of the proposed methodology. Finally, section 5 summarizes the key insights and concludes the paper.

2. Methodology

Our methodology is founded on simulations of the downlink decoy-state BB84 protocol carried out in MATLAB. The primary key rate formula for a downlink two-decoy-state BB84 protocol over a free-space link was adapted from [12]. This link model was integrated with satellite orbital data generated using the Skyfield library [24]. The two-line element set (TLE) data, which defines the satellite's orbit and position at any given time, was processed by a Python program utilizing Skyfield to produce a file containing satellite positions relative to a selected ground station for the specified time intervals. This file was subsequently used in the MATLAB program to simulate the QKD link. Furthermore, to account for background light, the simulation calculated the relative position of the Sun and incorporated the corresponding background radiation into the link characteristics.

Our MATLAB-based simulation tool takes as input the geographical coordinates of the ground station, the simulated time period, and the Python-generated files that provide the satellite's position relative to the ground station at a discrete set of time instants. The program simulates downlink decoy-state BB84 communication between the satellite and the ground station and computes the achievable secret key lengths for all satellite passes during which the satellite is visible to the ground station, defined in this study as at least 7 degrees above the horizon.

Sections 2.1–2.6.2 provide detailed explanations regarding the locations of the simulated ground stations, the simulated satellite orbits, the modelling of the communication link, and the use of weather data.

2.1. Ground station locations

In this study, we simulated three ground station locations across Finnish Lapland: (1) Rovaniemi, Apukka (66.56° N, 25.84° E); (2) Sodankylä, Tähtelä (67.37° N, 26.63° E); and (3) Utsjoki, Kevo (69.76° N, 27.01° E). Rovaniemi, Sodankylä, and Utsjoki are municipalities where the simulated ground stations are located, while Apukka, Tähtelä, and Kevo denote the specific observation sites used. These municipalities were selected to illustrate the impact of increasing latitude on ground station performance. The southernmost site, Rovaniemi, lies precisely on the Arctic Circle, whereas the northernmost site, Utsjoki, experiences more pronounced effects of polar night and polar day. The exact ground station locations were chosen from the list of Finnish Meteorological Institute (FMI) observatory sites provided in [25]. The positions of the ground stations in Finnish Lapland are depicted in figure 1.

2.2. Satellite orbits

Satellite orbits can be categorized into several types. A satellite in Geostationary Earth orbit (GEO) remains positioned above the equator, moving at the same rotational speed as Earth and thus appearing stationary relative to a point on the Earth's surface. Some initiatives aim to deploy GEO satellites for QKD [27]. However, the applicability of GEO satellites in polar regions is limited, as they remain above the equator and can only observe high-latitude areas at steep angles, if at all. From a QKD perspective, the most widely suggested option is the deployment of satellites in low Earth orbit (LEO) [9, 11–13, 28]. LEO satellites operate at altitudes of up to 2000 km and travel at approximately 7.8 km per second, completing an orbit around Earth in roughly 90 min. When the orbital inclination, defined as the tilt relative to the equator, is high and the satellite crosses the Earth's poles at an angle of up to 10°, the orbit is classified as a polar orbit [29].

The primary limitation of polar-orbiting satellites is their short visibility window. Due to their high orbital velocity, a satellite remains visible from a ground station only for a brief period during each pass, and only a fraction of that time occurs at optimal elevation angles. In practical terms, a satellite is considered visible when it reaches a sufficiently high elevation above the horizon, provided the ground station has an unobstructed line of sight. If the satellite is too close to the horizon, physical obstructions such as trees or buildings may impede successful communication. The duration of visibility depends on the satellite's trajectory over the ground station; however, for LEO satellites, this period is generally limited to a few minutes [11]. In this study, visibility is defined as an elevation angle of 7° above

Figure 1. Simulated ground station locations in Finnish Lapland. Base map: OpenStreetMap [26]; annotations and labels added by the authors. Reproduced from [26]. CC BY 2.0. www.openstreetmap.org/copyright.

the horizon. However, as demonstrated in section 3, this threshold may not always suffice to generate a usable amount of key material.

2.2.1. The satellite orbits utilized in this study

The TLE format is a standardized representation of a satellite's orbital parameters, enabling the calculation of its position relative to a ground station at any given time. A TLE contains basic satellite identification information along with key orbital elements required for trajectory computation, such as mean motion, inclination, and eccentricity [30]. Using any suitable tool, the satellite's position at a specific time can be determined, provided its TLE data is available. In this study, satellite orbit data was generated by supplying the appropriate TLE parameters to the Python-based Skyfield library [24], which produced a dataset including elevation angles and distances as observed from a designated ground station.

The satellite orbits used in this work were those of the Suomi100 satellite and a slightly modified version of Suomi100, which we refer to as QKDLapland in this study. The Suomi100 satellite is a Sun-synchronous polar orbit satellite, launched in 2018 [31]. This satellite trajectory was chosen for this study because it is ideal for communication with ground stations located in Finland, as its orbit goes above Finland several times a day. TLE data for the Suomi100 satellite was retrieved from space-track.org [32].

Although the Suomi100 satellite passes over Finland multiple times per day, it poses a significant limitation for QKD: the most favourable passes, defined as those where the satellite reaches its highest elevation angles relative to Finnish ground stations, occur predominantly during daylight hours. The satellite's Sun-synchronous orbit maintains a relatively stable schedule for these optimal passes, with only minor day-to-day variations. From a QKD perspective, daylight passes are largely ineffective due to the adverse impact of background light on achievable key rates, as noted in, e.g. [11]. To examine the influence of satellite overpass timing, we modified the TLE data of Suomi100 to simulate an orbital configuration in which the most favourable passes occur during night-time or twilight conditions. This adjustment was implemented by altering the epoch parameter within the TLE lines. In this study, we refer to this simulated satellite as QKDLapland. QKDLapland is an entirely hypothetical satellite created solely for the purposes of this work to illustrate the significance of satellite pass timing in polar regions. While the optimal overpasses of the Suomi100 satellite occurred primarily between 07:00 and 20:00, those of QKDLapland were concentrated between 19:00 and 08:00, encompassing the darkest period of the day.

2.3. Link parameters

In this section, we present an overview of the modelling approach for the free-space link between the satellite and the ground station, as well as the method used to calculate the length of the generated secret key. The rate at which a secret key can be extracted from the quantum communication channel depends on two factors: (i) the pulse transmission frequency and (ii) the number of secret bits generated per transmitted pulse. The Secret Key Rate (SKR) characterizes factor (ii), with $0 \leqslant \mathrm{SKR} \leqslant 1$. In practice, SKR is influenced by the characteristics of the free-space link, namely the losses and errors introduced by atmospheric conditions. The SKR formula employed in this work is adapted from the decoy-state BB84

Table 1. The parameters employed in this study for determining the length of the secret key generated over the free-space channel.

Parameter	Explanation	Value in this work
μ	Expected photon number, signal	0.5
ν	Expected photon number, decoy	0.1
q	Basis sifting factor	0.5
λ	Wavelength of the signal	850 nm
f_{pulse}	Pulse frequency	100 MHz
f_{dark}	Dark count rate	50 Hz
Δt	Detection time window	1 ns
w_0	Initial beam width	4.5 cm (0.045 m)
Ω_{FOV}	Receiver field of view	5.383×10^{-8} sr
R_{rec}	Receiver radius	0.4 m and 0.6 m
$\Delta\lambda$	Filter bandwidth	0.3 nm
η_{atm_0}	Zenith atmospheric transmittance	0.79
$\eta_{\text{atm}(\theta_{ze})}$	Atmospheric transmittance	$\eta_{\text{atm}_0}^{(1/\cos(\theta_{ze}))}$
$\eta_{\text{fs}}(L)$	Receiver collection efficiency at range L	$1 - e^{-\frac{2R_{\text{rec}}^2}{w(L)^2}}$
$w(L)$	Beam radius at range L	$w_0\sqrt{1 + (\frac{L\lambda}{\pi w_0^2})^2}$
η_{rec}	Receiver efficiency	0.5
η_{tr}	Transmitter efficiency	0.5
η_{point}	Pointing efficiency	0.5
η_{tot}	Total transmittance through free-space link	$\eta_{\text{atm}}\eta_{\text{fs}}\eta_{\text{rec}}\eta_{\text{tr}}\eta_{\text{point}}$
$\frac{N_\mu}{N_\mu+N_\nu}$	Fraction of signal photons	0.5
$f(E_\mu)$	Error correction efficiency	1.22
ϵ_{sec}	Security parameter	$10^{-10}(\approx 2^{-33})$ and 2^{-128}
ϵ_{cor}	Correctness parameter	same as ϵ_{sec}
Q_μ	Detection probability for intensity μ	Equation (7)
E_μ	QBER for intensity μ	Equation (8)
Q_1^L	Lower bound for single-photon gain	Equation (10)
e_1^U	Upper bound for single-photon error	Equation (11)
$H_2(x)$	Binary entropy function	$-x\log_2(x) - (1-x)\log_2(1-x)$
$\frac{N_\mu}{N_\mu+N_\nu}$	fraction of signal pulses	0.5
n	Number of detected signal pulses	$Q_\mu \times q \times x \times \frac{N_\mu}{N_\mu+N_\nu}$
k	Number of detected decoy pulses	$Q_\mu \times q \times x \times 1 - \frac{N_\mu}{N_\mu+N_\nu}$
x	Number of pulses during overpass	$f_{\text{pulse}} \times$ visibility time

free-space link model presented in [12]; however, to account for finite-size effects, minor modifications have been introduced, which are briefly described. The parameters used in this model and in the calculation of the secret key length for this study are summarized in table 1.

Parameters were selected to represent a high-performance yet technologically feasible link, enabling estimation of the upper bound on achievable SKRs. Among these, the operating wavelength plays a central role. We adopt $\lambda = 850$ nm, as this wavelength experiences favourable atmospheric transmission, offers reduced beam divergence compared to longer wavelengths, and aligns well with the peak detection efficiency of silicon-based single-photon avalanche photodiodes (SPADs) [11, 33]. Furthermore, 850 nm has been employed in previous free-space QKD studies [34, 35], making it a practical and established choice for satellite-based QKD simulations.

The initial beam width w_0 is chosen as a trade-off between optimal performance and a realistic size for a satellite. A larger beam waist can help mitigate diffraction losses [9], but in practice the initial beam width is limited by the transmitter aperture and the physical constraints of the satellite. Using the formulas provided in [11, 36], we calculate that the maximum beam waist is approximately 4.5 cm for a 10 cm transmitter aperture. In this work, we adopt $w_0 = 4.5$ cm as a realistic value for a small satellite.

Zenith atmospheric transmittance at 850 nm refers to the transmittance along a vertical (zenith) path through the atmosphere from a source at zenith, accounting for attenuation due to atmospheric particles. In our analysis, this quantity is set to 0.79, consistent with the value reported for 850 nm in [37]. In combination with the satellite's zenith angle, it determines the atmospheric transmittance along the optical propagation path through the atmosphere.

In this work, we adopt a ground-receiver radius R_{rec} of 40 cm, which is relatively large but still feasible in practice; [38] demonstrates a functioning QKD receiver with an 80 cm diameter. To obtain a clearer picture of how the receiver size affects performance, we also run comparable simulations with a 60 cm aperture radius. These results are discussed in more detail in section 3.4. The remaining link

parameters (f_{pulse}, η_{rec}, η_{tr}, η_{point}, Δt, $\Delta\lambda$, Ω_{FOV}) are selected to be close to values commonly used in prior satellite-based QKD studies, e.g. [12, 15, 39].

Although [12] served as the primary reference for our parameter choices, certain adjustments—specifically a stricter spectral filter bandwidth $\Delta\lambda$ and a larger receiver radius R_{rec}—were necessary. Using the looser parameters from earlier work would have prevented any performance gains during less-optimal twilight passes. Therefore, our parameters correspond to an optimized, high-performance ground receiver, while remaining consistent with commonly adopted values in the literature. This allows us to estimate the upper bound of the achievable SKR under realistic conditions.

2.4. SKR formula

In [12], the SKR is given by

$$R \geqslant q\frac{N_\mu}{N_\mu + N_\nu}\left[-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L\left(1 - H_2\left(e_1^U\right)\right)\right]. \tag{1}$$

This SKR formula assumes an infinite number of signals, a condition that can only be asymptotically approached in practical implementations. In reality, the exchanged keys are of finite length, which necessitates accounting for statistical fluctuations arising from limited sample sizes. Security assessment of a QKD protocol relies on statistical analysis of quantum particle behaviour; therefore, these fluctuations directly impact the assurance of key security. This phenomenon is known as the finite-size effect. In this study, we incorporate the finite-size effect into our SKR formula by integrating the correction term proposed in [40]. This term compensates for statistical uncertainty by subtracting a number of bits, thereby compressing the entropy of the key into a smaller space and enhancing the security of the final secret key. The correction depends on the key length and the number of bits used for error-rate estimation, which serves as a proxy for the error rate across the entire raw key. In the original work [40], this correction parameter is denoted by μ; however, to avoid confusion with other variables, we denote this finite-size penalty term as ξ_{finite} in this study. Following [40], ξ_{finite} is given by

$$\xi_{\text{finite}} = \sqrt{\frac{n+k}{nk}\frac{k+1}{k}\ln\frac{2}{\epsilon_{\text{sec}}}} \tag{2}$$

where n, k and ϵ_{sec} refer to the block size, error rate estimation subset size and security parameter, respectively (values for this work provided in table 1). To accurately account for the finite-size effect, upon receiving the simulation output for a single satellite overpass, we computed the total number of detection events and errors occurring during the overpass and applied equation (3) to determine the number of extractable secure bits, given the chosen security parameter. Since all decoy-state signals were used for parameter estimation, n (k) in equation (2) was calculated as the expected number of signal (decoy) pulses that resulted in a detection event at the ground station.

The integration of ξ_{finite} into the SKR formula presented in [12] was carried out by the authors of this study. By combining these two formulas, the length of the secret key generated over the free-space link during a single satellite overpass is given by:

$$l \geqslant q \times x \times \frac{N_\mu}{N_\mu + N_\nu}\left[-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L\left(1 - H_2\left(e_1^U + \xi_{\text{finite}}\right)\right)\right] - \log\left(\frac{2}{\epsilon_{\text{sec}}^2 \epsilon_{\text{cor}}}\right) \tag{3}$$

where all parameter definitions are provided in table 1 and section 2.5.

To calculate the total number of secret bits achieved during a given day, we first computed the secret bits obtained from a single satellite overpass, incorporating finite-size effects as described above, and then summed the bit gains across all overpasses for that day. In this approach, the security parameter was fixed for all satellite passes, while the total secret-bit count consisted of multiple blocks of varying lengths. Some overpasses yielded negative key rates; however, this negativity is purely theoretical, as the key rate cannot be less than zero in practice. Negative key rates occur when post-processing requires truncating the generated key material to such an extent that it consumes all produced secret bits. In these cases, we assigned zero secret bits to the total sum.

2.5. Background light

Daylight varies over a 24 h period due to Earth's rotation, which alternately exposes each location to the Sun or turns it away. Seasonal changes in illumination arise from Earth's axial tilt, approximately 23.5°,

combined with its orbit around the Sun. This leads to strong seasonal contrasts at high latitudes: regions tilted away from the Sun experience polar night in winter, while those tilted toward the Sun undergo continuous daylight in summer. In contrast, areas near the equator show only minor seasonal variation in daylight.

Background light poses a significant challenge for QKD because quantum signals are encoded in photons, which are themselves light. Photon detectors used in QKD systems are highly sensitive and cannot inherently distinguish between a signal photon originating from the sender and a photon from background illumination [11]. This results in increased background noise and reduced key generation efficiency.

In this work, the background noise contribution is modelled as

$$N = H_{\mathrm{b}} \times \Omega_{\mathrm{FOV}} \times \pi R_{\mathrm{rec}}^2 \times \Delta\lambda \times \Delta t \tag{4}$$

where H_{b} denotes the background spectral radiance ($\mathrm{W\,m^{-2}\,sr^{-1}\,\mu m^{-1}}$), Ω_{FOV} is the receiver field of view, R_{rec} is the receiver-aperture radius, $\Delta\lambda$ is the optical bandwidth, and Δt is the detector time window. H_{b} is modelled as a constant value 10^{-4} for Sun-altitude angles $\leqslant -18°$, corresponding to astronomical night, following the methodology of [12]. During twilight, when the Sun is between $-18°$ and $-10°$ relative to the horizon, H_{b} is smoothly increased from 10^{-4} to 10^{-3} according to

$$H_{\mathrm{b}} = 10^{-4} \cdot 10^{(\mathrm{alt}+18)/8} \tag{5}$$

where alt denotes the altitude of the Sun in degrees (negative when the Sun is below the horizon). This provides a simplified yet conservative sky-brightness model, avoiding overly optimistic performance estimates. Contributions from moonlight were neglected to maintain consistency with the referenced methodology and to avoid introducing additional model complexity unrelated to the primary focus of this work.

The effect of background radiation is incorporated into the key-rate model of section 2.4 as

$$Y_0 = \eta_{\mathrm{rec}} \frac{N}{hc/\lambda} + 4\Delta f_{\mathrm{dark}} \Delta t \tag{6}$$

where h is Planck's constant, c is the speed of light, and the other variables are given in table 1;

$$Q_\mu = Y_0 + 1 - \mathrm{e}^{-\eta_{\mathrm{tot}}\mu} \tag{7}$$

$$E_\mu = \frac{e_0 Y_0 + e_{\mathrm{det}}\left(1 - \mathrm{e}^{-\eta_{\mathrm{tot}}\mu}\right)}{Y_0 + 1 - \mathrm{e}^{-\eta_{\mathrm{tot}}\mu}} \tag{8}$$

$$Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \tag{9}$$

$$Q_1^L = \mu \mathrm{e}^{-\mu} Y_1^L \tag{10}$$

$$e_1^U = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^L \nu}. \tag{11}$$

Because the background-radiation model determines the background rate Y_0, increases in H_{b} directly raise Y_0. This elevated dark-count level then propagates through the key-rate model: it increases the overall gain Q_μ and raises the quantum-bit error rate E_μ, thereby amplifying the amount of leaked error-correction information $H2(E_\mu)$. Although the gain Q_μ becomes larger, this increase comes solely from noise and does not enhance the single-photon contribution that produces secure key bits. As a result, higher background radiation reduces the final secret-key rate in our simulations. Several studies (e.g. [21, 22]) have demonstrated that positive key rates are still achievable during twilight and even full daylight when advanced spectral and spatial filtering is employed. These aspects and their implications for our modelling choices are discussed further in section 4.

In this study, simulations were conducted for all three geographic locations throughout the entire year to account for the substantial seasonal variation in lighting conditions characteristic of Arctic regions. Additionally, to examine the effects of seasonal variations, we conducted supplementary simulations over shorter time intervals representative of different seasons. These simulation intervals were as follows: spring (16–25 March 2024), summer (16–25 June 2024), autumn (16–25 September 2024),

and winter (16–25 December 2024). The winter and summer periods encompass the respective solstices, thereby capturing the most pronounced contrasts in lighting conditions. In contrast, the spring and autumn intervals include the March and September equinoxes, which offer comparable lighting conditions. However, the probability of cloud cover and other weather conditions differed between these transitional seasons, as discussed in the following section.

2.6. Local weather data

In addition to background-radiation noise, the performance of a free-space QKD link is strongly influenced by atmospheric attenuation caused by weather conditions. Whereas background radiation primarily increases the dark-count probability and hence degrades the signal-to-noise ratio, adverse weather introduces additional channel loss that reduces the number of detected signal photons. To incorporate the effects of weather-induced attenuation, we used meteorological observations from the Finnish Meteorological Institute's open data archive [25], including quantitative cloud-cover data as well as textual descriptions of the prevailing weather conditions. The archive provides freely accessible measurements from multiple observatory sites across Finland.

In this work, the relevant weather conditions considered were cloud cover, rain, snowfall, ice crystals, and fog. All three ground-station locations considered in this study (Rovaniemi/Apukka, Sodankylä/Tähtelä, and Utsjoki/Kevo) are co-located with meteorological observation stations operated by the FMI. For Sodankylä and Utsjoki, both cloud-cover measurements and descriptive weather-type observations were directly available from the Tähtelä and Kevo observatories. In the case of Rovaniemi, however, the Apukka station reports cloud-cover information but does not provide descriptive weather observations (only some FMI stations report the full set of variables; see [41]). For this reason, the cloud-cover and weather-type data used to model the Apukka ground station were taken from the Rovaniemi railway station site, which provides both. This substitution is considered a sufficiently accurate approximation of the weather conditions at Apukka. The model for calculating link loss due to these factors is explained in more detail in the next subsections.

2.6.1. Cloudiness

Clouds impede signal transmission to the ground station because the signal is absorbed by cloud molecules. Finland lies in a region with relatively high cloud coverage, suggesting that cloud cover will likely be a significant limiting factor for the deployment of satellite-based QKD in these areas. The impact of cloud cover was incorporated into the simulation as follows. Cloudiness information from FMI were recorded at one-hour intervals and reported in oktas, indicating how many eighths of the sky dome are covered by clouds during each observation interval. For instance, a value of 1/8 indicates that one-eighth of the sky was obscured by clouds. Cloud cover is therefore not binary; the sky can be partially cloudy. Cloud observations were collected throughout the year 2024, and monthly averages of the probability of a cloud-free sky were derived by converting cloud cover measurements into probabilities that a free-space link would be obstructed by clouds. For instance, a cloud cover value of 2/8 was interpreted as a 0.25 probability of cloud cover. All cloud cover observations were converted into probability values, after which the probability of a cloudy sky, $P(\text{cloudy})$, was computed as an average of all cloud cover observations for the given month. Since a satellite may, in principle, appear at any position on the sky dome, the instantaneous probability of line-of-sight (LOS) can be approximated by the fraction of the sky that is cloud-free. We refer to this as the LOS probability. This probability, $P(\text{LOS})$, was obtained as the complement of the cloud-cover probability, i.e. $P(\text{LOS}) = 1 - P(\text{cloudy})$. This probability was evaluated separately for each month. For example, the value of $P(\text{LOS})$ for December was computed as the average clear-sky probability based on all samples recorded between 1 and 31 December 2024:

$$P(\text{LOS}_{\text{Dec}}) = \frac{\sum_{i=1}^{n_{\text{Dec}}} \left(1 - \frac{\text{cloudiness}_i}{8}\right)}{n_{\text{Dec}}}. \tag{12}$$

Here n_{Dec} denotes the number of samples recorded in December. The probabilities of cloud-free conditions for the different locations and months are provided in the supplementary data.

Our model assumes that whenever clouds obstruct the line of sight between the satellite and the ground station, the link budget is zero. This assumption is justified by the fact that the wavelength considered in our model (850 nm) cannot meaningfully penetrate cloud cover [42]. In the simulation, the achievable amount of secret bits was modelled by first assuming cloud-free conditions and then incorporating the effect of cloud cover by multiplying the amount of secret bits by the LOS probability. This approach yields an average expected amount of secret bits over an extended period rather than a realistically achievable key rate at any given moment. Accordingly, this work assumes that the SKR for a free-space link under cloudy conditions is zero.

Table 2. Weather conditions modelled in the simulation.

Weather class	Link transmittance	Parameters
Weak snowfall	$\eta_{\text{tot}} \times \eta_{\text{snow}}$ (equation (19))	$S = 1.0$, $a = 5.42 * 10^{-5} * \lambda + 5.495\,8776$, $b = 1.38$
Moderate snowfall	$\eta_{\text{tot}} \times \eta_{\text{snow}}$ (equation (19))	$S = 2.5$, $a = 5.42 * 10^{-5} * \lambda + 5.495\,8776$, $b = 1.38$
Weak sleet	$\eta_{\text{tot}} \times \eta_{\text{snow}}$ (equation (19))	$S = 2.5$, $a = 1.023 * 10^{-4}\lambda + 3.785\,5466$, $b = 0.72$
Moderate sleet	$\eta_{\text{tot}} \times \eta_{\text{snow}}$ (equation (19))	$S = 1.0$, $a = 1.023 * 10^{-4}\lambda + 3.78\,5466$, $b = 0.72$
Light rain	$\eta_{\text{tot}} \times \eta_{\text{rain}}$ (equation (17))	$R = 2.5$, $a = 1.07$, b = 0.67
Moderate rain	$\eta_{\text{tot}} \times \eta_{\text{rain}}$ (equation (17))	$R = 8.0$, $a = 1.07$, b = 0.67
Fog or mist	$\eta_{\text{tot}} \times \eta_{\text{fog}}$ (equation (21))	$V = 1.0$, $q = 0.5$
Ice crystals	$\eta_{\text{tot}} \times \eta_{\text{fog}}$ (equation (21))	$V = 5.0$, $q = 1.14$
No relevant weather phenomena	η_{tot}	given in table 1

2.6.2. Rain, snow and fog

In addition to cloud cover, several weather phenomena can affect the transmission of an optical satellite link, including fog, rain, and snowfall. Because the link budget in this work is assumed to be zero whenever clouds obstruct the line of sight, these phenomena influence the link only during periods when LOS is available but precipitation or fog occurs at the ground station or along the optical path. To quantify these effects, we collected hourly FMI observations for all ground-station sites, recording both the cloud-cover value and the corresponding weather description at each hour (e.g. '7/8, Light snowfall'). FMI provides weather descriptions in textual form, and across the full dataset we identified 37 distinct weather types. These were grouped into nine aggregated classes: Light snowfall, Moderate snowfall, Light sleet, Moderate sleet, Light rain, Moderate rain, Ice crystals or snow grains, Mist or fog, and No relevant weather phenomena. A table mapping the original FMI descriptions (37 in total) to these nine categories is provided in supplementary data. This simplification was adopted because the FMI weather descriptions are purely verbal and do not provide quantitative information such as visibility or precipitation rates. As a result, the available data were insufficient to model all 37 weather types individually, and a coarser categorization was required. Certain phenomena, such as 'Dense snowfall', were excluded because their associated LOS probability was zero; that is, they never occurred under conditions in which the link would have been operational, and therefore did not need to be represented in the simulation.

To determine how probably each weather class affects the link when LOS is available, we evaluated the conditional LOS probability associated with each weather class. For every ground station and each month of 2024, we computed FMI statistics linking cloud-cover values, and thus LOS probabilities, to the observed weather types. The data were hourly and aggregated using arithmetic means. For each weather class w, the conditional LOS probability $P(\text{LOS} \mid w)$ was calculated as the mean cloud-free fraction across all observations in which that weather type occurred:

$$P(\text{LOS} \mid w) = \frac{1}{n_w} \sum_{i=1}^{n_w} P(\text{LOS}) \tag{13}$$

where n_w denotes the number of samples for weather class w in the given month. Having determined both the frequency of each weather type and its correlation with LOS availability, we then inverted the relationship. Conditioning on LOS being available, the probability of observing weather class w at that moment was computed as

$$P(w \mid \text{LOS}) = \frac{P(\text{LOS} \mid w)\, P(w)}{P(\text{LOS})}. \tag{14}$$

This yields the likelihood that each weather class occurs under conditions in which the link is operational. An important advantage of this approach is that it avoids imposing arbitrary binary thresholds between 'cloudy' and 'clear,' which would be inherently subjective given the okta-based cloud-cover measurement system. The complete LOS-condition probabilities for different locations and months are provided in supplementary data. The attenuation models associated with each weather class are presented in table 2 and are described in detail below.

We assumed that snow and rain originate from cloud layers at an altitude of approximately 3 km, which is a reasonable assumption for precipitation in the Arctic region [43]. Accordingly, attenuation was applied only to the portion of the optical path below 3 km from the Earth's surface. The same approach was used for fog and ice crystals, which were likewise limited to the lowest 3 km, consistent with their confinement to the near-surface troposphere. Attenuation values provided in units of dB km^{-1}

were converted to total attenuation (dB) over the 3 km layer and subsequently transformed into transmittance values η_{snow}, η_{rain} and η_{fog}.

To obtain the total attenuation coefficient for the entire link path, we first computed the length of the path segment located at or below 3 km altitude, denoted L, as

$$L = \frac{3}{\sin(90^\circ - \theta)} \tag{15}$$

where θ is the zenith angle of the satellite. The attenuation coefficient for rain was modelled using the Carbonneau formulation [44]:

$$a_{\text{rain}} = 1.076\,R^{0.67}\ \text{dB km}^{-1} \tag{16}$$

where R denotes the rainfall rate in units of mm h^{-1}. This formulation is widely used in free-space optical (FSO) link modelling, including at wavelengths around 850 nm [45, 46], and has also been applied in modelling rain attenuation for BB84-type QKD links [47]. In our simulation, we used rainfall rates of $R = 2.5$ mm h^{-1} for light rain, $R = 8$ mm h^{-1} for moderate rain, and $R = 15.9$ mm h^{-1} for heavy rain. To obtain the total attenuation coefficient, the specific attenuation (dB km^{-1}) was first multiplied with the path length L to yield the total attenuation along the affected section of the link. This total attenuation in decibels was then converted into a transmittance value η_{rain}, i.e.

$$\eta_{\text{rain}} = 10^{-L a_{\text{rain}}/10}. \tag{17}$$

Attenuation due to snowfall was modelled using the commonly adopted power-law formulation

$$a_{\text{snow}} = a\,S^{b}\ \text{dB km}^{-1} \tag{18}$$

where S denotes the snowfall rate in water-equivalent units of mm h^{-1}, and the coefficients a and b are provided separately for dry snow and sleet in table 2. This formulation is widely used in the literature for modelling snowfall attenuation in FSO links, including at wavelengths around 850 nm as employed in this study [45, 48]. In the simulations, light snowfall was modelled with an intensity $S = 1.0$ mm h^{-1} and moderate snowfall with $S = 2.5$ mm h^{-1}. The total transmittance η_{snow} was computed analogously to the rain case, such that

$$\eta_{\text{snow}} = 10^{-L a_{\text{snow}}/10}. \tag{19}$$

Mist and fog were modelled using the Kim model [49], which provides the attenuation coefficient per kilometre as

$$a_{\text{fog}} = \frac{3.91}{V}\left(\frac{\lambda}{550}\right)^{-q}\ \text{dB km}^{-1} \tag{20}$$

where V is the visibility in kilometres, and the values of q are listed in table 2, following the parameterization in [49]. This model was adopted because empirical measurements indicate that the Kim model provides reliable predictions of fog attenuation at 850 nm [48], and it has also been used for modelling BB84-link attenuation under fog conditions (e.g. [47]). The total fog attenuation along the affected portion of the path was then computed in the same manner as for rain and snow, i.e.

$$\eta_{\text{fog}} = 10^{-L a_{\text{fog}}/10}. \tag{21}$$

The Kim model accounts for fog-specific attenuation beyond that caused by normal atmospheric aerosols and is included in the link budget only when FMI observations explicitly report fog or mist conditions. To simplify the model, we set $V = 1$ km for all instances of this weather class, as this value lies between the WMO definitions of mist and fog [50].

In this study, ice-crystal attenuation was modelled using the visibility-based Kim formulation (equation (20)), with an effective visibility of 5 km. This choice reflects two considerations. First, ice crystals are sometimes treated as fog-like (indeed, they can themselves form fog), yet they are also classified as a subtype of snow, making a purely 'snow-based' or purely 'fog-based' treatment ambiguous [51]. Second, the Kim model is specifically designed for attenuation scenarios parameterized by visibility and incorporates relevant scattering characteristics [49]. Because FMI does not report visibility during ice-crystal conditions, $V = 5$ km was adopted as a pragmatic compromise between clear-air and fog-like conditions, corresponding approximately to 'haze' in the Kim taxonomy. We emphasize that the 'ice crystals'

class used here does not include 'ice fog', which is treated separately under the fog category (see supplementary data). While this modelling choice is approximate, it provides a reasonable first-order estimate of ice-crystal-induced attenuation.

To obtain the total link transmittance during snowfall, rain, ice crystals, or fog, the corresponding attenuation coefficients were applied multiplicatively to the nominal clear-air link transmittance, as shown in table 2. If the weather class corresponded to 'no relevant weather phenomenon', the nominal transmittance without additional attenuation was used. These transmittance values and their corresponding weather-condition probabilities were incorporated into the simulation as a probability-weighted expected transmittance, such that the overall channel transmittance for a given month was modelled as

$$T_{\text{total}} = \sum_{i=1}^{n} p(w_i)\, T(w_i) \tag{22}$$

where $p(w_i)$ denotes the probability of weather type i during LOS conditions and $T(w_i)$ is the corresponding channel transmittance. Equation (22) therefore represents the expected channel transmittance for a given location and month, with each transmittance value weighted by its occurrence probability. Importantly, this is not the instantaneous transmittance at any particular moment but rather a long-term expectation. Although this approximation is not physically exact, it is appropriate for evaluating the usability of a satellite-based QKD system, in which satellite visibility is limited to short, infrequent passes and secret keys must be accumulated in a buffer. For such systems, long-term expected key-generation performance is more relevant than moment-to-moment link quality.

3. Results

In this section, we present the simulation results obtained using the methodology described in section 2, applying a security parameter of 10^{-10}. Figure 2 depicts the annual distribution of extracted secret bits for three simulated ground station locations when communicating with the Suomi100 satellite. The key rates were computed on a daily basis and subsequently weighted by the monthly LOS probability. For example, the expected number of secret bits on day 48 in Rovaniemi was determined by simulating the QKDLapland satellite link on 17 February, aggregating all secret bits collected during different overpasses, and multiplying this total by the probability of LOS conditions in Rovaniemi for February.

Although the Suomi100 satellite follows a Sun-synchronous orbit, its exact trajectory exhibits slight variations from day to day, which manifest as fluctuations in the achievable key rates. The influence of daylight is evident in figure 2: as the amount of daylight increases toward summer, the key rates progressively decline until they reach zero. Conversely, toward the end of the year, the key rates rise again, peaking around the winter solstice. The outage period, defined as the interval during which no secret bits can be extracted, depends on the ground station location. In Sodankylä and Rovaniemi, this period extends from 13 February to 9 October, whereas in Utsjoki it spans from 13 February to 8 October. Because the Suomi100 satellite is scheduled to pass over Finland closer to daylight hours, extended outage periods are not unexpected. Indeed, one might equally argue that the persistent darkness of the winter season enables key generation even from a satellite whose overpass timing would otherwise be suboptimal for QKD. Consequently, there are 238 consecutive days without key material in Sodankylä and Rovaniemi, and 239 d in Utsjoki. When averaged over the entire year, the expected daily generation of secret bits is 40 336 for Rovaniemi, 50 207 for Sodankylä, and 46 832 for Utsjoki.

Similarly, figure 3 illustrates the annual distribution of extracted secret bits for the three simulated ground station locations when communicating with the QKDLapland satellite. The overall behaviour resembles that observed with Suomi100; however, due to a shift in optimal overpass times, QKDLapland can generate secret key material during the spring and autumn periods when the Suomi100 QKD link is completely unavailable. Nevertheless, as summer approaches, this advantage diminishes because the high background light levels render the timing of satellite passes inconsequential. When averaged over the entire year and weighted by the probability of line of sight, the expected daily extraction of secret bits is 93 018 for the Rovaniemi link, 115 603 for the Sodankylä link, and 127 381 for the Utsjoki link. For Rovaniemi, this represents a 131% increase compared to the secret bits obtained from the Suomi100 satellite; for Sodankylä and Utsjoki, the corresponding increases are 130% and 172%, respectively. In Rovaniemi and Sodankylä, the period of excessive background light, during which no key material can be generated, begins on 24 March and ends on 15 September. In Utsjoki, this period extends from 26 March to 19 September. Consequently, the outage durations amount to 176, 176, and 178 consecutive

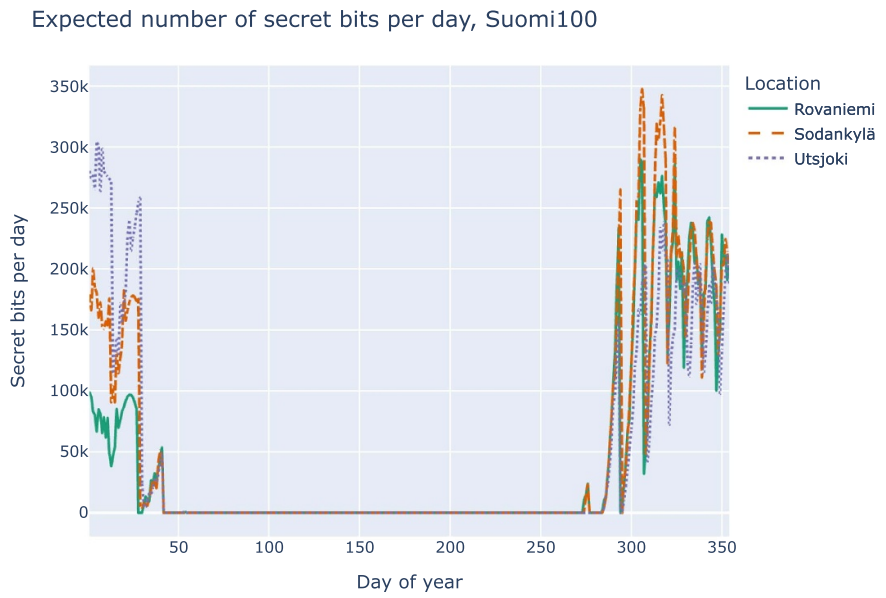

Figure 2. Daily extractable secret bits from the Suomi100 satellite to three ground station locations, considering cloud cover and other weather phenomena. The security parameter is set to 10^{-10}. During the brightest period of the year, no secret key material can be generated due to the high levels of background light in polar regions. In other seasons, the number of secret bits depends on the probability of clear skies, the intensity of background light, and daily variations in the satellite's trajectory.

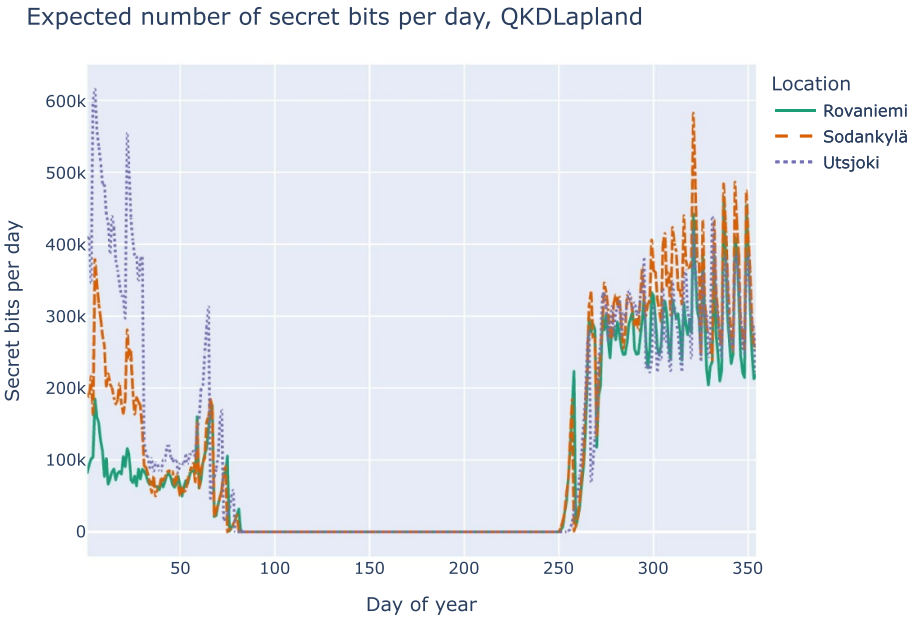

Figure 3. Daily extractable secret bits from the QKDLapland satellite to three ground station locations, considering cloud cover and other weather phenomena. The security parameter is set to 10^{-10}. As illustrated in the figure, key generation is inhibited during summer due to excessive background light; however, this outage period is shorter than that observed for the Suomi100 satellite, owing to the optimization of QKDLapland's overpass timing.

days for Rovaniemi, Sodankylä, and Utsjoki, respectively. In each case, the length of the outage period was reduced by 26% compared to the Suomi100 satellite link.

QKDLapland exhibits a markedly higher capacity for secret-key generation during spring and autumn. The primary reason is that the optimal passes of QKDLapland occur during night-time, while those of Suomi100 coincide with daylight hours. In the context of Finnish Lapland, orbital scheduling becomes particularly critical during spring and autumn, when each day contains both dark and light periods. During the polar day, continuous illumination renders scheduling irrelevant; conversely, in

winter, scheduling passes during night-time improves performance, although precise timing matters less due to the extended hours of darkness. Despite the optimized timing of QKDLapland's passes, the system still experiences substantial outage periods. This arises from the fact that QKDLapland encounters two daily passes with particularly favourable elevation angles, and the current schedule is optimal in the sense that both passes fall within night-time during the darker half of the year. This optimization, however, entails a trade-off: neither pass occurs exactly at local midnight. The outage period could be reduced by shifting the single best overpass to coincide with midnight; however, doing so would likely decrease the total key generated during winter, as only one high-quality pass per day would then occur under optimal conditions. Nevertheless, the results clearly demonstrate that optimizing satellite overpass timing can significantly mitigate outage periods caused by background illumination.

3.1. Impacts of cloud cover and weather conditions

The impact of cloud cover is substantial. During the months most favourable for key exchange with respect to ambient light (November–January), the probability of a cloud-free LOS is only 0.31–0.46, which at best reduces the achievable key rate to approximately one half of what would be obtained under persistently clear-sky conditions. In the summer months, the probability of LOS is highest, yet no secret key can be generated due to excessive background illumination.

When considering the effects of other meteorological factors, as reported in supplementary data, one observes that during summer the probability of precipitation coinciding with LOS conditions is low, typically below five per cent. January, however, reveals an unexpected pattern: in Sodankylä, as many as 22% of all LOS occurrences are, in expectation, associated with light snowfall. The likely explanation for this behaviour is discussed in more detail in section 4.2. In Utsjoki, the corresponding value was only 12%, which has a clear impact on the expected link transmittance. For example, during QKDLapland's first overpass on 31 January, which was visible from both Utsjoki and Sodankylä, the weather-dependent reduction in expected transmittance was 14% in Utsjoki and 29% in Sodankylä, relative to the assumption of no precipitation. This difference contributes to the superior January performance of the Utsjoki link; the lower probability of light snowfall during LOS conditions alone increases its expected link capacity noticeably. Even light snowfall renders the link almost unusable. For instance, at a satellite zenith angle of 8° (82° above the horizon), the path transmittance through light snowfall was only about 0.02, leaving very little margin for successful key generation. In other words, approximately 98% of the optical signal was attenuated by the snowfall alone.

Ice crystals appear to have the smallest impact on link capacity. For example, at a satellite zenith angle of 7°, the path transmittance through ice crystals was approximately 0.71, whereas at a zenith angle of 82° (8° above the horizon, barely visible), it decreased to roughly 0.07. This indicates that ice crystals do not impede key generation during otherwise favourable high-elevation overpasses, but at low elevation angles they can significantly degrade, and potentially eliminate, the link capacity.

3.2. Impacts of background light and satellite elevation

Naturally, the lengths of secret keys obtained during individual satellite overpasses vary, primarily as a function of the satellite's maximum elevation angle. For example, in Utsjoki in December 2024 with the QKDLapland satellite, the shortest secret key block (where key length $\geqslant 0$) contained 7 bits, whereas the longest reached 580 073 bits. The efficiency of a single overpass appears to be governed mainly by the highest elevation angle achieved during that pass. This parameter is particularly relevant in the context of QKD, as it determines the optical path length through the atmosphere: a signal arriving near zenith traverses less atmospheric material than one arriving at a shallow angle, which must propagate diagonally through a greater thickness. In some cases, the satellite becomes visible but remains at such a low elevation that, given the prevailing noise level, no secure key bits can be generated. This outcome reflects both the limited number of signals exchanged and the substantial signal loss caused by the high channel error rate. If the amount of secret bits discarded during error correction and other post-processing steps exceeds the number of bits generated during the overpass, the resulting key rate becomes negative. Moreover, the finite-size security analysis penalizes short keys more severely, favouring longer key lengths. Based on our results, achieving a maximum elevation of approximately 16 degrees during an overpass appears to be a prerequisite for obtaining a positive key length.

However, background noise also strongly affects the link's ability to generate secret keys. To illustrate this, consider two QKDLapland overpasses above the Sodankylä station shortly after 21:00, each reaching an almost ideal elevation of approximately 87°, i.e. near zenith. During the December overpass at 21:01, the Sun is 37° below the horizon. In this case, the upper bound on the single-photon error rate is $e_1^U = 3.13 \times 10^{-2}$, and the single-photon gain is $Q_1^L = 1.94 \times 10^{-4}$. By contrast, during the March overpass at 21:08, the Sun is only 13° below the horizon. The increased background illumination raises

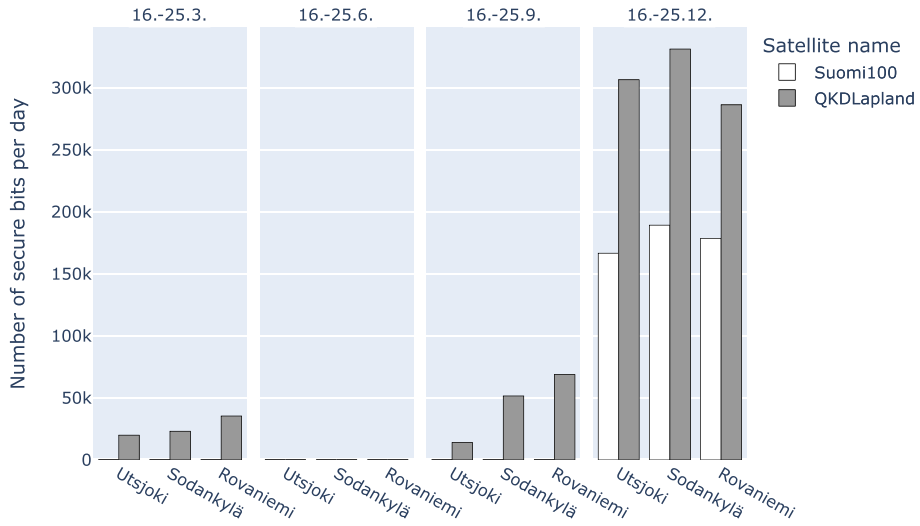

Figure 4. Daily extractable secret bits for the QKDLapland and Suomi100 satellites across different ground-station locations, averaged over 10 d periods and considering cloud cover and other weather phenomena. Because QKDLapland's passes are scheduled predominantly during night-time, a greater number of overpasses can be utilized, resulting in improved daily key rates.

noise levels to the point that $e_1^U = 5.255 \times 10^{-1}$, while the single-photon gain becomes $Q_1^L = 1.57 \times 10^{-2}$. (We report gain Q_1^L; since $Q_1^L = \mu e^{-\mu} Y_1^L$, gain trends directly reflect yield.) According to equation (3), no secret key can be extracted in this case: the single-photon privacy-amplification term alone incurs a penalty of approximately $H2(0.52) \approx 100\%$, precluding any positive key rate even before accounting for error correction or finite-size effects. In the December case, by contrast, the link yielded a total of 688 117 secret bits. With $e_1^U \approx 3.12 \times 10^{-2}$, the privacy-amplification penalty is only $H2(0.03) \approx 20\%$, which still leaves a substantial number of secure bits from a high-quality pass. It is noteworthy that although the single-photon gain appears larger in the March overpass, this increase is driven primarily by noise photons, which also contribute to the single-photon yield. The associated error rate grows even faster, ultimately destroying the link capacity. These data show that the key-rate expression penalizes sunrise and sunset conditions so severely that an almost perfectly favourable elevation geometry is required to obtain any secret bits at all, and even then, the Sun must lie much closer to 18° than to 10° below the horizon. This explains why the secret-key yields for both satellites decrease sharply as summer approaches: once the duration of astronomical darkness no longer covers the optimal overpasses, key generation becomes effectively impossible.

3.3. Impacts of ground station location

Figure 4 shows the expected daily number of secret bits, averaged over ten-day periods and weighted by the probability of clear-sky conditions. To better understand the structure behind this figure, it is useful to examine the number of overpasses that are potentially usable during the darkest period of the year: 16–25 December 2024, when conditions are most favourable for key generation. Without accounting for weather, i.e. selecting overpasses solely on the basis of Sun and satellite geometry, the QKDLapland satellite provides 48, 39, and 35 usable passes for Utsjoki, Sodankylä, and Rovaniemi, respectively. When cloud-cover statistics are incorporated, the expected numbers decrease to 13.76, 12.09, and 13.02 passes. For the Suomi100-Utsjoki link, the corresponding pass counts are 18, 16, and 15 without weather filtering, and 5.44, 4.65, and 5.88 once weather data is included.

These values highlight that Utsjoki's location is intrinsically more favourable for a polar-orbiting satellite than the more southerly stations. Because a satellite in near-polar orbit passes close to the North Pole on every revolution, the Utsjoki ground station, being located at higher latitude, can establish a link even during passes that do not traverse directly above Finland. The effect of solar-illumination differences between the sites can be ruled out, as all key-generating passes during this period occurred with the Sun at an altitude below −18°, ensuring effectively constant background-light modelling throughout. However, once weather statistics are introduced, the balance shifts: Sodankylä experiences a markedly lower probability of snowfall during December 2024, resulting in higher key rates despite its

Table 3. Daily secret bit yield and number of usable overpasses for the QKDLapland-Utsjoki link under selected parameter adjustments. Values are 10 d averages over the periods listed in the time column. In the ϵ_{sec} columns, the receiver diameter is held at its original value; in the R_{rec} columns, the security parameter remains at its original value. The baseline ('Original setting') link parameters are those specified in table 1.

	Original setting		ϵ_{sec}: $10^{-10} \longrightarrow 2^{-128}$		R_{rec}: 40 cm $\longrightarrow$ 60 cm	
Time	secret bits	overpasses	secret bits	overpasses	secret bits	overpasses
16–25 March 2024	5.26×10^4	0.7	3.62×10^4 (−31%)	0.6 (−14%)	1.5×10^5 (+184%)	0.9 (+29%)
16–25 June 2024	0	0	0 (+0%)	0 (+0%)	0 (+0%)	0 (+0%)
16–25 September 2024	3.32×10^4	0.6	2.19×10^4 (−34%)	0.4 (−33%)	9.86×10^4 (+197%)	0.7 (+17%)
16–25 December 2024	9.58×10^5	4.3	8.03×10^5 (−16%)	3.7 (−14%)	2.46×10^6 (+157%)	4.6 (+7%)

less favourable orbital geometry. In this period, weather, not geometry, is the dominant factor determining relative performance.

In spring and autumn, background illumination becomes the primary factor limiting the number of usable passes. During 16–25 March 2024, the Utsjoki, Sodankylä, and Rovaniemi links were able to establish a connection to QKDLapland during 7, 8, and 10 passes, respectively, without incorporating weather data. Thus, during spring and autumn, the more southerly locations benefit from lower background illumination, enabling a higher number of operational passes despite their less favourable geometry. Nevertheless, weather remains a substantial contributor to the final expected key-generation performance, significantly reducing the effective number of usable passes even during periods when daylight conditions would otherwise permit successful link operation.

3.4. Tuning the link parameters

In this section, we examine how tuning selected link parameters affects the achievable key rates. Our aim is not to exhaustively optimize the link over all tunable quantities, but rather to identify parameter choices whose impact varies with season in a high-latitude environment. Among many possibilities, we focus on the composable security parameter ϵ_{sec} and the receiver-aperture radius R_{rec}. Considered together, these two parameter choices expose season-dependent sensitivities that would be obscured in a high-dimensional sweep; a comprehensive exploration of the full parameter space is left for future work.

Table 3 summarises the seasonal effects of tuning these two parameters. Specifically, we evaluate how tightening ϵ_{sec} from 10^{-10} (approximately 2^{-33}) to 2^{-128}, comparable, for example, to the decapsulation failure rate of ML-KEM [52], influences the achievable secret-key rate, and how increasing R_{rec} from 40 cm to 60 cm mitigates loss arising from beam broadening and seasonal variations in elevation geometry.

As expected, tightening ϵ_{sec} lowers the retained key: stronger composable guarantees require discarding more bits during post-processing. With a tighter security parameter, the finite-size correction term increased by 284 bits per pass. The effect is distinctly seasonal. In winter, the relative reduction is modest (≈16%), because larger blocks and lower QBER dilute the privacy-amplification overhead and the finite-size correction term, yielding only ≈10%–11% loss per strong overpass. By contrast, in spring the blocks are smaller and the effective privacy-amplification factor is higher, so the same absolute bit removal consumes a much larger fraction of the key and can push borderline passes to zero, producing an average reduction of ≈31%.

Seasonal structure is equally clear on the optical side. Beam broadening over the slant path limits the fraction of photons captured at the ground station. Increasing the receiver aperture from 40 cm to 60 cm correspondingly raises the captured fraction, improving both the number of usable overpasses and the per-pass key, often by a multiplicative factor. This holds across all seasons except midsummer, when background illumination, rather than aperture, becomes the binding constraint. In practice, the aperture choice must balance performance against cost. Even large receivers cannot restore summertime availability under the background model considered here.

3.5. Inter-ground-station communication

In this section, we examine inter-ground-station communication using the one-time pad (OTP) encryption scheme. OTP provides information-theoretic security by encrypting each bit of the message with a corresponding bit of the key [53]. An OTP-based key exchange between two ground stations, each connected to a satellite, can be implemented as follows: (i) the satellite establishes key A with ground station A and key B with ground station B; (ii) the satellite computes the XOR (exclusive OR) of key A and key B and transmits this result to station A; (iii) since station A knows key A, it can derive key B; (iv) stations A and B then use key B to encrypt their bilateral communication. De Grossi *et al* [12] discusses

several considerations for optimizing a network of ground stations and satellites employing this protocol. For the purposes of this paper, it suffices to note that the length of the inter-ground-station key derived from the above procedure is limited by the shorter of the two keys, as OTP requires the encryption key to be at least as long as the message being encrypted.

As an illustrative example, we consider establishing a communication link between Utsjoki and Rovaniemi using satellite-QKD-distributed OTP keys under a security parameter of 10^{-10}. We assume that key material accumulated over an entire day is generated between the satellite and the two ground stations, and subsequently, upon reappearing within view, the satellite transmits the XOR of these keys to the other station. (This protocol implicitly requires the satellite to maintain simultaneous QKD links to both Utsjoki and Rovaniemi, as portions of their favourable key-establishment windows are likely to overlap. As this is merely an illustrative example, we do not examine this issue in further detail).

In this scenario, it is necessary to determine the key length that the satellite can generate with each ground station; the inter-ground-station link capacity is then constrained by the shorter of the two keys. The amount of key material available for encrypting such a link is therefore determined by the minimum of the key lengths exchanged between the satellite and each ground station. For the simulated year 2024, we compute the average smallest secret-key length for the Rovaniemi and Utsjoki links as $\frac{1}{366}\sum_{i=1}^{366}\min(\mathrm{Roi}_i, \mathrm{Uts}_i)$, where Roi_i and Uts_i denote the expected number of secret bits gathered in the Rovaniemi and Utsjoki links on day i. Note that the year 2024 contained 366 d due to the leap day. Based on our simulation results, with QKDLapland satellite, this calculation yields an average of 85 927 bits per day for the Rovaniemi–Utsjoki link. Using this value as an approximation of the achievable symmetric key for the link, the following calculations can be performed.

Assuming OTP is employed, this key material would suffice for encrypting 85 927 bits per day. For illustration, this corresponds to approximately 10 740 UTF-8 encoded characters, which, depending on font size, would amount to roughly four pages of human-readable text. Alternatively, at a transmission rate of 1 Mbps, only about 0.09 s of video call could be encrypted using OTP. If, instead of OTP, the key material were divided into multiple fixed-length keys for use with a symmetric encryption algorithm such as AES [54], a substantially larger volume of data could be encrypted, as symmetric schemes permit multiple records to be secured with the same key. For example, the aforementioned 85 927 secret bits could be partitioned into 335 individual 256-bit AES keys each day, excluding any additional keys required for authentication and initialization vectors.

Using AES for encryption would enable the provision of key material to applications with substantially larger data flows and allow for multiple daily symmetric key refreshes. Consequently, such a link cannot feasibly support large-scale consumer services; rather, it is suitable for encrypting highly selective information transmitted infrequently. This limitation confines the use case to one or a few high-security links. The relevance of maintaining a satellite-QKD link for such communications is discussed in greater detail in section 4.

4. Discussion

This study has assessed the feasibility of satellite-based QKD in Finnish Lapland. The findings indicate that, although satellite-based QKD is known to face inherent limitations, in polar regions the inter-seasonal environmental variability affects communication efficiency more significantly than in other parts of the world, resulting in service interruptions caused by ambient light. This raises a critical question regarding the practicality of any system that remains inoperative for a substantial portion of the year. While aggressive background-light filtering could enable key generation during summer, the fundamental challenge lies in the unpredictability introduced by cloud cover. Consequently, the availability of key material cannot be guaranteed on any given day. Although the BB84 protocol does not require simultaneous connectivity to both ground stations, the operational sequence for inter-station key establishment remains complex. For instance, in the case analysed in section 3.5, once the key material is depleted, the satellite must first reconnect with Rovaniemi, then Utsjoki, and subsequently revisit one of the stations to deliver the combined key. This final step could be optimized by transmitting the key to whichever station is currently visible; however, such an approach cannot be relied upon when large volumes of key material are required promptly. Therefore, the constellation would need to depend on storing excess key material during favourable key-establishment periods and consuming that stock at a sufficiently moderate rate to ensure continuity. When key material needs to be retained to account for service interruptions during brighter periods, the secure storage of this material becomes a critical concern. In this context, the nature of key management in satellite-based QKD differs substantially from

approaches leveraging PQC, where key material can be generated on demand, provided that a standard network connection is available.

As a consequence of the reduced key generation potential during summer, potential use cases are restricted to communication scenarios where: (1) long-term confidentiality is critical and computational security is insufficient, thereby necessitating QKD; (2) the data volume is sufficiently modest for the available key material to suffice; and (3) reliable backup solutions exist, such as reverting to a pre-shared key reserve in the event of service interruptions. Regarding confidentiality, stringent security parameters can be achieved, even though reducing the security parameter from 10^{-10} to a more stringent 2^{-128} suppresses the secret key generation rate. However, the key rates associated with the looser security parameter likely already impose strict limitations on application domains, meaning that this reduction in daily secret key bits would probably have only a minor impact on the intended use of the key material.

4.1. Background illumination modelling

Extended outage periods motivate the use of advanced background-light filtering for satellite QKD in Arctic conditions. For instance, [21] explores the use of polarization filtering in free-space QKD. The underlying principle is that during dusk and dawn, solar background light exhibits strong polarization, enabling its suppression through polarization filters. In that study, at a wavelength of 780 nm, polarization filtering during dawn allowed recovery of nearly 75% of the key length achievable under completely dark conditions. In Finnish Lapland, dusk and dawn constitute a substantial fraction of daylight hours; during winter, these periods can extend for several hours. From this perspective, the polarization filtering technique proposed in [21] appears promising, as it could enable key generation during virtually all winter satellite passes, excluding those obstructed by cloud cover or other weather phenomena. For example, in 2025, polar night at Utsjoki began on 25 November and ended on 17 January 2026. During this time, the Sun does not rise above the horizon, potentially allowing 52 consecutive days without background light interference, provided twilight periods can also be utilized. This possibility remains an avenue for future investigation.

Daylight operation has likewise been explored. A short-range prototype achieved 33 kbps over a 14 m free-space link [22], though its reliance on $\geqslant 10^8$ bit blocks and limited atmospheric path length reduce direct applicability to satellite links. More comparable terrestrial free-space results over 20 km reported an average secure key rate of 495 ps using 100 kbit blocks [55]; while the security parameter there 10^{-7} differs from ours, both studies demonstrate that daytime background can be mitigated with tailored optics and processing. Beyond discrete-variable methods, continuous-variable (CV) protocols can be inherently more tolerant to background light but face pronounced loss sensitivity, requiring specialized techniques for satellite scenarios [56–58].

A useful direction for future work is to quantify snow-albedo-induced backscatter into the line of sight and design corresponding filters, an effect not treated in this work. It would also be valuable to assess feasibility under auroral activity, which we leave for future study. Furthermore, employing more sophisticated atmospheric-radiance modelling tools, such as those referenced in [42], would enable a more precise characterization of background illumination. Integrating such models into our simulation framework, alongside the advanced filtering strategies discussed above, would yield a clearer assessment of the ultimate performance envelope for satellite-based QKD in polar regions.

4.2. Cloud cover model

While the cloud-cover model adopted in this work provides a reasonable first-order estimate, it has several limitations. The cloudiness data are approximate and specific to 2024, so inter-annual variability is not fully captured; nevertheless, they suffice to indicate the likely magnitude of cloud effects. It is essential to note that the expectation value obtained by multiplying the clear-sky key rate by the LOS probability does not represent the actual key length achievable on any given day; rather, it reflects a long-term daily average. In practice, observed key rates are likely to exhibit a bimodal distribution: near zero during cloudy periods and substantially higher during clear conditions, when key exchange can proceed without obstruction by cloud cover.

More importantly, the cloud treatment is binomial: clouds are assumed either to block the link entirely or to allow LOS. This follows from the FMI dataset, which lacks cloud-thickness information. By contrast, studies that incorporate cloud optical depth and layering can distinguish partial attenuation from full blockage and thus yield more accurate key-rate estimates [16]; adopting a similar approach here would likely improve fidelity.

The same reasoning applies to other weather phenomena that affect transmittance, such as snowfall. Although the probability of snowfall is incorporated into the expected transmittance value, real-world

behaviour is more discontinuous. Occasional snowfall would typically divide the key-generation windows into two categories: favourable intervals with no snowfall, during which the link is usable, and intervals with snowfall, during which key generation is effectively impossible. This also relates to the fact that, in our model, the weather categories are mutually exclusive by construction. In reality, multiple phenomena—for example, fog and precipitation—may occur simultaneously. The model therefore represents a simplification. From the standpoint of the overall analysis, however, the most critical factor is the fraction of time with clear, unobstructed conditions, as virtually any adverse weather phenomenon substantially degrades the link capacity. Consequently, in practice, only a small portion of secret key generation would be achievable during periods when any of the listed weather conditions are present.

Finally, the okta-based cloudiness representation introduces artefacts in joint weather–LOS probabilities. To quantify precipitation and fog occurring under LOS conditions, we formed conditional probabilities based on cloud-cover levels (0–8) associated with these phenomena. This produced surprising values; for example, a LOS-coincident snowfall probability of 0.23, seemingly at odds with the fact that snowfall implies cloud. The most plausible explanation is methodological: a large fraction of 'light snowfall' cases are labelled 7/8 okta, which, under the interpretation adopted in this study, corresponds to 12.5% clear-sky probability. When such per-phenomenon clear-sky probabilities are weighted by the overall frequency of the phenomenon, numerous 7/8 cases accumulate substantial 'LOS mass,' even if true unobstructed LOS during snowfall is rare. This behaviour aligns with a known weakness of okta classification: overrepresentation of 1/8 and 7/8 categories. 1/8 may be assigned upon observing a small cloud, and 7/8 may be assigned despite only a small break in the cloud layer [59]. Consequently, the nominal 12.5% clear-sky probability during light snowfall (and the derived LOS-coincident snowfall likelihood) is likely biased upward.

5. Conclusions

This study examined satellite-based QKD to three optical ground stations located in Finnish Lapland. Free-space links were simulated using MATLAB, and achievable secret key lengths, including finite-size effects, were calculated for each day of the year. The simulated satellites included the Suomi100 satellite and a modified version of Suomi100, in which the most favourable overpasses were scheduled to take place primarily during the darker periods of the day. Cloudiness and weather effects were incorporated using local meteorological data collected in 2024. The novelty of this work lies in simulating satellite-based QKD in polar regions, which are rarely addressed in the literature, and integrating local weather data into the simulation. The results indicate that satellite-based QKD in Finnish Lapland is feasible with polar-orbit satellites, although certain limitations persist. From a QKD perspective, the phenomenon of the midnight Sun poses a significant challenge, creating an extended period during which key generation is virtually impossible without advanced filtering techniques. This leads to prolonged key outages and necessitates special arrangements for key management. Conversely, the polar night provides an exceptionally favourable environment for QKD: the absence of ambient light enables near-continuous key generation, provided other atmospheric conditions are suitable. Adjusting the satellite's orbital schedule can increase the amount of obtainable key material; however, this improvement remains strongly dependent on seasonal variations. From the viewpoint of Finnish Lapland, ambient cloud coverage appears to be the most significant obstacle to large-scale deployment of satellite-based QKD. Future research should incorporate more detailed atmospheric models, advanced filtering techniques, and the potential effects of auroral activity to achieve a more precise assessment of the viability of satellite-based QKD on latitudes above the Arctic Circle.

Acknowledgments

This research was funded by European Commission, Grant Number 101091479. All text has been written by the authors, but the Copilot AI tool has been used for language polishing.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Supplementary data 1 available at https://doi.org/10.1088/2399-6528/ae57f7/data1.

Author contributions

Sara Nikula 0000-0002-2299-8030
Formal analysis (lead), Investigation (lead), Methodology (lead), Software (equal), Visualization (lead), Writing – original draft (lead), Writing – review & editing (lead)

Kokkatil Gopalkrishnan 0009-0004-3942-975X
Methodology (supporting), Software (equal), Writing – original draft (supporting)

References

[1] Shor P 1994 Algorithms for quantum computation: discrete logarithms and factoring *Proc. 35th Annual Symp. on Foundations of Computer Science* pp 124–34
[2] NIST 2025 *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process* (available at: https://csrc.nist.gov/pubs/ir/8545/final)
[3] European Commission 2025 EU reinforces its cybersecurity with post-quantum cryptography (available at: https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography)
[4] Bennett C and Brassard G 2014 Quantum cryptography: public key distribution and coin tossing *Theor. Comput. Sci.* **560** 7–11
[5] Guarda G, Ribezzo D, Occhipinti T, Zavatta A and Bacco D 2024 Long-distance quantum key distribution supported by a PIC-based interferometer *2024 Optical Fiber Communications Conf. and Exhibition (OFC)* pp 1–3
[6] Sax R *et al* 2023 High-speed integrated QKD system *Photon. Res.* **11** 1007–14
[7] Pathak N K, Chaudhary S, Sangeeta and Kanseri B 2023 Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization *Sci. Rep.* **13** 15868
[8] Wang S *et al* 2022 Twin-field quantum key distribution over 830-km fibre *Nat. Photon.* **16** 154–61
[9] Lu C-Y, Cao Y, Peng C-Z and Pan J-W 2022 Micius quantum experiments in space *Rev. Mod. Phys.* **94** 035001
[10] ESA 2022 *ESA—Eagle-1 Infographic* (available at: www.esa.int/ESA_Multimedia/Images/2022/10/Eagle-1_infographic) (Accessed 2 March 2026)
[11] Orsucci D, Kleinpass P, Meister J, Marco I D, Häusler S, Strang T, Walenta N and Moll F 2024 Assessment of practical satellite quantum key distribution architectures for current and near-future missions *Int. J. Satell. Commun. Netw.* **43** 164–92
[12] De Grossi F, Alberico S and Circi C 2024 Orbit design of satellite quantum key distribution constellations in different ground stations networks *Adv. Space Res.* **73** 5446–63
[13] Giannoulis G, Stathis A, Ntanos A, Lyras N K, Papastamatiou I, Kourelias P, Prnjat O, Koumantaros K, Panagopoulos A D and Avramopoulos H 2024 Satellite-to-ground QKD feasibility analysis for high altitude rural areas: a case study in Greece *2024 Int. Workshop on Fiber Optics in Access Networks (FOAN)* pp 38–42
[14] Kumar A G A, Malhotra Y and Parikh J 2025 Design and simulation of a decoy-state BB84 satellite QKD constellation for indian ground stations *Int. J. Inf. Technol.* (https://doi.org/10.1007/s41870-025-02860-y)
[15] Bourgoin J-P, Meyer-Scott E, Higgins B L, Helou B, Erven C, Hübel H, Kumar B, Hudson D, D'Souza I and Girard R 2013 A comprehensive design and performance analysis of low earth orbit satellite quantum communication *New J. Phys.* **15** 023006
[16] Wang X, Li T, Dong C, Wei J, Yu H, Zhao S and Shi L 2023 Exploiting potentialities for space-based quantum communication network: downlink quantum key distribution modelling and scheduling analysis *New J. Phys.* **25** 055001
[17] Attema T, Bosman J W and Neumann N M P 2021 Optimizing the decoy-state BB84 QKD protocol parameters *Quantum Inf. Process.* **20** 154
[18] Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution *Phys. Rev. A* **72** 012326
[19] Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503
[20] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504
[21] Simmons C, Barrow P and Donaldson R 2024 Dawn and dusk satellite quantum key distribution using time- and phase-based encoding and polarization filtering *Opt. Quantum* **2** 381–9
[22] Avesani M *et al* 2021 Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics *npj Quantum Inf.* **7** 93
[23] Cheng J, Chen Y, Liu A, Sun X, Guo J, Yang B, Yin P, Liu W, Chen L and Dong C 2025 Feasibility and parameter optimization of ground-to-satellite uplink continuous-variable quantum key distribution *New J. Phys.* **27** 023011
[24] Rhodes B 2019 Skyfield: high precision research-grade positions for planets and Earth satellites generator *ASCL* ascl:1907.024 (available at: https://ui.adsabs.harvard.edu/abs/2019ascl.soft07024R%2F/abstract)
[25] Ilmatieteen Laitos n.d. *Open Data Sets—Finnish Meteorological Institute* (available at: https://en.ilmatieteenlaitos.fi/open-data-sets-available) (Accessed 2 March 2026)
[26] OpenStreetMapcontributors 2026 *OpenStreetMap* (available at: www.openstreetmap.org/)
[27] Thales Alenia Space 2025 Thales Alenia Space and Hispasat start the development of the world's first quantum key distribution system capacity from geostationary orbit (available at: www.thalesaleniaspace.com/en/press-releases/thales-alenia-space-and-hispasat-start-development-worlds-first-quantum-key) (Accessed 2 March 2026)
[28] Behera S R and Sinha U 2024 Estimating the link budget of satellite-based quantum key distribution (QKD) for uplink transmission through the atmosphere *EPJ Quantum Technol.* **11** 66
[29] ESA 2020 *ESA—Types of Orbits* (available at: www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits) (Accessed 2 March 2026)
[30] Suomi 100 satellite project n.d. *CelesTrak: NORAD Two-Line Element Set Format* (available at: https://celestrak.org/NORAD/documentation/tle-fmt.php) (Accessed 2 March 2026)
[31] Suomi 100 Satellite Project n.d. *Suomi 100—satelliitti* (available at: www.suomi100satelliitti.fi/) (Accessed 2 March 2026)
[32] U.S. Space Force / U.S. Department of Defense n.d. *Space-Track.org* (available at: www.space-track.org/#/gp) (Accessed 2 March 2026)
[33] Abasifard M, Cholsuk C, Pousa R G, Kumar A, Zand A, Riel T, Oi D K L and Vogl T 2024 The ideal wavelength for daylight free-space quantum key distribution *APL Quantum* **1** 016113

[34] Eso E, Simmons C, Buller G S and Donaldson R 2024 Impact of visibility limiting conditions on satellite and high-altitude platform quantum key distribution links *Opt. Express* **32** 26776–92
[35] Tepper J, Hellerhoff N and Comin A 2024 Free space daylight ground-ground QKD in the near-IR *ECOC 2024; 50th European Conf. on Optical Communication* pp 1424–6
[36] Klein B J and Degnan J J 1974 Optical antenna gain. 1: transmitting antennas *Appl. Opt.* **13** 2134–41
[37] Giggenbach D and Shrestha A 2021 Atmospheric absorption and scattering impact on optical satellite-ground links *Int. J. Satell. Commun. Netw.* **40** 157–76
[38] Amairi-Pyka S, Fischer C, Kravtsov K, Santis G D, Grosso A, Fischer E, Kudielka K and Grieve J A 2024 Versatile optical ground station for satellite-based quantum key distribution in Abu Dhabi (arXiv:2412.03872 [quant-ph])
[39] Muskan R M and Banerjee S 2023 Performance analysis of satellite-based QKD protocols using the circular beam model (available at: https://api.semanticscholar.org/CorpusID:260378647)
[40] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Tight finite-key analysis for quantum cryptography *Nat. Commun.* **3** 634
[41] Finnish Meteorological Institute n.d. *Observation Stations* (available at: https://en.ilmatieteenlaitos.fi/observation-stations) (Accessed 2 March 2026)
[42] Hearne S, Horgan J, Boujnah N and Kilbane D 2025 Wavelength selection for satellite quantum key distribution *Appl. Sci.* **15** 1308
[43] World Meteorological Organization 2017 *Nimbostratus* (available at: https://cloudatlas.wmo.int/en/observation-of-clouds-from-aircraft-descriptions-nimbostratus.html) (Accessed 2 March 2026)
[44] Carbonneau T H and Wisely D R 1998 Opportunities and challenges for optical wireless; the competitive advantage of free space telecommunications links in today's crowded marketplace *Proc. SPIE* **3232** 119–28
[45] Muhammad S, Kohldorfer P and Leitgeb E 2005 Channel modeling for terrestrial free space optical links *Proc. 2005 7th Int. Conf. Transparent Optical Networks* vol 1 pp 407–10
[46] Ghoname S, Fayed H A, El Aziz A A and Aly M H 2020 Performance evaluation of an adaptive hybrid FSO/RF communication system: impact of weather attenuation *Iran. J. Sci. Technol. Trans. Electr. Eng.* **44** 119–28
[47] Sharma A and Kaur S 2025 Performance investigation of quantum key distribution system through free-space optics *Optik* **339** 172535
[48] Naboulsi M, Sizun H and Fornel F 2005 Propagation of optical and infrared waves in the atmosphere *Proc. 28th URSI General Assembly* (available at: https://api.semanticscholar.org/CorpusID:6277869)
[49] Kim I I, McArthur B and Korevaar E 2001 Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications *Proc. SPIE* **4214** 26–37
[50] World Meteorological Organization 2017 *Fog Compared with Mist* (available at: https://cloudatlas.wmo.int/en/fog-compared-with-mist.html) (Accessed 2 March 2026)
[51] Kartalopoulos S V 2011 *Free Space Optical Networks for Ultra-Broad Band Services* (Wiley) (https://doi.org/10.1002/9781118104231)
[52] National Institute of Standards and Technology 2024 Module-lattice-based key-encapsulation mechanism standard *Technical Report Federal Information Processing Standards Publication (FIPS PUBS)* 203 (U.S. Department of Commerce) (https://doi.org/10.6028/NIST.FIPS.203)
[53] Shannon C E 1949 Communication theory of secrecy systems *Bell Syst. Tech. J.* **28** 656–715
[54] NIST 2001 *FIPS 197, Advanced Encryption Standard (AES)* (available at: https://csrc.nist.gov/pubs/fips/197/final)
[55] Cai W-Q *et al* 2024 Free-space quantum key distribution during daylight and at night *Optica* **11** 647–52
[56] Zheng X-T, Zhang Q-F, Ling J, Guo G-C and Han Z-F 2025 Free-space continuous-variable quantum key distribution under high background noise *npj Quantum Inf.* **11** 52
[57] Dequal D, Vidarte L T, Rodriguez V R, Vallone G, Villoresi P, Leverrier A and Diamanti E 2021 Feasibility of satellite-to-ground continuous-variable quantum key distribution *npj Quantum Inf.* **7** 3
[58] Chen D, Jin C, Ao L, Lanjian C, YuJie C, Peng Y and TianYi W 2025 Machine learning for optimal parameter prediction in free space continuous-variable quantum key distribution *New J. Phys.* **27** 043021
[59] Karlsson K-G, Johansson E and Devasthale A 2015 Advancing the uncertainty characterisation of cloud masking in passive satellite imagery: probabilistic formulations for NOAA AVHRR data *Remote Sens. Environ.* **158** 126–39