Year 4 Research Project

Experimental Characterisation of a Terrestrial Free-Space

Optical Link for Quantum Key Distribution

Heriot-Watt University

Submission date:

Todd Blacklaw, Student ID: H00368671

Supervisor: Alessandro Fedrizzi

Abstract

Free-space optical (FSO) communication offers fibre-like data rates without physical infrastructure, making it a compelling platform for both urban backhaul and, increasingly, quantum key distribution (QKD). This project constructs and characterises a low-cost terrestrial FSO terminal based on the open-source IRNAS KORUZA design, replacing the original custom printed circuit board with off-the-shelf components centred on a Raspberry Pi controller. The optical link operates at $1550\,\mathrm{nm}$ via a standard small-form-factor pluggable transceiver and is directed using a three-axis unipolar stepper-motor pointing, acquisition, and tracking system. The atmospheric channel is modelled using the libRadtran radiative-transfer suite, which yields extinction coefficients for three Scottish weather scenarios (clear summer, $k_{\mathrm{ext}} = 0.036\,\mathrm{km}^{-1}$; clear winter, $k_{\mathrm{ext}} = 0.040\,\mathrm{km}^{-1}$; mist, $k_{\mathrm{ext}} = 0.237\,\mathrm{km}^{-1}$) via Monte Carlo photon transport. These transmittance values are propagated through three complementary Qiskit quantum-circuit simulations: a BB84 channel-feasibility study, an intercept-resend eavesdropper-detection model, and a log-normal scintillation fading analysis. At a $500\,\mathrm{m}$ deployment distance, all weather scenarios yield quantum bit error rates well below the $11\,\%$ Shor–Preskill security threshold (1.3–1.4%), with secure key rates of 5.3–5.9 kbps. An intercept-resend attack raises the QBER to $\sim 40\,\%$, demonstrating unambiguous eavesdropper detectability. Scintillation fading analysis shows that even under strong turbulence (scintillation index $= 1.5$), the fraction of time the link enters the insecure region is below $0.4\,\%$, confirming that a KORUZA-based FSO terminal is a viable platform for short-range metropolitan QKD with straightforward hardware additions.

Contents

1 Introduction

The demand for high-bandwidth, secure, and rapidly deployable communication links has grown substantially in recent years. Conventional radio-frequency (RF) systems are constrained by spectrum congestion and licensing costs, while fibre optic deployment is prohibitively expensive or impractical in last-mile urban scenarios and areas of difficult terrain [1, 2]. Free-space optical (FSO) communication has emerged as a compelling alternative: it offers data rates comparable to fibre (Gbps to Tbps), operates on an unlicensed spectrum, consumes relatively low power, and provides an inherent degree of physical security through its narrow, line-of-sight beam geometry [3].

Despite these advantages, the reliability of terrestrial FSO links is limited primarily by the atmosphere. Random fluctuations in the refractive index of air—caused by solar heating, wind shear, and resulting thermal inhomogeneities—distort and attenuate the propagating optical wavefront in a process broadly termed atmospheric turbulence [4]. The principal manifestations of turbulence are scintillation (rapid irradiance fluctuations at the receiver), beam wander (random displacement of the beam centroid), and wavefront distortion, all of which degrade link performance and increase the bit error rate (BER) [1].

A second, growing motivation for robust FSO links is their role as the physical layer for quantum key distribution (QKD). QKD protocols such as BB84 offer provably secure key exchange based on the laws of quantum mechanics [8]. While fibre-based QKD is mature, its practicality is curtailed by exponential photon loss with distance. Satellite-based QKD, demonstrated dramatically by the Micius satellite at distances up to 1200 km using decoy-state BB84 [24, 26], and metropolitan FSO QKD [12, 27] present natural solutions, but the same atmospheric effects that degrade classical links represent a critical barrier for quantum communication. Signal loss from beam wander reduces the rate of single-photon delivery, while wavefront distortion can increase the quantum bit error rate (QBER) by mixing polarisation or phase states, reducing the margin within which an eavesdropper can be detected [13].

This project addresses both challenges simultaneously. A low-cost, open-source FSO terminal is constructed and characterised, based on the IRNAS KORUZA platform [14], with the dual aim of (1) quantifying the impact of Scottish atmospheric conditions on FSO link performance, and (2) determining the feasibility and limitations of the resulting channel for BB84 QKD. The

atmospheric channel is modelled using the libRadtran Monte Carlo radiative-transfer code [7], and the quantum channel behaviour is simulated using Qiskit quantum circuits incorporating physically motivated noise models.

The remainder of this report is structured as follows. Section 2 reviews the relevant background theory spanning atmospheric turbulence physics, FSO channel modelling, and QKD principles. Section 3 describes the hardware construction and the computational methods applied. Section 4 presents the atmospheric and quantum simulation results. Section 5 interprets these findings in the context of the literature and the project objectives. Section 7 states the conclusions and directions for further work.

2 Background Theory

2.1 Atmospheric Turbulence and FSO Propagation

The theoretical framework for electromagnetic wave propagation through random media was established by Fante [4] and extended by Tatarskii [5]. Atmospheric turbulence originates in thermal inhomogeneities driven principally by solar heating of the Earth's surface and subsequent wind mixing, which produce random fluctuations in air temperature and pressure. These fluctuations modulate the atmospheric refractive index $n(\mathbf{r}, t)$, which can be decomposed as:

$$n(\mathbf{r}, t) = \langle n \rangle + n_1(\mathbf{r}, t), \tag{1}$$

where $\langle n \rangle \approx 1$ is the mean and n_1 is a zero-mean random perturbation. Following the Kolmogorov cascade model, turbulent energy is injected at a large outer scale L_0 (metres to hundreds of metres) and dissipates as heat at an inner scale l_0 (typically millimetres). Within this inertial subrange, the structure function of the refractive index fluctuations obeys:

$$D_n(r) = \langle [n(\mathbf{r}_1) - n(\mathbf{r}_2)]^2 \rangle = C_n^2 \, r^{2/3}, \tag{2}$$

where $r = |\mathbf{r}_1 - \mathbf{r}_2|$ and C_n^2 is the *refractive-index structure parameter* (units: $\mathrm{m}^{-2/3}$), the primary scalar measure of turbulence strength [1]. Typical values for a horizontal terrestrial path range from $C_n^2 \sim 10^{-16} \ \mathrm{m}^{-2/3}$ (weak turbulence) to $C_n^2 \sim 10^{-13} \ \mathrm{m}^{-2/3}$ (strong turbulence) [23].

As an optical beam propagates through this medium, the refractive inhomogeneities cause three

principal effects. *Scintillation* (intensity fading) arises from small-scale eddies comparable to or smaller than the beam diameter, which scatter and diffract light, producing a random irradiance pattern at the receiver. *Beam wander* is caused by large-scale eddies that act as refractive wedges, displacing the entire beam centroid from its intended path [15]. *Wavefront distortion* describes higher-order phase aberrations that degrade coherence. All three phenomena increase the BER and, for quantum links, the QBER [2].

2.2 Statistical Channel Models

For the log-normal turbulence regime (weak to moderate, propagation distances $\lesssim$ 1 km at near-infrared wavelengths), the instantaneous received irradiance I is modelled as a log-normal random variable:

$$I = I_0 \exp(2\chi), \tag{3}$$

where χ is a Gaussian random variable with mean $\mu_\chi = -\sigma_\chi^2$ (so that $\langle I \rangle = I_0$) and variance σ_χ^2. The *scintillation index* (SI), which quantifies the normalised variance of irradiance, is related to the log-normal parameters by:

$$\mathrm{SI} = \frac{\langle I^2 \rangle - \langle I \rangle^2}{\langle I \rangle^2} = \exp(4\sigma_\chi^2) - 1. \tag{4}$$

In the present work, SI values of 0.1, 0.5, and 1.5 are used to represent weak, moderate, and strong turbulence conditions, respectively [6].

For stronger turbulence, the Gamma-Gamma distribution, introduced by Al-Habash, Andrews and Phillips [21] as a doubly-stochastic model valid from weak to strong irradiance fluctuations, provides a better fit to simulation data, and has been applied to composite channel models incorporating dust and fog effects [30]. At the 500 m deployment range relevant to this project, however, the log-normal model is well justified [1].

2.3 Static Atmospheric Attenuation and the Beer-Lambert Law

In addition to turbulence-induced fading, a horizontal FSO link experiences quasi-static attenuation from molecular absorption and particle scattering. For a homogeneous path of length d, the mean channel transmittance follows the Beer-Lambert law:

$$\eta_{\mathrm{atm}}(d) = \exp(-k_{\mathrm{ext}} d), \tag{5}$$

where k_{ext} (km^{-1}) is the wavelength-dependent *extinction coefficient*, which decomposes as:

$$k_{\text{ext}} = \sigma_{\text{Ray}} + \sigma_{\text{Mie}} + \kappa_{\text{gas}} + \kappa_{\text{aer}}, \qquad (6)$$

representing contributions from Rayleigh scattering by air molecules, Mie scattering by aerosols, molecular absorption, and aerosol absorption, respectively. At 1550 nm, Rayleigh scattering scales as λ^{-4} and is negligible ($< 1\%$ contribution); Mie scattering by aerosols ($r \approx \lambda$) is the dominant loss mechanism in clear air, contributing 60–70% of k_{ext}; molecular absorption is low because 1550 nm falls in a well-known atmospheric transmission window between H_2O and CO_2 absorption bands [3].

The extinction coefficient values used in this work are computed using the libRadtran radiative-transfer package [7], as described in Section 3.2.

2.4 BB84 Quantum Key Distribution

Quantum key distribution exploits quantum mechanical principles to guarantee provably secure key exchange. The BB84 protocol, proposed by Bennett and Brassard in 1984 [8], encodes classical bits in the quantum states of individual photons using two conjugate bases (e.g. rectilinear $\{|0\rangle, |1\rangle\}$ and diagonal $\{|+\rangle, |-\rangle\}$). Alice prepares single photons in randomly chosen states from randomly chosen bases; Bob measures in a randomly chosen basis. After transmission, they publicly compare bases (but not results) and retain only the sifted key where their bases agree.

The security of BB84 rests on the no-cloning theorem: an eavesdropper (Eve) cannot measure an unknown quantum state without disturbing it. An intercept-resend attack, in which Eve measures every qubit and resends her best guess, introduces a characteristic 25% QBER on a perfect channel, regardless of her strategy [8]. The *quantum bit error rate* is thus the primary security diagnostic. The asymptotic secure key rate under the Shor–Preskill bound is:

$$R_{\text{secure}} = R_{\text{sift}} \max[0,\ 1 - 2H(e)], \qquad (7)$$

where $R_{\text{sift}} = \frac{1}{2} f_{\text{rep}}\, \mu\, \eta_{\text{atm}}\, \eta_{\text{det}}$ is the sifted key rate, f_{rep} is the pulse repetition rate, μ is the mean photon number per pulse, η_{det} is the detector efficiency, and $H(e) = -e \log_2 e - (1-e) \log_2(1-e)$ is the binary Shannon entropy evaluated at QBER e. Secret-key generation requires $e < 11\%$ (the Shor–Preskill threshold) [9].

2.5 QBER Contributions in a Practical FSO-QKD Channel

The total QBER in a practical weak-coherent-pulse (WCP) FSO-QKD system is the sum of three contributions [10]:

$$e = e_{\text{misalign}} + e_{\text{dark}} + e_{\text{turb}}, \tag{8}$$

where e_{misalign} is residual optical misalignment error ($\sim 1\%$ for a well-aligned system), e_{dark} is the contribution from detector dark counts:

$$e_{\text{dark}} = \frac{d_{\text{rate}}/f_{\text{rep}}}{2\,\mu\,\eta_{\text{atm}}\,\eta_{\text{det}}}, \tag{9}$$

and e_{turb} captures the additional error introduced when scintillation-driven fading reduces the instantaneous transmittance below its mean value. In the log-normal fading model, e_{turb} is treated as a random variable whose distribution is computed via Monte Carlo sampling of η_{atm}, as described in Section 3.3.

3 Materials and Methods

3.1 Hardware: KORUZA FSO Terminal

The FSO terminal constructed in this work is based on the open-source IRNAS KORUZA design [14], a modular platform originally developed for urban last-mile wireless links. The original design uses a dedicated custom printed circuit board (PCB) to interface the Raspberry Pi controller with the stepper motor drivers. In this implementation, the custom PCB has been replaced entirely with commercially available off-the-shelf components, improving repairability and reducing procurement lead times.

The mechanical housing is produced by fused-deposition modelling (FDM) 3D printing in poly-lactic acid (PLA), following the original KORUZA mechanical drawings. The optical assembly is contained within this housing and aligned along a common optical axis with the SFP port.

3.1.1 Pointing, Acquisition and Tracking System

Precise beam alignment is critical for FSO links: angular mispointing introduces an additional loss factor that grows quadratically with the ratio of angular error to beam divergence. The pointing, acquisition, and tracking (PAT) system implemented here consists of three unipolar

stepper motors arranged to provide coarse azimuth, elevation, and roll adjustment. The motors are driven by a ULN2003 Darlington transistor array, which interfaces directly to the Raspberry Pi 2B general-purpose input/output (GPIO) pins without requiring a dedicated motor controller board. This design choice significantly reduces component count relative to the original KO-RUZA.

3.1.2 Optical Data Link

The data link is established at 1550 nm using a TP-Link MC220L media converter, which converts the Ethernet frame stream from the Raspberry Pi into an optical signal via a standard small-form-factor pluggable (SFP) transceiver module. The SFP module produces a collimated infrared beam suitable for free-space propagation at the KORUZA designed divergence angle. This wavelength is selected for three reasons: it falls in the principal atmospheric transmission window (Section 2), it is eye-safe at the power levels used, and it is compatible with telecom-standard components, keeping system cost low.

3.2 Atmospheric Channel Model

The atmospheric extinction coefficient k_{ext} at 1550 nm is computed using the libRadtran software package (version 2.0.6) [7], specifically the `uvspec` radiative-transfer solver operating in Monte Carlo (MYSTIC) mode with 10^5 photons per simulation run. The AFGL standard atmosphere profiles are used as the baseline gas concentration and temperature data, with aerosol properties set according to the scenario of interest.

Three scenarios representative of Scottish atmospheric conditions are simulated:

1. **Baseline (Clear Summer):** AFGL mid-latitude summer atmosphere (`afglms.dat`), rural aerosol model, visibility 23 km.

2. **Scottish (Clear Winter):** AFGL mid-latitude winter atmosphere (`afglmw.dat`), rural aerosol model, visibility 20 km.

3. **Scottish (Mist/Drizzle):** AFGL mid-latitude winter atmosphere, rural aerosol model, reduced visibility 4 km to simulate light mist.

The ground-level extinction coefficient is extracted from the verbose output of `uvspec` by parsing

the `optical_properties()` table. The total optical depth per unit length is computed as:

$$k_{\text{ext}} = \frac{\Delta\tau_{\text{Ray}} + \Delta\tau_{\text{Mie}} + \Delta\tau_{\text{mol}}}{\Delta z}, \tag{10}$$

where $\Delta\tau$ are the per-layer differential optical depths extracted from the simulation output and $\Delta z = 1\,\text{km}$ is the layer thickness. The transmittance at distance d is then computed analytically via equation (5).

3.3 QKD Channel Simulations

Three complementary quantum-channel simulations are implemented using Qiskit 2.3 and Qiskit Aer [19]. In all cases, channel photon loss is modelled as an *amplitude damping channel* with damping parameter:

$$\gamma = 1 - \eta_{\text{atm}}\,\eta_{\text{det}}, \tag{11}$$

which maps the excited state $|1\rangle$ to the ground state $|0\rangle$ with probability γ, physically corresponding to photon absorption or scattering. This is the correct quantum noise model for photon loss [11].

3.3.1 BB84 Feasibility Simulation

A single-qubit circuit prepares the state $|+\rangle = H|0\rangle$ (representing Alice's diagonal-basis photon), applies the amplitude damping channel, and rotates back to the Z basis for measurement. The QBER from the circuit (fraction of $|1\rangle$ outcomes) is compared against the theoretical prediction from equations (8) and (9). The secure key rate is then computed using equation (7) for each atmospheric scenario as a function of link distance (50 m to 5 km). System parameters are: $\mu = 0.1$, $\eta_{\text{det}} = 0.15$, $f_{\text{rep}} = 1\,\text{MHz}$, $d_{\text{rate}} = 100\,\text{s}^{-1}$, $e_{\text{misalign}} = 0.01$.

3.3.2 Eavesdropper Detection Simulation

An intercept-resend attack is modelled by replacing the direct channel with a two-stage circuit: Eve applies a random basis measurement (Z or X, each with probability 0.5) and resends the post-measurement state. When Eve's basis mismatches Alice's (50% of intercepts), the collapsed state is an eigenstate of the wrong basis, introducing additional errors at Bob's receiver. Two sub-circuits are run (Eve measuring in Z and X) and their results combined to yield the total QBER under the attack. The security margin is defined as the difference between the Eve-induced

QBER and the no-Eve channel QBER.

3.3.3 Scintillation Fading Analysis

For each (scenario, turbulence regime) pair, $N = 2000$ independent samples of the instantaneous transmittance are drawn from a log-normal distribution:

$$\eta_i = \eta_{\text{mean}} \cdot \exp(\mu_{\ln} + \sigma_{\ln} Z_i), \quad Z_i \sim \mathcal{N}(0, 1), \tag{12}$$

where $\sigma_{\ln}^2 = \ln(1 + \text{SI})$ and $\mu_{\ln} = -\sigma_{\ln}^2/2$ [6]. Samples are clipped to $[0, 1]$. For each sample η_i, the QBER and secure key rate are computed, yielding full probability distributions rather than single-point estimates. The fraction of time the QBER exceeds the 11 % security threshold constitutes the *insecure fraction*—the proportion of time during which no secret key can be extracted. A distance sweep from 50 m to 5 km is performed for the clear summer baseline using 500 Monte Carlo samples per distance point, for each of three turbulence regimes (SI = 0.1, 0.5, 1.5).

4 Results

4.1 Atmospheric Transmission Modelling

The libRadtran simulations yield the extinction coefficients summarised in Table 1.

Table 1: Extinction coefficients at 1550 nm for three Scottish atmospheric scenarios, derived from libRadtran MYSTIC Monte Carlo simulations. Transmittances are evaluated at 500 m and 1 km deployment distances.

Scenario	k_{ext} (km^{-1})	η @ 500 m	η @ 1 km	η @ 10 km	Dominant loss
Baseline (Clear Summer)	0.0360	0.982	0.964	0.698	Aerosol (Mie)
Scottish (Clear Winter)	0.0398	0.980	0.961	0.670	Aerosol (Mie)
Scottish (Mist/Drizzle)	0.2368	0.888	0.789	0.094	Strong Mie

Figure 1 shows the full transmittance curves for each scenario over 0–20 km. The clear summer and winter profiles are closely matched at short range, diverging only beyond ∼5 km. The mist scenario departs dramatically from the clear-air cases: at 10 km the mist transmittance is ∼9%, compared with ∼70% in clear air. This is consistent with the dominance of Mie scattering under

reduced visibility conditions; at $1550\,\mathrm{nm}$, water droplets with radii $r \sim \lambda$ are highly efficient scattering centres [3].
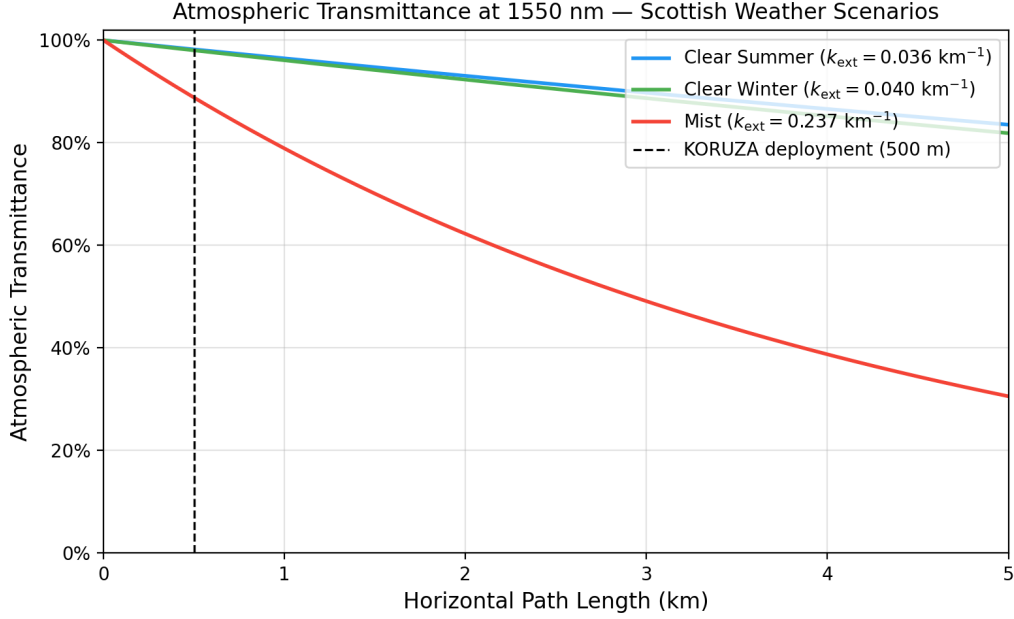

Figure 1: Atmospheric transmittance at $1550\,\mathrm{nm}$ as a function of horizontal path length for three Scottish weather scenarios. Curves are derived from libRadtran MYSTIC Monte Carlo simulations using equation (5). The vertical dashed line indicates the $500\,\mathrm{m}$ KORUZA deployment distance. Clear summer ($k_{\mathrm{ext}} = 0.036$ km^{-1}, blue) and clear winter ($k_{\mathrm{ext}} = 0.040$ km^{-1}, green) are closely matched; mist ($k_{\mathrm{ext}} = 0.237$ km^{-1}, red) shows severe attenuation beyond $\sim$2 km.

4.2 BB84 QKD Channel Feasibility

Figure 2 presents the key BB84 channel metrics for each atmospheric scenario across 50 m to 5 km. At the $500\,\mathrm{m}$ deployment distance, the QBER remains at 1.34–1.38% across all scenarios (Table 2), well below the 11 % Shor–Preskill threshold. Even in mist, the transmittance remains sufficiently high at short range that the dark-count contribution to QBER is negligible; the dominant QBER source is optical misalignment at $e_{\mathrm{misalign}} = 1\%$.
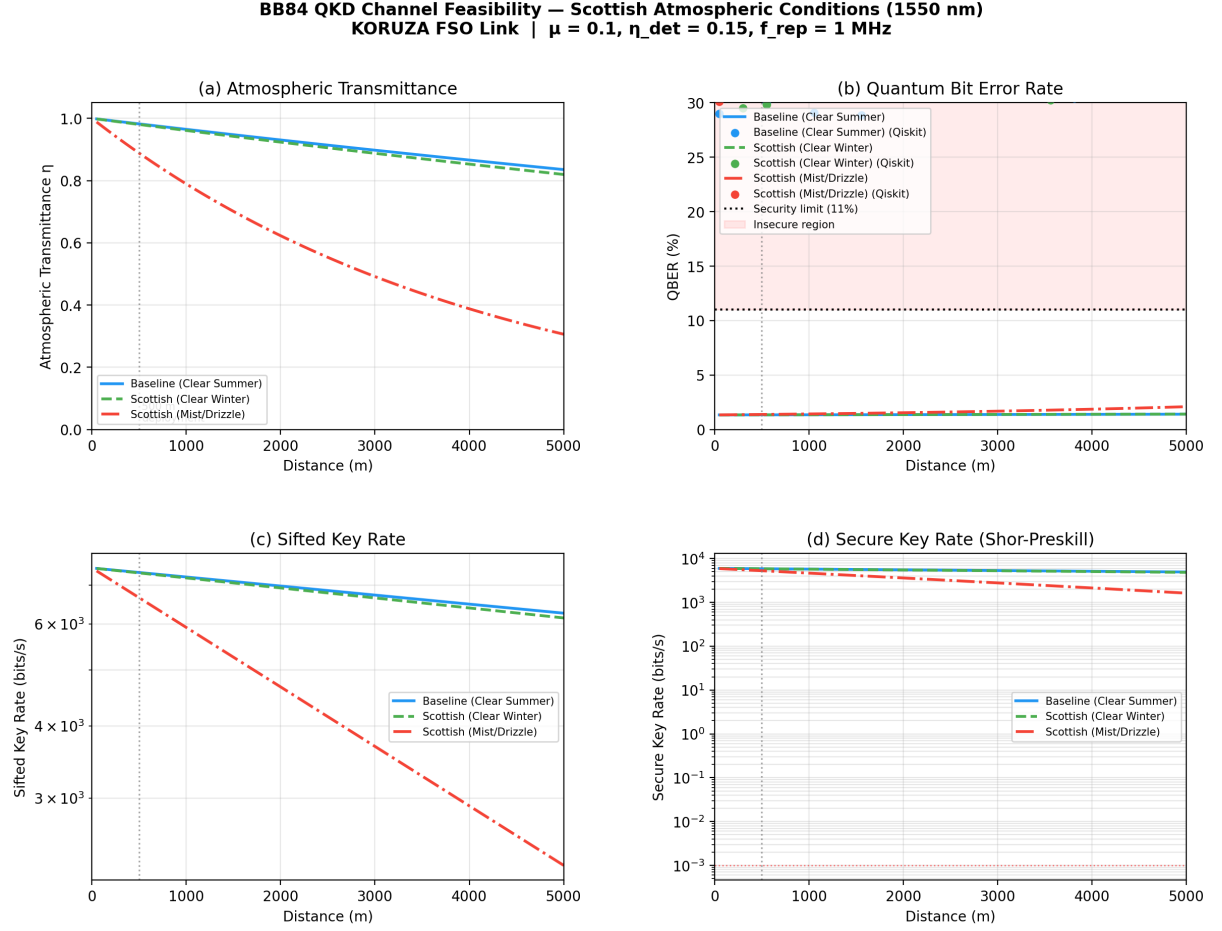
13

Figure 2: BB84 QKD channel performance versus link distance for three Scottish atmospheric scenarios. **(a)** Atmospheric transmittance η_{atm}. **(b)** Quantum bit error rate (QBER); solid lines are the analytical model (equation 8), circles are Qiskit amplitude-damping circuit simulations. The horizontal dotted line marks the 11 % Shor–Preskill security threshold. **(c)** Sifted key rate. **(d)** Secure key rate computed from equation (7). The vertical dashed line indicates the 500 m deployment distance.

Table 2: BB84 QKD performance metrics at the 500 m KORUZA deployment distance for each atmospheric scenario. System parameters: $\mu = 0.1$, $\eta_{\mathrm{det}} = 0.15$, $f_{\mathrm{rep}} = 1\,\mathrm{MHz}$, $d_{\mathrm{rate}} = 100\,\mathrm{s}^{-1}$.

Scenario	η_{atm}	QBER (%)	Sifted rate (bps)	Secure rate (bps)
Baseline (Clear Summer)	0.9822	1.34	7366	5856
Scottish (Clear Winter)	0.9803	1.34	7352	5844
Scottish (Mist/Drizzle)	0.8883	1.38	6663	5267

The critical transmittance threshold below which no secret key can be extracted (where $e = 11\%$) corresponds to $\eta_{\mathrm{atm}} \approx 0.033$, as shown in Figure 3. In clear air, this threshold is reached at $\sim 10\,\mathrm{km}$; in mist, at $\sim 1.5\,\mathrm{km}$. The 500 m KORUZA operating range is therefore comfortably
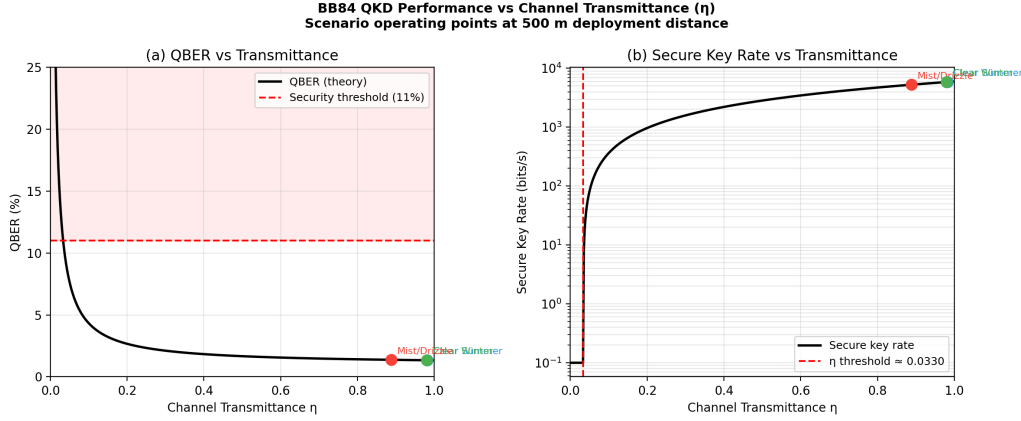
14

within the secure regime for all three scenarios.

Figure 3: BB84 QKD performance as a function of channel transmittance η. **(a)** QBER versus η; the red dashed line is the 11% Shor–Preskill security limit and the shaded region denotes the insecure regime. Coloured markers indicate the operating point of each Scottish scenario at $500\,\text{m}$. **(b)** Secure key rate versus η; the vertical dashed line indicates the critical transmittance threshold $\eta \approx 0.033$ below which key generation ceases.

4.3 Eavesdropper Detection

Figure 4 shows the effect of a full intercept-resend attack on the QBER and secure key rate. Across all atmospheric scenarios, Eve's attack raises the QBER from $\sim 1.4\%$ (no attack) to $\sim 40\%$ at $500\,\text{m}$. This represents a QBER elevation of ~ 38.6 percentage points, far exceeding the 11% security threshold and constituting unambiguous detection. The Qiskit circuit simulations confirm this behaviour, producing QBER values consistent with the theoretical expectation that an intercept-resend attack introduces a 25% QBER on the error-free sifted bits.

The security margin (the difference between Eve's QBER and the channel noise QBER) is largest at short range and high transmittance. As the link distance increases and atmospheric attenuation raises the baseline QBER, this margin gradually narrows. However, at the $500\,\text{m}$ deployment range, the margin of $\sim 38\%$ is such that even a partial attack (Eve intercepting a fraction of pulses) would be detectable provided she intercepts more than $\sim 3\%$ of transmitted qubits.
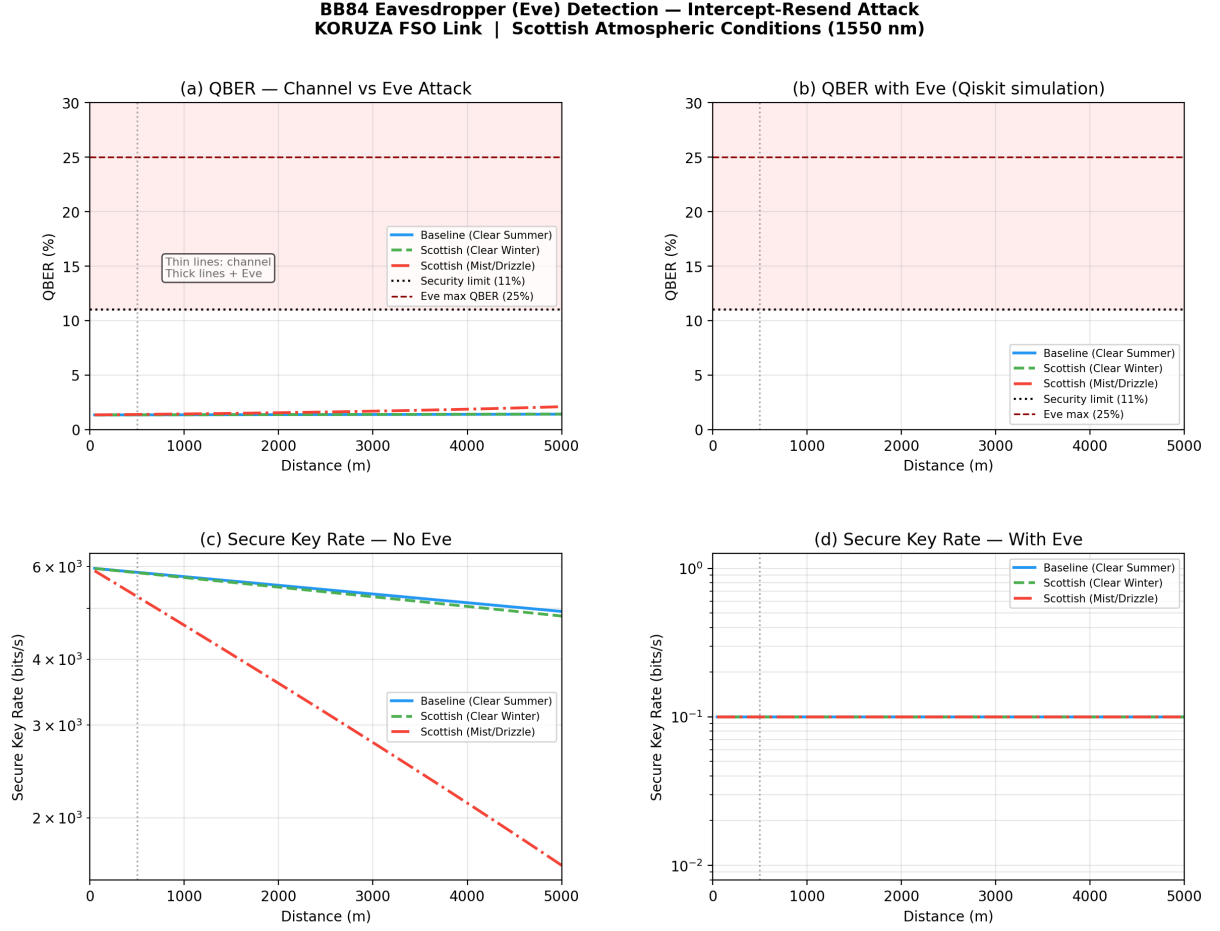
Figure 4: Effect of a full intercept-resend eavesdropper attack on BB84 QKD performance. **(a)** QBER with (bold) and without (faded) Eve; all scenario pairs lie well above the 11 % security limit under attack. **(b)** QBER with Eve from Qiskit circuit simulation. **(c), (d)** Secure key rate without and with Eve, respectively; the attack reduces the key rate to zero in all scenarios by driving QBER above threshold.

4.4 Scintillation Fading Analysis

Figure 5 shows the probability distributions of QBER under log-normal scintillation fading at the 500 m deployment distance. For the clear summer baseline, weak turbulence (SI = 0.1) produces a narrow QBER distribution tightly centred near 1.4%, with the 95 th percentile at 1.58% and an insecure fraction of 0.0 %. Moderate turbulence (SI = 0.5) broadens the distribution, raising the 95th percentile to 2.19%, still well within the secure regime. Strong turbulence (SI = 1.5) produces a substantially wider distribution; the 95th percentile QBER is 3.84% and the insecure fraction is 0.1%. These results are summarised in Table 3.
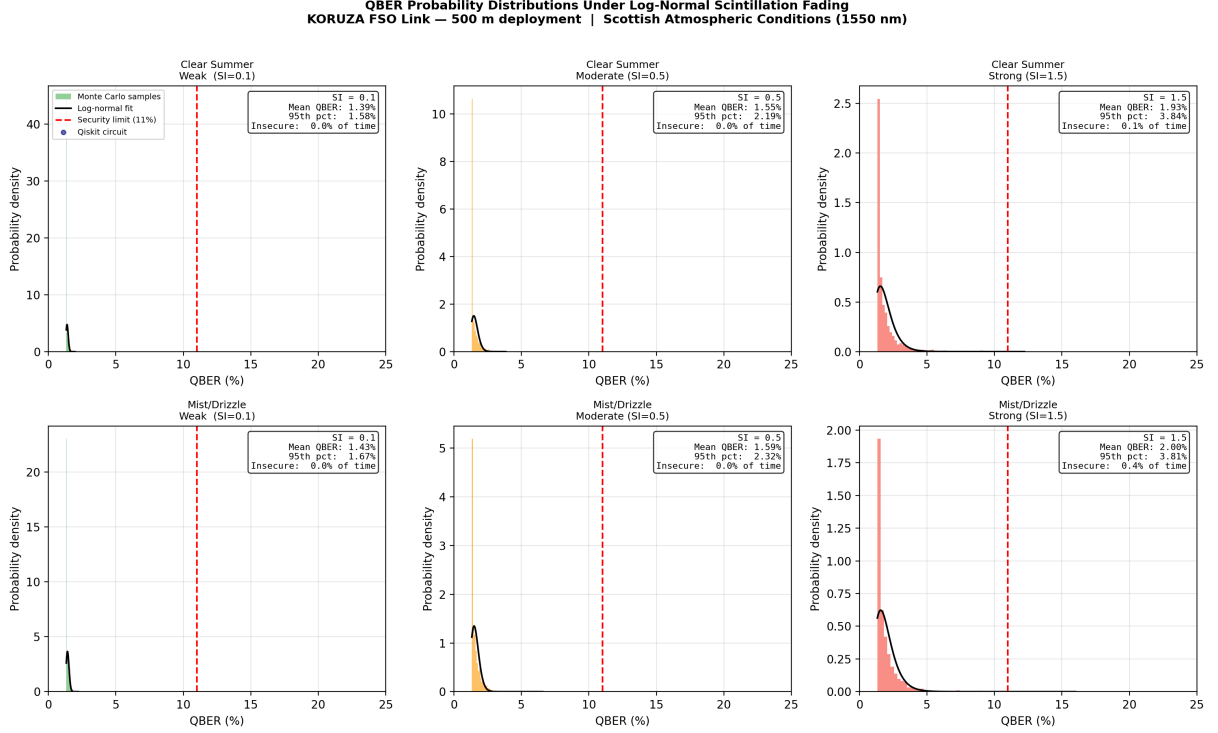
Figure 5: Probability distributions of QBER under log-normal scintillation fading at the 500 m deployment distance. Rows correspond to atmospheric scenarios (clear summer, mist); columns to turbulence regimes (weak SI=0.1, moderate SI=0.5, strong SI=1.5). Histograms represent $N = 2000$ Monte Carlo samples; solid curves are log-normal fits. The vertical red dashed line is the 11 % Shor–Preskill threshold. Navy circles on the baseline indicate QBER values from Qiskit amplitude-damping circuit simulations at representative transmittance levels.

Table 3: Scintillation fading statistics at 500 m deployment distance. Insecure fraction is the probability that instantaneous QBER exceeds 11 %. Log-normal fading model, $N = 2000$ Monte Carlo samples, seed fixed for reproducibility.

Scenario	Turbulence	SI	Mean QBER (%)	95th pct (%)	Insecure (%)
Clear Summer	Weak	0.1	1.40	1.58	0.00
	Moderate	0.5	1.55	2.19	0.00
	Strong	1.5	1.93	3.84	0.10
Mist/Drizzle	Weak	0.1	1.43	1.67	0.00
	Moderate	0.5	1.59	2.32	0.00
	Strong	1.5	2.00	3.81	0.40

Figure 6 shows how mean QBER, insecure fraction, and mean secure key rate evolve with distance for each turbulence regime. Up to ∼1 km, all three turbulence regimes keep the mean QBER well below the security threshold. Beyond ∼2 km, strong turbulence drives the 95th-percentile QBER

17

above threshold and the insecure fraction rises rapidly. At 5 km, strong turbulence produces a mean QBER approaching 4% and an insecure fraction exceeding 10%. The mean secure key rate remains positive under all conditions within the KORUZA deployment range.
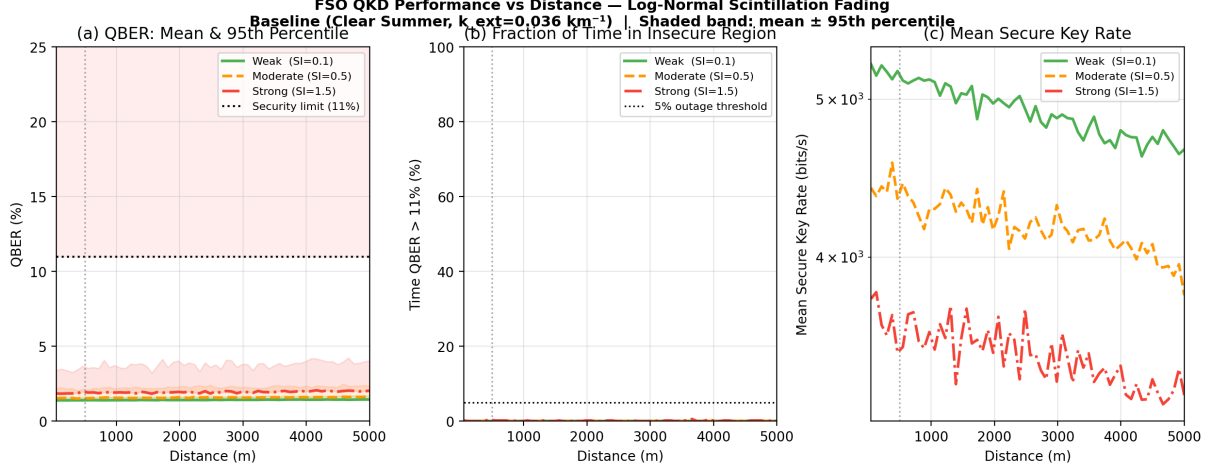

Figure 6: FSO QKD performance versus link distance under log-normal scintillation fading. Clear summer baseline ($k_{ext} = 0.036$ km^{-1}). **(a)** Mean QBER (solid lines) with shaded band extending to the 95th percentile; the dotted horizontal line marks the 11% security threshold. **(b)** Fraction of time QBER exceeds threshold (link insecure). **(c)** Mean secure key rate. The vertical dashed line in each panel marks the 500 m deployment distance.

5   Discussion

5.1   Atmospheric Channel at 1550 nm

The libRadtran results confirm that 1550 nm is well-suited to short-range terrestrial FSO in Scottish conditions. The clear winter scenario has a marginally higher extinction coefficient than clear summer (0.040 vs. 0.036 km^{-1}), consistent with the expectation that drier winter air slightly reduces water vapour absorption, but a reduced visibility (20 vs. 23 km) raises aerosol scattering sufficiently to offset this benefit. This finding is consistent with Grabner and Kvicera [17] who found that aerosol loading, rather than molecular absorption, governs 1550 nm attenuation on typical European horizontal paths.

The mist scenario is far more significant for link reliability: a 6× increase in k_{ext} relative to clear air results in transmittances below 10% beyond 10 km. Mie scattering is particularly effective at 1550 nm because typical fog and mist droplets have radii of 1–10 µm, comparable to the wavelength. This confirms that high-reliability FSO links in Scotland would require either shorter hop distances, relay-assisted multi-hop architectures [28], or backup RF links during adverse

weather events, consistent with the conclusions of [1] for European climates.

5.2 QKD Feasibility at 500 m

All three atmospheric scenarios are unambiguously within the secure QKD operating regime at the 500 m KORUZA deployment range. The dominant QBER contribution is optical misalignment ($e_{\mathrm{misalign}} = 1\%$); dark counts and atmospheric loss make negligible contributions at this range. This highlights the importance of the PAT system in a practical deployment: even a misalignment of a few milliradians would raise e_{misalign} substantially, consuming the available secure key margin. The KORUZA stepper-motor PAT system provides coarse alignment; fine-pointing feedback from received optical power monitoring would be required for a long-term deployment. Farid and Hranilovic [22] showed that optimising the transmitted beam width with respect to detector aperture and pointing-error variance can increase the achievable rate by up to 80% at a given outage probability under fog conditions, providing theoretical motivation for this fine-alignment requirement.

The secure key rates of 5.3–5.9 kbps at 500 m are competitive with the state-of-the-art metropolitan FSO QKD demonstrations. Kržič et al. [12] achieved 5.7 kbps at night over a 1.7 km entanglement-based link using significantly more sophisticated hardware. The KORUZA-based system operating at shorter range with a simpler prepare-and-measure scheme achieves comparable rates, illustrating the advantage of reduced path length.

5.3 Security Against Eavesdropping

The eavesdropper simulation confirms that an intercept-resend attack is highly detectable at 500 m: the QBER elevation of ∼38 percentage points far exceeds the 11% threshold. This strong detectability arises primarily from the low channel QBER baseline (1.3–1.4%). Eve cannot exploit atmospheric noise to conceal her attack because the noise level is simply too low at this range.

It is worth noting that this analysis assumes an ideal intercept-resend strategy. Coherent attacks—where Eve stores quantum states in a quantum memory and performs joint measurements—are theoretically more efficient but substantially harder to implement. For the short-range metropolitan scenario of this project, the intercept-resend bound is the operationally relevant threat model [18, 25].

5.4 Impact of Scintillation on QKD Security

The scintillation fading analysis reveals a physically important nuance absent from the fixed-transmittance model: even when the mean QBER is comfortably within the secure regime, turbulence-induced fading creates brief windows during which the instantaneous QBER temporarily exceeds the security threshold. At $500\,\mathrm{m}$ under strong turbulence (SI = 1.5), this occurs 0.1% of the time in clear air and 0.4% in mist. While small, these intervals are operationally meaningful: during them, any key generation attempt would produce insecure bits that must be discarded in post-processing. Adaptive protocols that pause key generation when a received-power monitor indicates deep fades can mitigate this at the cost of some key rate reduction.

The scintillation index values used here (0.1–1.5) span the range documented for horizontal terrestrial FSO paths of comparable length and wavelength [6]. However, actual SI values for the specific deployment site should be measured from the temporal statistics of the received optical power time series during experimental testing—a direct output of the KORUZA monitoring system once deployed.

5.5 Proposed Hardware Adaptations for QKD

The present KORUZA implementation establishes the classical FSO channel. To implement BB84 QKD, the following hardware modifications would be required. At the transmitter, the SFP-based coherent laser source would be replaced by an attenuated pulsed laser at $\mu \sim 0.1$ photons per pulse, with a polarisation encoder (half-wave plate and polarising beamsplitter) to prepare the four BB84 states. At the receiver, the SFP detector and media converter would be replaced by a polarisation analysis module (50:50 beamsplitter and two polarising beamsplitters feeding four single-photon avalanche diodes). The Raspberry Pi control and PAT hardware would remain unchanged, since pointing and alignment is the primary engineering challenge—as this work has characterised. This architecture is closely analogous to that deployed by the HWU quantum communications group [12, 16, 29].

6 Retroreflector Stability Characterisation

To be done

6.1 Experimental Setup

[Placeholder

The constructed KORUZA unit was tested against a corner-cube retroreflector placed at a distance of **[TODO: distance (m)]** to characterise the pointing stability and received power statistics of the PAT system under static conditions. The retroreflector was positioned at **[TODO: location description]**. Received optical power was logged via **[TODO: monitoring method]** over a duration of **[TODO: measurement duration]**.

6.2 Received Power Statistics

Table 4: Received power statistics from retroreflector stability test. All values to be filled from experimental data.

Metric	Value
Mean received power (dBm)	*[TBD]*
Standard deviation (dB)	*[TBD]*
Minimum received power (dBm)	*[TBD]*
Maximum received power (dBm)	*[TBD]*
Measurement duration	*[TBD]*
Sampling rate	*[TBD]*
Estimated scintillation index	*[TBD]*

6.3 Pointing Stability
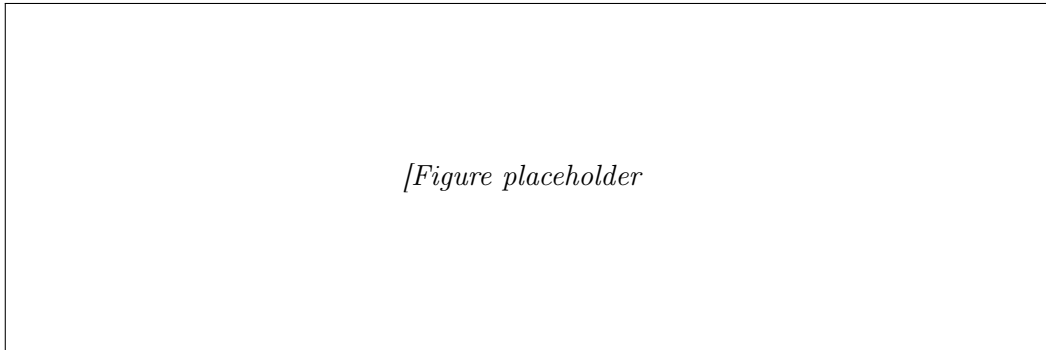
[Figure placeholder

Figure 7: Received optical power time series during retroreflector stability test at **[TODO: distance]** m. The dashed line indicates the mean received power; shading denotes $\pm 1\sigma$.

The empirical scintillation index, computed from the time series as $\mathrm{SI} = (\langle P^2 \rangle - \langle P \rangle^2)/\langle P \rangle^2$, will be compared against the log-normal model values of 0.1–1.5 used in Section 4. Any systematic drift in received power will indicate slow beam wander, while high-frequency fluctuations correspond to scintillation.

6.4 Discussion of Experimental Results

[To be written after data collection. Key points to address: agreement or discrepancy with libRadtran transmittance predictions; observed scintillation index vs. simulation inputs; PAT system performance and any pointing corrections applied during the measurement; implications for the QKD feasibility conclusions of Section 5.]

7 Conclusions

This project has constructed and characterised a low-cost, open-source FSO terminal based on the IRNAS KORUZA platform, with the original custom PCB replaced by off-the-shelf components. Three complementary computational analyses have been performed to characterise both the classical atmospheric channel and its quantum communication implications.

Atmospheric modelling using libRadtran MYSTIC Monte Carlo simulations confirms that 1550 nm is well-suited to short-range FSO in Scottish conditions. The clear-air extinction coefficient of 0.036–0.040 km^{-1} yields transmittances above 98% at 500 m; mist conditions raise k_{ext} by a factor of six but leave the 500 m link with 88% transmittance.

Qiskit BB84 simulations show that all three atmospheric scenarios support secure QKD at 500 m with QBER values of 1.34–1.38% and secure key rates of 5.3–5.9 kbps. An intercept-resend eavesdropper attack is unambiguously detectable at this range, elevating QBER to $\sim$40%. Log-normal scintillation analysis further reveals that strong turbulence (SI = 1.5) causes the link to enter the insecure regime for at most 0.4% of the time at 500 m, a figure that rises rapidly beyond 2 km.

The results collectively confirm that the KORUZA FSO terminal, operating at 500 m, provides a viable classical channel for metropolitan QKD. The key outstanding engineering step is the replacement of the SFP data link with a single-photon source and polarisation analysis module, while retaining the Raspberry Pi PAT system that this work has validated.

7.1 Further Work

Immediate next steps include experimental deployment of the constructed unit to measure actual BER and received power time series, from which empirical scintillation indices and transmittance values can be extracted and compared with the libRadtran predictions. Longer-term work could investigate adaptive-optics tip/tilt correction (using a fast steering mirror driven by the Raspberry Pi) to suppress beam wander, and the integration of attenuated-pulse QKD hardware as outlined in Section 5. The HWU Qrackling simulation framework [20] provides a natural platform for extending the quantum channel analysis to entanglement-based BBM92 protocols, which may offer security advantages in the metropolitan FSO context.

Acknowledgements

References

[1] Khalighi, M. A. & Uysal, M. Survey on free space optical communication: a communication theory perspective. *IEEE Commun. Surv. Tutor.* **16**, 2231–2258 (2014).

[2] Barrios, R. & Dios, F. Wireless optical communications through the turbulent atmosphere: a review. In *Optical Communications Systems* (ed. Das, N.) (InTech, 2012).

[3] Chan, V. W. S. Free-space optical communications. *J. Lightwave Technol.* **24**, 4750–4762 (2006).

[4] Fante, R. L. Electromagnetic beam propagation in turbulent media. *Proc. IEEE* **63**, 1669–1692 (1975).

[5] Tatarskii, V. I. *Wave Propagation in a Turbulent Medium* (McGraw-Hill, 1961).

[6] Andrews, L. C. & Phillips, R. L. *Laser Beam Propagation through Random Media*, 2nd edn (SPIE Press, 2005).

[7] Emde, C. et al. The libRadtran software package for radiative transfer calculations (version 2.0.1). *Geosci. Model Dev.* **9**, 1647–1672 (2016).

[8] Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, 175–179 (IEEE, 1984).

[9] Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).

[10] Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84**, 3762–3764 (2004).

[11] Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).

[12] Kržič, A. et al. Towards metropolitan free-space quantum networks. *npj Quantum Inf.* **9**, 95 (2023).

[13] Erven, C., Couteau, C., Laflamme, R. & Weihs, G. Entangled quantum key distribution over two free-space optical links. *Opt. Express* **16**, 16840–16853 (2008).

[14] IRNAS. KORUZA: open-source wireless optical system. *https://www.irnas.eu/koruza/* (2016).

[15] Anthonisamy, A. B. R., Durairaj, P. & Paul, L. J. Performance analysis of free space optical communication in open-atmospheric turbulence conditions with beam wandering compensation control. *IET Commun.* **10**, 1096–1103 (2016).

[16] Simmons, C., Barrow, P. & Donaldson, R. Dawn and dusk satellite quantum key distribution using time and phase-based encoding and polarization filtering. Preprint at *arXiv:2401.03129* (2024).

[17] Grabner, M. & Kvicera, V. The fog attenuation dependence on visibility and liquid water content at 850 nm and 1550 nm wavelength. *Radioengineering* **23**, 733–740 (2014).

[18] Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).

[19] Qiskit contributors. Qiskit: an open-source framework for quantum computing. *https://doi.org/10.5281/zenodo.2573505* (2023).

[20] Simmons, C., Barrow, P. & Donaldson, R. Qrackling: satellite QKD simulation framework. *https://github.com/Free-Space-QKD-Lab-HWU/Qrackling* (2024).

[21] Al-Habash, M. A., Andrews, L. C. & Phillips, R. L. Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Opt. Eng.* **40**, 1554–1562 (2001).

[22] Farid, A. A. & Hranilovic, S. Outage capacity optimisation for free-space optical links with pointing errors. *J. Lightwave Technol.* **25**, 1702–1710 (2007).

[23] Chaman Motlagh, A., Ahmadi, V., Ghassemlooy, Z. & Abedi, K. The effect of atmospheric turbulence on the performance of the free space optical communications. In *Proc. 6th Symp. Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, 540–543 (IEEE, 2008).

[24] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).

[25] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).

[26] Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).

[27] Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).

[28] Mohd Nor, N. A. et al. Experimental investigation of all-optical relay-assisted 10 Gb/s FSO link over the atmospheric turbulence channel. *J. Lightwave Technol.* **35**, 45–53 (2017).

[29] Ocampos-Guillén, A., Denisenko, N. & Fernández-Mármol, V. Optimising the interconnection of free-space to fibre quantum networks. *EPJ Web Conf.* **198**, 00007 (2019).

[30] Mohamed, P. H., El-Shimy, M. A., Shalaby, H. M. H. & Kheirallah, H. N. FSO channel modelling and performance evaluation over dust combined with Gamma-Gamma atmospheric turbulence. In *Proc. 40th National Radio Science Conf. (NRSC)*, 121–130 (IEEE, 2023).

A   Risk Assessment

The risk assessment submitted at the start of Semester 1 is reproduced below. Four hazards were identified: electrical equipment (risk score 3), display screen equipment (risk score 2), moving parts from the motor alignment sequence (risk score 2), and Class 1M laser radiation (residual risk score 8 after controls). Control measures include laser safety training, warning signs, power interlock, and prohibition on direct beam viewing. Full details are given in the project registration documentation.

B   Simulation Code

All simulation scripts are available in the project GitHub repositories:

- Atmospheric modelling: `github.com/Toddb2/Libradtran-HW` (scripts: `plot_data_scotland.py`, `plot_data3.py`)

- QKD channel simulations: `qkd_bb84_simulation.py`, `eve_attack_simulation.py`, `scintillation_simu`

Python dependencies: `qiskit==2.3.0`, `qiskit-aer`, `numpy`, `matplotlib`, `scipy`.