Finite-Key Analysis of Phase-Matching QKD Type Protocol over a Satellite Channel under Atmospheric Turbulence

Pranav Surapuraju
Indian Institute of Information Technology Sri City
Andhra Pradesh, India

Lokendra Chouhan
Indian Institute of Information Technology Sri City
Andhra Pradesh, India

***Abstract*—This paper evaluates the feasibility of a phase-matching type quantum key distribution (PM-QKD) over a satellite downlink under atmospheric turbulence and finite-key constraints. Extending finite-key security analysis to a highly asymmetric fading channel, the system consists of a ground fiber link and a satellite-based free-space channel. Atmospheric fading is modeled using the Gamma-Gamma distribution with parameters derived from Rytov variance across varying conditions. Results indicate positive secure key rates under nocturnal conditions, demonstrating the potential of PM-QKD for satellite-based quantum communication with finite resources. However, daytime operation is not feasible due to increased background noise leading to phase error rates beyond acceptable finite-key limits.**

I. Introduction

Quantum key distribution provides a secure means of communication that is backed by a promise of security using the laws of quantum mechanics. However, while conventional quantum key distribution is restricted by the linear repeaterless bound known as the PLOB bound [1], recent quantum key distribution protocols have shown to be able to achieve this bound without the need for repeaters, including twin-field quantum key distribution [2] and phase-matching quantum key distribution [3], in which single-photon interference is used in the measurement device. PM-QKD is preferred here because its robust continuous-phase randomization efficiently mitigates the dynamically evolving channel asymmetries of LEO passes. In order to implement quantum key distribution on a global scale, satellite quantum key distribution [4] is needed to overcome physical distance limitations. However, in using quantum key distributions in satellite downlinks in practice, significant free space channel impairments exist.

Practical QKD systems require finite-key security analysis. While efficient finite-key frameworks exist for fiber-based PM-QKD [5], extending them to dynamic free-space channels remains challenging. Dutta *et al.* [6] studied asymptotic satellite-based PM-MDI QKD, and Waghmare and Kothari [7] developed finite-key analysis for turbulent CV-QKD channels. However, finite-key security for PM-QKD over turbulent satellite-to-ground fading channels remains largely unexplored.

To address this gap, this paper presents the first finite-key analysis for a PM-QKD type protocol operating over a satellite downlink. We extend the asymptotic satellite framework of [6] by integrating the finite-key methodology of [5]. We model the atmospheric fading using a Gamma-Gamma distribution mapped to the Rytov variance [7], evaluating the finite-size secret key rates across six distinct atmospheric conditions for zenith angles ranging from 0° to 70°.

II. Protocol And Security Framework

The protocol is adopted from [5]. Alice and Bob send optical pulses to the untrusted relay, Charlie. Each round, they independently choose a label from {"0", "10", "11", "2"} with probabilities p_0, p_{10}, p_{11}, and p_2, respectively:

- Label "0" (signal): Generates a random bit $a \in \{0, 1\}$ and sends a coherent pulse $(-1)^a\sqrt{\mu}$.
- Label "10" (test): Sends the vacuum.
- Label "11" (test): Sends a phase-randomized coherent pulse, intensity $\mu_1 > \mu$.
- Label "2" (test): Sends a phase-randomized coherent pulse, intensity $\mu_2 < \mu_1$.

Charlie combines the received pulses in a 50-50 beamsplitter, and the pulses are measured. In-phase and anti-phase are called. Alice and Bob call their respective labels. K_0 is defined as the rounds in which both parties have "0", here the sifted keys are created using the random bits that are generated and kept in the intensity. For in-phase, they have the same bits, and for anti-phase, Bob flips his bits. K_{10}, K_{11}, and K_2 are defined as the rounds in which both parties have chosen "10", "11", and "2", respectively. $K_1 = K_{10} + K_{11}$.

In signal modes, key bits are accumulated, while in test modes, information leakage is checked. K_1 and K_2 estimate the phase error rate by using decoy-state methods and operator dominance, respectively.

After N_{tot} rounds, H_{EC} syndrome bits are used for error correction, with correctness verified by universal hashing using ζ' bits. Privacy amplification results in a key length given by:

$$G = K_0 - \left\lceil K_0\, h\left(\frac{f(K_1, K_2)}{K_0}\right)\right\rceil - H_{\text{EC}} - \zeta - \zeta', \quad (1)$$

where $h(\cdot)$ is the binary entropy function, $\zeta = 66$, $\zeta' = 32$, and $N_{\text{tot}} = 10^{13}$.

Security proof. Following the finite-key framework of Maeda *et al.* [5], security is established using a virtual X-basis in which the relevant quantity is the phase-error rate

$$e_{\mathrm{ph}} = \frac{K_0^{(\mathrm{even})}}{K_0}. \tag{2}$$

Since phase errors cannot be observed directly, they are estimated from the statistics collected in the test rounds. The sets K_1 and K_2 provide information about Eve's possible attack through the decoy-state method and the operator-dominance condition. From these observed quantities, an upper bound $f(K_1, K_2)$ is constructed such that

$$\Pr\{K_0^{(\mathrm{even})} \leq f(K_1, K_2)\} \geq 1 - \varepsilon. \tag{3}$$

Thus, except with probability ε, the phase-error events are bounded by $f(K_1, K_2)$ and can be removed through privacy amplification.

The protocol is $\varepsilon_{\mathrm{sec}}$-secure, where $\varepsilon_{\mathrm{sec}} = \sqrt{2}\sqrt{\varepsilon + 2^{-\zeta}} + 2^{-\zeta'}$ and $\varepsilon = 2^{-66}$. The central ingredient of the proof is the operator dominance condition, which relates the statistics of the test states to the even photon number component of the signal states. This allows the unobservable phase error rate to be bounded using experimentally observable quantities.

$$p_{10}^2\,\tau(0)\otimes\tau(0) + p_{11}^2\,\tau(\mu_1)\otimes\tau(\mu_1) \geq \Gamma\,\tau(\mu_2)\otimes\tau(\mu_2) + \Lambda\,\rho^{(\mathrm{even})}, \tag{4}$$

where $\tau(\mu)$ is a phase-randomized coherent state of intensity μ, and $\Gamma, \Lambda > 0$. This reduces finite-key security to classical random sampling bounded via Chernoff inequalities. The phase error bound is:

$$f(K_1, K_2) = \frac{p_0^2 P_{\mathrm{even}}}{\Lambda}\left(\Delta K + \nu\sqrt{-\ln(\varepsilon/2)}\right), \tag{5}$$

where

$$\Delta K = K_1 - \frac{\Gamma}{p_2^2} K_2, \tag{6}$$

$$P_{\mathrm{even}} = e^{-2\mu}\cosh(2\mu), \tag{7}$$

and

$$\nu = \frac{\sqrt{2\Gamma(p_2^2 + \Gamma)}}{p_2^2}\sqrt{K_2} + \sqrt{2\left(1 + \frac{\Lambda}{p_0^2 P_{\mathrm{even}}}\right)}\sqrt{\max(\Delta K, 0)}. \tag{8}$$

The quantity $f(K_1, K_2)$ upper bounds the phase-error events, where ΔK represents the observed test-state statistics and ν accounts for finite-size fluctuations.

The bit error rate is modeled as:

$$e_{\mathrm{bit}} = \frac{\left(1 - \sqrt{1-d}\,e^{-2e_m\eta\mu}\right)\left(1 + \sqrt{1-d}\,e^{-2(1-e_m)\eta\mu}\right)}{2\left[1 - (1-d)e^{-2\eta\mu}\right]}. \tag{9}$$

where d is the detector dark count probability and e_m is the misalignment error. This formula accounts for both photon click statistics and channel-dependent losses. Here we Assume symmetric transmittance $\eta_A = \eta_B = \eta$, detector dark count probability d, and misalignment error $e_m = 0.03$ [8]. Error correction costs $H_{\mathrm{EC}} = 1.1\,K_0\,h(e_{\mathrm{bit}})$. Protocol parameters $\{\mu, \mu_1, \mu_2, p_0, p_{10}, p_{11}, p_2\}$ are optimized via the Nelder-Mead method using multiple initial parameter guesses to reduce sensitivity to local optima.

III. Satellite Channel Model

A. Geometry and Loss Budget

In this downlink scenario, Bob sends optical pulses to Charlie for interference measurement, and Alice is connected to Charlie through an optical fiber. The zenith altitude of the satellite, i.e., the distance at $\varphi = 0°$, is assumed to be $L = 500\,\mathrm{km}$ [6]. The slant distance from the satellite to the ground station is:

$$L_B = \frac{L}{\cos\varphi}, \tag{10}$$

here φ is the zenith angle. We analyze $0° \leq \varphi \leq 70°$; larger angles are excluded due to severe atmospheric attenuation and reduced link efficiency.

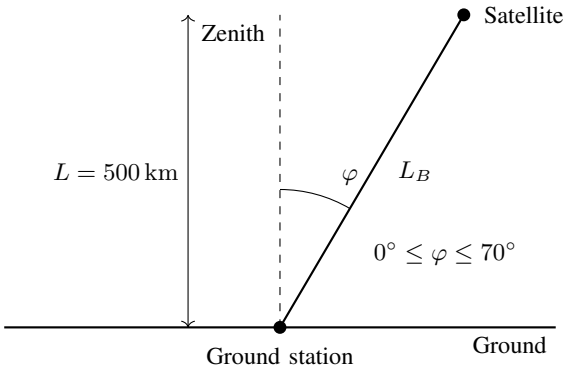

Fig. 1. Geometry of the satellite-to-ground free-space link. The slant distance depends on the zenith angle as $L_B = L/\cos\varphi$, where $L = 500\,\mathrm{km}$ is the satellite altitude.

B. Loss Budget

As per [5], Alice's link to Charlie is assumed to have a loss of 0.2 dB/km. Her detector efficiency is given by:

$$\eta_{d,\mathrm{fiber}} = 0.3, \tag{11}$$

Alice's transmittance is given by:

$$\eta_A = \eta_{d,\mathrm{fiber}} \cdot 10^{-0.2L_1/10}, \tag{12}$$

where L_1 is the fiber length in km.

Bob connects to Charlie through a free-space downlink. Total channel loss (in dB) [7] is:

$$L_{\mathrm{tot}} = L_{\mathrm{atm}} + L_{\mathrm{geo}} + L_{\mathrm{poi}} + L_{\mathrm{det}}, \tag{13}$$

- $L_{\mathrm{atm}} = 0.36$ dB: Atmospheric absorption.
- $L_{\mathrm{geo}} = 10\log_{10}\left(1 + (L_B/10)^2\right)$ dB: Slant-distance-dependent geometric beam spreading.
- $L_{\mathrm{poi}} = 2.00$ dB: Pointing error loss.

- $L_{\text{det}} = 0.46$ dB: Detector loss at Charlie.

Excluding turbulence fading, the deterministic free-space transmittance is:

$$T_0 = 10^{-L_{\text{tot}}/10}. \tag{14}$$

This represents the fixed loss component of Bob's channel.

C. Atmospheric Turbulence Model

Atmospheric turbulence causes random intensity fluctuations in Bob's free-space channel. Bob's transmittance is represented as $\eta_B = T_0\eta_{\text{fad}}$ where η_{fad} varies following the Gamma-Gamma distribution [7]:

$$P(\eta \mid T_0, \alpha, \beta) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} \left(\frac{\eta}{T_0}\right)^{(\alpha+\beta)/2-1} \times K_{\alpha-\beta}\left(2\sqrt{\alpha\beta\frac{\eta}{T_0}}\right)\frac{1}{T_0}, \tag{15}$$

where $\Gamma(\cdot)$ is the Gamma function and $K_{\alpha-\beta}(\cdot)$ is the modified Bessel function of the second kind. The Gamma-Gamma model is particularly well-suited for moderate-to-strong atmospheric turbulence regimes typical of LEO satellite downlinks [7], and captures both beam wandering and scintillation effects via two shape parameters.

The turbulence parameters α and β depend on the Rytov variance σ^2 [7]:

$$\alpha = \left(\exp\left(\frac{0.49\,\sigma^2}{(1+1.11\,\sigma^{12/5})^{7/6}}\right) - 1\right)^{-1}. \tag{16}$$

$$\beta = \left(\exp\left(\frac{0.51\,\sigma^2}{(1+0.69\,\sigma^{12/5})^{5/6}}\right) - 1\right)^{-1}. \tag{17}$$

The Rytov variance quantifies accumulated phase distortion:

$$\sigma^2 = 1.23\,C_n^2\,k^{7/6}\,L^{11/6}, \tag{18}$$

Here, $k = 2\pi/\lambda$ ($\lambda = 1550$ nm) and C_n^2 is the refractive index structure constant. The path length L only covers the turbulent atmospheric slab of $H_{\text{ATM}} = 20$ km [9], giving an effective length:

$$L = \frac{H_{\text{ATM}}}{\cos\varphi} \times 1000 \text{ m} \tag{19}$$

This slant path correction increases L from 20 km at $\varphi = 0^\circ$ to 58.5 km at $\varphi = 70^\circ$, amplifying σ^2 roughly sevenfold.

We evaluate six atmospheric conditions from [6], representing realistic satellite operation:

TABLE I
ATMOSPHERIC TURBULENCE PROFILES

Condition	C_n^2 ($\text{m}^{-2/3}$)	R_{bg} (Hz)
Night-1 (clear)	1.12×10^{-16}	100
Day-1 (no wind)	1.64×10^{-16}	1000
Night-2 (slightly foggy)	5.50×10^{-16}	100
Day-2 (moderate wind)	8.00×10^{-16}	1000
Night-3 (moderately foggy)	1.10×10^{-15}	100
Day-3 (windy)	1.60×10^{-15}	1000

Note: These conditions represent realistic operational scenarios: night passes have low background noise ($R_{\text{bg}} = 100$ Hz from moonlight), while daytime passes experience significant solar background ($R_{\text{bg}} = 1000$ Hz).Atmospheric conditions from [6].

Background photons increase Charlie's dark-count probability per gate:

$$d = 1 - (1 - p_d)(1 - d_{\text{bg}}), \qquad d_{\text{bg}} = 1 - e^{-R_{\text{bg}}\tau}, \tag{20}$$

assuming intrinsic dark-count rate $p_d = 10^{-8}$ [5] and gate width $\tau = 500$ ps.

D. Asymmetric Channel Fading and Finite-Key Averaging

Unlike symmetric setups, the satellite-to-ground link is highly asymmetric. Alice transmits through a static fiber with a deterministic transmittance η_A, while Bob transmits through a free-space channel with a fluctuating transmittance $\eta_B = T_0\eta_{\text{fad}}$, where η_{fad} follows a Gamma-Gamma distribution.

Because the instantaneous transmittance is almost never perfectly balanced ($\eta_A \neq \eta_B$), the interference at Charlie's beam splitter is imperfect. The effective intensities at the constructive interference port (I_+) and the destructive interference port (I_-) are modified by the interference visibility $V = 1-2e_m$ (where $e_m = 0.03$ is the misalignment error). A fixed visibility model is adopted in this work. While turbulence can introduce additional visibility fluctuations, these effects are not explicitly modeled and are left for future investigation:

$$I_+ = \frac{\mu}{2}\left(\eta_A + \eta_B + 2(1-2e_m)\sqrt{\eta_A\eta_B}\right), \tag{21}$$

$$I_- = \frac{\mu}{2}\left(\eta_A + \eta_B - 2(1-2e_m)\sqrt{\eta_A\eta_B}\right). \tag{22}$$

In a perfectly symmetric channel, I_- would be near zero. However, due to the channel asymmetry, incomplete destructive interference causes photons to continuously leak into the I_- port.

This leakage directly drives the error rate. The probabilities of registering no click at the respective detectors are $P_{0+} = \sqrt{1-d}e^{-I_+}$ and $P_{0-} = \sqrt{1-d}e^{-I_-}$. The total probability of registering a valid click is $P_{\text{click}} = 1 - P_{0+}P_{0-}$. A phase error occurs if the wrong detector (the destructive I_- port) clicks. Accounting for this leakage, as well as the random 50% bit assignment that occurs if both detectors click simultaneously, the expected error probability is $P_{\text{error}} = \frac{1}{2}(1 - P_{0-})(1 + P_{0+})$. The instantaneous bit error rate is then defined as $e_{\text{bit}} = P_{\text{error}}/P_{\text{click}}$.

The expected counts $\langle K_0\rangle$, $\langle K_1\rangle$, and $\langle K_2\rangle$ are obtained by averaging the corresponding detection events over the Gamma-Gamma fading distribution.

Since the full pulse block is accumulated under a fluctuating channel, detection yields are averaged over the Gamma-Gamma fading distribution before key extraction. η_{fad} is normalized to a mean of 1, an upper integration limit of 20 captures $> 99.9\%$ of the probability mass. The expected key bit counts for the signal mode (K_0) and test modes (K_1, K_2) are:

$$\langle K_0\rangle = N_{\text{tot}} \int_0^{20} p_0^2\, P_{\text{click}}(\mu) P_{GG}(\eta_{\text{fad}}) d\eta_{\text{fad}}, \tag{23}$$

$$\langle K_1\rangle = N_{\text{tot}} \int_0^{20} \left[p_{11}^2 P_{\text{click}}(\mu_1) + p_{10}^2 d\right] P_{GG}(\eta_{\text{fad}}) d\eta_{\text{fad}}, \tag{24}$$

$$\langle K_2 \rangle = N_{\text{tot}} \int_0^{20} p_2^2 \, P_{\text{click}}(\mu_2) P_{GG}(\eta_{\text{fad}}) d\eta_{\text{fad}}. \quad (25)$$

The averaged bit error rate is obtained as the ratio of averaged error events to averaged click events:

$$\langle e_{\text{bit}} \rangle = \frac{\int_0^{20} p_0^2 \, P_{\text{error}}(\mu) P_{GG}(\eta_{\text{fad}}) d\eta_{\text{fad}}}{\int_0^{20} p_0^2 \, P_{\text{click}}(\mu) P_{GG}(\eta_{\text{fad}}) d\eta_{\text{fad}}}. \quad (26)$$

IV. Numerical Results and Discussion

In this section, we describe the finite-key rate analysis for the satellite-based PM-QKD protocol. The simulation is based on a Low Earth Orbit (LEO) satellite located at a zenith height of 500 km and considers the downlink for zenith angles from $0°$ to $70°$. To mimic realistic system limitations, the block size is fixed to $N_{tot} = 10^{13}$ pulses, and the misalignment error is given by $e_m = 0.03$. The composable security is set to $\varepsilon = 2^{-66}$.

A. Key Rate Performance under Night Conditions

We now proceed to analyze the secure key rate generation for a range of atmospheric turbulence during nighttime operations, for which the background noise rate is given by $R_{bg} = 100$ Hz. Figure 2 shows the key rate penalty as a function of the zenith angle, while Figure 3 shows the same key rate penalty as a function of the total physical slant distance of the optical link.

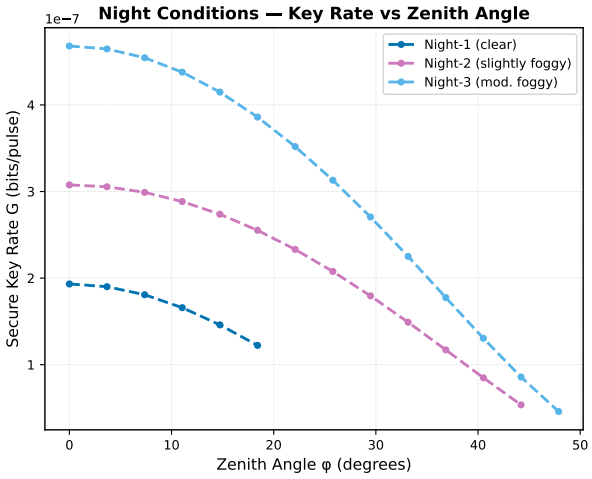

Fig. 2. Secure key rate G as a function of the zenith angle ϕ for various nighttime turbulence profiles.

The numerical evaluation yields a mathematically consistent but physically counter-intuitive hierarchy in protocol performance. As observed in Figure 2, the "Night-3" (moderately foggy) condition achieves the highest baseline key rate of 4.68×10^{-7} bits/pulse at zenith. It outperforms the "Night-1" (clear) condition, which achieves a lower baseline of 1.932×10^{-7} bits/pulse. Furthermore, the Night-1 connection degrades below the useful threshold at a maximum operating angle of approximately $18°$, whereas the Night-3 connection persists across a significantly wider range of zenith angles.

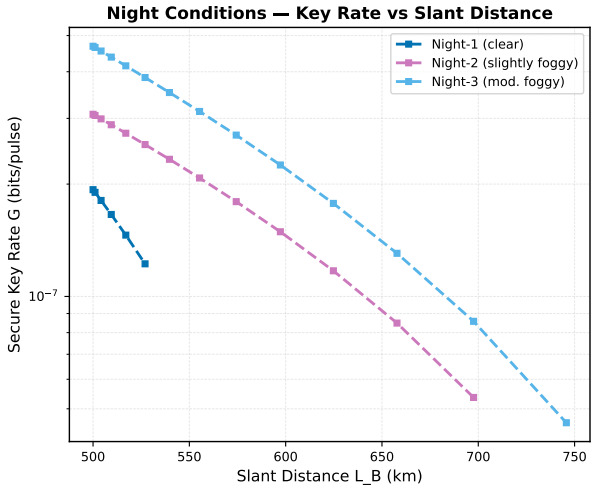

Fig. 3. Secure key rate G mapped against the total slant distance L_B (logarithmic scale).

TABLE II
Comparison of finite-key effects and atmospheric turbulence under Night-1 clear-sky conditions at zenith ($\phi = 0°$).

Case	Key Rate (bits/pulse)
Asymptotic PM-QKD	5.77×10^{-7}
Finite-Key PM-QKD	1.93×10^{-7}
No Turbulence	6.24×10^{-7}
Gamma-Gamma Turbulence	1.93×10^{-7}

Table II compares the finite-key results with asymptotic PM-QKD estimates under identical channel conditions. The finite-key framework reduces the achievable key rate from 5.77×10^{-7} to 1.93×10^{-7} bits/pulse, corresponding to an approximately 66.5% reduction. This reduction arises from finite-size statistical fluctuations and composable security overheads.

Table II also illustrates the impact of atmospheric turbulence. Under clear-night zenith conditions, the key rate decreases from 6.24×10^{-7} bits/pulse in the absence of turbulence to 1.93×10^{-7} bits/pulse when Gamma-Gamma fading is included, corresponding to an approximately 69.1% reduction.

Scintillation Saturation Artifact: Paradoxically, our model also demonstrates that foggy conditions (Night-3) produce a higher key rate than clear sky (Night-1). This phenomenon, while counterintuitive, is a mathematical artifact of the Gamma Gamma model in strong turbulence channels, i.e., $\sigma^2 > 1$. The scintillation index actually saturates, causing the variance and bit error rate for Night-3 to artificially decrease. This problem, while requiring a correction to match our intuition, can be accomplished by incorporating strong turbulence models, e.g., log-normal Rician or elliptical beams, in the future.

B. The Daylight Operation Bottleneck

We also tested the viability of the protocol under daylight passes, i.e., $R_{bg} = 1000$ Hz. Under the assumptions of the present model, the computed key rate was zero for all

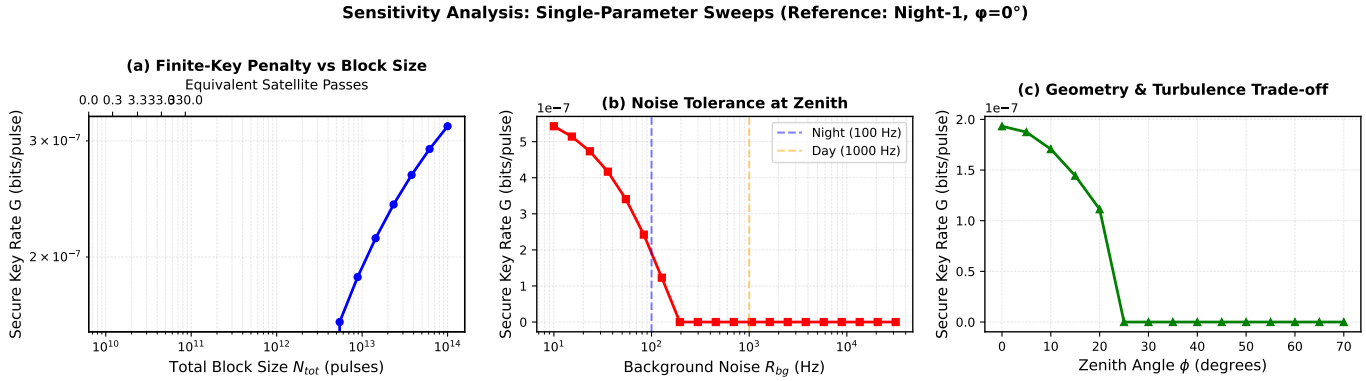

Fig. 4. Sensitivity analysis detailing single-parameter sweeps for (a) total block size, (b) background noise, and (c) zenith angle under baseline Night-1 conditions.

daytime conditions and zenith angles considered. This is due to the physical limitation of the hardware. The high rate of background solar photons completely swamps the quantum signal, halting the distillation process. The exact mechanism of this threshold is further investigated under the sensitivity analysis.

C. Sensitivity and Hardware Constraints

To determine the satellite QKD system's operational limits, we conducted single-parameter sweeps under baseline Night-1 (clear) conditions at zenith (0°), shown in Figure 4.

Finite-Key Penalty (Block Size): To overcome statistical fluctuations, the system requires a minimum block size of roughly 5.45×10^{12} pulses before producing a positive key rate (Figure 4(a)). For a 1 GHz transmitter during a 300-second LEO pass, data must be aggregated across multiple orbits to extract a single key. Such aggregation does not affect the security proof directly, provided the accumulated data are included within the same finite-key processing block.

Background Noise Tolerance: Figure 4(b) explains the daytime blackout. Increasing background noise R_{bg} elevates false dark counts, dropping the key rate to zero at $\sim$194.7 Hz. The 1000 Hz daylight noise floor exceeds this tolerance fivefold, necessitating advanced optical filtering or temporal gating to achieve daytime operation. This threshold arises primarily from the increased effective dark-count probability caused by background photons, which is further amplified by finite-key statistical penalties.

Geometry and Turbulence Trade-off: Figure 4(c) isolates the zenith angle's effect. The key rate decays rapidly beyond 10°, reflecting the severe compounding penalties of geometric beam spreading and increased atmospheric thickness at lower elevations.

V. Conclusion

This work presented a finite-key analysis of PM-QKD over a satellite-to-ground channel incorporating Gamma-Gamma atmospheric turbulence. Positive secret-key generation was demonstrated for nighttime operation with block sizes exceeding 5.45×10^{12} pulses, while daytime operation was not feasible under the considered background-noise levels. Comparison with asymptotic results showed a finite-key penalty of approximately 66.5% , and turbulence reduced the achievable key rate by approximately 69.1%. Future work will investigate stronger turbulence models and hardware techniques enabling daylight satellite QKD.

References

[1] M. Pittaluga *et al.*, "600-km repeater-like quantum communications with dual-band stabilization," *Nat. Photonics*, vol. 15, pp. 530–535, 2021.

[2] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.

[3] J. Lin and N. Lütkenhaus, "Simple security analysis of phase-matching measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 98, p. 042332, 2018.

[4] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nat. Photonics*, vol. 11, pp. 509–513, 2017.

[5] K. Maeda, T. Sasaki, and M. Koashi, "Repeaterless quantum key distribution with efficient finite-key analysis resting on operational setups," *Nat. Commun.*, vol. 10, p. 3140, 2019.

[6] A. Dutta, S. Banerjee, and A. Pathak, "Satellite-based communication for phase-matching measurement-device-independent quantum key distribution," *Ann. Phys.*, vol. 537, no. 9, p. e202500134, 2025.

[7] C. Waghmare and A. Kothari, "Finite-size secret key rate analysis of a discrete-modulated continuous-variable quantum key distribution protocol for satellite-to-ground fading channel," *Opt. Commun.*, p. 132044, 2025.

[8] W. Li *et al.*, "Twin-field quantum key distribution without optical frequency dissemination," *Nat. Commun.*, vol. 14, p. 6022, 2023.

[9] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New J. Phys.*, vol. 21, p. 093055, 2019.