

# Qiskit-Enabled Simulation of Quantum Key Distribution over Starlink Satellite Networks

Yudai Takihara, Hoang D. Le, Cuong T. Nguyen, and Anh T. Pham

Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan

**Abstract**—This paper investigates the performance of free-space optics (FSO)-based satellite-assisted quantum key distribution (QKD). Specifically, we develop a simulation framework using the IBM Quantum Experience (IQX) simulator with Qiskit that closely emulates real-world QKD implementations. The low Earth orbit (LEO) satellite quantum channels, incorporating the atmospheric loss, atmospheric turbulence, and pointing misalignment, are taken into account. Using the developed framework, we investigate QKD performance, including quantum bit error rate (QBER) and secret key rate (SKR), by simulating the key generation rate by IQX, considering the impact of satellite quantum channels over SpaceX’s Starlink networks. The obtained results provide insights into the QKD performance under various quantum channel conditions in satellite-based FSO/QKD systems.

**Index Terms**—Quantum key distribution (QKD), Starlink LEO satellite, free-space optics (FSO), IBM IQX, Qiskit.

## I. INTRODUCTION

Security is one of the most critical challenges in the Internet era. The rapid proliferation of the Internet of Things (IoT) and cloud computing has led to large-scale storage and transmission of sensitive data, such as personal and medical information, across networks. This intensifies the demand for reliable protection mechanisms. Traditional communication infrastructures rely on key distribution systems (KDS) based on public key cryptography, whose security is grounded in the computational intractability of problems like large integer factorization. However, the emergence of quantum computing and algorithms such as Shor’s algorithm constitutes a significant threat to these classical schemes. In contrast, the quantum key distribution (QKD) leverages the principles of quantum mechanics rather than computational complexity and has been theoretically proven to offer unconditional security [1].

QKD has emerged as a promising method to achieve information-theoretic security by securely sharing secret keys between legitimate communicating parties based on the principles of quantum mechanics. The BB84 is the first QKD protocol proposed in 1984 by Bennett and Brassard [2]. Since then, several QKD protocols have been introduced for different applications. In addition, QKD can be implemented over optical fiber, free-space optics (FSO)-based terrestrial systems, and FSO-based satellite systems. For global/seamless QKD services, satellite-based FSO/QKD systems have emerged as a potential architecture. Such systems can provide QKD services to a diverse range of users, including secure IoT devices in remote areas and secure Internet of vehicles (IoV), which is usually not effective using optical fiber or FSO-based terrestrial systems.

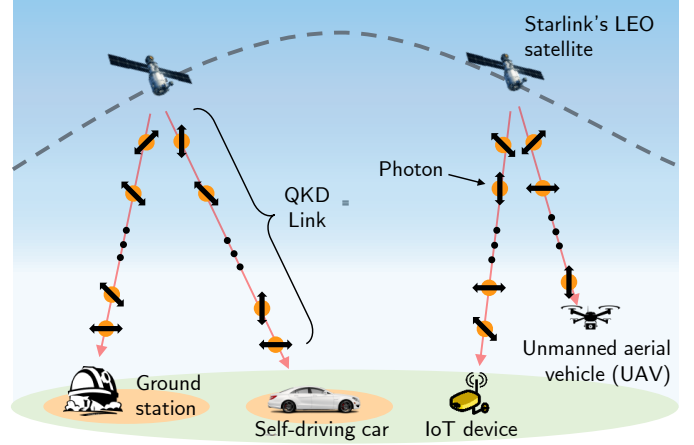


Fig. 1. Illustration of various QKD services enabled by LEO satellite-based FSO/QKD systems.

A significant breakthrough in the LEO satellite-to-ground QKD system was inaugurated by the Micius satellite, where a non-zero key rate was achieved over 1200 km in 2016. Thereafter, a series of experiments and implementations have ushered in the new era of LEO-based QKD systems [3]–[6]. As depicted in Fig. 1, LEO satellite-based FSO/QKD enables various QKD services, such as IoV with self-driving cars and unmanned aerial vehicles (UAVs), IoT devices, and ground stations in rural and remote areas. Such QKD systems extend secure communication capabilities beyond users with fixed locations, supporting a variety of practical scenarios, including mobile users and rural/oceanic/remote areas.

For the design and simulation of such QKD systems, quantum computing platforms have received much attention from researchers. One of the well-known platforms is the IBM Quantum Experience (IQX), an open platform provided by IBM for quantum computing services. IQX is an open platform for researchers/engineers to develop applications/systems and simulate them using a quantum simulator at IBM. It offers a quantum simulator accessible through Qiskit [7], a software development kit for quantum programming. IQX enables the systematic design and simulation of practical QKD implementations, which have been recently addressed in optical fiber and terrestrial-based FSO/QKD systems [8]–[10]. However, the Qiskit-based simulations using IQX, which incorporates realistic quantum channel characteristics specific to satellite-to-ground communication, have not yet been available in the

literature.

This paper, therefore, aims to develop a Qiskit-enabled simulation framework for LEO satellite-based FSO/QKD systems. Particularly, we employ the well-known IBM quantum platform, called IQX, to simulate the BB84 protocol over LEO satellite quantum channels. The platform is utilized via Qiskit, an open-source software development kit (SDK) for quantum computing. Via IQX simulations, we assessed the key generation rate and runtime under several conditions and verified the practical feasibility of our Qiskit application. LEO satellite quantum channels, incorporating the atmospheric loss, atmospheric turbulence, and pointing misalignment, are taken into account. Using the developed framework, we investigate QKD performance, including quantum bit-error rate (QBER) and secret key rate (SKR), over the considered SpaceX Starlink satellite networks.

## II. SYSTEM DESCRIPTION & QUANTUM CHANNEL MODEL

### A. System Description

In this paper, we consider an LEO satellite-to-ground FSO/QKD system, as shown in Fig. 1. In particular, the LEO satellite (Alice) will prepare and share key materials with a ground station (Bob) via a quantum FSO channel. For a practical consideration, we assume that single-photon sources are not available, and Alice adopts a weak laser source. This implies that the number of photons in each pulse follows the Poisson distribution, and the probability that a given pulse contains  $i$  photons is [11]

$$P_i(\mu) = e^{-\mu} \frac{\mu^i}{i!}, \quad (1)$$

where  $i$  is the number of photons and  $\mu$  is the mean photon number of the laser source. It is worth noting that the source has a non-zero chance of emitting a multiple-photon pulse, which can pave the way for the photon-number splitting (PNS) attack. Specifically, Eve, assumed to have unlimited technological power, will stop all single-photon pulses and derive information from multiple-photon pulses. This allows Eve to gain information about the secret key without being detected and can compromise the system's security completely [12].

To tackle this issue, we consider the two-decoy-state BB84 protocol using vacuum and weak decoy states [13]. The key idea of this method is to prepare and transmit some decoy states along with signal states, which allows Alice and Bob to have a better analysis and detection of the eavesdropping activity. As a result, the system with the decoy-state BB84 protocol can extract a higher SKR compared to the one with the conventional BB84 protocol [6].

### B. Quantum Channel Model

To characterize the effect of quantum states propagating in FSO channels, we consider the transmittance, which is defined as the fraction of input photons that make it to the output

TABLE I  
TRANSMITTANCE EFFICIENCY VERSUS VISIBILITY AT  $\lambda = 850$  NM

Visibility (km)	Transmittance efficiency at zenith ( $\tau_{zen}$ )
23	0.81
15	0.75
5	0.55

on average [14]. According to [14], the transmittance of the quantum LEO-to-ground channel can be expressed as

$$\eta = \eta_\ell I_a \eta_p, \quad (2)$$

where  $\eta_\ell$  is the deterministic atmospheric attenuation,  $I_a$  represents random fluctuations caused by atmospheric turbulence, and  $\eta_p$  denotes the fluctuating fraction of received optical power captured by a finite aperture telescope, accounting for both pointing errors and beam divergence losses. Details of these components are as follows.

1) *Atmospheric Attenuation*: In this work, we restrict the considered scenarios to the cases where the zenith angle is below 70 degrees. As a result, the atmospheric turbulence is mainly due to the absorption or scattering by air molecules or aerosols, which can be readily estimated as [4]

$$\eta_\ell = \tau_{zen}^{\sec(\xi)}, \quad (3)$$

where  $\xi$  represents the zenith angle, and  $\tau_{zen} \in [0, 1]$  denotes the transmittance efficiency at zero-degree zenith angle. The transmission efficiency for different scenarios can be derived via the calculator tool on the MODTRAN website [15]. Table I exemplifies some values of  $\tau_{zen}$  versus visibility at the optical wavelength value of 850 nm.

2) *Atmospheric Turbulence*: This phenomenon refers to the random fluctuations of received photons due to the inhomogeneities of the refractive index along the quantum channel. Under the consideration of weak turbulence conditions, the random variable  $I_a$  can be modeled as a log-normal (LN) random variable as [16]

$$f_{I_a}(I_a) = \frac{1}{I_a \sqrt{2\pi\sigma_R^2}} \exp \left[ -\frac{\left( \ln I_a + \frac{\sigma_R^2}{2} \right)^2}{2\sigma_R^2} \right], \quad (4)$$

where  $\sigma_R^2$  denotes the Rytov variance and can be given as [16]

$$\sigma_R^2 = 2.25 \left( \frac{2\pi}{\lambda} \right)^{\frac{7}{6}} \sec^{\frac{11}{6}}(\xi) \int_{H_g}^{H_{atm}} C_n^2(h) (h - H_g)^{5/6} dh, \quad (5)$$

where  $H_{atm}$  denotes the atmospheric altitude,  $H_g$  is the receiver altitude, and  $\lambda$  is the optical wavelength. Moreover,  $C_n^2(h)$  is the altitude-dependent refractive index structure parameter profile, and can be described by the well-known Hufnagel-Valley model as [17]

$$C_n^2(h) = 0.00594 \left( \frac{v_{wind}}{27} \right)^2 (10^{-5}h)^{10} \exp \left( -\frac{h}{1000} \right) + 2.7 \times 10^{-16} \exp \left( -\frac{h}{1500} \right) + C_n^2(0) \exp \left( -\frac{h}{100} \right), \quad (6)$$

where  $C_n^2(0)$  is the ground level turbulence, and  $v_{\text{wind}}$  denotes the root-mean-squared wind speed.

3) *Beam Spreading Loss and Misalignment*: The beam spreading loss arises from the divergence of a laser beam as it propagates through free space, which reduces the fraction of power that can be collected. Misalignment loss refers to the reduction in received photons due to imperfect pointing accuracy, which causes the center of the beam spot to be offset from that of the receiver aperture. Given the radial displacement  $r$ , the value of  $\eta_p$  can be approximated as [18]

$$\eta_p \approx A_0 \exp\left(-\frac{2r^2}{w_{L_{\text{eq}}}^2}\right), \quad (7)$$

where  $A_0 = [\text{erf}(\nu)]^2$  represents the maximum fraction of received power if there is no misalignment,  $\nu = \frac{\sqrt{\pi}a}{\sqrt{2}w_L}$ ,  $\text{erf}(\cdot)$  is the Gauss error function [14],  $a$  is the aperture radius, and  $w_{L_{\text{eq}}}$  is the equivalent beam width, which is given as [17]

$$w_{L_{\text{eq}}}^2 = w_L^2 \frac{\sqrt{\pi}\text{erf}(\nu)}{2\nu \exp(-\nu^2)}, \quad (8)$$

where  $w_L \simeq \theta L$  is the radius of the beam footprint,  $L$  is the slant distance and  $\theta$  is the divergence half-angle. By taking into account random jitter in both  $x$  and  $y$  axes, the radial displacement  $r$  can be generally modeled by the four-parameter Beckmann distribution, whose PDF is given as [19]

$$f_r(r) = \frac{r}{2\pi\sigma_x\sigma_y} \times \int_0^{2\pi} \exp\left[-\frac{(r\cos\Theta - \mu_x)^2}{2\sigma_x^2} - \frac{(r\sin\Theta - \mu_y)^2}{2\sigma_y^2}\right] d\Theta, \quad (9)$$

where  $(\mu_x, \mu_y)$  are the means of the Gaussian-distributed jitters along the  $x$  and  $y$  axes, respectively;  $(\sigma_x, \sigma_y)$  are the standard deviations of these distributions. Both  $\sigma_x$  and  $\sigma_y$  can be calculated based on the standard deviations of angle-jitter  $\sigma_{\theta_x}$  and  $\sigma_{\theta_y}$  as  $\sigma_x \simeq L\sigma_{\theta_x}$  and  $\sigma_y \simeq L\sigma_{\theta_y}$ .

For the ease of analysis, we will estimate (9) as the PDF of the Rayleigh distribution as [19]

$$f_r(r) = \frac{r}{\sigma_{\text{mod}}^2} \exp\left(-\frac{r^2}{2\sigma_{\text{mod}}^2}\right), \quad (10)$$

where  $\sigma_{\text{mod}} = \left(\frac{3\mu_x^2\sigma_x^4 + 3\mu_y^2\sigma_y^4 + \sigma_x^6 + \sigma_y^6}{2}\right)^{1/3}$  is the modified variance approximation. Combining (7) and (10), we can rewrite the PDF of  $\eta_p$  as

$$f_{\eta_p}(\eta_p) = \frac{\varphi_{\text{mod}}^2}{A_{\text{mod}}^{\varphi_{\text{mod}}^2}} \eta_p^{\varphi_{\text{mod}}^2-1}, \quad (11)$$

where  $A_{\text{mod}} = A_0 \exp\left(\frac{1}{\varphi_{\text{mod}}^2} - \frac{1}{2\varphi_x^2} - \frac{1}{2\varphi_y^2} - \frac{\mu_x^2}{2\sigma_x^2\varphi_x^2} - \frac{\mu_y^2}{2\sigma_y^2\varphi_y^2}\right)$ ,  $\varphi_x = w_{L_{\text{eq}}}/2\sigma_x$ ,  $\varphi_y = w_{L_{\text{eq}}}/2\sigma_y$ , and  $\varphi_{\text{mod}} = w_{L_{\text{eq}}}/2\sigma_{\text{mod}}$ .

4) *Composite channels*: Utilizing (2), (4), and (11) with some mathematical manipulations, the PDF of the overall transmittance is given as [14]

$$f(\eta) = \frac{\varphi_{\text{mod}}^2}{(A_{\text{mod}}\eta_{\ell})^{\varphi_{\text{mod}}^2}} \eta^{\varphi_{\text{mod}}^2-1} \int_{\frac{\eta}{A_{\text{mod}}\eta_{\ell}}}^{\infty} I_a^{-\varphi_{\text{mod}}^2} f_{I_a}(I_a) dI_a. \quad (12)$$

Applying [20, (3.322.1)], we derive the closed-form expression of the composite probability density of transmittance as [14]

$$f(\eta) = \frac{\varphi_{\text{mod}}^2}{2(A_{\text{mod}}\eta_{\ell})^{\varphi_{\text{mod}}^2}} \eta^{\varphi_{\text{mod}}^2-1} \text{erfc}\left[\frac{\ln\left(\frac{\eta}{A_{\text{mod}}\eta_{\ell}}\right) + \chi}{\sqrt{2}\sigma_R}\right] \times \exp[0.5\sigma_R^2\varphi_{\text{mod}}^2(1 + \varphi_{\text{mod}}^2)], \quad (13)$$

where  $\text{erfc}(x)$  is the complementary error function [14], and  $\chi = 0.5\sigma_R^2(1 + 2\varphi_{\text{mod}}^2)$ .

### III. SIMULATION & THEORETICAL FRAMEWORK

This section first presents our Qiskit-enabled simulation framework. Then, the theoretical computation of QBER is derived to verify the correctness of our simulation framework. We also investigate the SKR performance of the satellite-based QKD systems, which are calculated based on the derived QBER.

#### A. Qiskit-based Simulation Framework

In this work, we develop a simulation framework to investigate the QBER performance of BB84 protocols over satellite-based QKD systems. As shown in Fig. 2, the framework is centered around the Qiskit-based BB84 simulation. To model the random behavior of the FSO channel, an instantaneous transmittance value is first generated. Note that the transmittance over the satellite-based quantum channel is a random variable whose PDF is Eq. (12). Based on the instantaneous transmittance value, we then simulate the number of detection events due to signal pulses at Bob's side, which corresponds to the number of simulated quantum states. It is worth noting that if the number of simulated quantum states is too large, the program will take a long time to handle. As a result, we divide the simulated quantum states into different executions. The number of quantum states per execution will be investigated in Section IV.

In each execution, we utilize Qiskit to create a quantum circuit, where the behavior of quantum states in the BB84 protocol is simulated. In particular, for each input, we randomly generate one of four possible states, i.e.,  $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle$ , and  $|-\rangle$ . After that, Bob will randomly select one of two bases to measure a quantum state. To simulate the erroneous detection of quantum states, we consider the Pauli error model, which takes into account the instantaneous QBER value. After measuring all quantum states, Alice and Bob exchange their selected bases and eliminate all bits that do not share the same basis. After a few thousand times of generating transmittance value, we compute the average QBER based on the number of erroneous bits and the number of accumulated sifted bits.

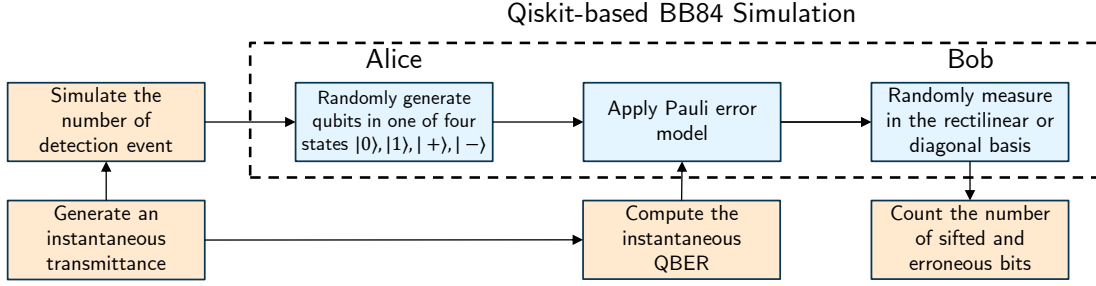


Fig. 2. Block diagram of the proposed simulation framework with the Qiskit-based BB84 simulation.

### B. Quantum Bit-error Rate (QBER)

To verify the validity of the simulator, we investigate the theoretical QBER, which is derived by averaging over the fading channel as [11], [21]

$$\langle E_\mu \rangle = \frac{\langle E_\mu Q_\mu \rangle}{\langle Q_\mu \rangle} = \frac{\int_0^\infty E_\mu Q_\mu(\eta) f(\eta) d\eta}{\int_0^\infty Q_\mu(\eta) f(\eta) d\eta}, \quad (14)$$

where  $\langle E_\mu Q_\mu \rangle$  is the average number of erroneous detections per pulse,  $E_\mu Q_\mu(\eta)$  is the conditional probability of erroneous detections per pulse and can be computed as [21]

$$E_\mu Q_\mu(\eta) = e_0 p'_{\text{dark}} + (e_{\text{pol}} + e_0 P_{\text{AP}}) (1 - e^{-\mu\eta}), \quad (15)$$

where  $p'_{\text{dark}} = p_{\text{dark}}(1 + P_{\text{AP}})$ ,  $p_{\text{dark}}$  is the background detection event rate,  $P_{\text{AP}}$  is after-pulsing probability,  $e_0$  is the error rate due to the background detection event,  $e_{\text{pol}}$  is the error rate due to the polarisation error. In addition,  $\langle Q_\mu \rangle$  denotes the probability of a detection event,  $Q_\mu(\eta)$  is the conditional probability of a detection event given the transmittance value  $\eta$ , which is given as [21]

$$Q_\mu(\eta) = p'_{\text{dark}} + (1 + P_{\text{AP}}) (1 - e^{-\mu\eta}). \quad (16)$$

### C. Secret Key Rate (SKR)

Another important performance metric considered in this work is SKR, which is defined as the average number of key materials that can be generated per second. Given the two-decoy-state BB84 protocol, the lower bound of the system's SKR is given as [22]

$$\text{SKR} \geq \mathcal{R} \text{spd} \left\{ -\langle Q_\mu \rangle f H_2(\langle E_\mu \rangle) + \langle Q_1^L \rangle [1 - H_2(\langle e_1^U \rangle)] \right\}, \quad (17)$$

where  $\mathcal{R}$  is the repetition rate,  $s$  denotes the sifting coefficient,  $p$  is the coefficient characterizing the parameter estimation,  $d$  is the fraction of signal pulses in the decoy-state method,  $f$  is the key reconciliation efficiency, and  $H_2(\cdot)$  is Shannon's entropy function. In addition,  $\langle Q_1^L \rangle = \int_0^\infty Q_1^L(\eta) f(\eta) d\eta$  [22], where  $Q_1^L$  denotes the lower bound of detection event probability of single-photon pulses and can be calculated as in [13, (35)]. Moreover,  $\langle e_1^U \rangle = [\int_0^\infty e_1^U(\eta) Q_1^L(\eta) f(\eta) d\eta] / \langle Q_1^L \rangle$  [22],

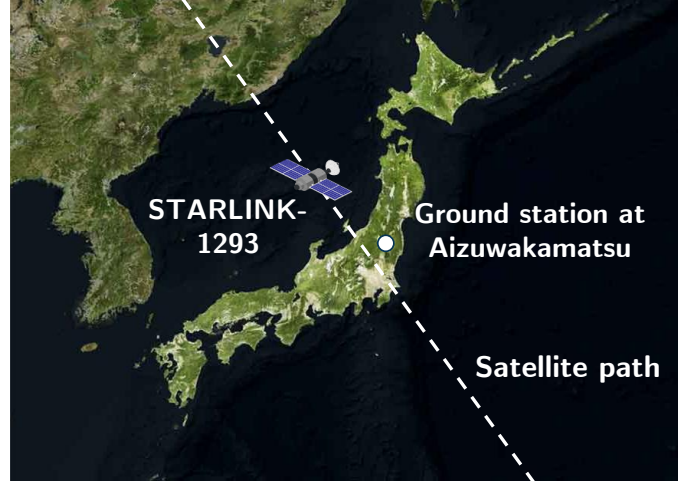


Fig. 3. Illustration of the orbit of the STARLINK-1293 over Japan from 11:28:00 UTC+9 on 23 December 2021, 16:09:20:00 UTC+9.

where  $e_1^U(\eta)$  denotes the upper bound of the error rate of single-photon pulses and can be computed as [13]

$$e_1^U(\eta) = \frac{E_\nu Q_\nu(\eta) e^\nu - e_0 p'_{\text{dark}}}{Y_1^L \nu}, \quad (18)$$

where  $\nu$  is the mean photon number of decoy pulse,  $E_\nu Q_\nu(\eta)$  can be computed as in (15), and  $Y_1^L$  is given in [13, (34)].

## IV. NUMERICAL RESULTS

This section presents the performance evaluation of LEO satellite-based FSO/QKD using Qiskit-based simulations. Different performance metrics, including quantum bit error rate and secret key rate, are investigated. Unless otherwise noted, system parameters considered in this paper are given in Table II. For a practical case study, as illustrated in Fig. 3, we consider the STARLINK-1293 satellite operated by SpaceX. We investigate the performance of the satellite pass over Japan, particularly the Aizu-Wakamatsu city, Fukushima. The satellite tracking process begins at the moment when the satellite reaches a zenith angle of  $\xi = 60^\circ$ , which we define as the initial reference time  $t = 0$ . This moment corresponds to the timestamp of 23 December 2021, 16:09:20:00 (UTC+9), marking the beginning of the communication session between the satellite and the ground station.

TABLE II  
SYSTEM PARAMETERS

Name	Symbol	Value
<b>LEO Satellite (Alice)</b>		
LEO satellite altitude	$H_s$	550 km
Divergence half-angle	$\theta$	$10 \mu\text{rad}$
Optical wavelength	$\lambda$	$0.85 \mu\text{m}$
Repetition rate	$\mathcal{R}$	$10^9$ pulses/s
<b>Ground Station (Bob)</b>		
Aperture radius	$a$	0.75 m
Ground station altitude	$H_g$	10 m
Error rate of the background	$e_0$	0.5
Probability of the polarization errors	$e_{\text{pol}}$	3.3%
Background detection probability	$p_{\text{dark}}$	$10^{-4}$
After-pulsing probability	$P_{\text{AP}}$	2%
<b>Quantum Channel</b>		
Atmospheric altitude	$H_{\text{atm}}$	20 km
Wind speed	$v_{\text{wind}}$	21 (m/s)
Mean of horizontal jitter	$\mu_x$	0
Mean of vertical jitter	$\mu_y$	0
Standard deviation of horizontal angle-jitter	$\sigma_{\theta_x}$	$\theta/5$
Standard deviation of vertical angle-jitter	$\sigma_{\theta_y}$	$\theta/5$
Ground-level refractive index	$C_n^2(0)$	$10^{-13}$
<b>QKD Protocol</b>		
Mean photon number of signal pulse	$\mu$	0.3
Mean photon number of decoy pulse	$\nu$	0.09
Sifting efficiency	$s$	0.5
Parameter estimation coefficient	$p$	0.75
Key reconciliation efficiency	$f$	1
Fraction of signal pulses	$d$	0.5

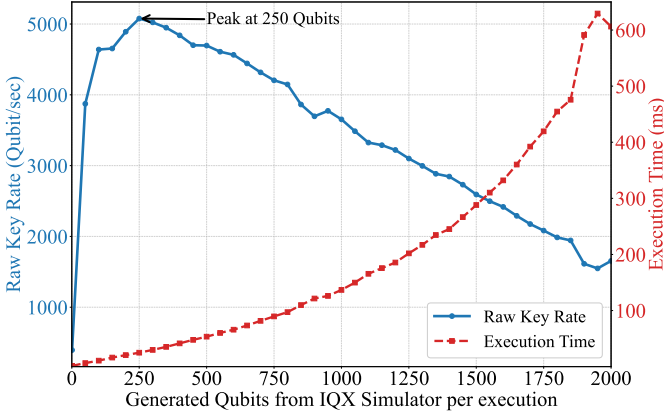


Fig. 4. Raw key rate and runtime versus the number of generated qubits by IQX.

First, we investigate the raw key rate and runtime over a range of the number of generated qubits per execution by IQX. Here, the raw key rate refers to the number of qubits per second that Alice can generate using the IQX simulator. Figure 5 shows the raw key rate (Qubits/sec) and execution time (ms) against the number of bits generated per execution by IQX. We can observe that an increase in the number of generated qubits leads to high computational complexity and longer runtimes. As a result, there exists an optimal number of generated qubits, which is to achieve the highest raw key rate. Using this figure, we can decide on the number of generated qubits from the IQX simulator, i.e., 250 qubits, to achieve a raw key rate of 5000 qubits/sec.

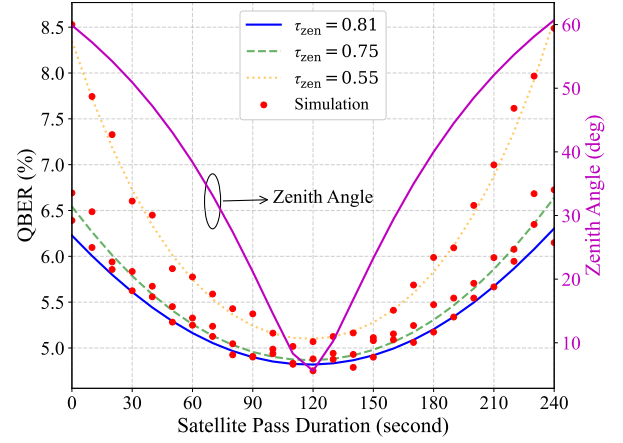


Fig. 5. QBER performance over the STARLINK-1293's pass duration with different atmospheric loss conditions.

Next, using 250 generated qubits/execution from the IQX simulator, we evaluate the QBER performance over the satellite pass duration in Fig. 5. Here, the satellite pass corresponds to a range of zenith angles from  $\xi = 60^\circ$  to  $\xi = -60^\circ$ . Also, different atmospheric loss conditions, i.e.,  $\tau_{\text{zen}} = 0.81$ , 0.75, and 0.55, are taken into account. As seen, higher zenith angle values lead to an increase in QBER performance. This is due to increased atmospheric path length and beam divergence at higher zenith angles, which lead to higher atmospheric loss and beam spreading loss. On the other hand, the performance of satellite-based FSO/QKD systems significantly degrades with lower values of  $\tau_{\text{zen}}$ . This is due to higher atmospheric loss reducing the number of detected photons and increasing the relative influence of background noise, which in turn raises the error rate during key generation. For instance, at the starting point of the satellite, the QBER values are 6.2 %, 6.6 %, and 8.4 % with  $\tau_{\text{zen}} = 0.55$ , 0.75, and 0.81, respectively. Using this figure, the analytical results closely match the simulated ones obtained using Qiskit. This confirms the accuracy and reliability of the proposed model and analytical method. In particular, even under different zenith transmittance conditions, the analytical and simulation values exhibit similar trends, suggesting that the theoretical model appropriately captures the actual physical phenomena. This supports the validity of the channel model and QBER evaluation method developed in this study for analyzing the performance of QKD in realistic satellite-to-ground communication scenarios.

Finally, we analyze the secret key rate performance over the satellite pass duration in Fig. 6. Also, different pointing misalignment conditions, i.e.,  $\theta_{\text{rad}}/5$  and  $\theta_{\text{rad}}/8$ , are considered. The simulation results clearly show that the secret key rate is significantly affected by the magnitude of beam angle jitter occurring during transmission. In particular, when the angle jitter is relatively small at  $\theta_{\text{rad}}/8$ , the secret key rate remains relatively high throughout the entire satellite pass. In particular, under the condition of a zenith transmittance  $\tau_{\text{zen}} = 0.81$ , the secret key rate approaches approximately



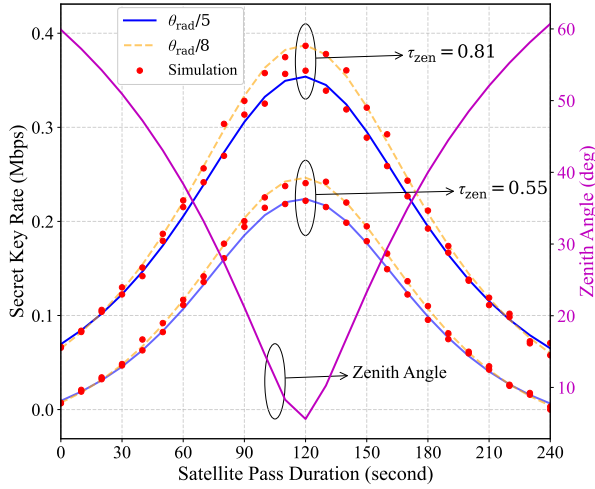


Fig. 6. SKR performance over the STARLINK-1293 pass duration with different pointing misalignment conditions.

0.6 Mbps, indicating favorable communication performance. On the other hand, when the jitter increases to  $\theta_{\text{rad}}/5$ , the performance significantly degrades, and the secret key rate drops substantially. The degradation of the key generation rate with increased jitter is due to a higher probability of beam misalignment, which reduces the coupling efficiency at the receiver. Furthermore, as shown in this figure, the analytical results obtained from the proposed theoretical model show excellent agreement with the simulation data over the full range of zenith angles from  $\xi = 60^\circ$  to  $\xi = -60^\circ$ . This high level of consistency strongly supports the accuracy and robustness of the proposed channel model and performance analysis method. The model appropriately captures the interplay of geometric loss, atmospheric effects, and pointing errors, providing a reliable framework for evaluating secret key distribution in realistic satellite-to-ground communication scenarios.

## V. CONCLUSIONS

In this paper, we developed a Qiskit-enabled simulation framework for LEO satellite-based FSO/QKD systems. In particular, we utilized Qiskit to simulate the random behavior of quantum states in the BB84 protocol. The close agreement between the analytical and simulation results verified the correctness of the proposed framework. The feasibility of our framework was also demonstrated by investigating the runtime under different conditions. Based on the framework, we investigated the practical Starlink satellite networks in terms of QBER and SKR. The investigation took into account major impairments over the FSO quantum channel, i.e., atmospheric loss, atmospheric turbulence, and pointing error.

## ACKNOWLEDGMENT

This work was supported by the Telecommunications Advancement Foundation (TAF) and the JSPS KAKENHI Grant number 24K14918.

## REFERENCES

- [1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, p. 1301, Sept. 2009.
- [2] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.
- [3] S. Ecker *et al.*, "Strategies for achieving high key rates in satellite-based QKD," *npj Quantum Inf.*, vol. 7, no. 1, p. 5, Jan. 2021.
- [4] D. Dequal *et al.*, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Inf.*, vol. 7, no. 1, p. 3, Jan. 2021.
- [5] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, no. 1, p. 30, 2017.
- [6] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, Dec. 2009.
- [7] Qiskit, "Qiskit," <https://qiskit.org/>.
- [8] M. H. Saeed, H. Sattar, M. H. Durad, and Z. Haider, "Implementation of QKD BB84 Protocol in Qiskit," in *Proc. Int. Bhurban Conf. Appl. Sci. Technol.*, 2022, pp. 689–695.
- [9] A. Pathare, P. Patil, A. Pimple *et al.*, "Experimental analysis on the bb84 quantum key distribution protocol using Qiskit and IBM quantum hardware," *TechRxiv*, Feb. 2025, preprint.
- [10] D. AL-Mubayedh, M. AL-Khalis, G. AL-Azman, M. AL-Abdali, M. Al Fosail, and N. Nagy, "Quantum cryptography on ibm qx," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6.
- [11] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, Jun. 2005.
- [12] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, Aug. 2003.
- [13] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, p. 012326, Jul. 2005.
- [14] P. V. Trinh *et al.*, "Statistical verifications and deep-learning predictions for satellite-to-ground quantum atmospheric channels," *Commun. Phys.*, vol. 5, p. 225, Sept. 2022.
- [15] Spectral Sciences Inc., "Modtran web app," [http://modtran.spectral.com/modtran\\_home](http://modtran.spectral.com/modtran_home), 2020.
- [16] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*. Bellingham, WA, USA: SPIE Press, 2005.
- [17] H. D. Le and A. T. Pham, "On the design of FSO-based satellite systems using incremental redundancy hybrid ARQ protocols with rate adaptation," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 463–477, Jan. 2022.
- [18] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *J. Light. Technol.*, vol. 25, no. 7, pp. 1702–1710, Jul. 2007.
- [19] R. Boluda-Ruiz, A. García-Zambrana, C. Castillo-Vázquez, and B. Castillo-Vázquez, "Novel approximation of misalignment fading modeled by beckmann distribution on free-space optical links," *Opt. Express*, vol. 24, no. 20, pp. 22 635–22 649, Sept. 2016.
- [20] I. Gradshteyn, I. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of integrals, series and products*. NY, USA: Academic Press, 2007.
- [21] A. Khanna, S. Majumder, A. Jain, and D. K. Singh, "Quantum BER estimation modelling and analysis for satellite-based quantum key distribution scenarios," *IET Quantum Commun.*, vol. 5, no. 2, pp. 157–163, Dec. 2023.
- [22] P. V. Trinh, S. Sugiura, C. Xu, and L. Hanzo, "Optical RISs improve the secret key rate of free-space QKD in HAP-to-UAV scenarios," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 8, pp. 2747–2764, Aug. 2025.