Analysis and Qiskit-based Simulation for QKD Satellite-to-Ground Systems with BB84 Protocol

Takihara Yudai, 1th year Master student
The University of Aizu

May. 21, 2025

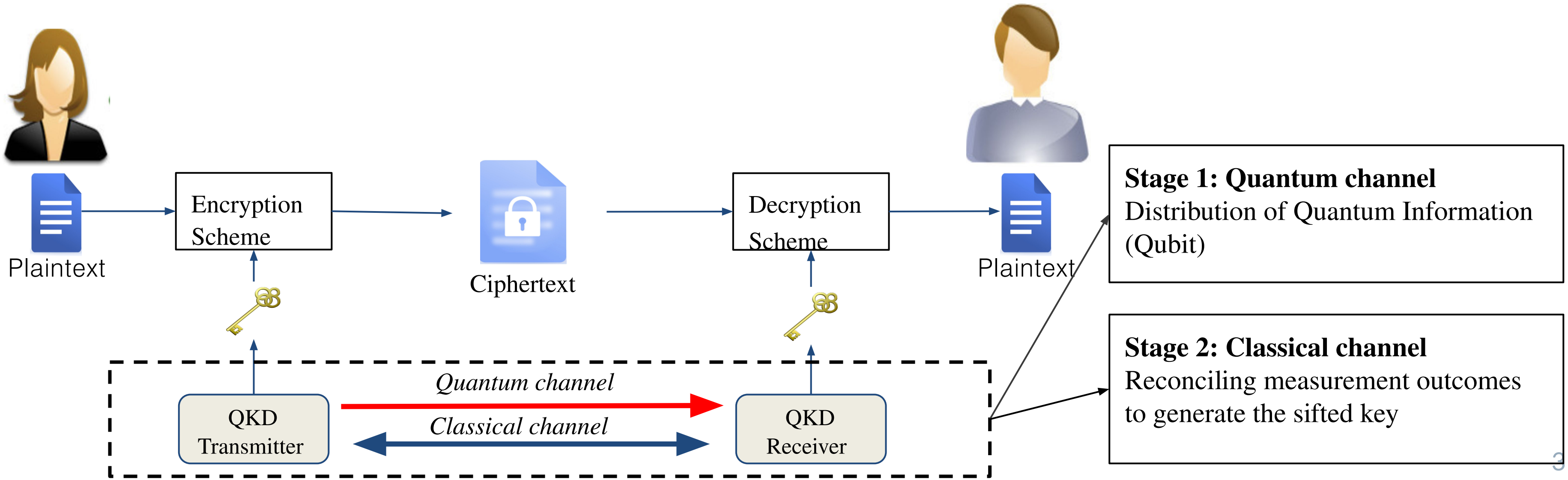
Outline

A I Z U
THE UNIVERSITY OF AIZU

- Quantum Key Distribution (QKD)
- Satellite-to-Ground QKD Systems
- Goals
- Our simulation framework based on Qiskit
- Performance Analysis
- Results
- Conclusion

Quantum Key Distribution (QKD)

- QKD is a promising method to ***distribute secure keys*** secretly between legitimate users
  - It bases on the laws of quantum physics.
  - First QKD protocol proposed by C. Bennett and G. Brassard in 1984, i.e., ***BB84 Protocol***
  - Some of best-known Japanese companies have been working on various QKD projects, e.g., Toshiba, NEC, and NTT



Satellite-to-Ground QKD Systems : Motivation

QKD can be implemented through <u>*terrestrial networks*</u> or <u>*satellite (non-terrestrial) platforms*</u>.

Conventional QKD systems mainly rely on optical fibers

>> Inflexible for mobile users and limited in transmission distance …

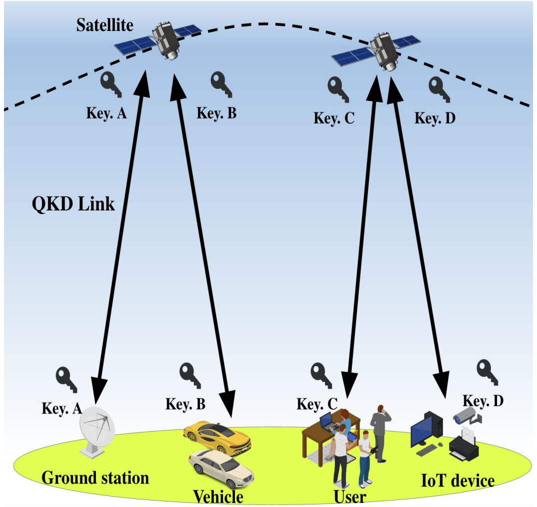
Challenge:

Limited support for global QKD services and scalable networks, particularly for mobile users

Solution:

Use satellite-based approaches for QKD systems, which offer flexible deployment and can cover wide geographic areas.

>> Enables support for applications such as mobile users and devices (e.g., self-driving cars) by providing secure communication by QKD.



Our Goals

1. Design a quantum channel for communication between a LEO (Low Earth Orbit) satellite and a ground station
   a. Make a transmittance model that accounts for various effects, such as beam misalignment and atmospheric turbulence.

2. Investigate the performance of channel model by applying a QKD protocol developed with Qiskit.
   a. *IBM Quantum Experience (IQX)* is used to implement *BB84* protocol using Qiskit.
   b. Simulations are conducted using *Starlink LEO satellite* date

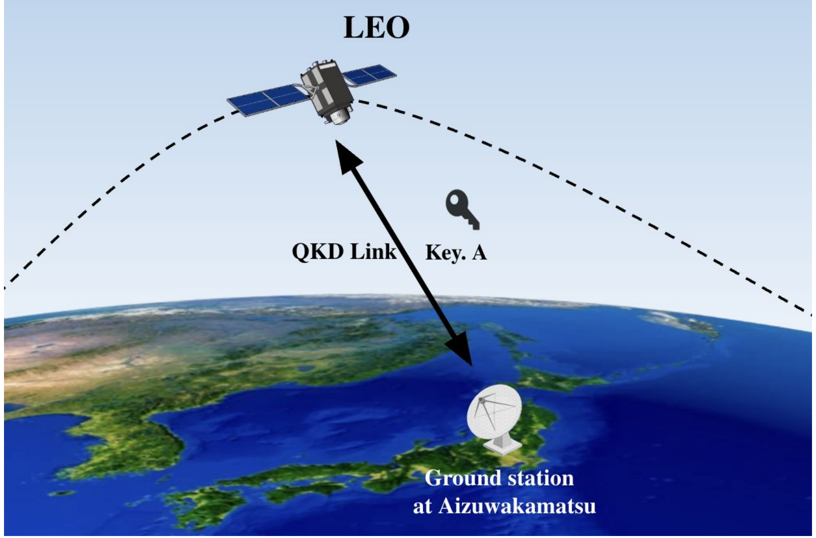
Our System Implementation

Our scenario:
P2P communication between LEO and ground station

1. LEO satellite transmits photons to Ground station(GS).
2. GS detect the photons, then create secret key.

QKD Protocol:

- Our system implements ***BB84*** QKD Protocol based on ***Qiskit***.
- Qiskit is a Python SDK developed by IBM that helps build QKD application, and is available on *IQX*



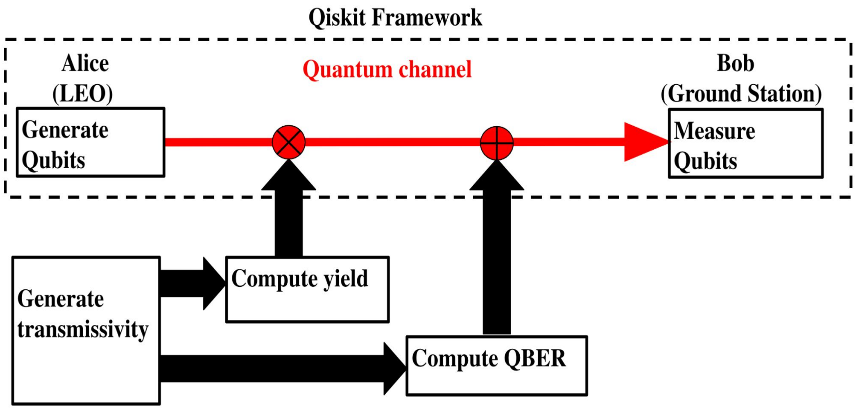
Qur Simulation Framework based on Qiskit

To investigate the performance of QKD system, a framework for simulation is built using Qiskit.

- ➢ Alice generate the Qubits and Bob measures them.

Integration of the channel model with the framework

1. Generate the transmittance of a quantum channel in a LEO satellite-to-ground link
2. Compute yield
   a. Measure probability of a detection given conditions of transmittance
3. Compute *Quantum Bit Error Rate(QBER)*
   a. Estimate the ratio of erroneous bits among detected signals at receiver based on the yield



- ➢ **These steps allow us to evaluate the performance and reliability of satellite-based quantum communication within the Qiskit framework.**

Quantum channel model

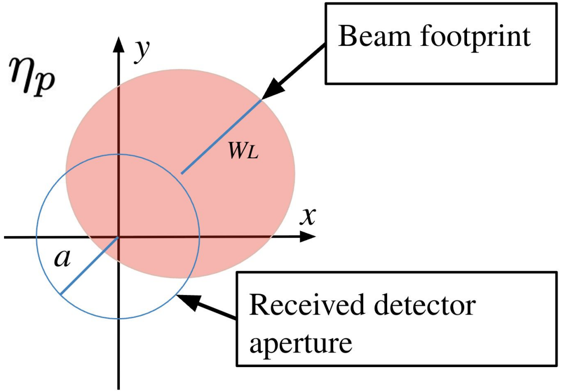
The transmittance of the quantum channel in the LEO satellite-to-ground link, taking into account the some impairments, is derived as follows.

$$\eta = \eta_\ell I_\mathrm{a} \eta_\mathrm{p}$$

η_ℓ: atmospheric attenuation due to absorption and scattering
I_a: random intensity fluctuations caused by atmospheric turbulence
η_p: fluctuating received power fraction at a aperture due to pointing errors and beam divergence

$$\eta_\ell = \tau_{\mathrm{zen}}^{\sec(\theta_{\mathrm{zen}})}$$

Visibility (km)	τ_{zen}(=deterministic transmittance efficiency at zenith)
23	0.81
15	0.75
5	0.55



Performance Analysis(1): QBER

QBER, representing the mismatch probability between sifted keys, is expressed with respect to the transmittance η.

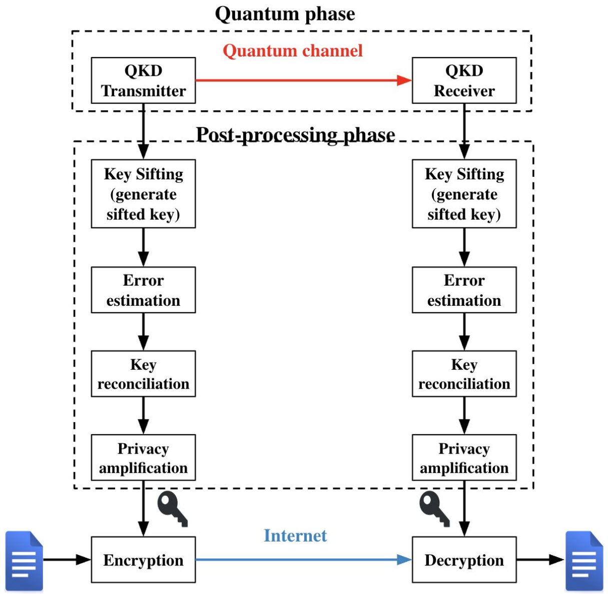
$$\overline{E}_\mu = \frac{\overline{EQ}_\mu}{\overline{Q}_\mu} = \frac{\int_0^\infty EQ_\mu(\eta) f(\eta)\,\mathrm{d}\eta}{\int_0^\infty Q_\mu(\eta) f(\eta)\,\mathrm{d}\eta}$$

$EQ_\mu(\eta)$: Conditional probability of erroneous detections per pulse, given a transmittance value η
$Q_\mu(\eta)$: Conditional probability of a detection event given the transmittance value η
$f(\eta)$: Probability density of the transmittance under atmospheric fading

Performance Analysis(2): Secret Key Rate

The SKR is defined as the average number of secret bits per second

$$\mathbf{SKR} \geq \mathcal{R}spd\left\{-\overline{Q}_{\mu} f H_2\left(\overline{E}_{\mu}\right) + \overline{Q}_1\left[1 - H_2\left(\overline{e}_1\right)\right]\right\}$$

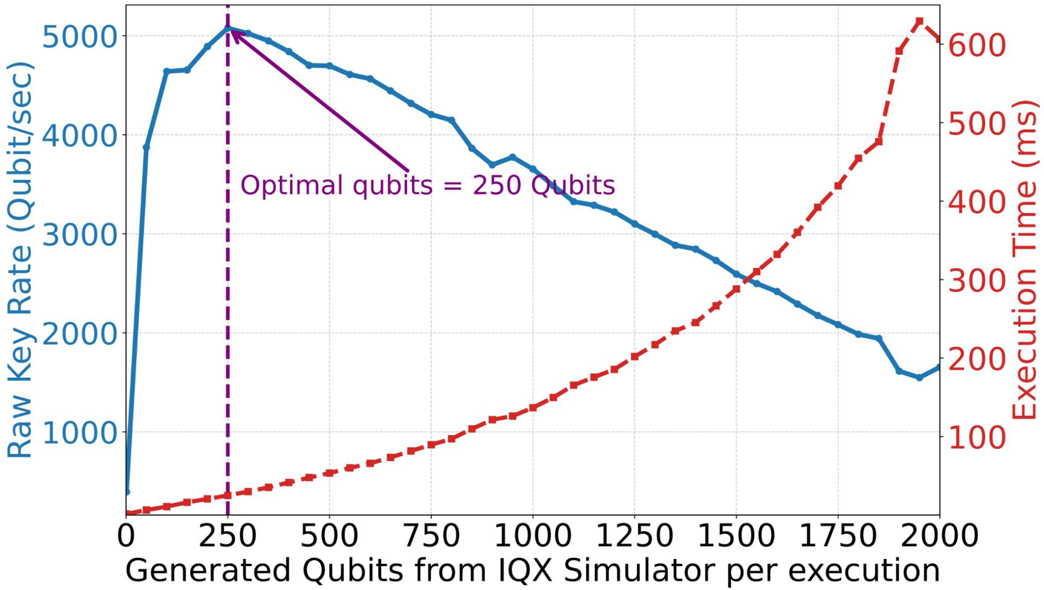


Symbol	Description
$\mathcal{R}$	Repetition rate (pulses per second)
s	Sifting coefficient; e.g., for BB84 protocol, $s = 0.5$
p	Parameter estimation coefficient
f	Key reconciliation efficiency
d	Fraction of bits remaining after the decoy-state method
H_2	Shannon's binary entropy function
$\overline{Q}_1$	Detection event probability of single-photon pulses
$\overline{e}_1$	Error rate of single-photon pulses

Numerical Result: Raw Key Rate

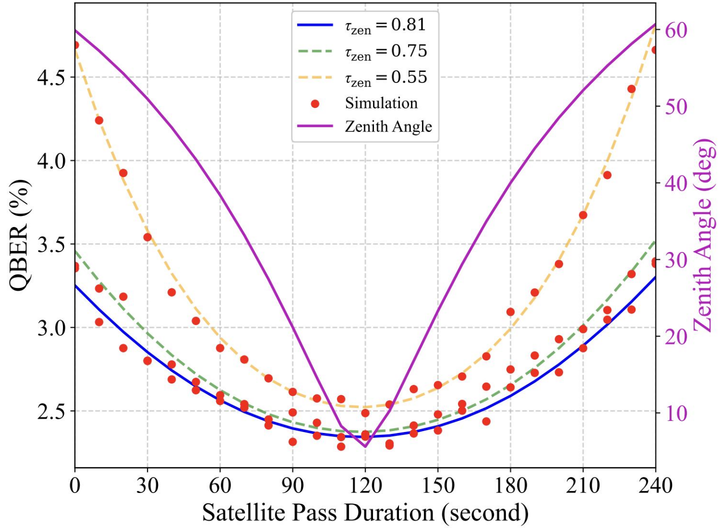
THE UNIVERSITY OF AIZU

Raw key rate is simulated by specifying the number of qubits (100–2000) generated per run on IBM Quantum Experience (IQX), and the corresponding runtime was also measured.



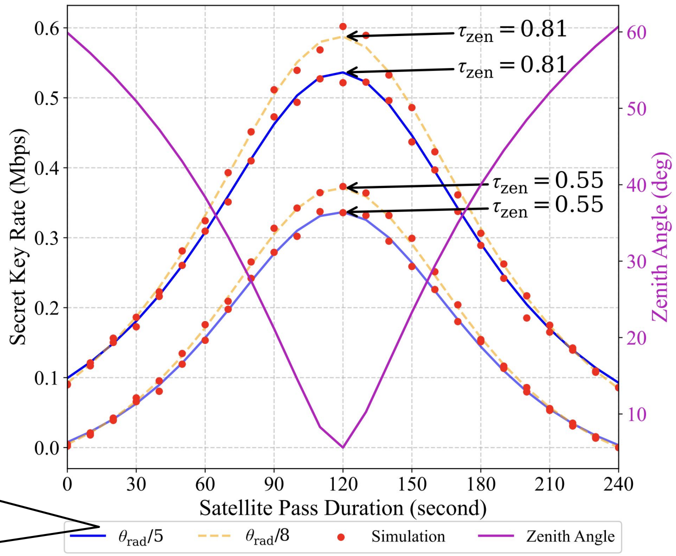
Numerical Result: QBER and Secret Key Rate

Results are analyzed under the impact of the effects of ***atmospheric attenuation***, ***turbulence-induced fading***, ***beam spreading loss, and misalignment***, using a Qiskit-based simulation to evaluate the QBER and Secret Key Rate.



QBER over the STARLINK-1293's pass duration with different deterministic transmittance efficiency.

standard deviation of horizontal and vertical beam angle-jitter



Secret Key Rate Simulation over STARLINK-1293’s Pass Duration under Varying Deterministic Transmittance Efficiencies and Beam Angle Jitter Standard Deviations

θ_{rad} : Half-divergence angle

Conclusion

THE UNIVERSITY OF AIZU

- We focused on and analysed the LEO satellite-ground-based QKD system.
- Using Qiskit, we built a simulation framework based on the BB84 protocol.
- A quantum channel model are designed and applied to the simulation framework
- The numerical results are given under the impact of the effects of atmospheric attenuation, turbulence-induced fading, beam spreading loss, and misalignment.

Thank you for your listening