Investigation of Satellite-Based Quantum Communication for FSO-QKD Systems in GEO-to-LEO Links

Takihara Yudai, 4th year Bachelor student
The University of Aizu

Feb. 26, 2025

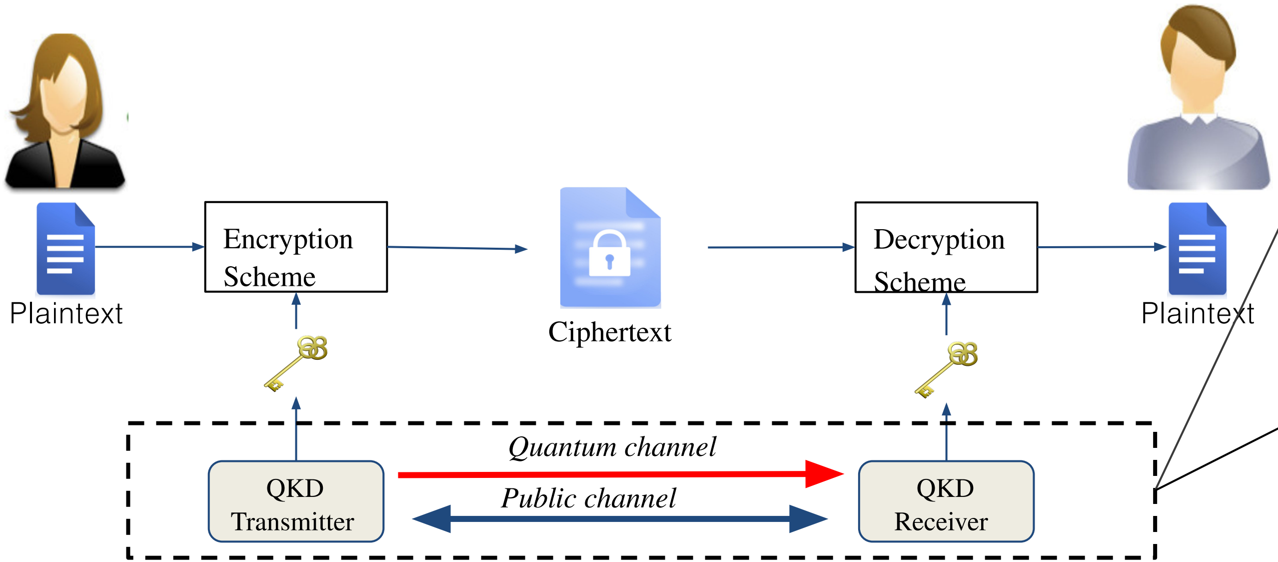
THE UNIVERSITY OF AIZU

Outline

- Introduction: QKD
- Why Is LEO-GEO Communication Essential for QKD?
- Photon Source
- Future works: Quantum channel loss

Introduction: QKD

- QKD is a promising method to ***distribute secure keys*** secretly between legitimate users
  - It bases on the laws of quantum physics
  - Some of best-known Japanese companies have been working on various QKD projects, e.g., Toshiba, NEC, and NTT
  - Toshiba has succeeded in building a QKD system for quantum communication at a distance of 600 km.[1]
    ([1]: https://www.nature.com/articles/s41566-021-00811-0)



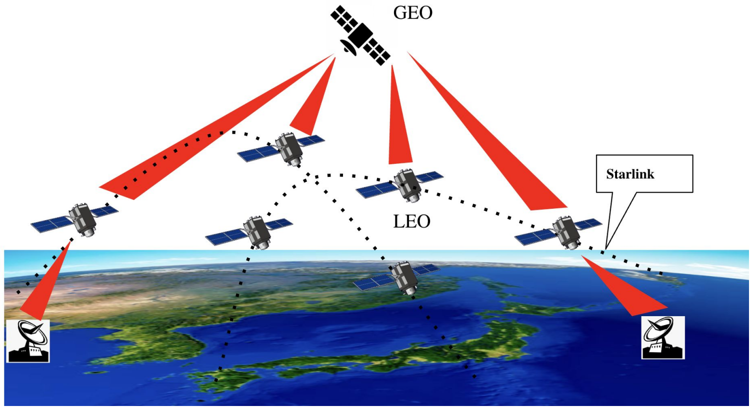
Stage1: Use Quantum channel
- Distribution of Qubit (Quantum state)
- Prevent information leakage and interception

Stage2: Use Public channel
- Comparing measurement methods to derived sifted key

Why Is LEO-GEO Communication Essential for QKD?

Major challenge of current QKD System

➢ The limitation of distance for secret key distribution in optical fiber communications



Solution: LEO-GEO satellite-based QKD offers a promising solution for long-distance key distribution.

➢ ***E.g., Starlink*** enables global internet coverage by using a constellation of LEO satellites.

Challenge for Satellite-based QKD

➢ Photon Source Generation Challenges

➢ Quantum Channel Loss on Long-Distance QKD

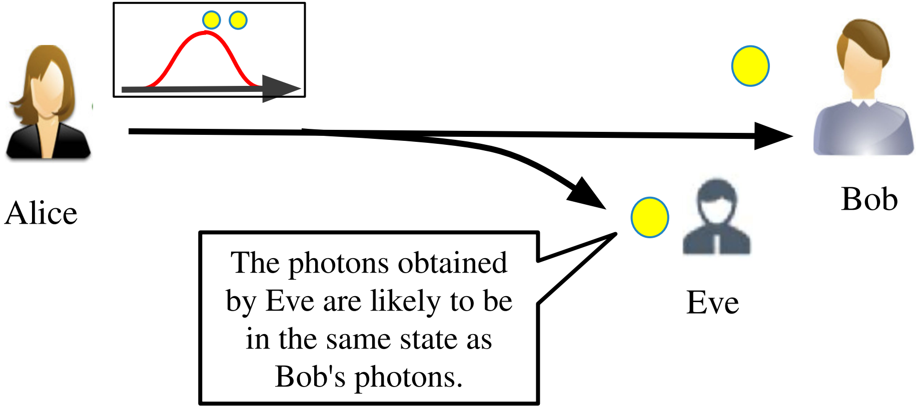
Photon Source(1)

QKD (e.g., BB84 and BBM92) protocol inherently assume a *Single Photon Source*.

- ➢ One pulse (a wave of electrical signals with a certain width) should contain **one photon**.

But, Non-zero probability of multiple photons in a single pulse (Multiphoton pluse)

- ➢ A **Photon Number Splitting** (**PNS**) attack could be exploited by Eve.



Reason for Non-detection

- Eve steal without disturbing Bob's the quantum state.

➢ To counter PNS attacks, a new method for generating photon sources is required.

Photon Source(2)

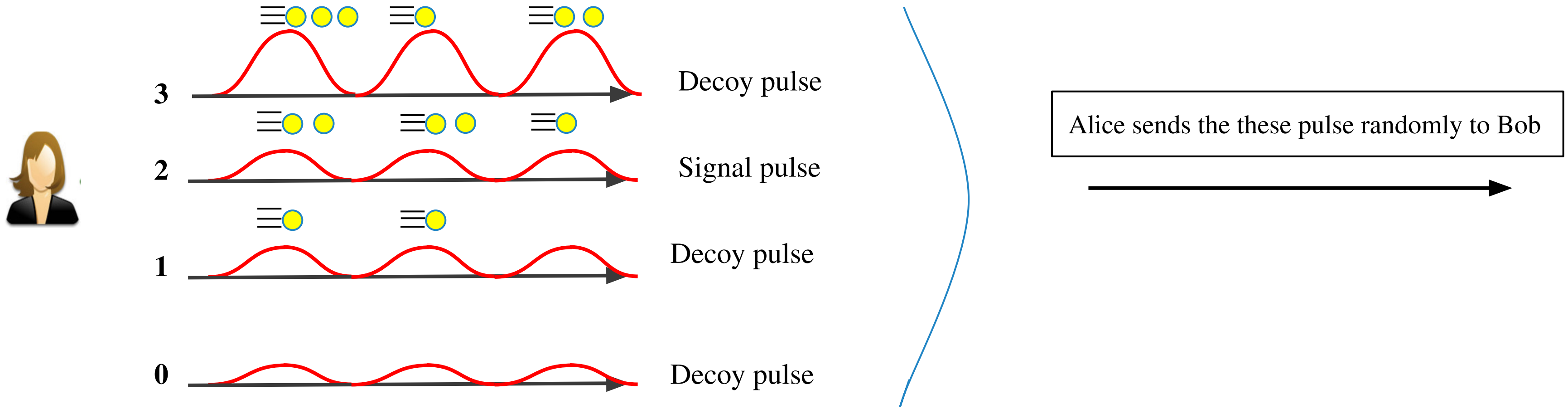
Solution:

Decoy State method: Method of transmitting a mixture of pulses with different photon numbers (decoy pulses).

➢ Eve cannot distinguish which pulses are real signal pulses, making it more difficult to attack.

How Decoy State method works:

1. Alice transmits a mixture of normal *signal pulses* and *decoy pulses*
   a. Signal pulses → normal light pulses for key generation
   b. Decoy pulses → dummy pulses of different intensity or number of photon



Photon Source

Solution:

Decoy State method: Method of transmitting a mixture of pulses with different photon numbers (decoy pulses).

- ➢ Eve cannot distinguish which pulses are real signal pulses, making it more difficult to attack.

How Decoy State method works:

2. Bob records the detection of each pulse from Alice and analyzes the statistics of the received pulses.
    a. Without Eve, the detection rate of signal and decoy pulses is close to a pre-designed theoretical ratio.
    b. If Eve has carried out a PNS attack, the ratio of the detection rate of decoy pulses to signal pulses collapses because the number of photons received by Bob changes.
    - ➢ Bob can detect anomalies.

The system mixes decoy pulses to make it easier to detect statistical discrepancies caused by Eve's PNS attacks.

Future work: Simulation for Quantum channel loss

- Modelling quantum channel losses in LEO-GEO long-distance QKD
  - Use the **Lossy Bosonic Channel** to correctly model ‘photon loss’
    (Lossy Bosonic Channel: a theory for modelling quantum communication using photons)

  - Transmissivity of lossy bosonic channels: **ηb** (**0 < ηb ≤ 1**)
    - **Percentage of photons that arrive at the receiver** through the channel.
  - The n probability distribution of the number of photons in the coherent state |μ⟩ follows a Poisson distribution:

$$P(n) = \frac{\mu^n e^{-\mu}}{n!}$$

μ: the average number of photons

  - If the input coherent state |μ⟩ passes through a channel with transmission η b, the average photon number at the output: $\mu' = \eta_b \mu$

    So, the probability distribution of n' is

$$P(n') = \frac{(\eta_b \mu)^{n'} e^{-\eta_b \mu}}{n'!}$$

Thank you for your listening