~The research progress~

Development of IQX-Based Satellite FSO-QKD Simulator

Takihara Yudai, 4th year Bachelor student
The University of Aizu
Supervisor: Prof. Anh T. Pham

Dec. 14, 2024

AIZU
THE UNIVERSITY OF AIZU

Outline

- **Research background**
  - QKD: Motivation
  - Development of QKD-based Chat app (Bachelor research)
  - Simulation QKD-based chat App

- **Scope of MS research**
  - Goal and Requirement
  - Why Satellite-based FSO/QKD?
  - Implementation of QKD: Scheme
  - The scheme for satellite-based FSO/QKD

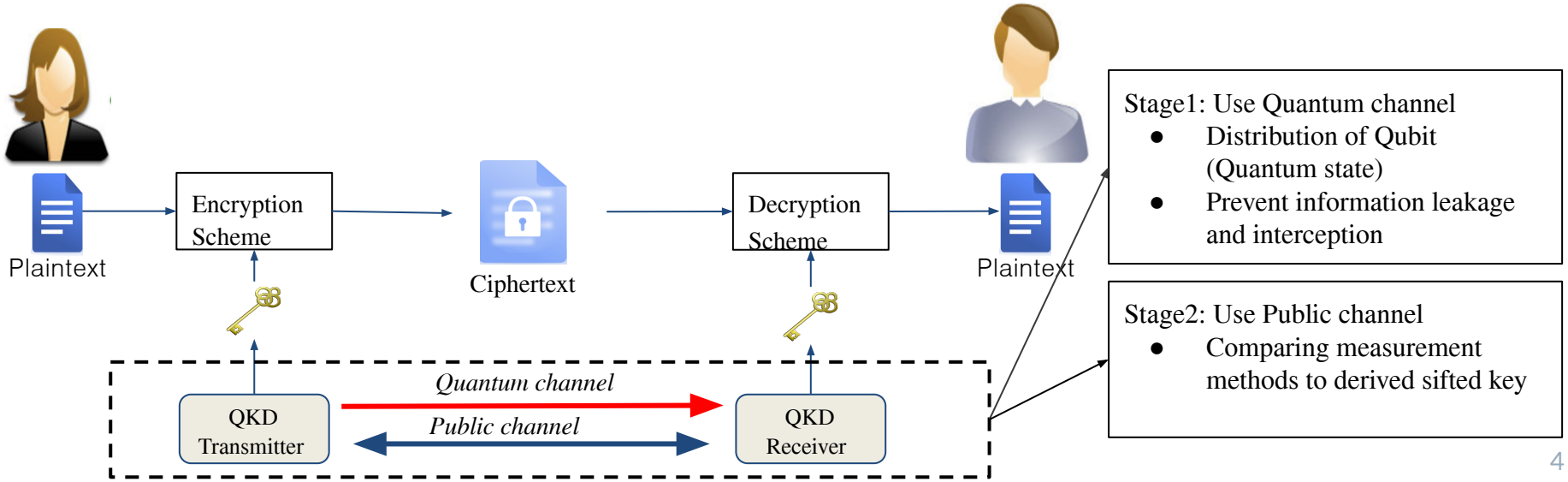
Outline

- **Research background**
  - QKD: Motivation
  - Development of QKD-based Chat app (Bachelor research)
  - Simulation QKD-based chat App

- **Scope of MS research**
  - Goal and Requirement
  - Why Satellite-based FSO/QKD?
  - Implementation of QKD: Scheme
  - The scheme for satellite-based FSO/QKD

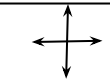
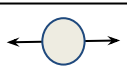
Quantum Key Distribution (QKD): Motivation

- 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



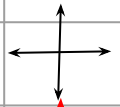
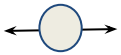
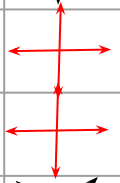
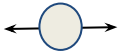
BB84 QKD Protocol

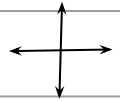
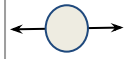
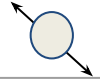
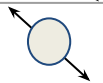
- BB84 uses photon polarization states to encode the bits of the key
- Each bit is encoded with a random polarization basis:  or 

Base \ Bit	0	1
		
		


Alice


Bob

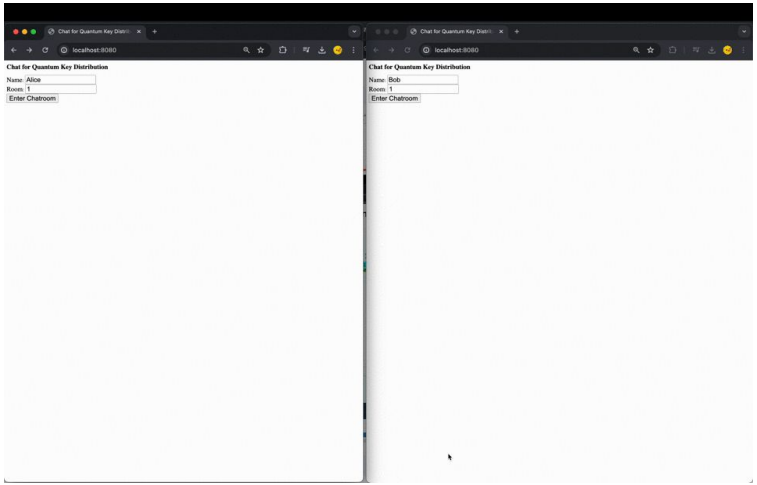
Bit	Base	Qubit State
0		
0		
1		
0		

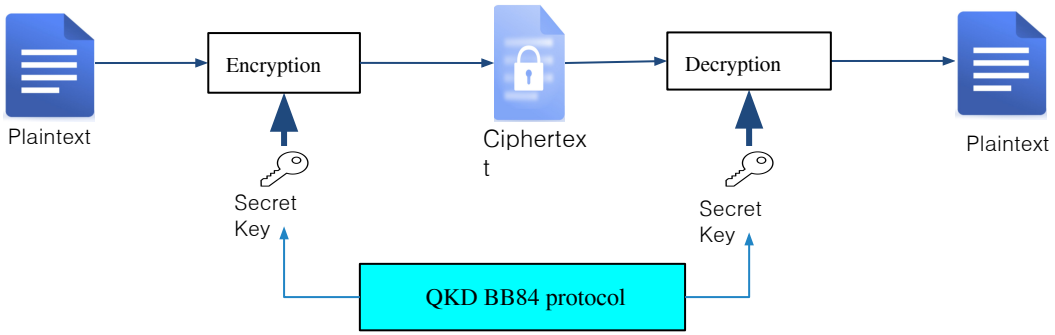
Base	Qubit State	outcome(bit)	sifted key
		0	0
		1	discard
		1	discard
		0	0

Development of QKD-based Chat Application(1)

Scope of BS research: To develop and simulate a secure Chat Application based on QKD

➢ ***The BB84 protocol*** can be applied for sharing secret keys between two legitimate users





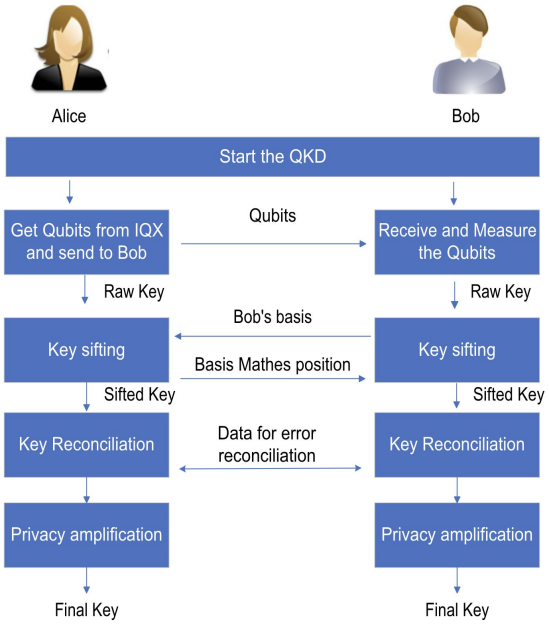
Develop and simulate Secure Chat Application using IBM Quantum Experience(IQX)

- IQX: an open platform offered by IBM and available for quantum computing services
- ***Qiskit***, open source SDK for quantum computing and support to develop and simulate application
  - Generate Qubit (the basic unit information for quantum computing)

Development of QKD-based Chat Application(2)

Conducted practical feasibility tests and simulations to evaluate the system's security.

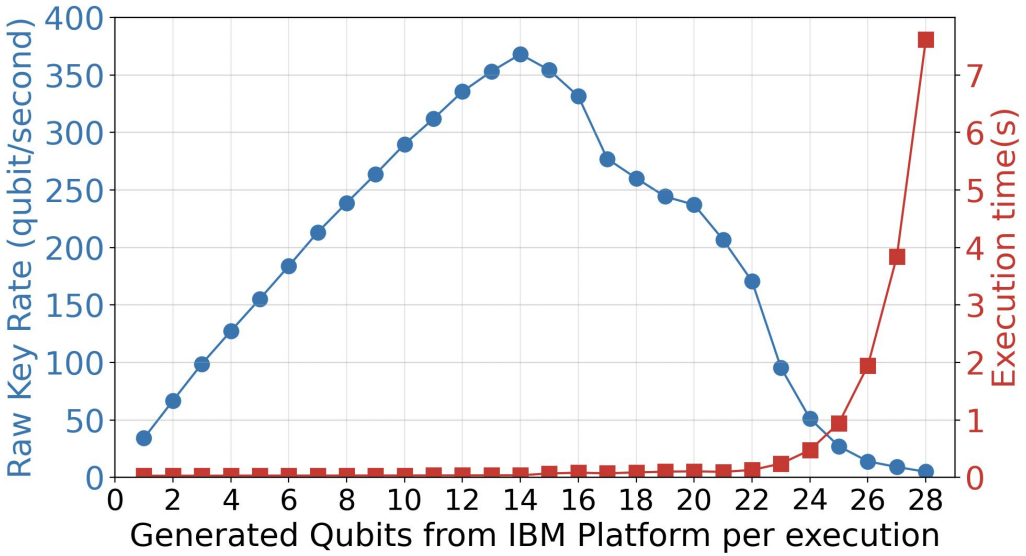
- **Raw key rate**
  - Find the number of qubits provided per second by IQX
- **Quantum Bit Error Rate(QBER)**
  - Calculated based on bit errors between Alice and Bob in the sifted key
  - Take account into intercept-and-resend attack (IRA) and quantum noise
- **Final key rate**
  - Use formula for final key rate based on the papers[1]



[1]: G. Bebrov, “On the (relation between) efficiency and secret key rate of qkd,” Scientific Reports, vol. 14, p. Article number: 3638, 2024

Simulation QKD-based chat App: Raw key rate

Raw key rate: How many Qubits are provided per second from IQX.

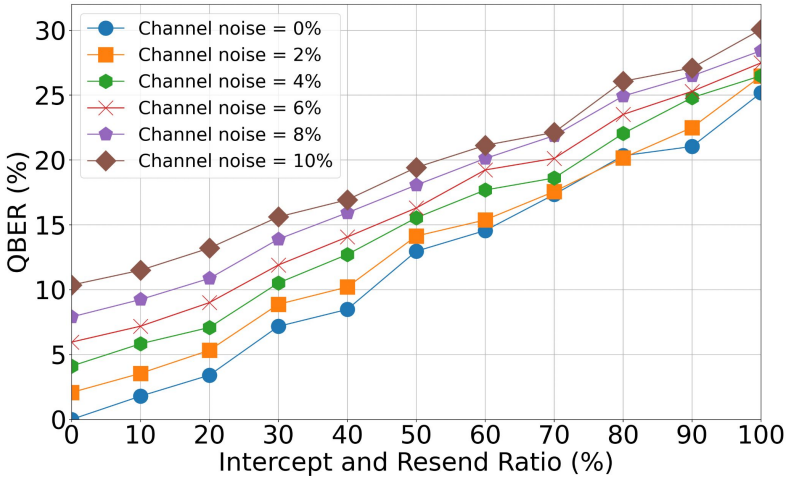


The highest raw key rate was found to be achieved with 14 qubits.

➢ Required key length can be generated in the shortest possible time.

Simulation QKD-based chat App: QBER

QBER: Calculated based on bit errors between Alice and Bob in the sifted key
>> Ratio of bit errors in sifted keys



- Increases with higher IRA ratios and channel noise frequencies, reflecting more bit errors in the sifted key between Alice and Bob.
- In an ideal BB84 QKD protocol without channel noise (0%), Alice and Bob measure a QBER of 25% under 100% eavesdropping. >> Same as theoretical rate.

Simulation QKD-based chat App: Final key rate

Final key rate: $R = c \times s \times p[H(A|E) - fH(A|B)]$

- Raw key rate
- Sifting coefficient (= 0.5 in case of BB84)
- Parameter estimation coefficient (0.75 ~ 0.9)
- The amount of information that Eve is uncertain about Alice's key after key reconciliation(KR) step

Notations

- $[H(A|E)]$ denotes the amount of information that Eve is uncertain about Alice's key after the sifting step.
- $[H(A|B)]$ denotes the theoretical amount of information that Alice and Bob need to exchange for KR, which is also the information leaked to Eve during the KR step.
- f is a is the efficiency of the error correction algorithm.

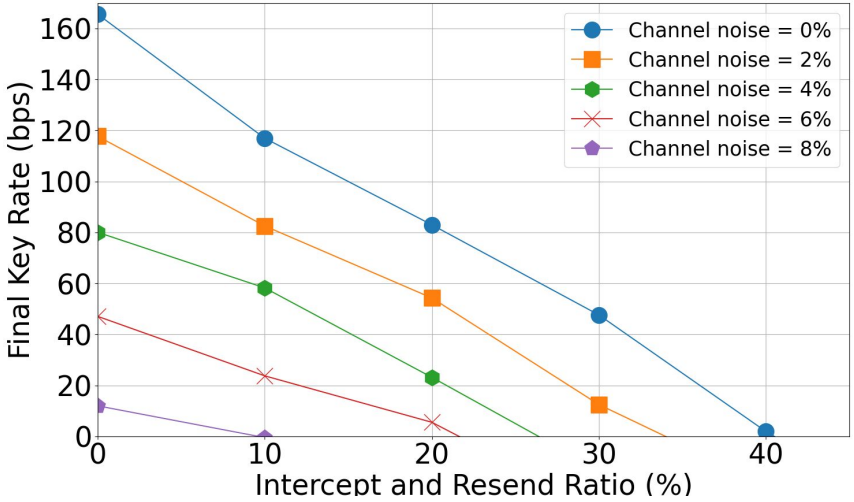
Remarks

- In the case of BB84, $H(A|E) = 1 - h(QBER)$, where is the binary entropy function: $H(A|B) = h(QBER)$

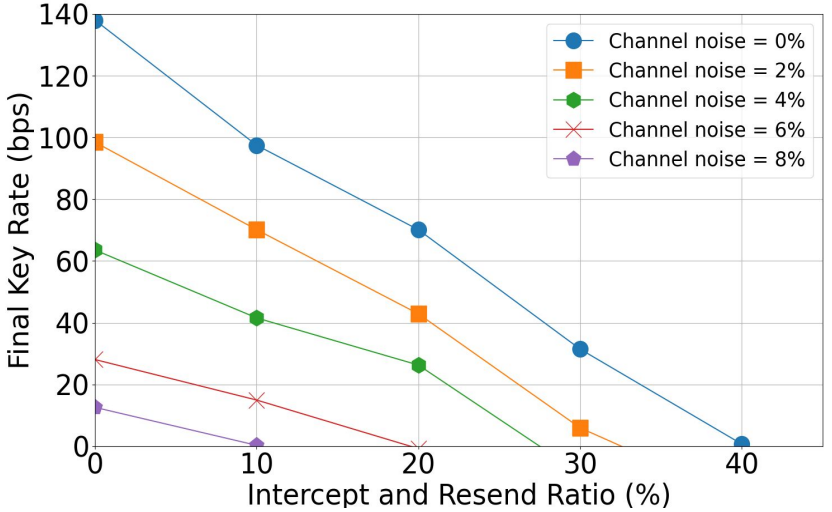
Simulation QKD-based chat App: Final key rate

Final key rate: $R = c \times s \times p[H(A|E) - fH(A|B)]$

Parameter	Value
c	368.0363931165903
p	0.9
s	0.5
f	1.22



Parameter	Value
c	368.0363931165903
p	0.75
s	0.5
f	1.22



The Final key rate falls as the Intercept and resend ratio and noise channel levels increase.

Conclusion

- ➢ We developed the secure chat application based on QKD
  - The implementation of the BB84 protocol utilizes the principles of quantum mechanics to guarantee the security of communications
  - IBM Quantum Experience (IQX) support that development and simulation the application

- ➢ We also conducted practical feasibility tests and simulations to evaluate the system's security.
  - *Raw key rate*: Find the number of qubits supplied by the IQX, where the required key length can be generated in the shortest possible time.
  - *QBER & Final key rate*: Similar behaviour to key generation with real QKD was observed with an increase in the intercept-resend attack ratio and the level of the noise channel.

But, for BS research,

- We don't consider the effect of quantum channel (e.g., optical fiber and Free Space Optics)
- We only focus on BB84 protocol >> Need to compare with other protocols (e.g, BBM92, E91)

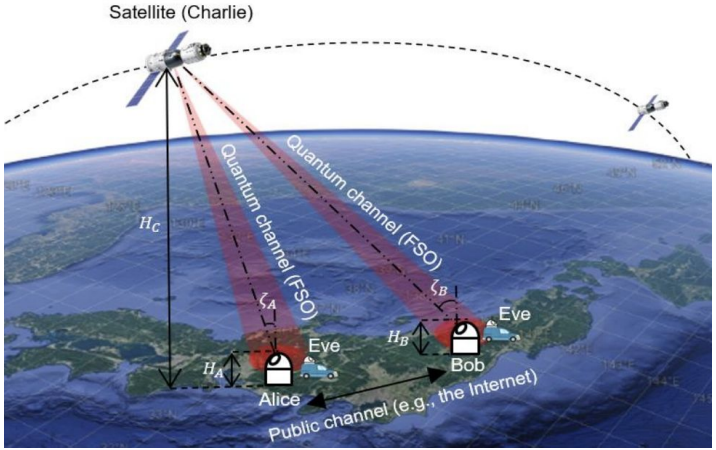
➢ As an extension for BS research, we will focu on these challenges as MS research.

Outline

- **Research background**
  - QKD: Motivation
  - Development of QKD-based Chat app (Bachelor research)
  - Simulation QKD-based chat App

- **Scope of MS research**
  - Goal and Requirement
  - Why Satellite-based FSO/QKD?
  - Implementation of QKD: Scheme
  - The scheme for satellite-based FSO/QKD

Goal and Requirement



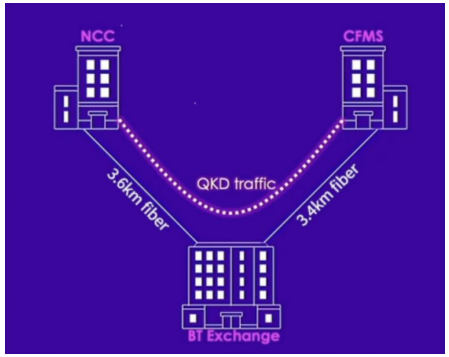
Goal: Developing a QKD Simulator using IQX

Requirement:

1. Develop satellite-based FSO/QKD system.
   a. Taking account into free-space channel conditions (e.g., free-space loss, background noise, atmospheric conditions) >> Implement using IQX
   b. Consider the distribution of keys from satellite to end-users, from satellite to satellites
2. Implement and compare the 3 QKD protocols, **BB84**, **BBM92** and **E91**.
   a. Build these simulator taking account into channel loss, FSO channel noise (build on Python)

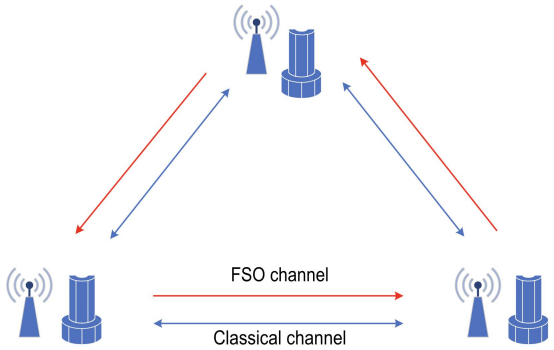
Why Satellite-based FSO/QKD?

Requirement 1: Develop satellite-based FSO/QKD system



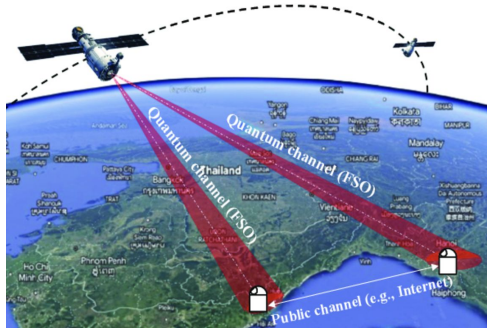
Optical fiber

- Common channel
- Available for only fixed user
- High cost



Terrestrial Free-space Optics (FSO)

- Wireless communication
- Flexibility & cost-effectiveness
- Obstructed by physical barriers such as tall buildings, trees, and other structures



Satellite-based FSO

- Wireless connection
- Covers wide-area communication possible

Optical fiber *and* ***Terrestrial Free-space Optics (FSO)*** *face notable challenges when it comes to spanning extensive geographical distances.*

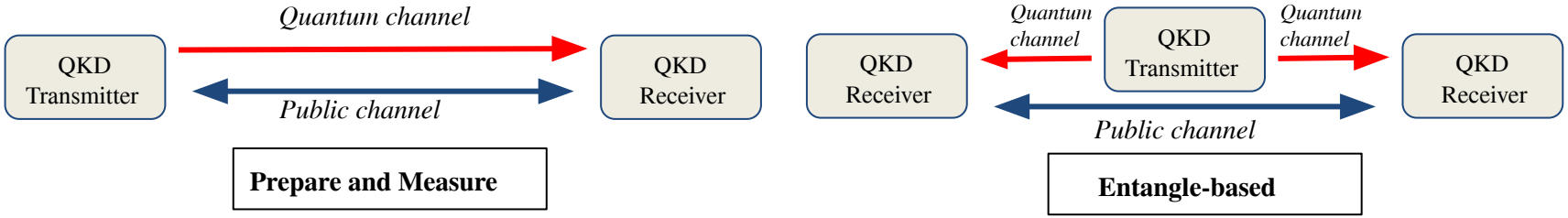
➢ Solution: Satellite-based FSO/QKD is enable the possibility the globalscale quantum networks for both fixed and mobile users

Implementation of QKD: Scheme

Requirement 2: Implement and compare the 3 QKD protocols, BB84, BBM92 and E91

- ***Prepare and Measure*:** Alice prepares a qubit in a certain state and sends it to Bob, Bob measures the qubit to determine its prepared state.
- ***Entangle-based* :** They uses photon pairs in a quantum entangled state and exploits the strong correlation of the measurement results to generate a secure key.
  - ***Entangled photon pairs* :** are pairs of photons that share a quantum state, exhibiting strong correlations regardless of the distance between them.

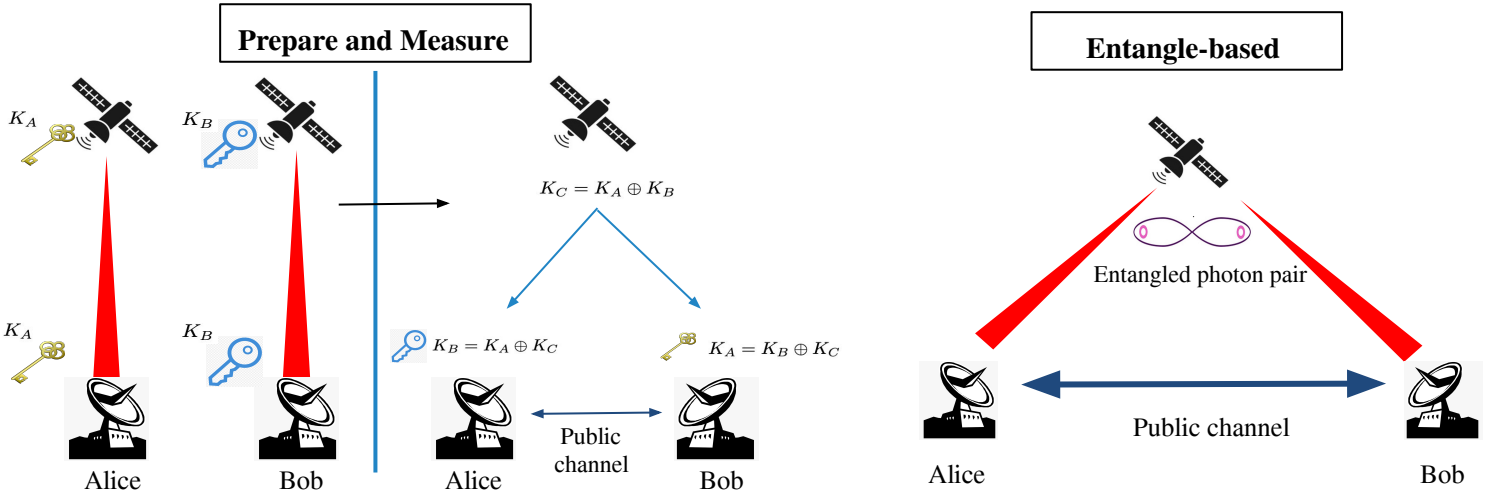
QKD Scheme	**Protocol**	**Quantum property**
Prepare and Measure	BB84	Single photon
Entangle-based	**BBM92, E91**	**Entangled photon**



The scheme for Satellite-based FSO/QKD

- **Prepare and Measure (PM) scheme:**
  - More than one phase is needed to distribute a key from Alice to Bob ultimately → **inefficiency**

- **Entangle-based scheme:**
  - Suitable for implementing a satellite-based FSO/QKD system
  - The satellite's trustworthiness requirements can be reduced compared to PM scheme



➢ We will focus on the development of simulator for satellite-based FSO/QKD utilizing these scheme.

Thank you for your listening