HAP-Assisted QKD for Secure IoT

Kaminaga Yuma
Computer Communication Laboratory, The University of Aizu

Outline

1. Introduction
2. System Model
3. Result

1. Introduction

IoT (Internet of Things) and Security Concern

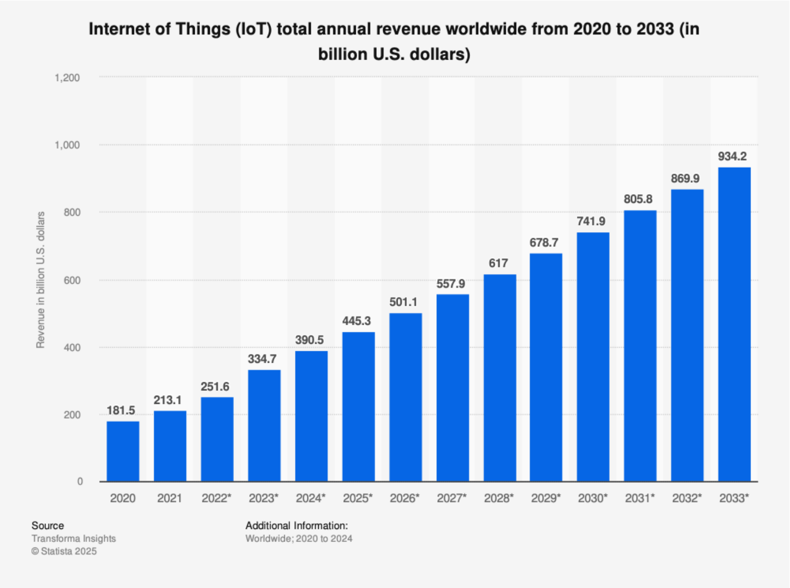
The IoT market is experiencing rapid growth

IoT Vulnerabilities:

- Diverse Operating Environments
- Resource Constraints

These characteristics can render conventional security approaches insufficient.
Also, Advancing quantum computers risk compromising current crypto (e.g., RSA).

→**New security technologies are needed, and QKD (Quantum Key Distribution) is attracting attention.**



Source: [1]

Possible Architecture : UAV-Assisted QKD

A proposed method from [2] applies QKD to IoT devices using UAV.

Key Delivery Mechanism:

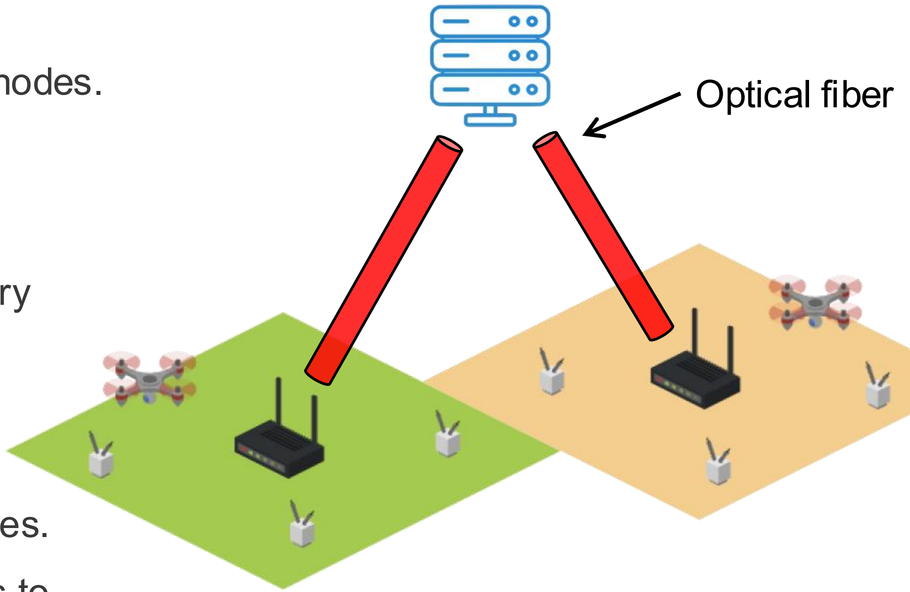
- Keys are generated between a server and gateway nodes.
- UAV physically deliver these keys to IoT devices.

Advantages:

- **Addresses Resource Constraints:** Physical delivery bypasses the resource limitations of IoT devices.

Disadvantages:

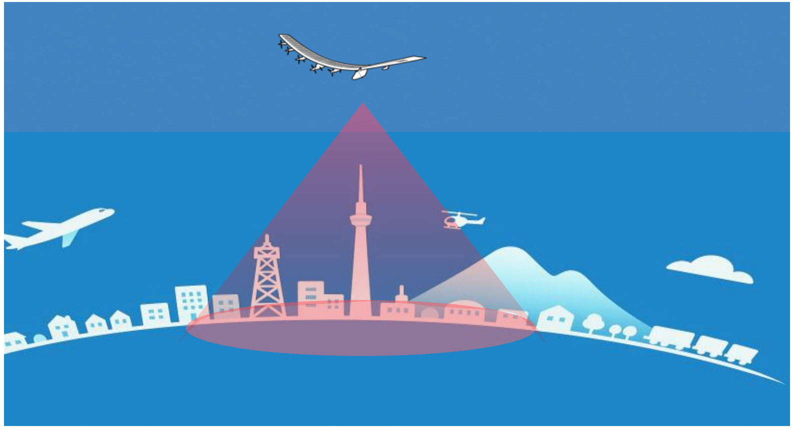
- **Optical Fiber Dependency:** Requires optical fiber deployment between the server and all gateway nodes.
- **Impractical for Remote Areas:** Laying optical fibers to remote locations (e.g., mountains, islands) is challenging and often not feasible.



HAP – Add QKD System

Proposed Architecture:

- **Server** ←→ **HAP** ←→ **Gateway Nodes** configuration.
- **Free-Space Optical (FSO) Links:** QKD is executed over FSO links between these elements.



Why HAP?

- **Alternative to Optical Fiber:** HAP replace the need for physical optical fiber links.
- **Addressing Remote Area Challenges:** Overcomes the impracticality of laying fibers in rural areas (e.g., mountains, islands).
- **Scalability for Gateways:** Eliminates the need for extensive fiber infrastructure to numerous gateways.

Motivation

- **Problem: Most of recent works for QKD over IoT networks have relied on optical fiber**
    - Not suitable (not flexible and cost effective) for global QKD networks and large-scale IoT networks
- **Possible Solution: using HAP-based FSO for QKD**
    - Advantage: can support for large-scale IoT networks, especially rural, oceanic, and remote areas
    - Low cost, flexible deployment
- **Research Questions:**

(1) How HAP-based FSO can provide QKD services for secure IoT Networks?

(2) What is the achievable secret key rate?

(3) What is an efficient QKD protocol to support multiple gateway nodes and massive IoT devices.

Goals

(1) Propose the architecture with HAP-based FSO for QKD in the context of secure IoT networks

- **HAP shares the key to multiple gateways via QKD (main focus for the conference)**
- Using UAV to relay the key between gateway to IoT devices (Future work)

(2) **Propose a simulation framework using Qskit-based IQX to evaluate the secret key rate as well as the QBER**

(3) Propose an efficient QKD protocols to support multiple users

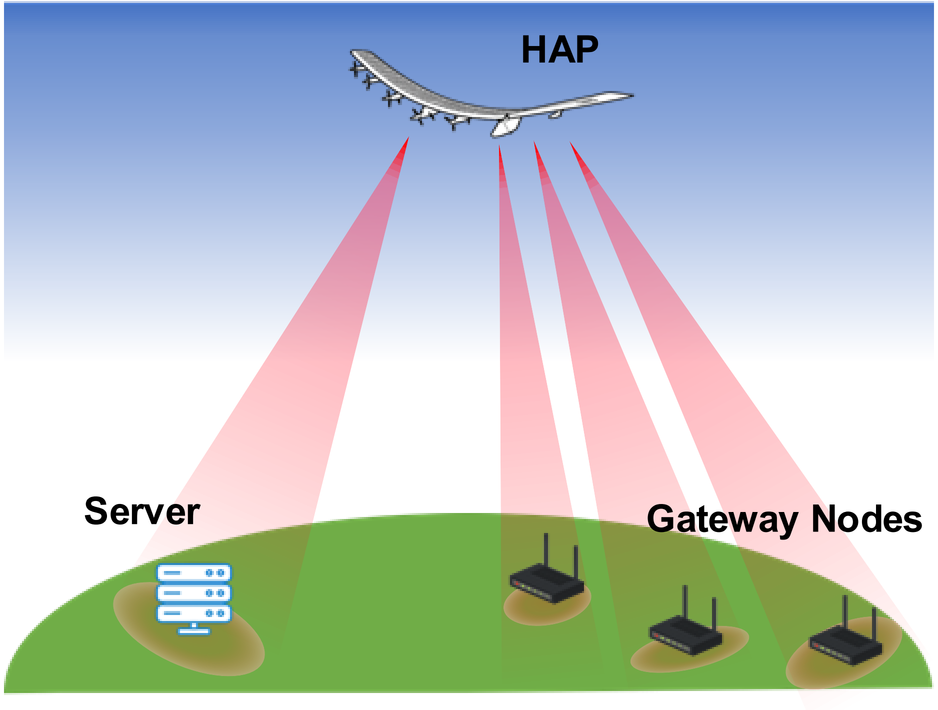
- **HAP to multiple gateways: QKD with TDMA**
- Gateways to multiple UAVs (Future work)

2. System Model

QKD Network Architecture

QKD Protocol: BBM92 for key generation and sharing.

Server: Network core for information management and overall operation.
HAP: Central for generating and distributing entangled photon pairs to the ground.
Gateway Nodes: Multiple regional nodes for secure communication with the server



BBM92 Protocol

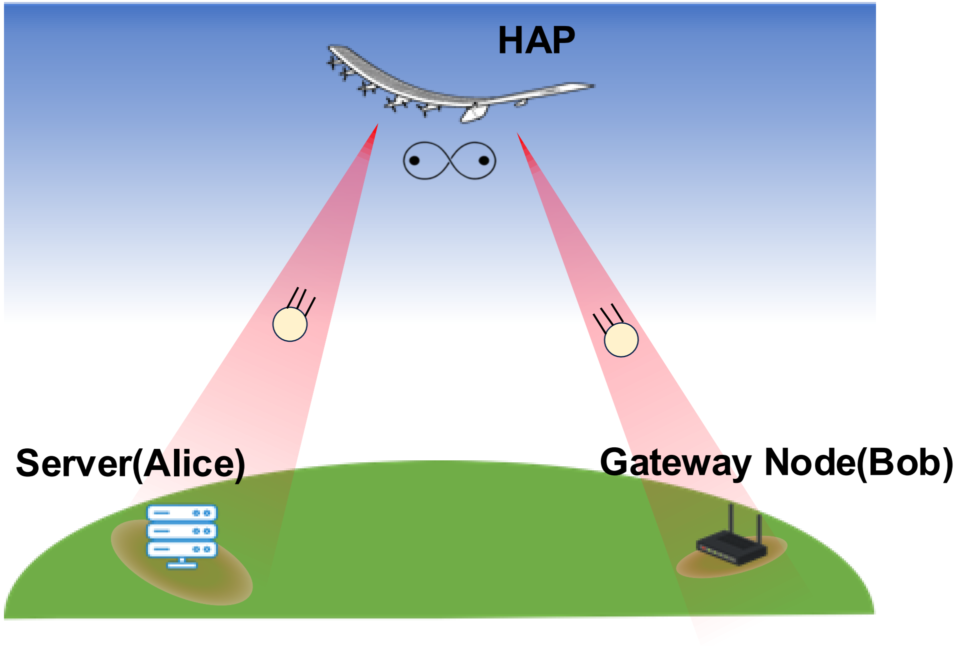
Leveraging Quantum Entanglement

The BBM92 protocol uses quantum entanglement for secure key generation.

Process:

- HAP generates entangled photon pairs.
- One photon sent to Server(Alice), the other to a Gateway Node(Bob).

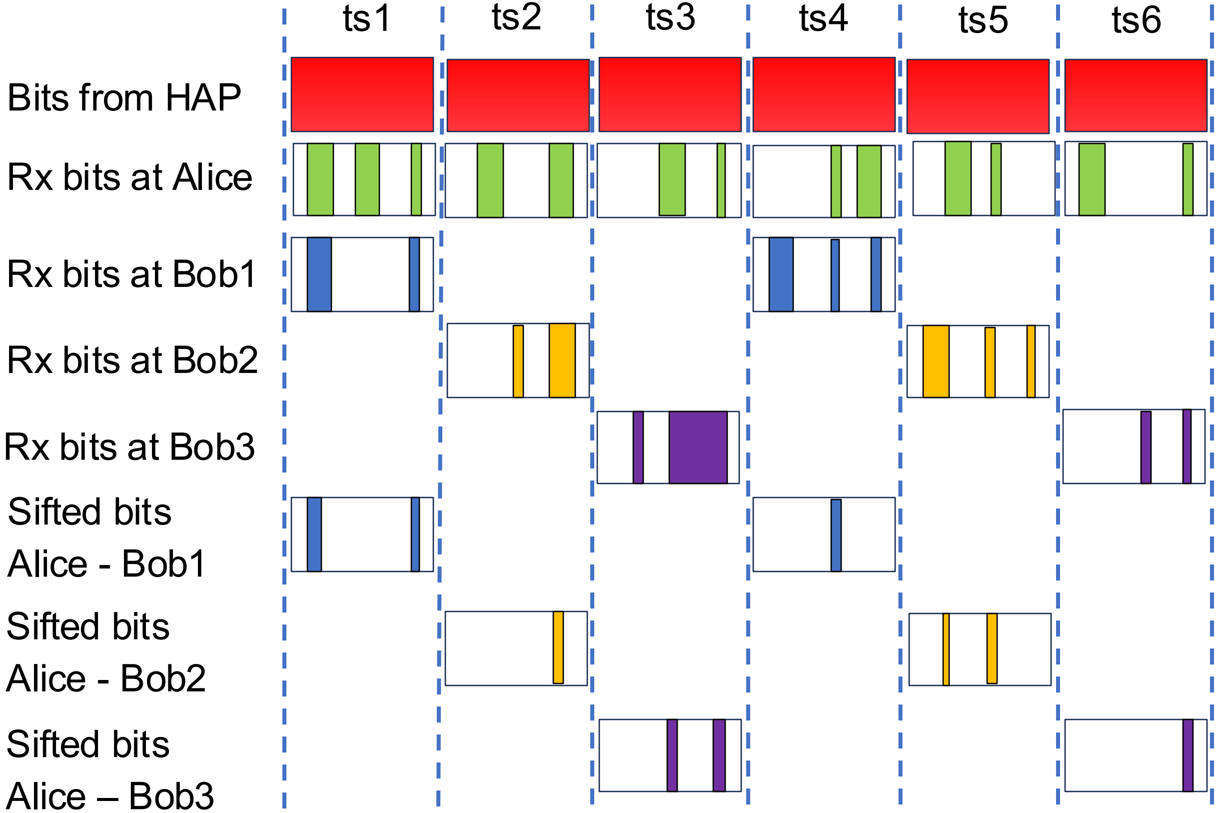
- Entangled photons have a strong correlation; measuring one instantly determines the other's state.
- If Alice and Bob measure their respective photons with the same basis, they obtain identical states, forming their shared secret key.



BBM92 protocol with TDMA (Time Division Multiple Access)

Developed with Qiskit

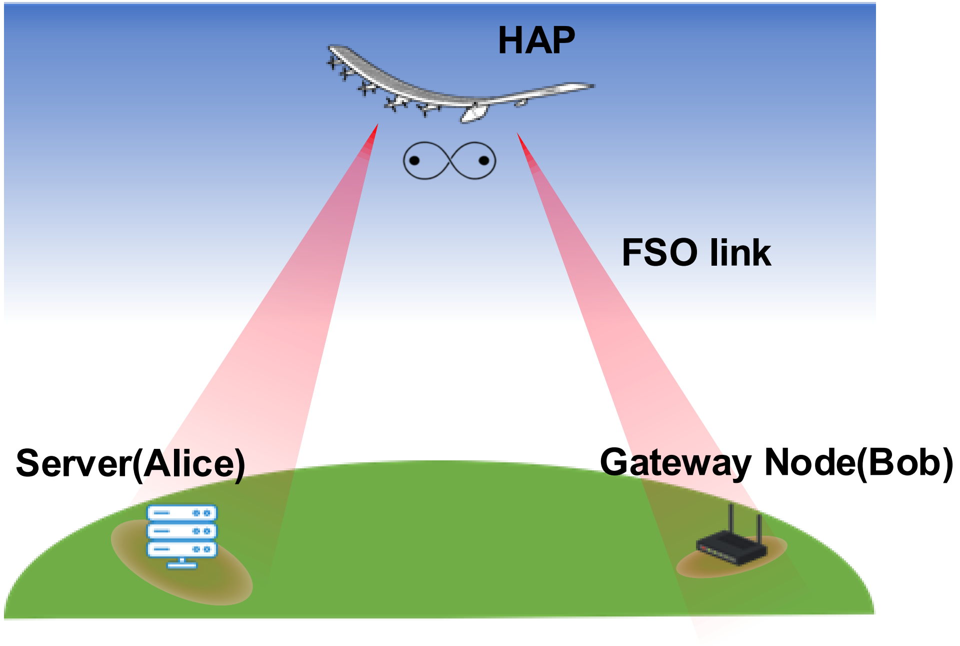
- Transmission from HAP
- Reception by Alice(Server) and each Bob(Gateway Node)
- Key generation for each time slot.



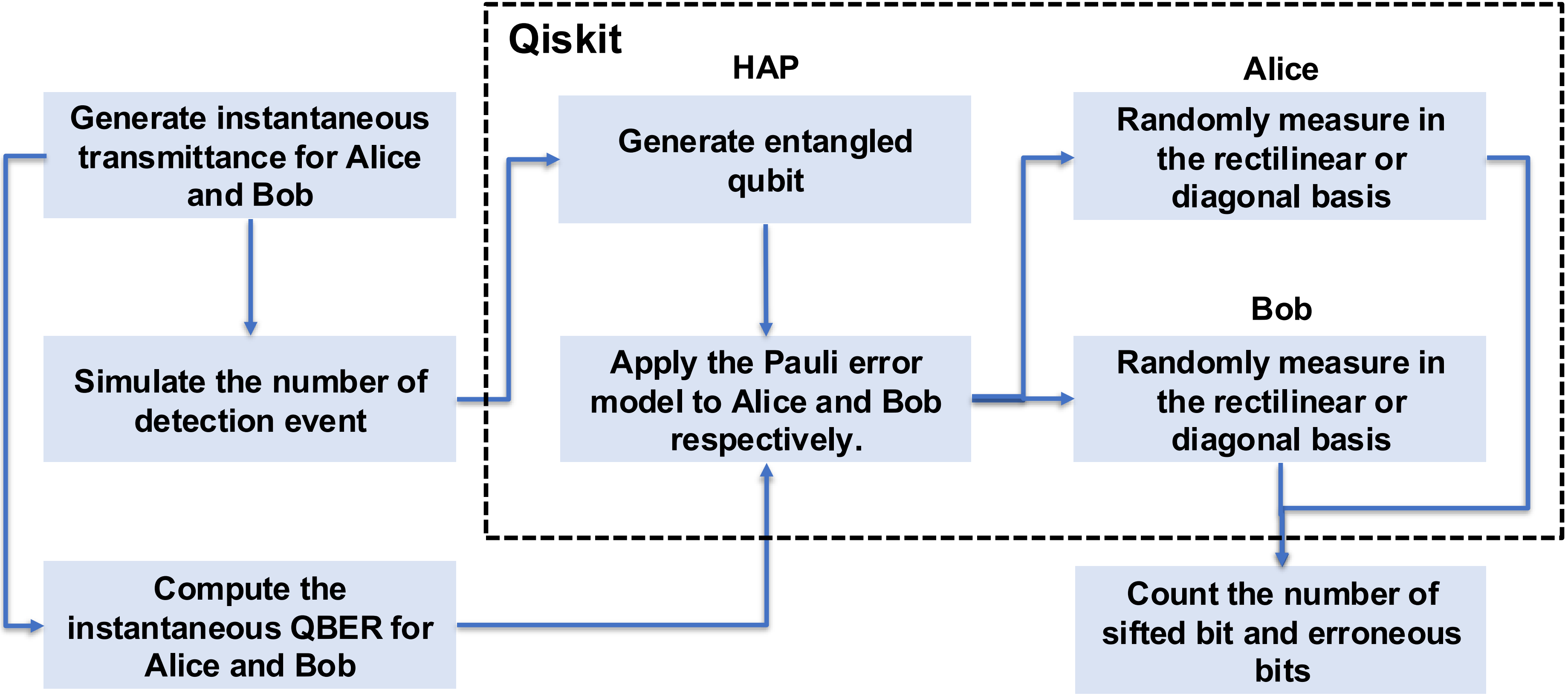
FSO link as Quantum Channel

Quantum channel model
The transmittance of FSO links takes the following three factors into consideration.

- **Atmospheric Attenuation**
- **Atmospheric Turbulence**
- **Beam Spreading Loss and Misalignment**

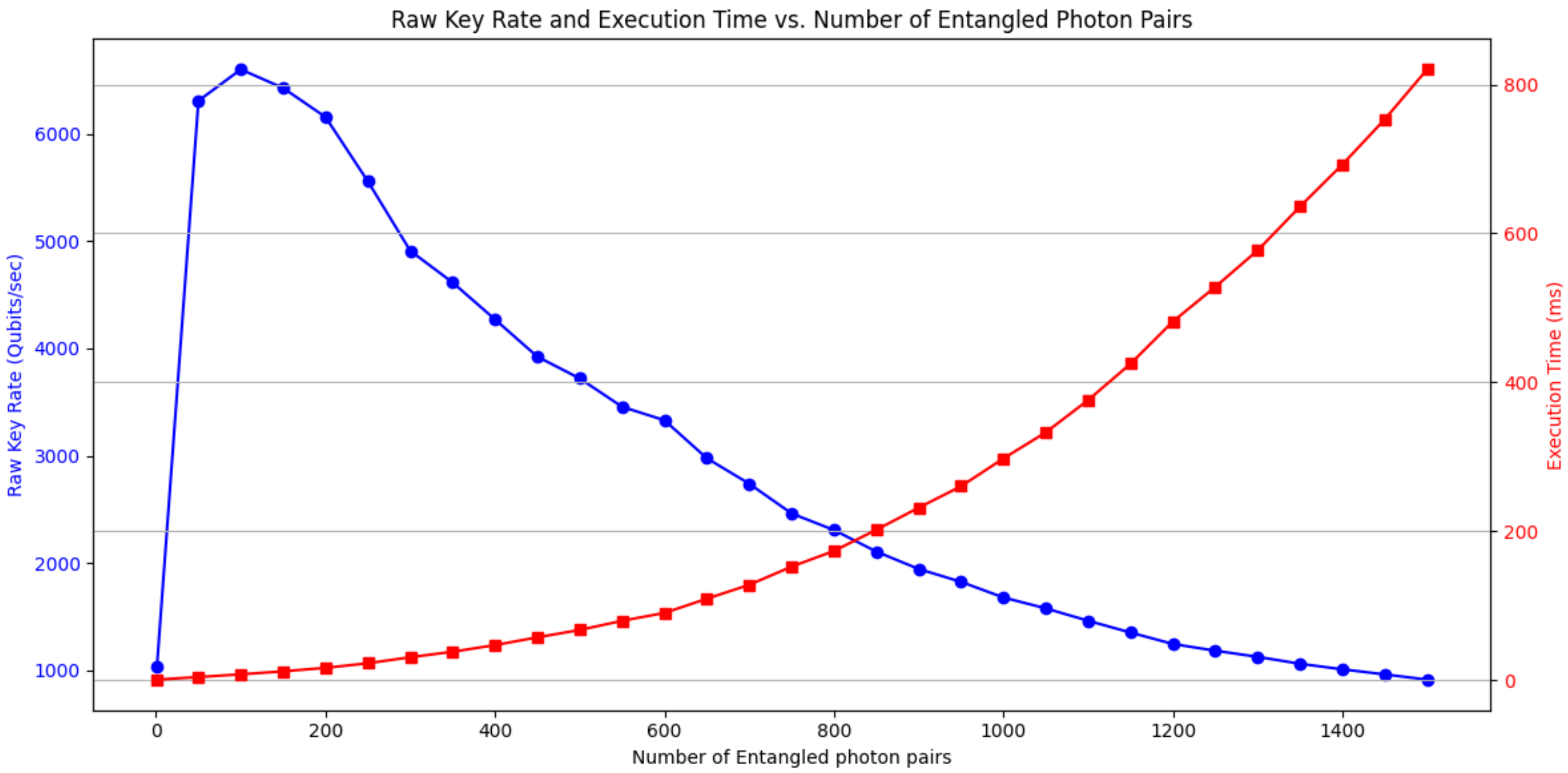


Flowchart of system model simulation



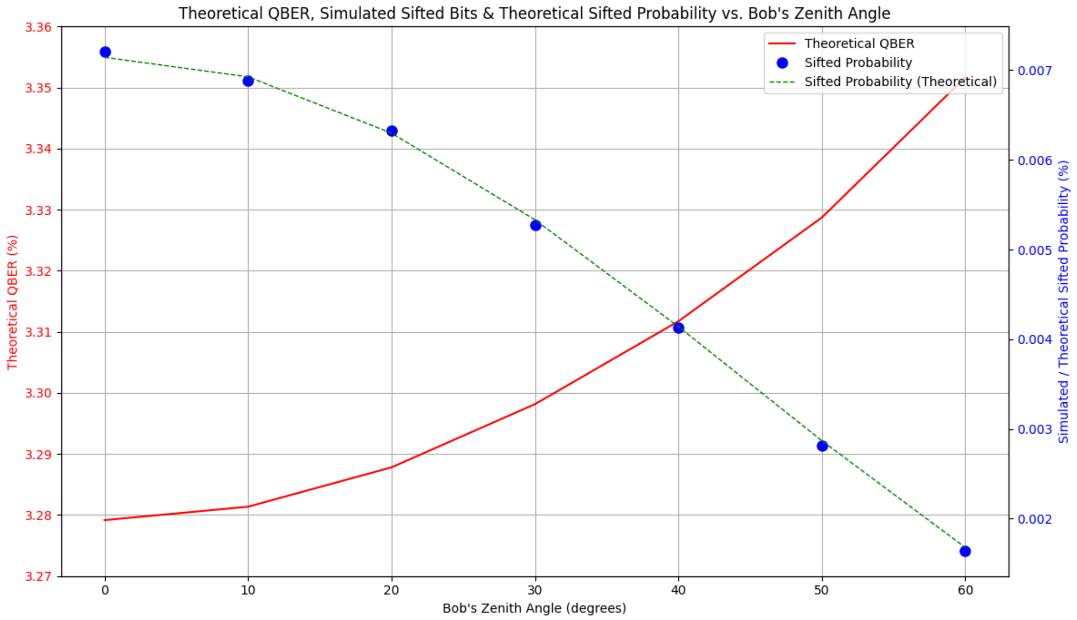
3. Result

Raw Key Rate and Execution Time from Qiskit



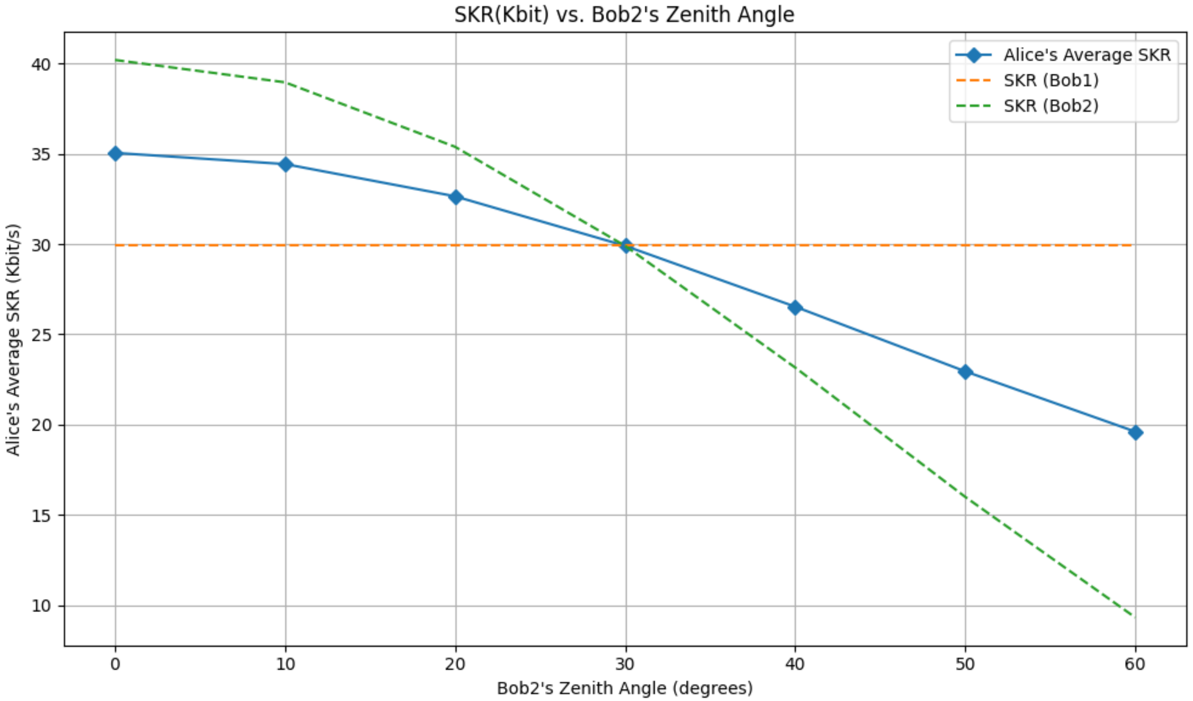
Theoretical result of QBER

Alice's position is at a zenith angle of 30°
Bob's position is at a zenith angle of 0° ~ 60°



Theoretical result of SKR for 2 Bobs

Alice's position is at a zenith angle of 30°
Bob1's position is at a zenith angle of 30°
Bob2's position is at a zenith angle of 0° ~ 60°



Reference

[1] : https://www.statista.com/statistics/1194709/iot-revenue-worldwide/

[2] : Kong, P.-Y. (2021). UAV-Assisted Quantum Key Distribution for Secure Communications With Resource Limited Devices. *IEEE Trans. Inf. Forensics Security*, 16, 3976–3988

Thank you for listening!