Development of QKD for IoT Networks

Kaminaga Yuma, Hoang D. Le , Anh T. Pham
Computer Communication Laboratory, The University of Aizu

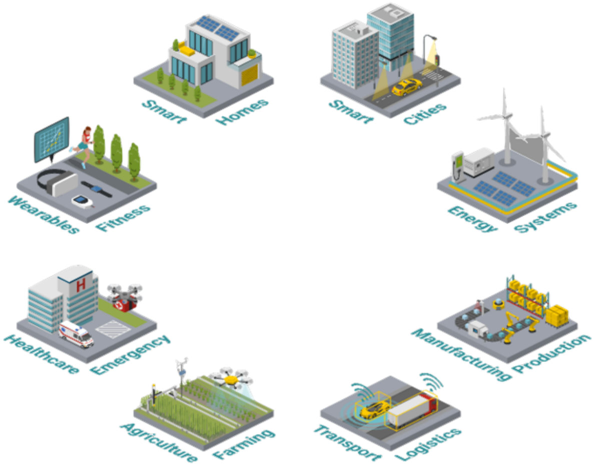
Outline

1. Research Background
2. Research Proposal
3. Research Progress

1. Research Background

IoT (Internet of Things) Network

- IoT refers to a system where various physical objects such as sensors, home appliances, and industrial equipment are interconnected via the Internet.
- IoT devices are no longer limited to computers, smartphones, or tablets. They also include televisions, digital cameras, smart speakers, household appliances, as well as sensors and actuators used in measurement and control systems.

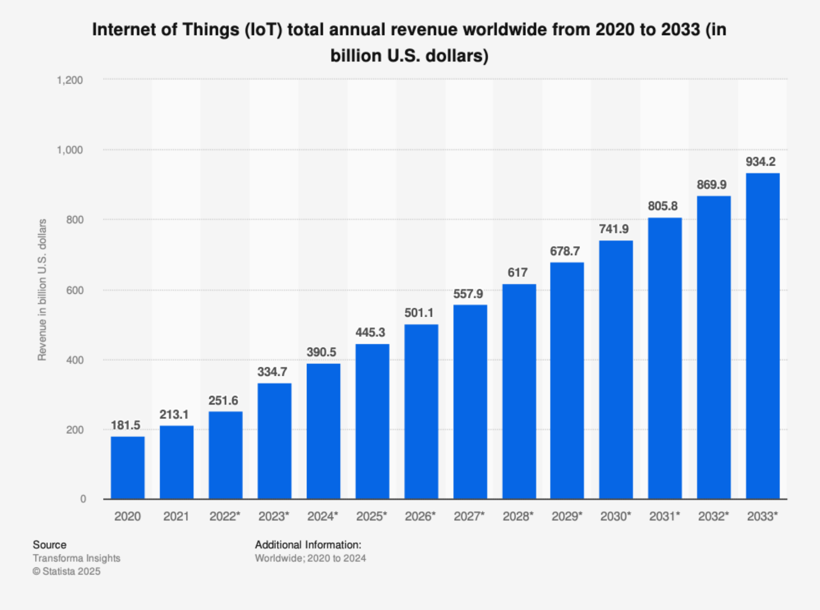


The spread of IoT and security issues

According to Statista, the global IoT market is valued at approximately USD 445.3 billion in 2025, and it is expected to grow to over USD 934 billion by 2033.The market revenue is projected to triple over the next 10 years, with the number of connected IoT devices worldwide also expected to triple during this period. [1]

Therefore, it is essential to protect these devices from malicious cyberattacks.

However, current public-key cryptography (such as RSA) may potentially be broken by future quantum computers. As a result, QKD (Quantum Key Distribution) is gaining significant attention as a next-generation security solution.



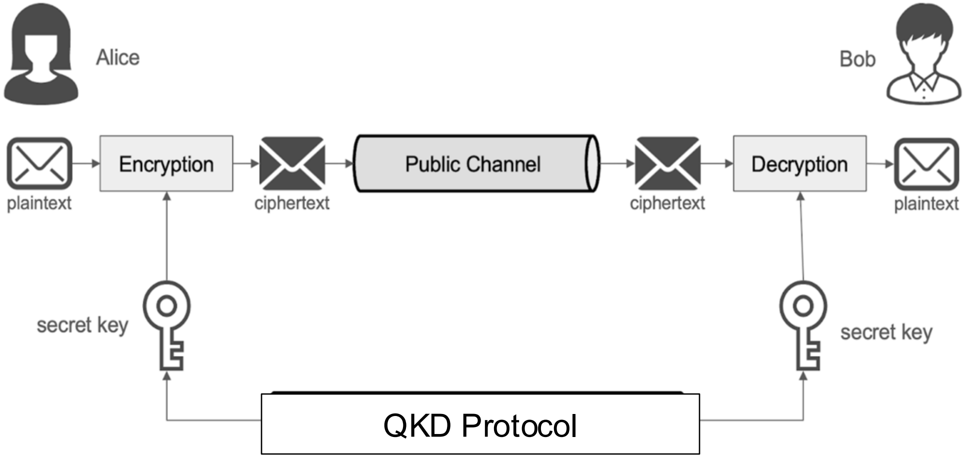
Internet of Things (IoT) total annual revenue worldwide from 2020 to 2033 (in billion U.S. dollars)

Source
Transforma Insights
© Statista 2025

Additional Information:
Worldwide; 2020 to 2024

QKD (Quantum Key Distribution)

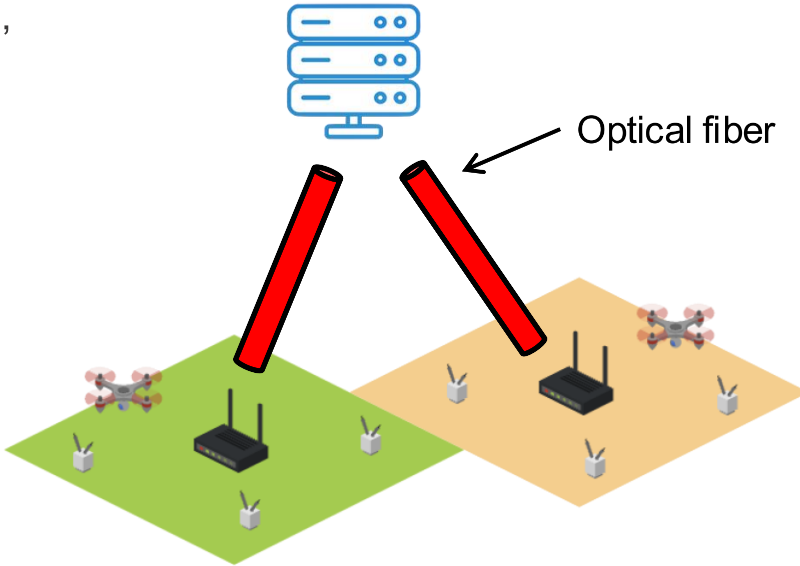
- QKD is a method of generating and sharing keys between two parties, based on the principles of quantum mechanics.
- Even if an eavesdropper attempts to intercept the key information, the quantum state of photons will be changed by the measurement process, allowing the legitimate parties to detect the presence of eavesdropping.



QKD for IoT

Challenges

- It is necessary to directly establish quantum channels (e.g., optical fiber) between each IoT device and the management center (central server or gateway node).
- In this case, each IoT device would need to be equipped with expensive quantum hardware (such as optical components), leading to high cost, power consumption and installation constraints.



→ In **the referenced paper** [2], keys generated using QKD between the central server and GNs are physically delivered to IoT devices using UAVs.

By using the distributed keys, IoT devices can securely communicate with the central server.

Motivation

- Optical fiber deployment is difficult in remote areas (such as islands or mountainous regions), making it technically and economically challenging to ensure continuous secure key distribution.
- By utilizing **HAP** (High Altitude Platform), it becomes possible to cover a wide area from the sky.
  → By establishing FSO links between HAP and GN, it enables geographically flexible and continuous secure key distribution, even to GNs in remote locations.

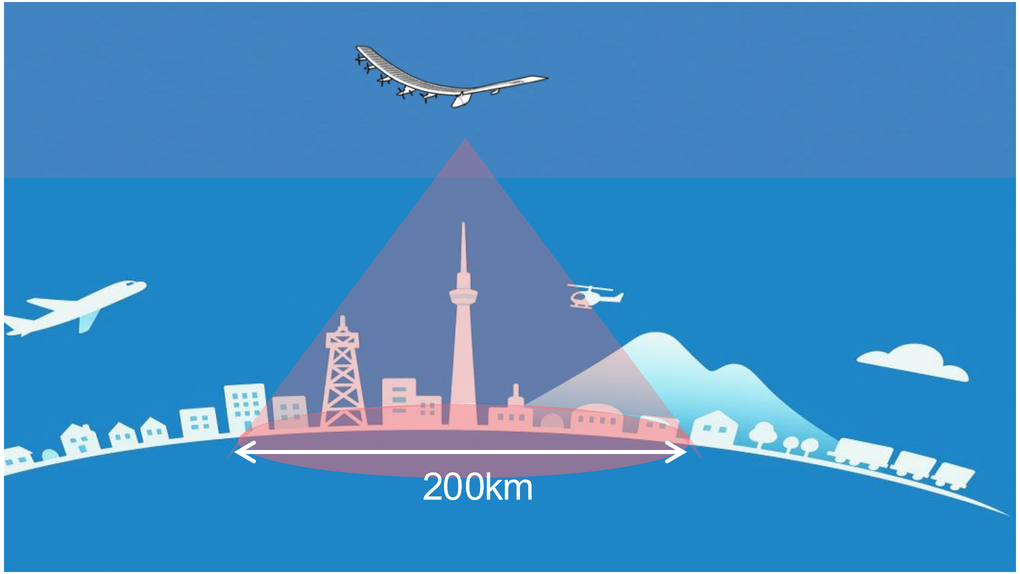
Compared to satellite-based solutions, HAP operates at much lower altitudes, enabling low-latency and mobile-direct communication with ground nodes.[3]

This characteristic makes HAP-assisted QKD a practical and flexible approach for secure key distribution in dynamic or hard-to-reach environments.

2. Research Proposal

HAP (High Altitude Platform)

- HAP is a communication platform located in the stratosphere.
- It can cover a communication area of up to 200 km in diameter, and is capable of providing stable Internet connectivity to regions where ground-based infrastructure is difficult to deploy, such as high-altitude areas, remote islands, mountainous regions, and developing countries. [3]



Proposed QKD network architecture

Using a HAP, quantum channels based on FSO (Free Space Optical) communication are established between:

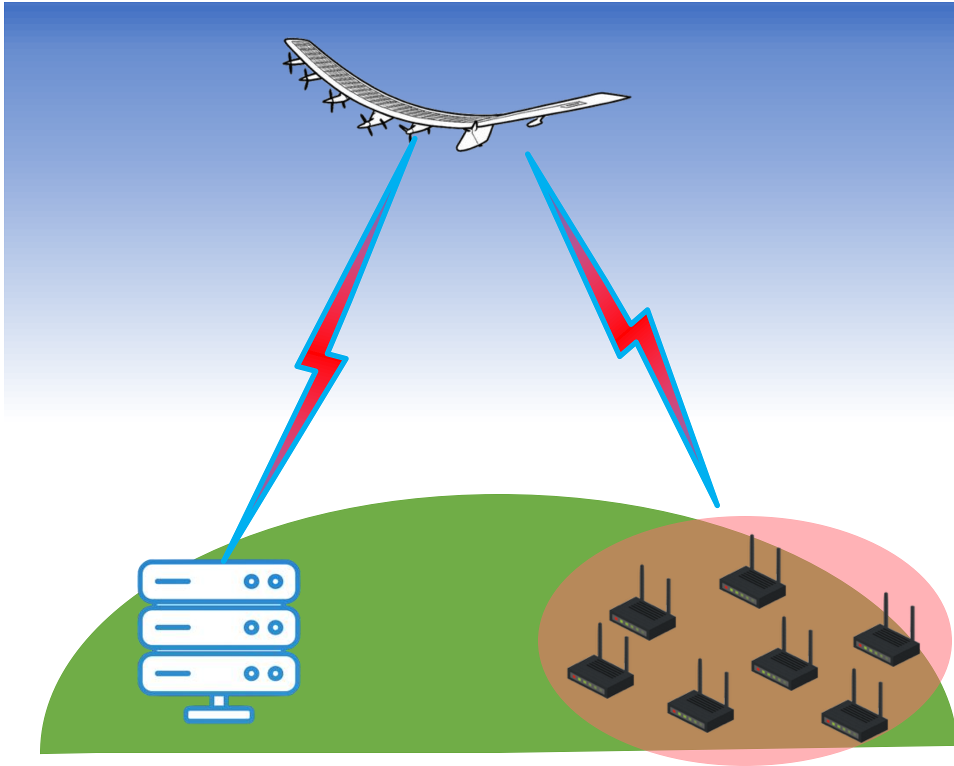
•the **central server** and the **HAP**, and

•the **HAP** and multiple **GNs** deployed in remote areas.

QKD is performed through these channels, and each GN and the central server generate and share the keys necessary for encrypting communications.

In this study, we propose a new QKD network utilizing HAP to enable secure key distribution to GNs that manage IoT devices.

Goals : Evaluate the SKR (secret key rate) and QBER (quantum bit error rate) for the number of GNs



3. Research Progress

Quantum Channel

First step: It is necessary to understand the **quantum channels**.

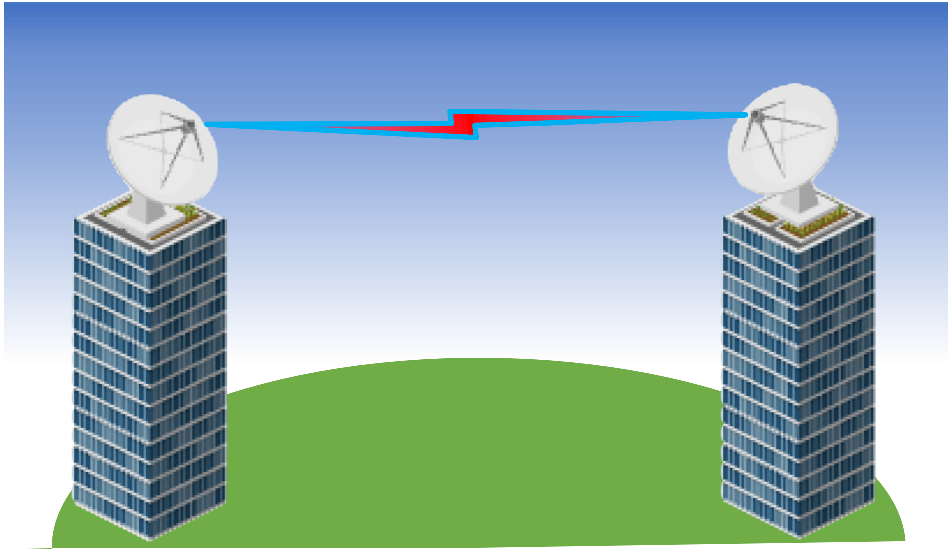
A horizontal FSO (Free Space Optical) link between two buildings in an urban environment as described in [4].

Quantum channel model

The following three factors are considered:

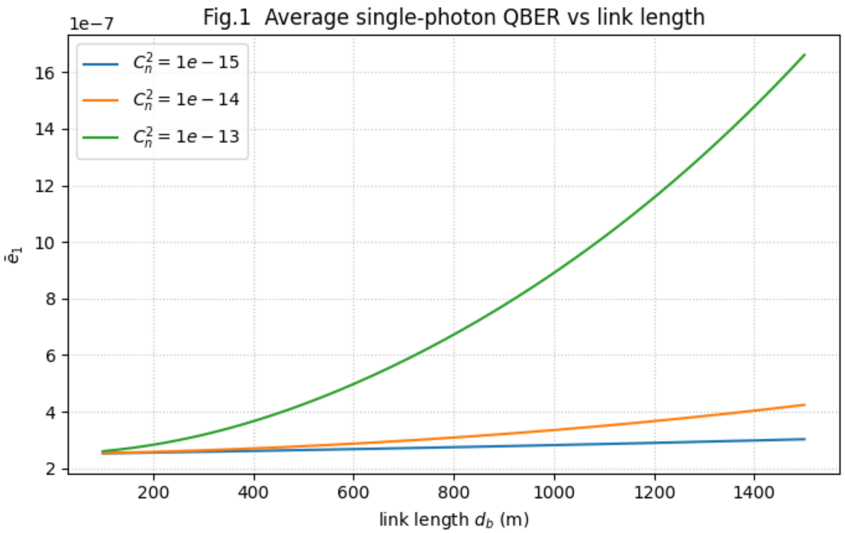
- **Atmospheric path loss**
- **Turbulence-induced fading**
- **Detector efficiency**

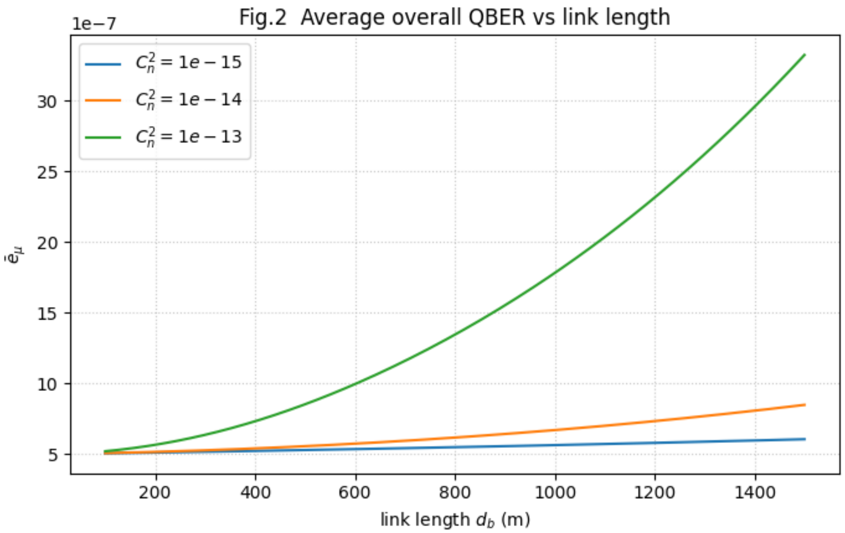
→Simulate QBER and SKR considering the quantum channel model.



Simulation Results of Single Photon Average QBER and Overall Average QBER

The results showed that QBER increases as turbulence intensifies, but the main factor affecting QBER is link distance.





Simulation Results of Secret Key Rate by atmospheric turbulence strength

The results showed that the effect on SKR was mainly influenced by the link distance and was relatively insensitive to the turbulence intensity.

Fig.3 SKR vs link length $(C_n^2 = 1e-15)$

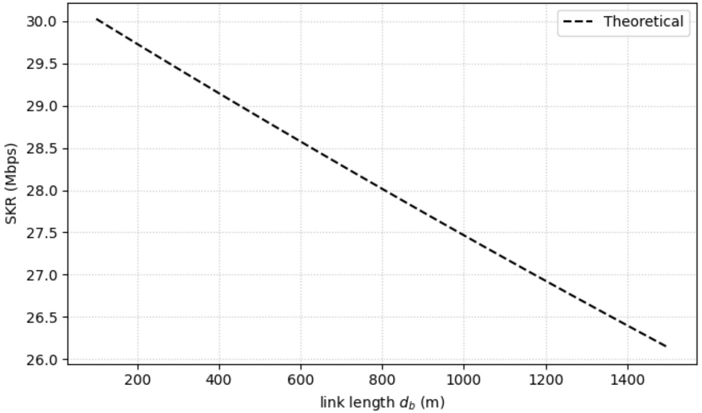


Fig.4 SKR vs link length $(C_n^2 = 1e-14)$

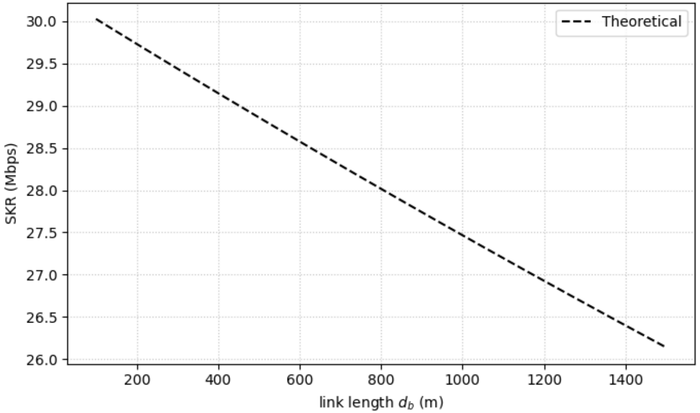
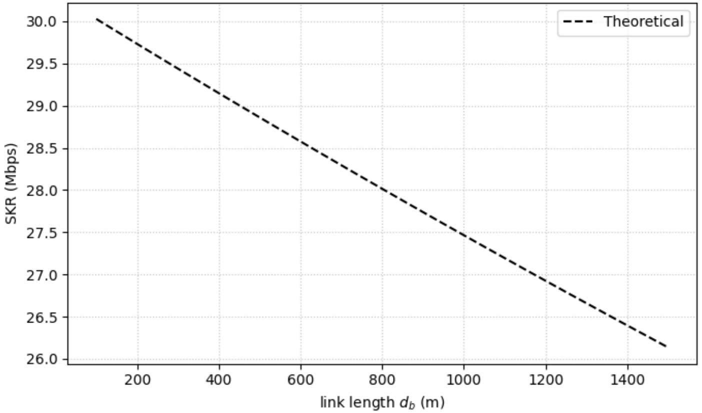
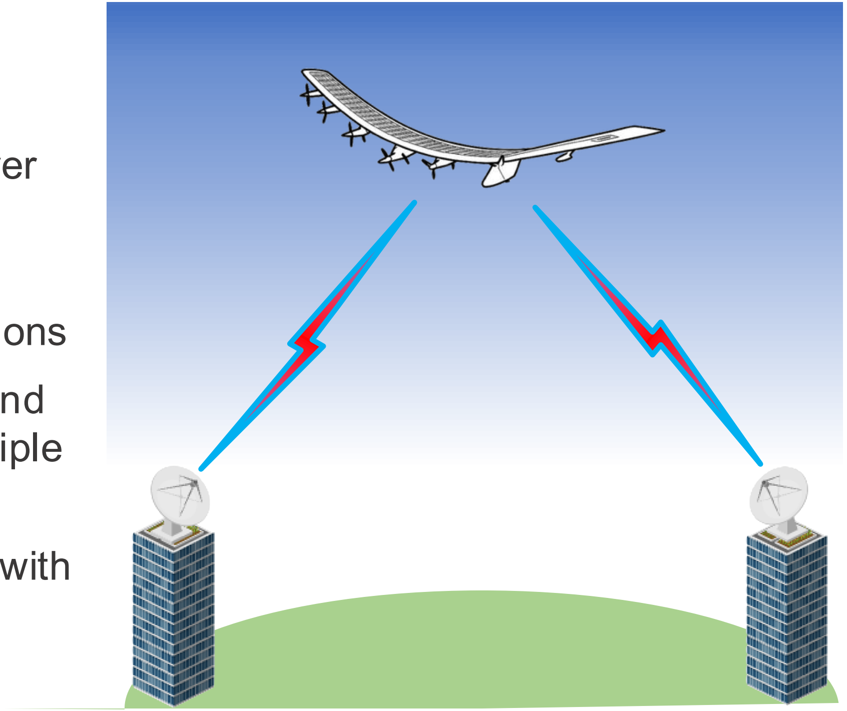


Fig.5 SKR vs link length $(C_n^2 = 1e-13)$



Future Works

- Detailed evaluation of vertical FSO channel characteristics
  → Analysis of the effects of atmospheric layer structure and weather conditions
- Impact assessment of beam misalignment caused by HAP vibration and attitude variations
- Scalability and feasibility of key generation and distribution via QKD between HAP and multiple GNs
- Performance evaluation of QBER and SKR with an increasing number of GNs



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.

[3] : https://www.softbank.jp/corp/philosophy/technology/special/ntn-solution/haps/

[4] : A. M. Shukla and N. K. Kundu, "Performance of DVQKD Protocol Over Gamma Gamma Turbulence Channel," *Proc. 2025 17th International Conference on COMSNETS (WQT Workshop)*, IEEE, 2025.

Thank you for listening!