Research Progress: Design of Blind Reconciliation for Satellite-based Quantum Key Distribution Systems

NGUYEN Trong Cuong

Computer Communications Lab.,
The University of Aizu, Japan

May 17th, 2024

Outline

I. Introduction

II. Proposed Design and Current Result

III. Directions of Extension

IV. Conclusion

Outline

I. Introduction

II. Proposed Design and Current Result

III. Directions of Extension

IV. Conclusion

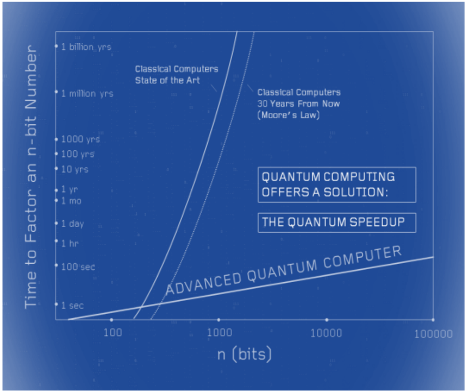
Internet of Vehicles (IoV)

- **Internet of Vehicles:** the network of vehicles and related entities
- **Applications:** speed warning, self-driving cars, vehicle tracking,...
- These applications can directly affect human safety.

Security becomes more and more important for the future IoV systems.

Figure: The Internet of Vehicles and its applications.

A Growing Threat from Quantum Computers



Quantum computers, utilizing the power of qubits, can increase the computational power exponentially.

This makes quantum computers, in principle, can **solve certain mathematical problems (e.g. factoring) much faster than classical computers.**

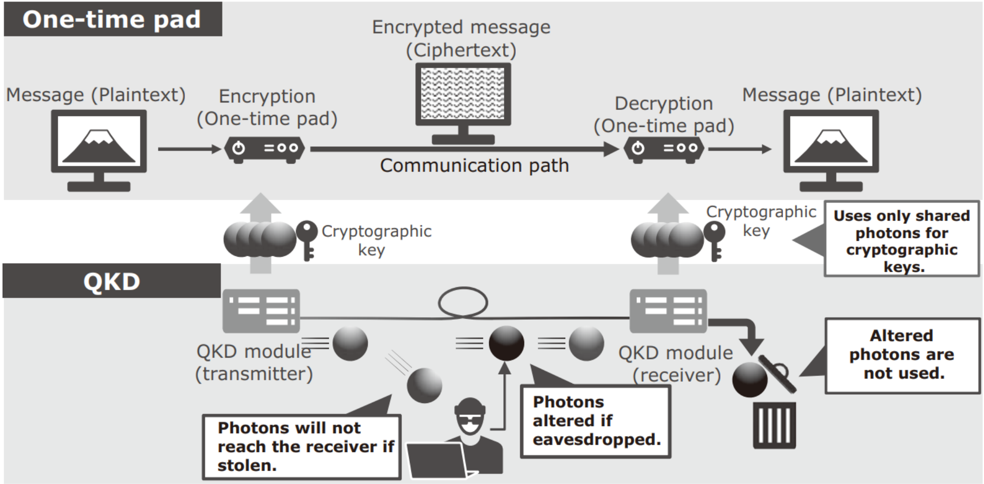
- These mathematical problems are the foundation for many modern cryptosystems, such as RSA. $\Longrightarrow$ *Pose a growing threat to today's security infrastructure.*

With the advance of quantum computers recently, many people believe that conventional cryptography schemes will soon be compromised.

➡ **Research efforts on quantum-safe solutions become more and more important.**

Quantum Key Distribution (QKD)

Quantum key distribution (QKD): *a key distribution protocol based on quantum mechanics*



Free Space Optical (FSO)-based Satellite QKD Systems

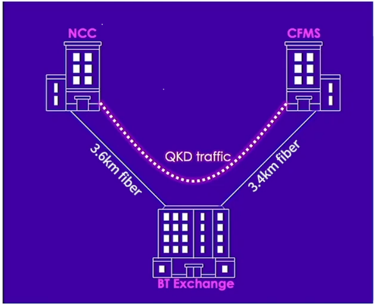


Figure: Optical fiber QKD systems.

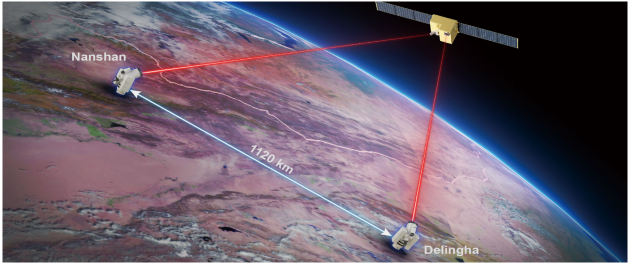


Figure: *Micius*, the world's first quantum satellite experiment

- Have been widely commercialized
- Can not support mobile users

- Can support mobile users via the FSO channel
- Provide global coverage using satellites

➡ **FSO-based satellite QKD systems are potential approaches for secured wireless applications.**

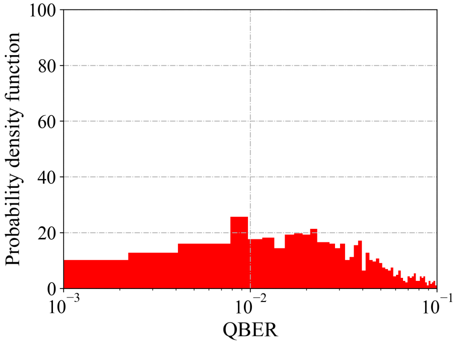
Challenging Issues: Uncertainty Channel

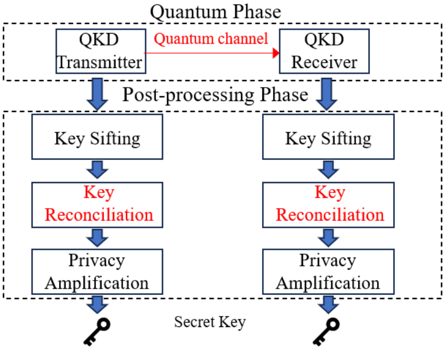
Uncertainty Channel:

- **Cause:** Adverse issues (such as, cloud coverage) and the mobility of satellite
- Lead to **fluctuating quantum bit-error rate (QBER)**

In general, QKD protocols always include a step in the post-processing phase to correct errors, namely **key reconciliation**.

$\Longrightarrow$ *It is necessary to have a proper design of key reconciliation for satellites QKD systems.*

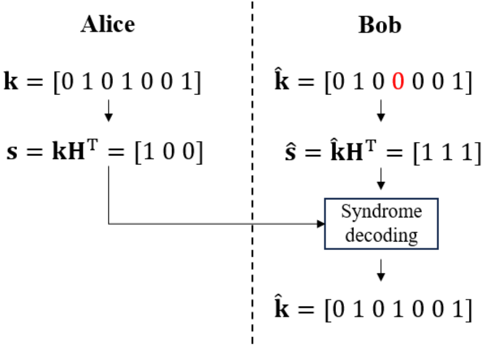




Key Reconciliation based on Error Correction Code

- **Key reconciliation:** Both users (Alice and Bob) try to correct the errors in their keys while minimizing the information leakage
- One of the main approaches is using the syndrome-based error correction codes
- **Low-density parity-check (LDPC) code** is widely considered thanks to its capacity-approaching performance and low-decoding complexity

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$



Existing Approaches and Motivations

There are three main approaches

1. **Fixed-rate Reconciliation:** A fixed code rate is used to reconcile all blocks
   $\Longrightarrow$ **Fixed-rate** KR may be *inefficient over turbulence FSO channels.*
2. **Adaptive-rate Reconciliation:** Based on estimated QBER, choose the best code rates among a set of code rates to reconcile
   - If the reconciliation fails, both sides discard their sifted keys.
   - To estimate the QBER, Alice and Bob will reveal a portion of sifted keys (10-25%)

   $\Longrightarrow$ This leads to *the reduction of the final key rate performance.*
3. **Blind Reconciliation:** If the reconciliation fails, incremental information will be sent to help decoding

Blind reconciliation is a potential approach for key reconciliation of satellite-based QKD systems.

However, to the best of our knowledge, blind reconciliation has not been considered for satellite-based QKD systems.

Our Goal

We propose a design of blind reconciliation and analyze its performance for satellite-based QKD systems.

Outline

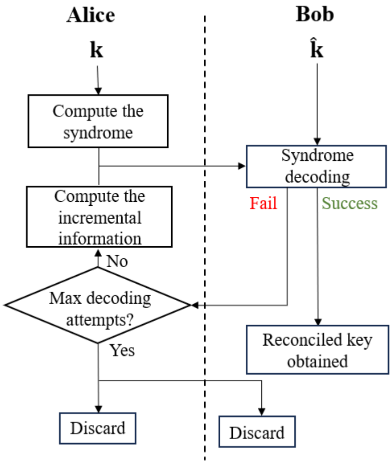
I. Introduction

II. Proposed Design and Current Result

III. Directions of Extension

IV. Conclusion

Flow Diagram of Blind Reconciliation



Proposed Structure of Rate-Compatible LDPC Code Family

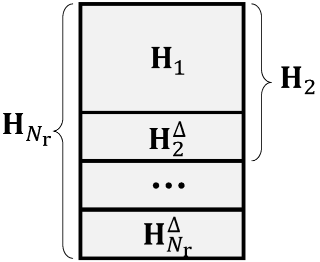


Figure: Proposed structure

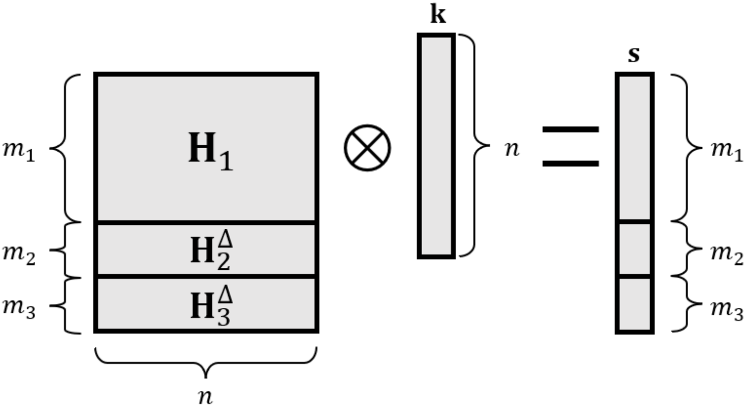
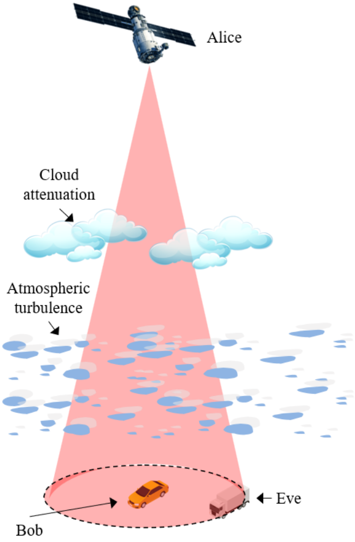


Figure: An example of nested syndrome with the proposed structure.

System Model



System model:

- An LEO satellite (Alice) distributes key materials to a ground vehicle (Bob)
- We consider the BB84 protocol with dual-threshold/ direct detection.

FSO Channel Model:

- Atmospheric Turbulence
- Cloud Attenuation
- Beam-spreading loss

An adversary's car (Eve) attempts to tap the transmitted signals within the beam footprint

Performance Metric: Final Key-rate

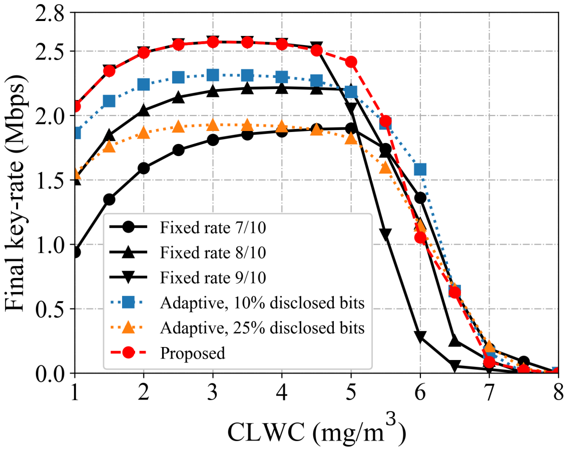
The final key rate is calculated as

$$\mathsf{KR} = \sum_{i=1}^{N_\mathsf{r}} \underbrace{\left(1 - \overline{\mathsf{FER}}_i\right)}_{\substack{\text{Prob. of}\\ \text{successful}\\ \text{reconciliation}}} \underbrace{\left(R_i - I_{AE}\right)}_{\substack{\text{Information after}\\ \text{privacy amplification}}} \underbrace{\frac{N}{R_\mathsf{b} P_\mathsf{sift}}}_{\substack{\text{Average}\\ \text{block rate}}}$$

where

- I_{AE}: mutual information between the sifted key of Alice and the information obtained by Eve
- N: block length
- R_b: the satellite's data rate
- P_sift: the sift probability.

Comparison among Other Reconcilition Methods



- The possible code rates of the blind reconciliation are $(0.9, 0.8, 0.7)$
- The performance of fixed-rate and adaptive-rate KR schemes are analyzed from the theoretical bounds

➡ The proposal design outperforms the other methods in most of the considered range.

Outline

I. Introduction

II. Proposed Design and Current Result

III. Directions of Extension

IV. Conclusion

1. Low-latency Blind Reconciliation for Satellite-based QKD Systems

Problem: Blind reconciliation may take several communication rounds over the public channel, resulting in high processing time

This problem becomes more critical in satellite networks, which have high propagation delay. $\Longrightarrow$ significantly affects the secret key rate performance.

Directions:

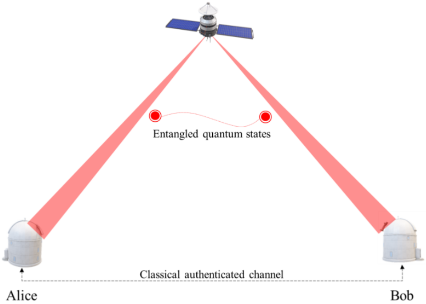
- *We would like to address a design of hybrid adaptive-blind reconciliation for low-processing time satellite-based QKD systems*
  - Integrate error estimation to the current design of blind reconciliation
  - Based on the estimated error, adaptive mechanisms will be conducted to reduce the number of communication rounds
- To confirm the effectiveness of the proposed design, it necessitates *addressing the latency-related metrics, such as the average number of communication rounds*
- We derive an analytical framework for these performance metrics and verify it with Monte Carlo simulations

2. KR Design for Entanglement-based Satellite QKD Systems

Entanglement-based (EB) satellite QKD systems: The LEO satellite (secret key source) distributes key material to Alice and Bob via two beams of entangled quantum states

- The model of quantum channels and classical channels are different from the previously considered scenario.

$\Longrightarrow$ *We investigate and optimize the performance metrics of the proposed design over the EB satellite-based QKD systems.*



Outline

I. Introduction

II. Proposed Design and Current Result

III. Directions of Extension

IV. Conclusion

Conclusion

1. Considered a design of blind reconciliation for satellite-based QKD systems
2. Highlighted the effectiveness of the proposal compared to conventional approaches
3. Discussed the directions for the paper's extension

Thank you for your attention!