Blind Reconciliation with Protograph LDPC Code Extension for FSO-based Satellite QKD Systems

Cuong T. Nguyen[*], Hoang D. Le[*], Vuong V. Mai[†], Phuc V. Trinh[‡], and Anh T. Pham[*]

[*] Computer Communications Laboratory, The University of Aizu, Japan
[†] Bradford-Renduchintala Centre for Space AI, University of Bradford, BD7 1DP Bradford, U.K.
[‡] Communications and Signal Processing Laboratory, The University of Tokyo, Tokyo, Japan

July 17th, 2024

Outline

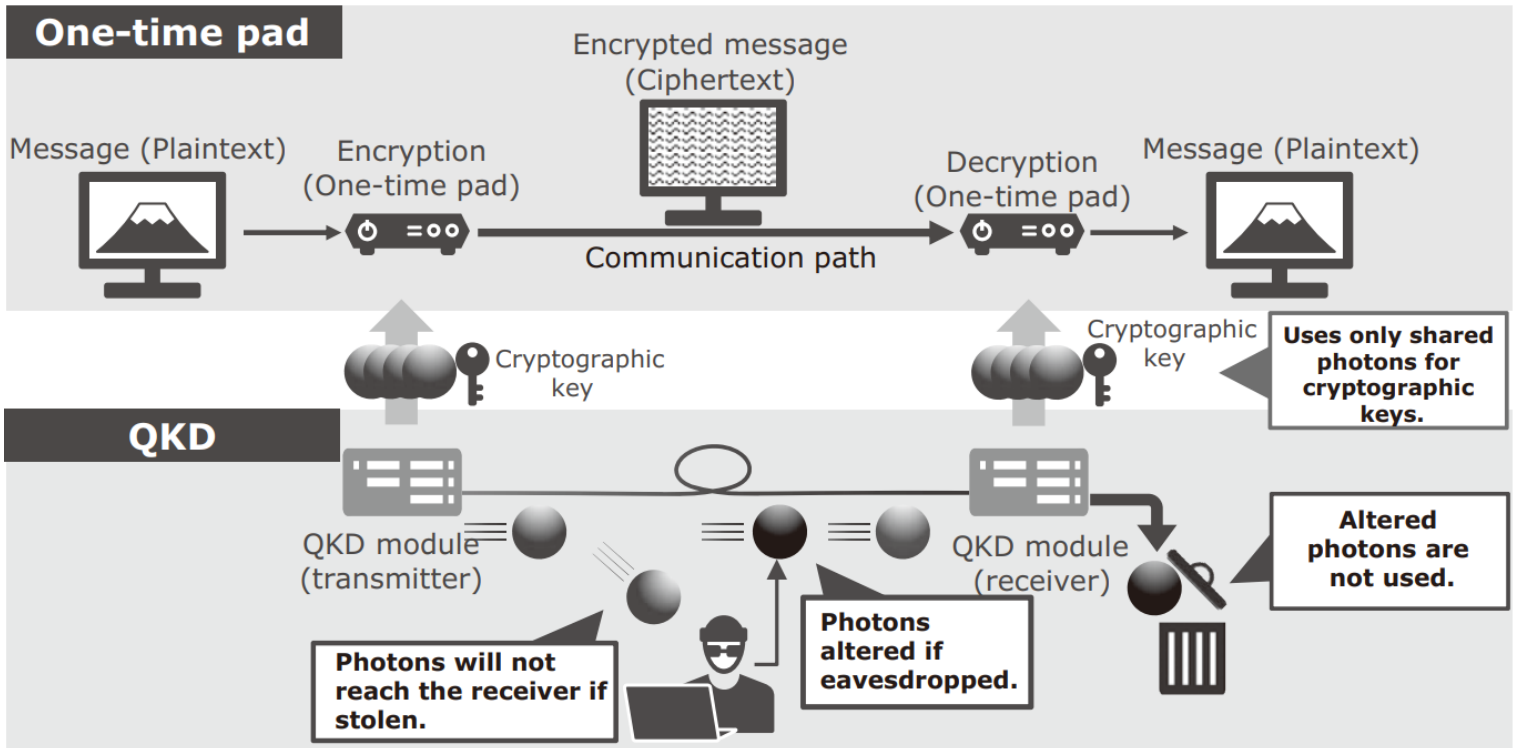
Outline

Quantum Key Distribution (QKD)

Recently, quantum computers have been advancing rapidly $\Longrightarrow$ *It poses a growing threat to key distribution systems using public-key cryptography.*

Quantum key distribution (QKD): key distribution protocols based on quantum mechanics.

- QKD can be combined with **one-time pad (OTP)** scheme to provide *unconditional security.*



Free Space Optical (FSO)-based Satellite QKD Systems

The feasibility of QKD systems has been widely demonstrated over various systems, *such as optical fiber or terrestrial free-space optical (FSO) systems.*

To enable global QKD services for wireless applications, a promising approach is **FSO-based satellite QKD systems.**

- Transmit quantum states via FSO channels
- Rely on satellites to provide global coverage
- **Applications:** Secured Intenet of Vehicles, etc.

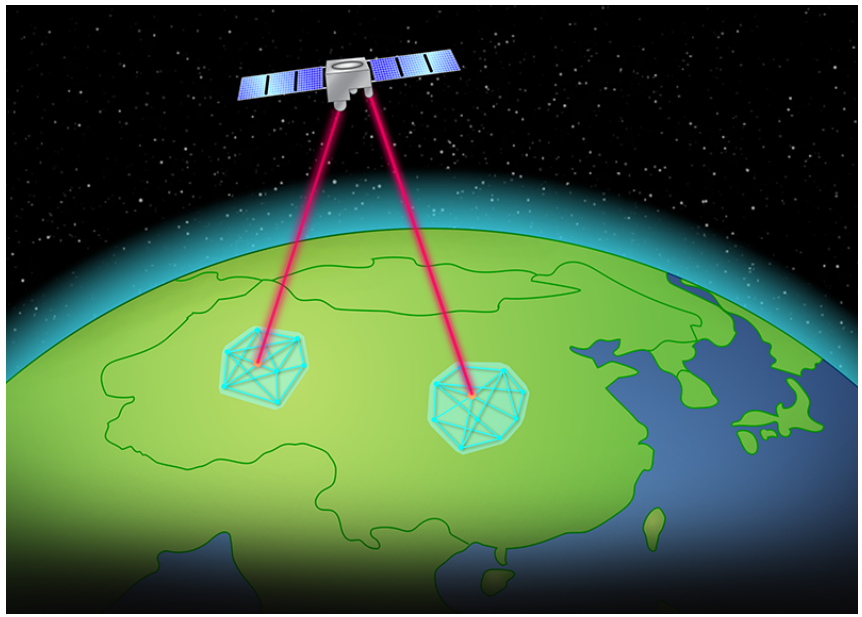


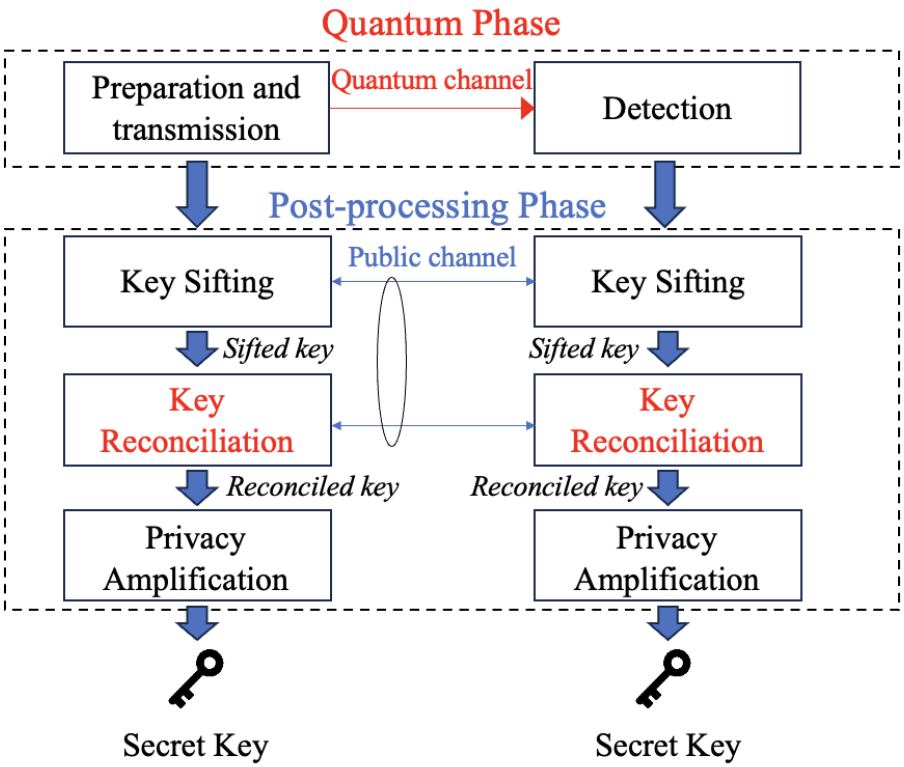
Figure: *Micius,* the first quantum satellite experiment [1]

[1] Chao-Y. Lu *et al.*, "Micius quantum experiments in space," *Rev. Modern Phys.*, vol. 94, no. 3, p. 035001, Jul. 2022.

A Pressing Concern: Key Reconciliation Design

The operation of QKD can be divided into two phases: **the quantum phase** and **the post-processing phase.**

Quantum phase: channel noise and/or eavesdroppers's attacks $\Longrightarrow$ Both side's sifted bits may be mismatched (**quantum bit-error rate (QBER)**)

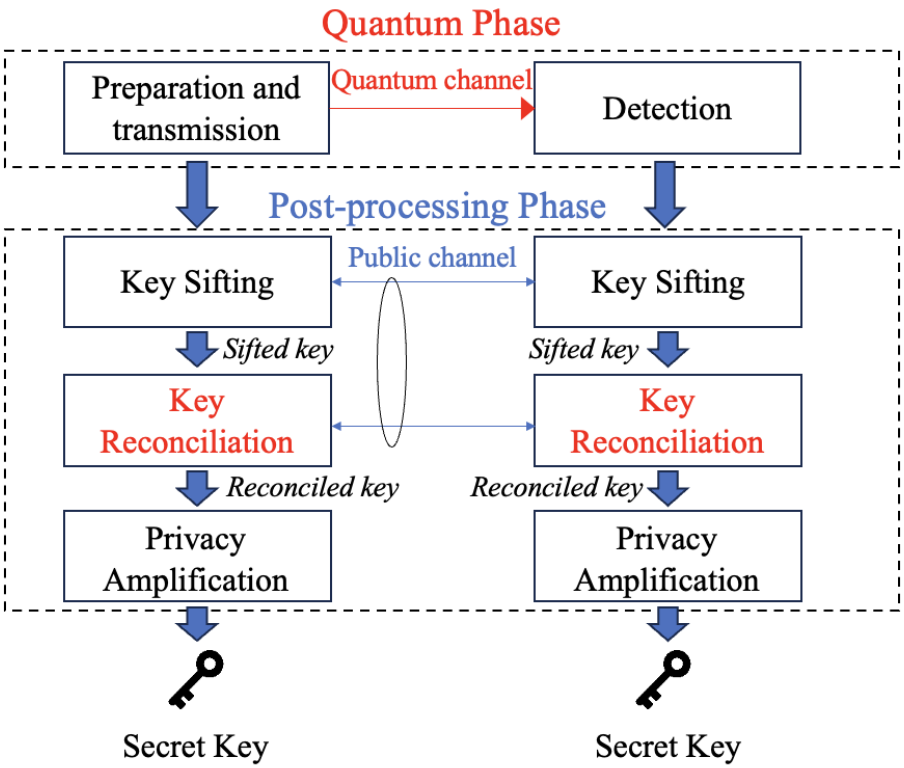


The errors will be corrected in the **key reconciliation (KR)** step of **the post-processing phase.**

- Both users exchange information via the public channel to reconcile their keys.
- Eavesdroppers can gain information about the key via exchanged information $\Longrightarrow$ **Final key length reduction.**

$\Longrightarrow$ *To achieve a high secret key rate, KR protocol needs to correct all errors while minimizing the leaked information.*

A Pressing Concern: Key Reconciliation Design (cont.)



Challenging issue: Fluctuating QBER

- **Cause:** Adverse issues (such as atmospheric turbulence) and the mobility of satellite

$\Longrightarrow$ *KR protocol needs to adapt to a wide range of QBER*

➡ *It is necessary to have a proper KR design for satellite-based QKD systems.*

Key Reconciliation Schemes based on Syndrome

- One of the main approaches is using the syndromes of linear block codes.
  - Among other ECCs, **low-density parity-check (LDPC) codes** are widely considered thanks to the capacity-approaching performance and low-decoding complexity.

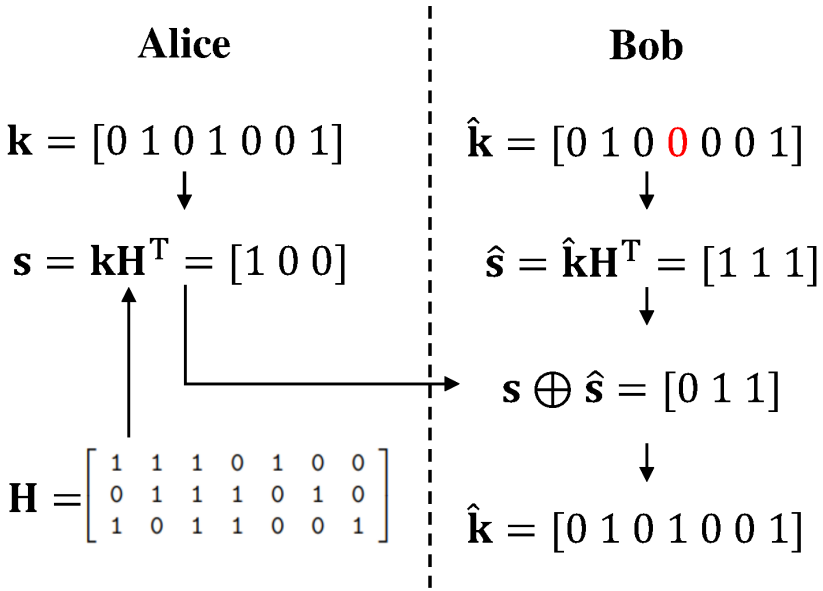


Figure: An example of key reconciliation using syndrome decoding

Existing Approaches and Motivations

There are three main approaches for LDPC-based KR schemes

1. **Fixed-rate Reconciliation:** Only a code rate is used to reconcile all blocks [1]
   $\Longrightarrow$ The method may be *inefficient over turbulence FSO channels.*

2. **Adaptive-rate Reconciliation:** Choose a code rate in a set of code rates to reconcile based on an estimated QBER [2]
   - If the reconciliation fails, both sides discard their 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.*

---

[1] D. Elkouss *et al.*, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory,* 2009, pp. 1879–1883.

[2] D. Elkouss *et al.*, "Rate compatible protocol for information reconciliation: An application to QKD," in *Proc. IEEE Inf. Theory Workshop,* 2009, 2010, pp. 1–5.

Existing Approaches and Motivations (cont.)

3. **Blind Reconciliation:** Try each code rate in a set of code rates until both keys are successfully reconciled [1]
   - If a reconciliation attempt fails, more information will be sent so the receiver can try the next attempt with a lower code rate.
   - **The rate-compatible (RC)-LDPC code family** is employed to reuse the transmitted information.

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 address the design of blind reconciliation and analyze its performance for satellite-based QKD systems.*

---

[1] J. Martinez Mateo *et al.*, "Blind reconciliation," *Quantum Inf. Comp.*, vol. 12, no. 9&10, pp. 791–812, May 2012.

Outline

Structure of Rate-Compatible LDPC Code Family

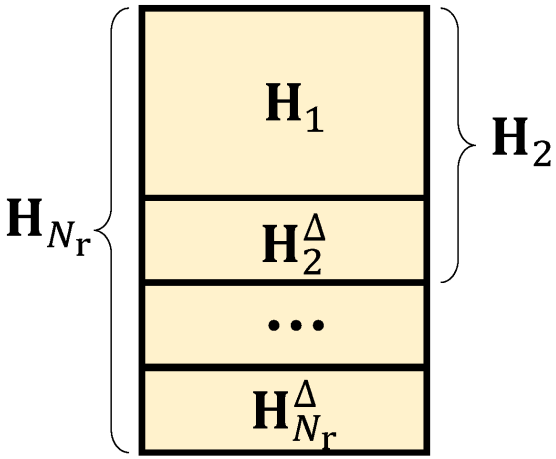


Figure: Parity check matrices of RC-LDPC code family

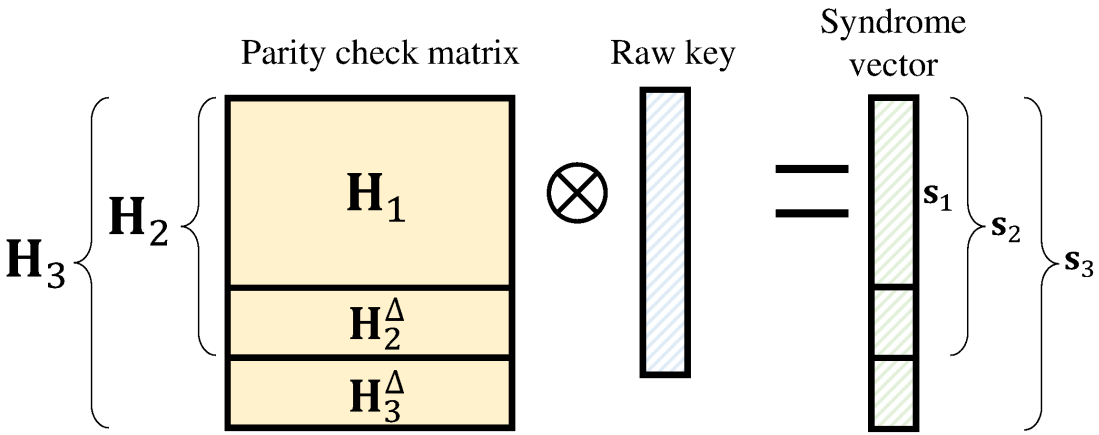
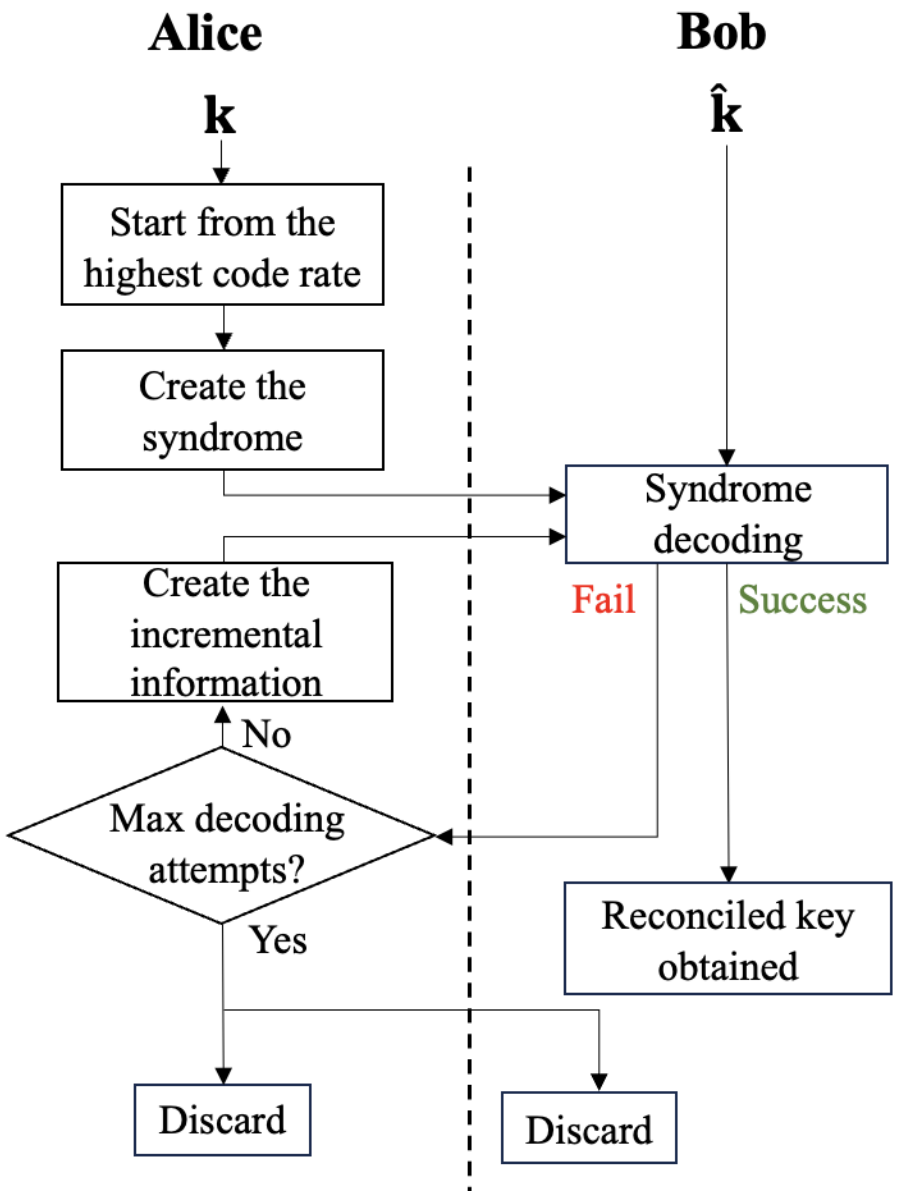


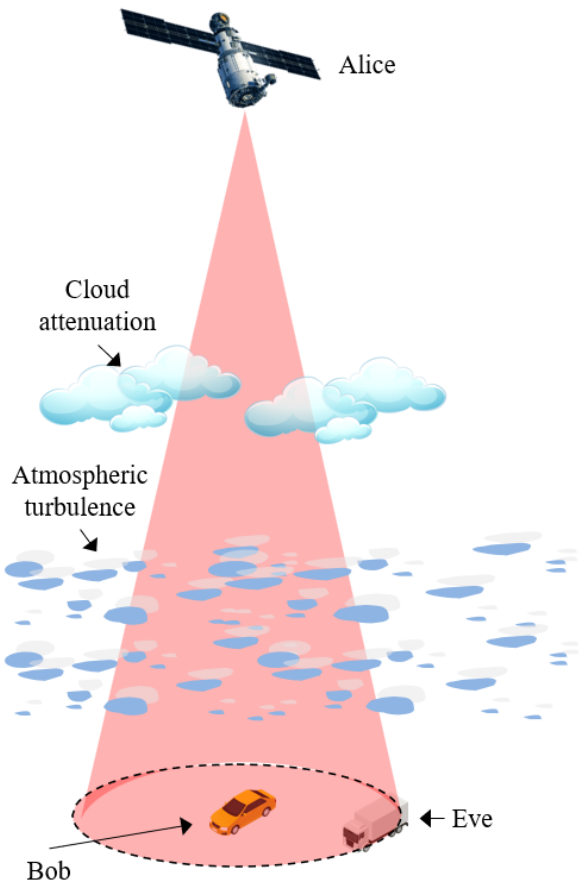
Figure: An example of nested syndrome encoding.

Flow Diagram of Blind Reconciliation



Outline

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 [1].

FSO Channel Model:

- *Atmospheric Turbulence:* Received power fluctuation
- *Cloud Attenuation:* Attenuation of received power due to water particles in clouds
- *Beam-spreading loss:* Geometric spread of the beam footprint $\Longrightarrow$ Only a fraction of power is received

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

[1] Phuc V. Trinh *et al.*, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, Jan. 2018.

Performance Metric: Final Key-rate

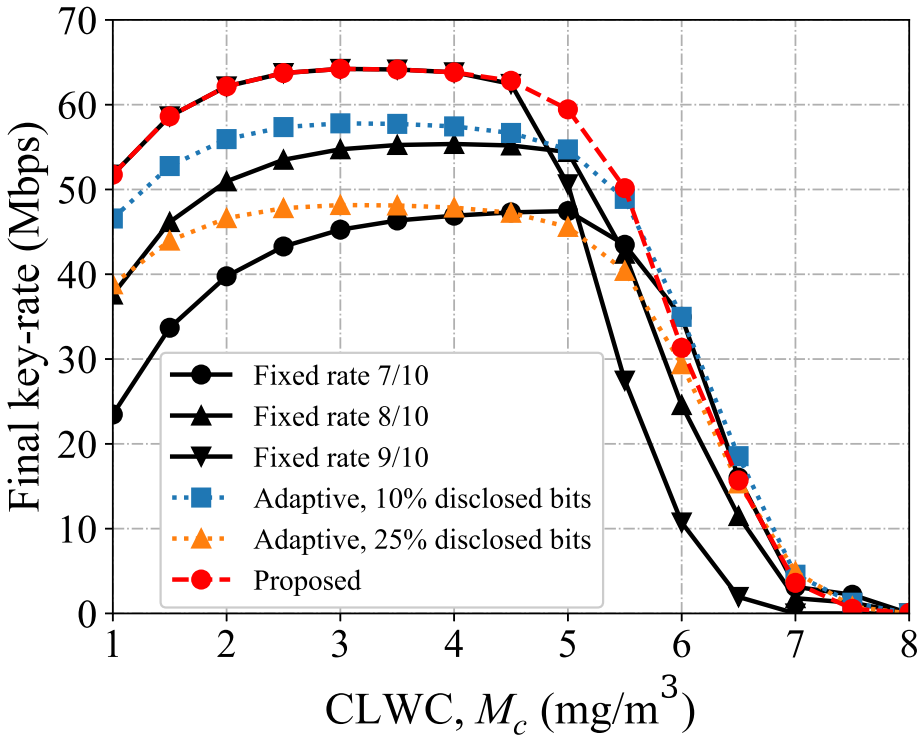
The final key rate is calculated as

$$\mathrm{KR} = R_{\mathrm{b}} P_{\mathrm{sift}} \sum_{i=1}^{N_{\mathrm{r}}} \underbrace{\left(1 - \overline{\mathrm{FER}}_i\right)}_{\substack{\text{Prob. of} \\ \text{successful} \\ \text{reconciliation}}} \left(\beta_i I_{\mathrm{AB}} - I_{\mathrm{E}}\right)$$

where

- R_{b}: the satellite's data rate
- P_{sift}: the sift probability
- β_i: reconciliation efficiency of i-th code rate
- I_{AB}: mutual information between the sifted key of Alice and that of Bob
- I_{E}: the upper bound on the information that the eavesdropper can obtain over the quantum channel

Comparison among Other Reconciliation Methods



Cloud liquid water content (CLWC)

- A measure of the total liquid water contained in a specified amount of air in the cloud
- The higher value of CLWC, the higher attenuation of the optical channel

The code rates for the adaptive-rate and the blind reconciliation are $(0.9, 0.8, 0.7)$

- The performance of fixed-rate and adaptive-rate KR are analyzed from the theoretical bounds

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

Thank you for your attention!