Protograph LDPC Code Extension for Key Reconciliation of Satellite-based Optical Key Distribution Systems

NGUYEN Trong Cuong

Computer Communications Lab.,
The University of Aizu, Japan

Febuary 27th, 2024

Outline

Outline

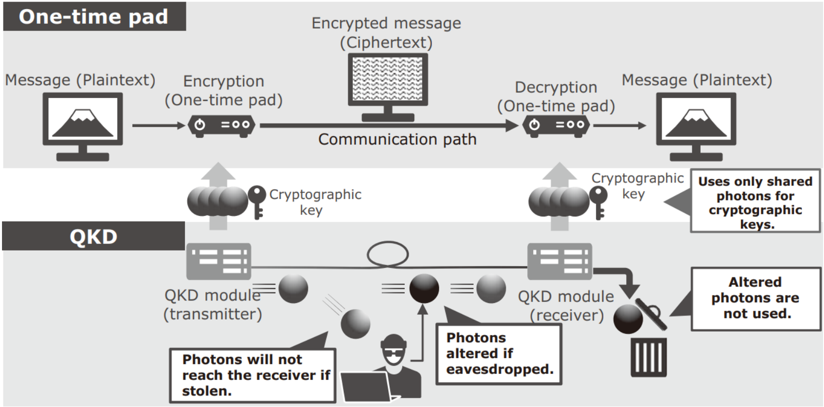
I. Introduction

II. Proposed Blind Reconciliation

III. Simulation Results

Quantum Key Distribution (QKD)

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



Free Space Optical (FSO)-based Satellite QKD Systems

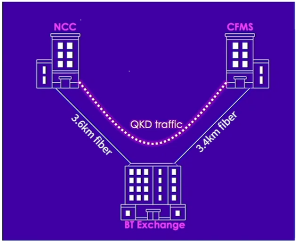


Figure: Optical fiber QKD systems.

- Have been widely commercialized
- Can not support mobile users

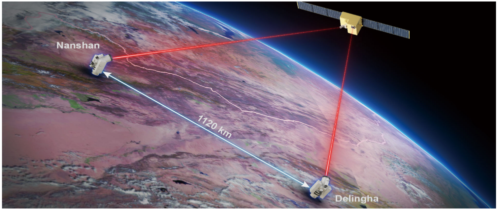


Figure: *Micius*, the world's first quantum satellite experiment

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

FSO-based satellite QKD systems are potential approaches for future mobile networks.

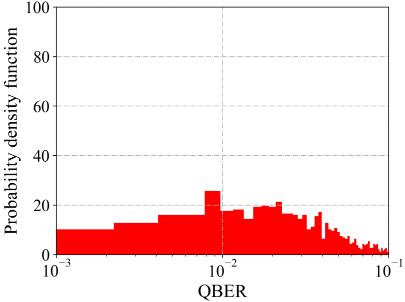
Challenging Issues: Uncertainty Channel

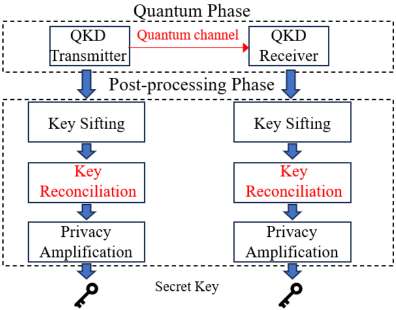
Atmospheric Turbulence:

- **Cause:** Inhomogeneity in refractive-index along the propagation path of the optical signal
- 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

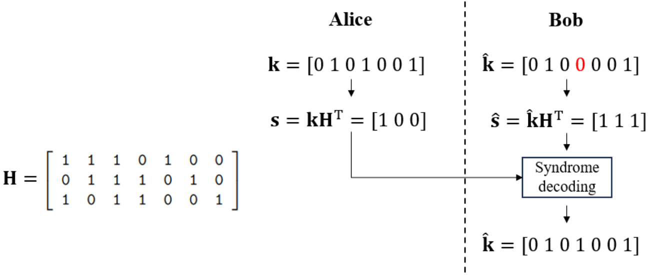


Figure: An example of syndrome decoding with linear block code

Existing Approaches

There are three main approaches

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

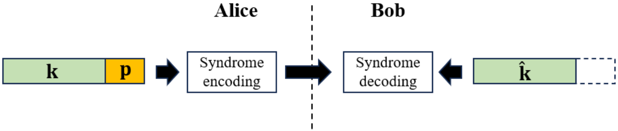
   $\Longrightarrow$ **Fixed-rate** and **adaptive-rate** may be *inefficient over turbulence FSO channels.*
3. **Blind Reconciliation:** If the reconciliation fails, incremental information will be sent to help decoding
   - Blind reconciliation was first proposed in [1] and has been investigated in several studies [2]–[5].

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

Blind Reconciliation based on Puncturing LDPC Codes

Key Idea: Alice adds a certain number of random bits to her key before syndrome encoding

- These bits are unknown to Bob, and he treats them as *punctured bits* when decoding
- Alice adjusts the code rates by revealing the values of these punctured bits.



The range of code rates depends on the *the percentage of added random bits*, α

$$R_{\text{max}} = \frac{R_{\text{base}}}{1-\alpha} \geq R \geq \frac{R_{\text{base}} - \alpha}{1-\alpha} = R_{\text{min}}$$

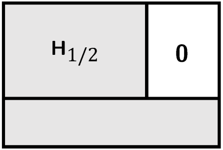
Limited code rate range $\Longrightarrow$ Inefficient for the considered systems

Motivations & Contributions

A viable solution to construct a rate-compatible (RC)-LDPC code family is **code extension** method

- A new parity check matrix is obtained by extending another parity check matrix.

$\mathbf{H}_{1/3} =$



Contribution:

We propose a design of blind reconciliation based on the RC-LDPC code extension.

Outline

I. Introduction

II. Proposed Blind Reconciliation

III. Simulation Results

Proposed Structure

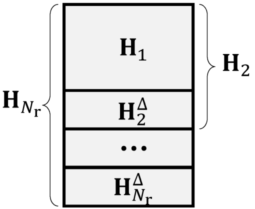


Figure: Proposed structure

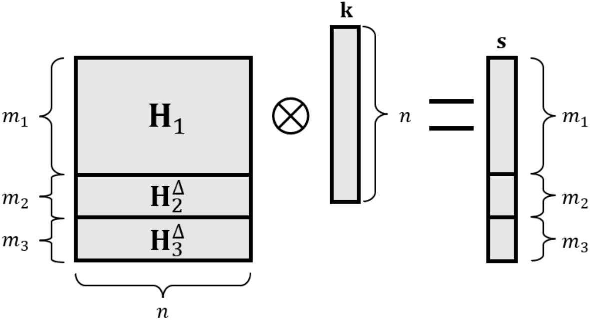
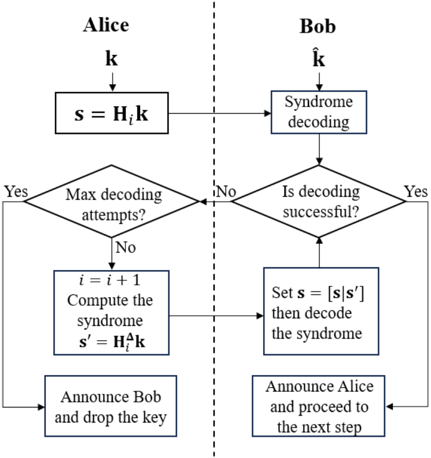


Figure: An example of nested syndrome with the proposed structure.

Flowchart of Proposed Blind Reconciliation

Initalization: Set $i = 1$



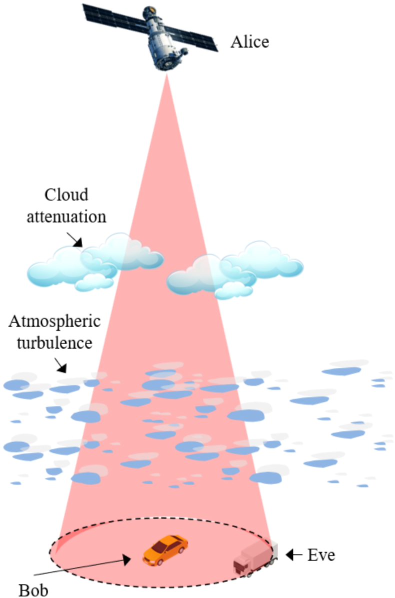
Outline

I. Introduction

II. Proposed Blind Reconciliation

III. Simulation Results

Considered System Model



System model:

- An LEO satellite (Alice) distributes key materials to a ground vehicle (Bob)
- Dual-threshold/direct detection key distribution is used

FSO Channel Model:

- Atmospheric Turbulence
- Cloud Attenuation
- Beam-spreading loss

An adversary's car (Eve) follows Bob and eavesdrops on the beam footprint.

Final Key Rate

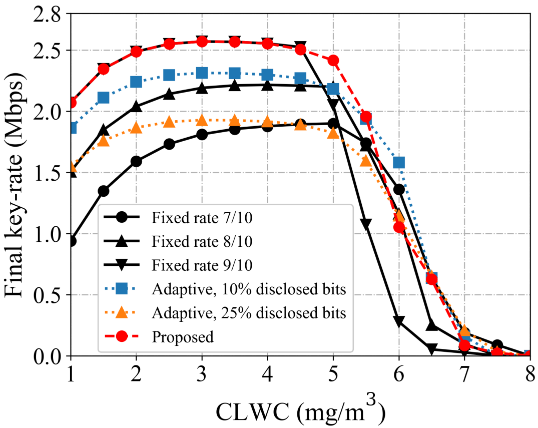
The final key rate is calculated as

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

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



- Consider code rate range $\left(\frac{9}{10}, \frac{8}{10}, \frac{7}{10}\right)$
- Fixed-rate and adaptive-rate consider perfect code rate

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

Thank you for your attention!

References

[1] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Blind reconciliation," (2013), [Online]. Available: https://arxiv.org/abs/1205.5729.

[2] E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution," *Phys. Rev. Appl.*, vol. 8, no. 4, p. 044 017, 2017.

[3] Z. Liu, Z. Wu, and A. Huang, "Blind information reconciliation with variable step sizes for quantum key distribution," *Scientific Reports*, vol. 10, no. 1, p. 171, 2020.

[4] E. O. Kiktenko, A. O. Malyshev, and A. K. Fedorov, "Blind information reconciliation with polar codes for quantum key distribution," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 79–83, 2021.

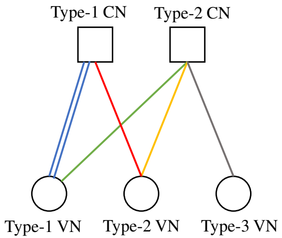
[5] H.-K. Mao, Y.-C. Qiao, and Q. Li, "High-efficient syndrome-based ldpc reconciliation for quantum key distribution," *Entropy*, vol. 23, no. 11, p. 1440, 2021.

Appendix: Protograph

- **Protograph** is a *small Tanner graph* serving as a template to construct the LDPC.
- **The structured LDPC codes** *inherits* from the protograph
  - Code rate & distributions of degree of nodes

  $\Longrightarrow$ The LDPC codes can be faster optimized by optimizing on the protograph level
- A protograph can be equivalently represented by a **base matrix**

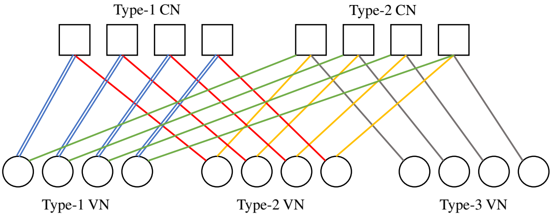
$$\mathbf{B} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$



Copy-and-Permute (1)

- The LDPCC with desired information length is derived from the protograph by a **"copy-and-permute" operation**
  - The derived graph is called *lifted graph*
- **First step:** Making T copies of the protograph

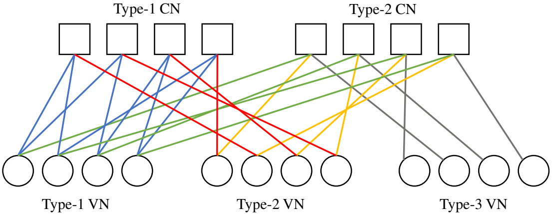
$$\mathbf{B}_4 = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$



Copy-and-Permute (2)

- **Second step:** Permuting the end-points of each edge between nodes of the same type

$$\mathbf{B}_4 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$



- Edges in the lifted graph are distributed following the edge types in the protograph

⇒ The lifted graph **inherits** properties of the protograph