Information Reconciliation with Polar Code for Satellite QKD Systems

Cuong Nguyen
Computer Communications Lab.
The University of Aizu

Nov. 13, 2024

Outline

- Part I: An Introduction to Polar Codes
- Part II: Information Reconciliation with Polar Code for Satellite QKD Systems

Overview of Polar Codes

Polar codes are a type of *error-correction code*, firstly introduced in 2009.

- ECC or channel code: error-control methods that add redundancy to the original message so that a certain number of errors can be corrected.

Key Features:

- One of the newest ECC
- Adopt for control channels of the 5G standards
- Provably capacity-approaching performance

Key idea behind polar code: Channel polarization, which is a technique that redistributes channel capacities among various instances of that channel.

	Control Channels	Data Channels
2G GSM	**Convolutional** Memory 4 Zero termination	**Convolutional** Memory 4, 6 Zero termination
3G UMTS	**Convolutional** Memory 8 Zero termination	**Turbo** Memory 3 Nonregular π
4G LTE	**Convolutional** Memory 6 Tail-biting termination	**Turbo** Memory 3 Contention-free π
5G New Radio	**Polar** Reliability index-sequence CRC-aided decoding	**LDPC** Protograph lifting Raptor-like

Table. Overview of Channel Code Used in Wireless Mobile Telecommunications Generations.

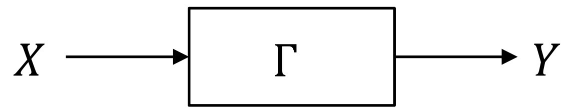
This presentation will cover:

- Channel polarization, which is a fundamental concept of polar codes
- Decoding algorithm: Successive Cancellation (SC)

Review of Channel Capacity

Channel capacity is the *theoretical maximum information rate* that can be reliably transmitted over a communication channel.

- Reliability: bit-error rate can be made arbitrarily small

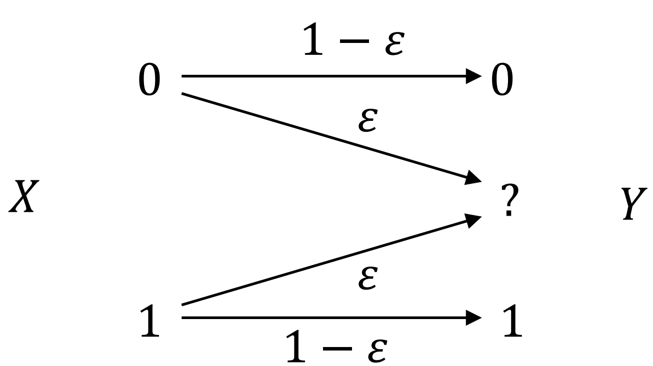


X, Y: random variables representing the input and output of the channel. Γ presents the channel.

The channel capacity can be computed as

$$C = \max_{\{\Pr(x)\}} I(X;Y),$$

Example: A binary erasure channel (BEC)



Channel input: $X \in \{0,1\}$

ε: channel erasure probability

Channel output: $Y \in \{0,1,?\}$, where $?$ is the erasure symbol

Channel capacity of BEC:

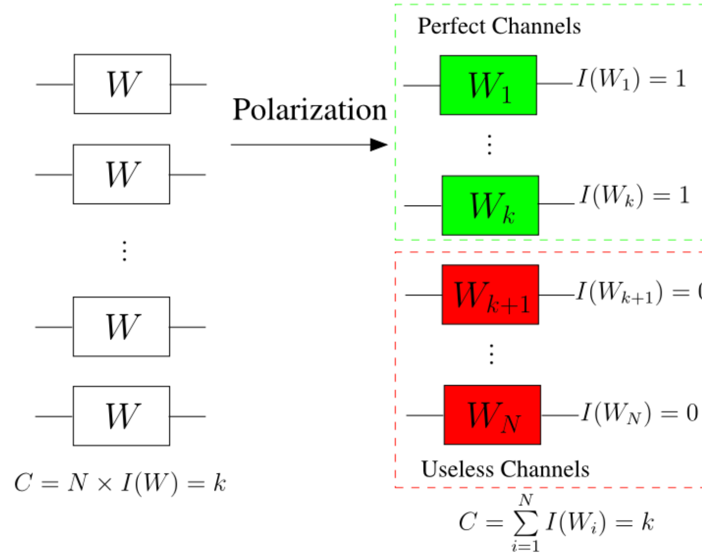
$$C = 1 - \varepsilon$$

When $\varepsilon = 0 \Rightarrow C = 1$, the channel is noiseless

When $\varepsilon = 1 \Rightarrow C = 0$, the channel is totally unreliable

Channel Polarization: A Basic Transformation

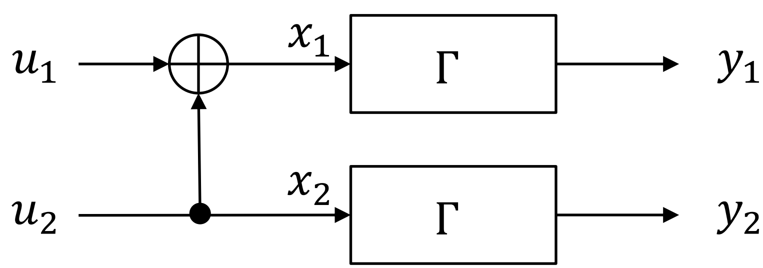
Channel polarization: A technique that <u>redistribute channel capacities among various instance of a channel</u> while *conserving the total capacity of them.*



To achieve the channel polarization, we can apply ***channel combining to these channels.***

<u>A basic transformation of channel combining</u>

Take two bits (u_1, u_2) and generate two bits (x_1, x_2), in which $x_1 = u_1 \oplus u_2$, $x_2 = u_2$



The capacity of the compound channel: $I(U_1, U_2; Y_1, Y_2) = I(X_1, X_2; Y_1, Y_2) = 2I_\Gamma$

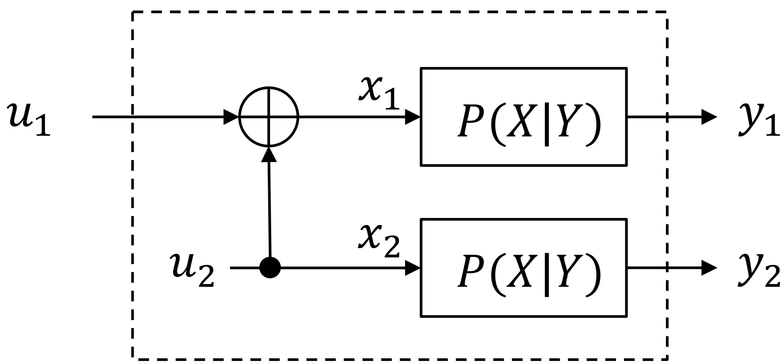
Remark: The basic transformation does not reduce the channel capacity.

Equivalent Channels

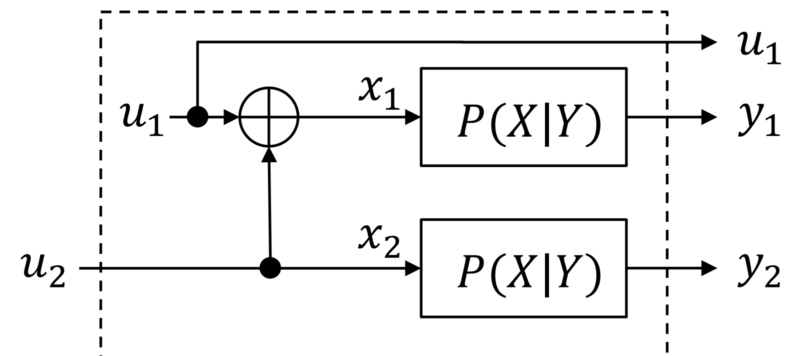
Applying some mathematical manipulations, we can rewrite the capacity of the compound channel as

$$\begin{aligned} 2I_\Gamma &= I(X_1, X_2; Y_1, Y_2) \\ &= \underbrace{I(U_1; Y_1, Y_2)}_{\text{Channel } \Gamma^-} + \underbrace{I(U_2; Y_1, Y_2, U_1)}_{\text{Channel } \Gamma^+} \end{aligned}$$

This implies that the compound channel can be split into two channels with different channel capacities, i.e., Γ^+ and Γ^-.

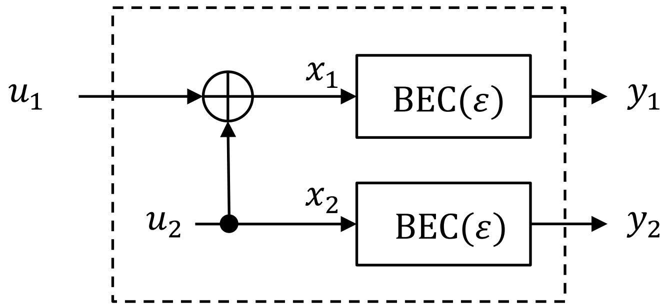


$\Gamma^-: u_1 \rightarrow (y_1, y_2)$



$\Gamma^+: u_2 \rightarrow (y_1, y_2, u_1)$

Equivalent Channels - Example



$\Gamma^-: u_1 \rightarrow (y_1, y_2)$

Possible outputs	Trans. Prob.	Can we recover u_1?
(y_1, y_2)	$(1-\varepsilon)^2$	Yes, $u_1 = y_1 \text{ XOR } y_2$
$(?, y_2)$	$\varepsilon(1-\varepsilon)$	✗
$(y_1, ?)$	$\varepsilon(1-\varepsilon)$	✗
$(?, ?)$	ε^2	✗

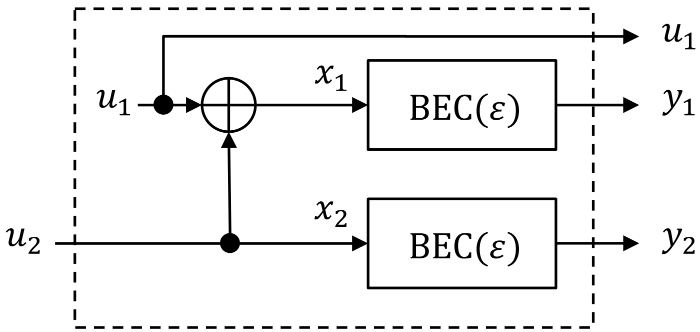
We can only recover u_1 if we have both y_1 and y_2

$$\Rightarrow \quad \Gamma^-: u_1 \rightarrow \begin{cases} u_1 \ \text{ with prob. } \ (1-\varepsilon)^2 \\ ? \ \text{ with prob. } \ 2\varepsilon - \varepsilon^2 \end{cases}$$

$\Rightarrow$ Γ^- can be equivalently presented as a BEC with the erasure probability $2\varepsilon - \varepsilon^2$

$$\Gamma^-: \ \text{BEC}(2\varepsilon - \varepsilon^2)$$

Equivalent Channels – Example (Cont.)



$\Gamma^+ : u_2 \to (y_1, y_2, u_1)$

Possible outputs	Trans. Prob.	Can we recover u_2?
(u_1, y_1, y_2)	$(1-\varepsilon)^2$	Yes
$(u_1, ?, y_2)$	$\varepsilon(1-\varepsilon)$	Yes
$(u_1, y_1, ?)$	$\varepsilon(1-\varepsilon)$	Yes, $u_2 = u_1 \text{ XOR } y_1$
$(u_1, ?, ?)$	ε^2	✗

With u_1 at the output, we can always recover u_2 unless both y_1 and y_2 are erased.

$$\Rightarrow \quad \Gamma^+ : u_2 \to \begin{cases} u_2 & \text{with prob. } 1-\varepsilon^2 \\ ? & \text{with prob. } \varepsilon^2 \end{cases}$$

$\Rightarrow$ Γ^+ can be equivalently presented as a BEC with the erasure probability ε^2

$$\Gamma^+ : \ \mathrm{BEC}(\varepsilon^2)$$

Channel Polarization: Remarks

Regarding Γ^-: $\text{BEC}(2\varepsilon - \varepsilon^2)$, we see that $2\varepsilon - \varepsilon^2 \geq \varepsilon$ for $\varepsilon \in [0,1]$

$\Rightarrow$ Channel capacity of Γ^- is smaller than that of the original BEC, i.e., $C(\Gamma^-) \leq C(\Gamma)$.

Regarding Γ^+: $\text{BEC}(\varepsilon^2)$, we see that $\varepsilon^2 \leq \varepsilon$ for $\varepsilon \in [0,1]$

$\Rightarrow$ Channel capacity of Γ^+ is larger than that of the original BEC, i.e., $C(\Gamma^+) \geq C(\Gamma)$.

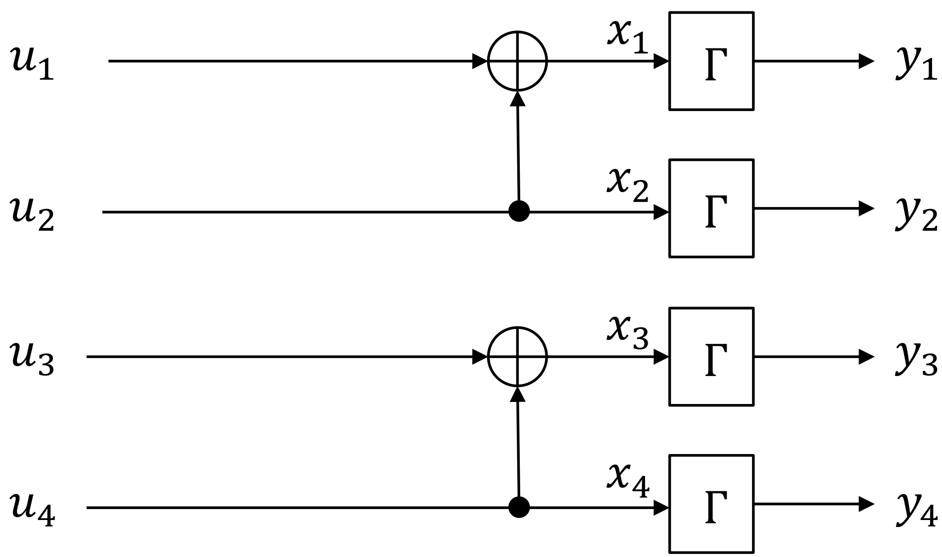
Example: $\varepsilon = 0.5$. We have $C(\Gamma^-) = 0.25 \leq C(\Gamma) \leq C(\Gamma^+) = 0.75$.

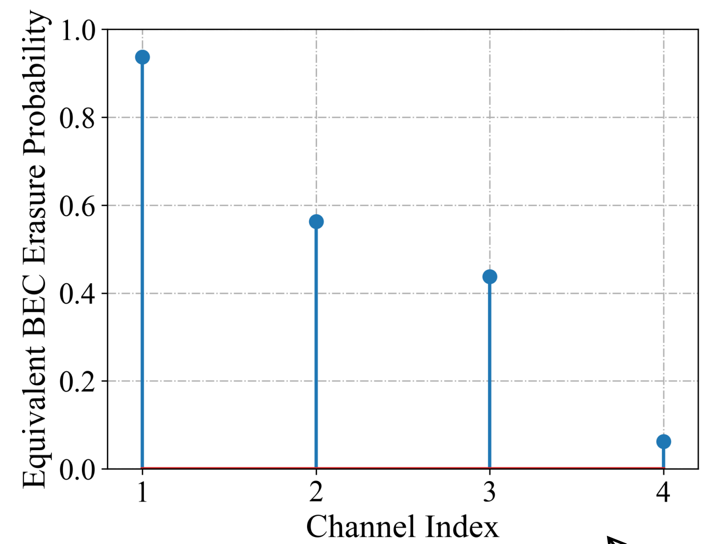
Remark:

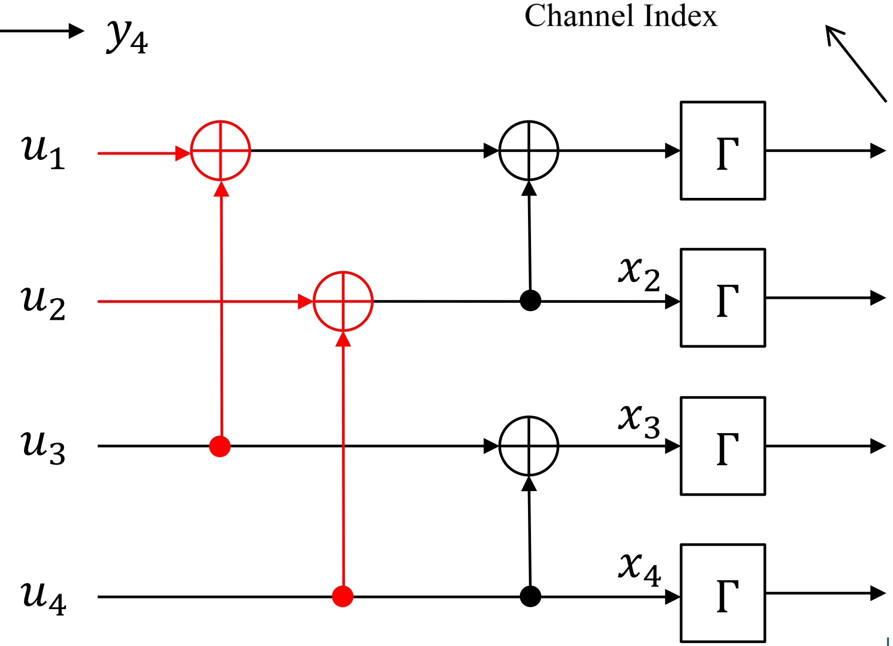
- Basic channel transformation generates two new artificial channels.
  - One of these new channels has a higher capacity.
  - The other has a lower capacity.

$\Rightarrow$ *Further channel polarization can be done by continuing recursively apply the channel combining.*

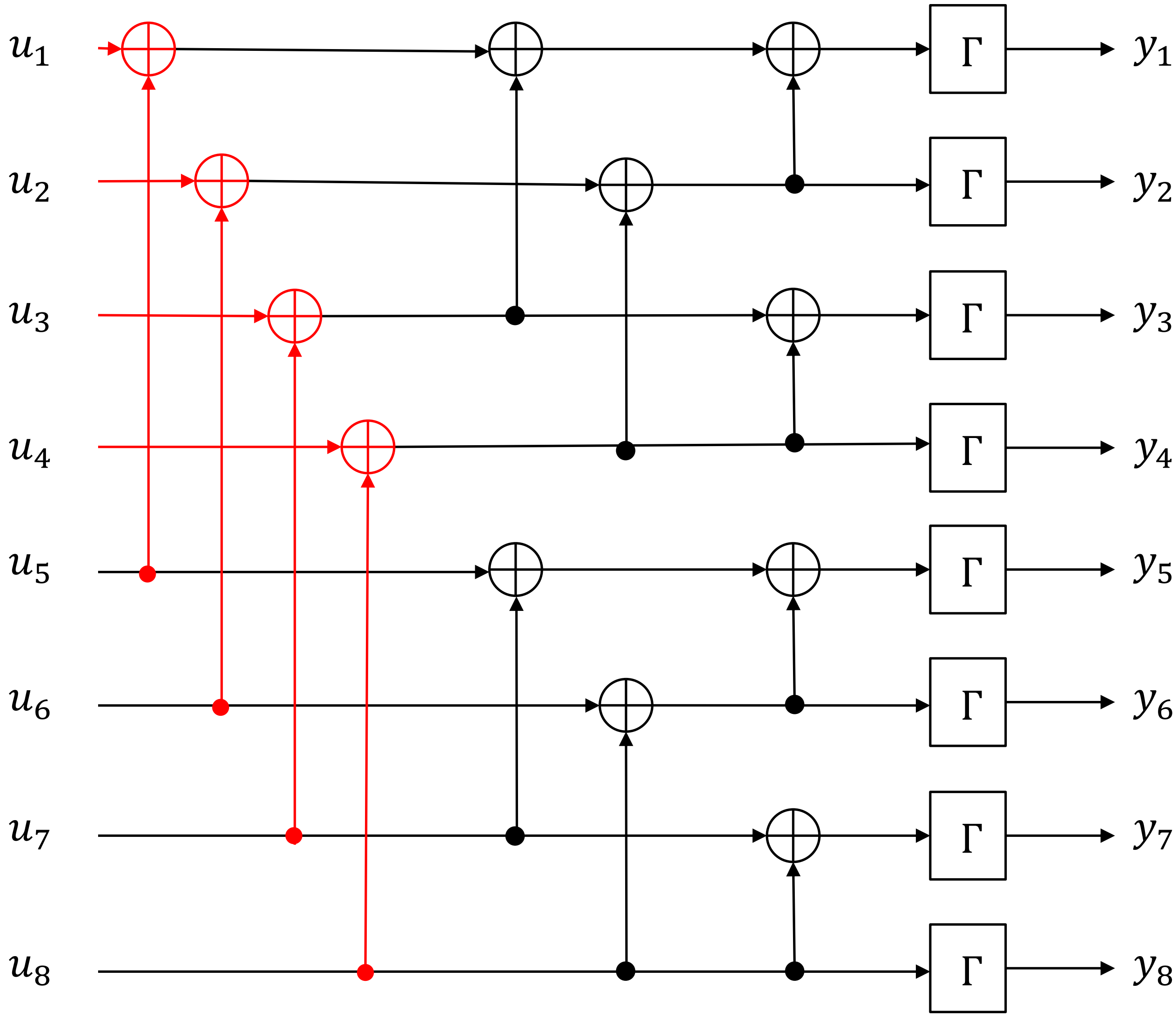
Two-fold of The Basic Transformation





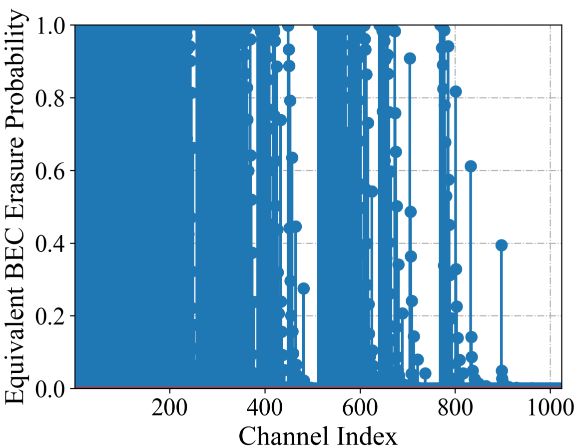


Three-fold of The Basic Transformation

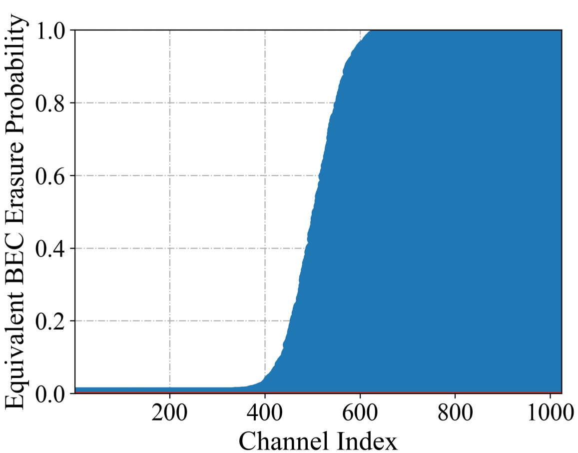


Equivalent Channel Performance

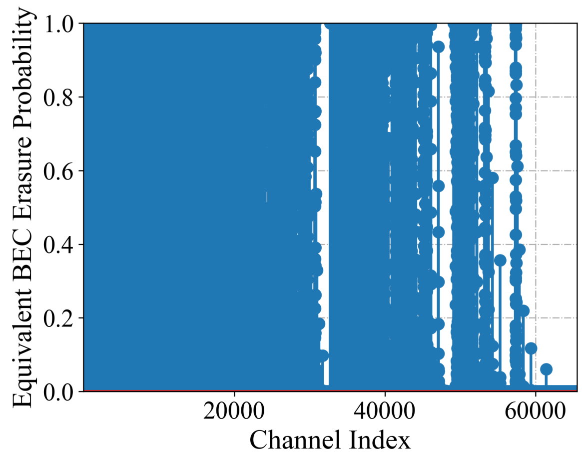
$n = 2^{10}, \varepsilon = 0.5$



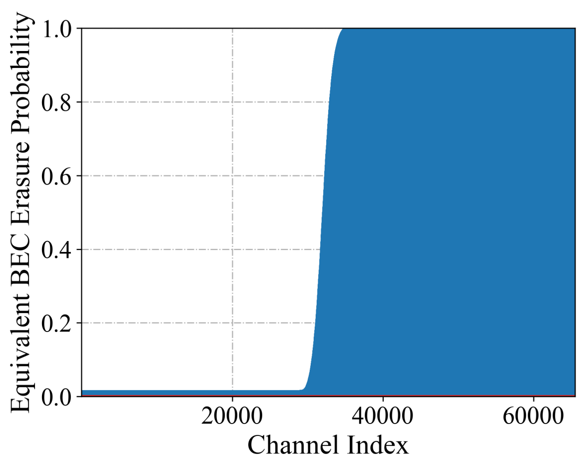
sorted



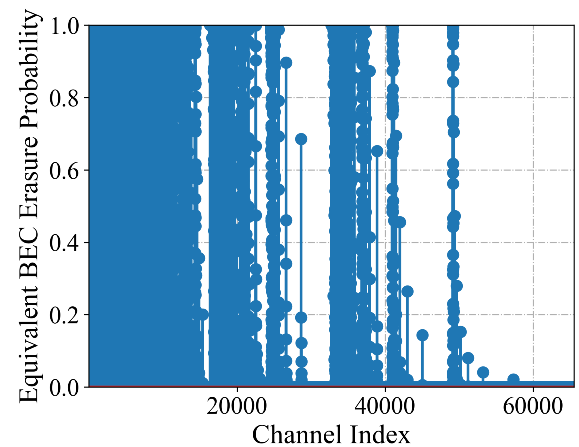
$n = 2^{16}, \varepsilon = 0.5$



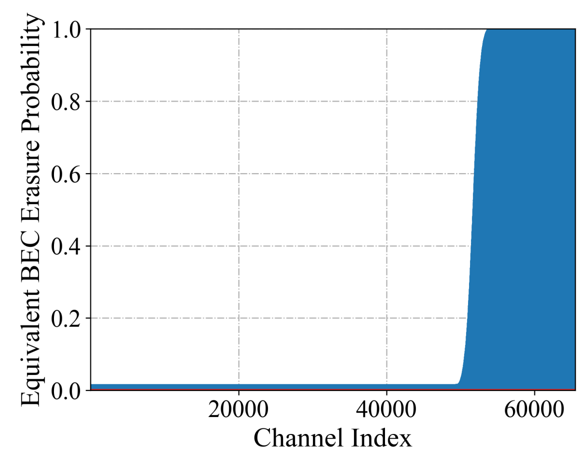
sorted



$n = 2^{16}, \varepsilon = 0.2$



sorted



n: Number of channels, ε: BEC erasure probability

ECC Based on Channel Polarization

Remark from channel polarization phenomenon

1. After applying η-fold of the basic transformation, we have a total of 2^{η} channels.
2. When η approaches infinity ($\eta \to \infty$),
   - The number of channels with moderate values approaches zero.
   - All the other channels are either perfectly reliable ($I(\Gamma^{\cdots}) \to 1$) or totally unreliable ($I(\Gamma^{\cdots}) \to 0$).
3. The fraction of channels that become perfectly reliable *approximately equals the capacity of the channel.*

Key ideas of polar codes

1. Assign determined values, *denoted as frozen bits*, on the unreliable channels.
2. Assign information bits on the reliable channels.

Remarks

- Very long code length is needed for efficient polarization to happen => *Theoretically, polar codes can achieve capacity with a very long code length.*
- For finite η, there are intermediate channels which are neither good nor bad. A simple solution is to transmit also frozen bits on these channels, leading to a *rate loss*.

Encoding: Notations & Example

The polar encoding depends on three parameters:

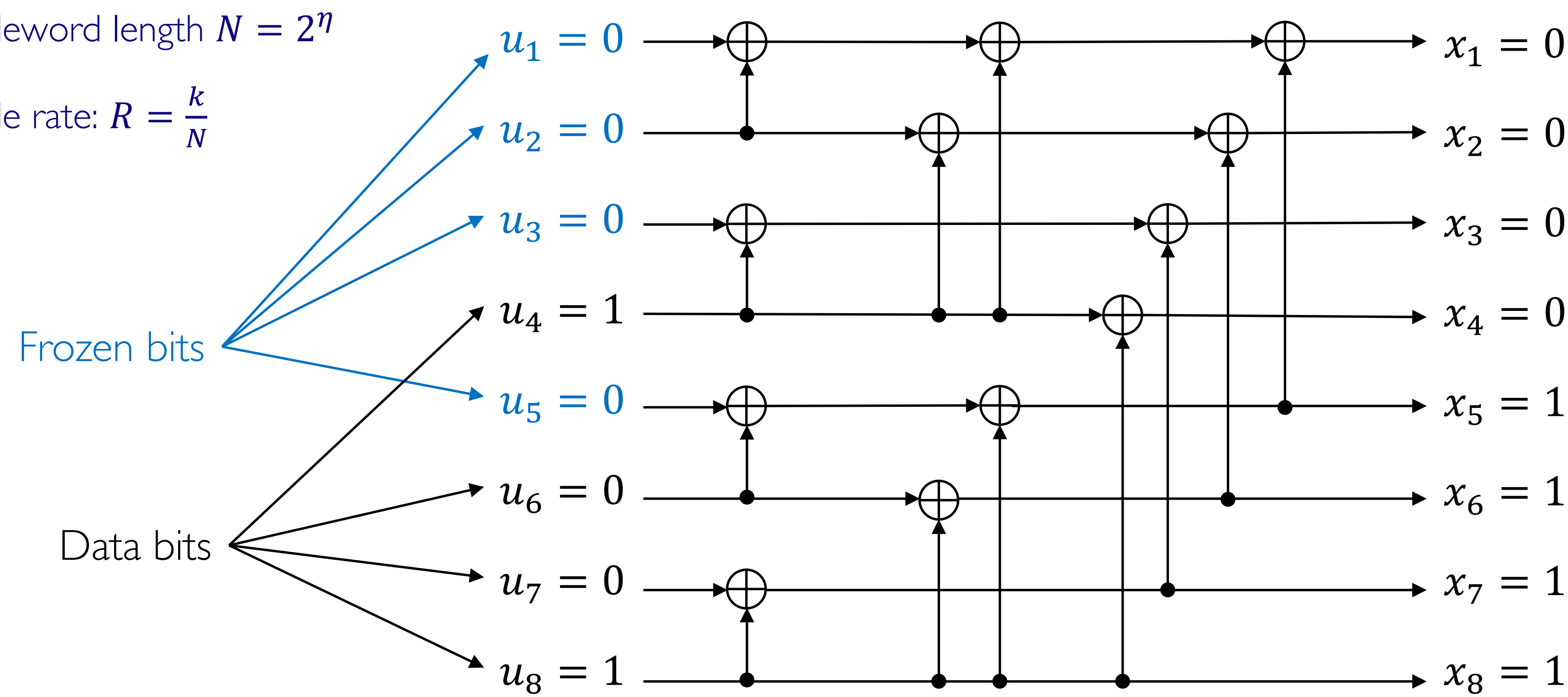
- k: # of information bits
- N: codeword length
- $\mathcal{F}$: location of the frozen bits

Codeword length $N = 2^\eta$

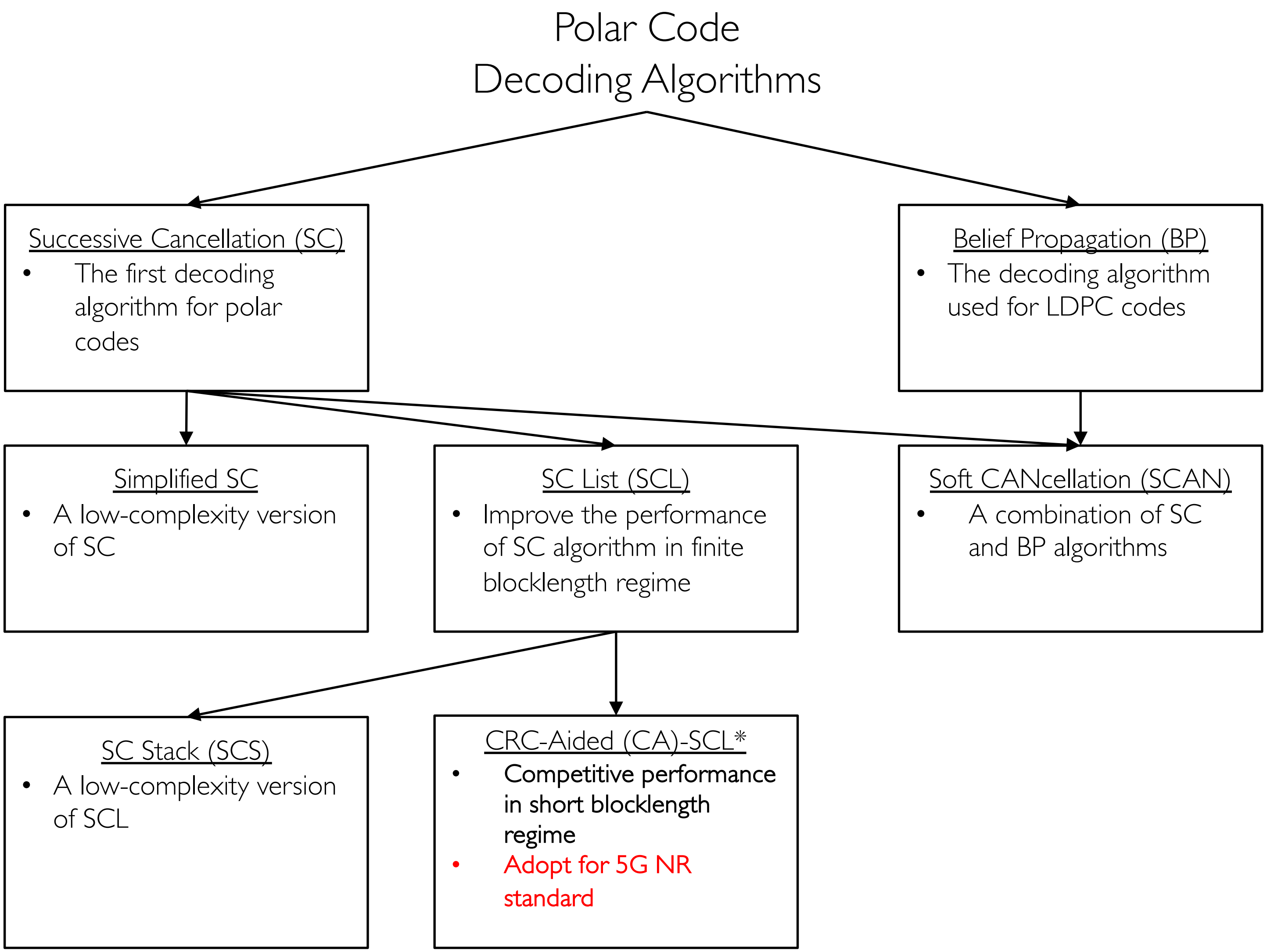
Code rate: $R = \frac{k}{N}$

<u>Example:</u> An $N = 8$ polar code having $k = 4$, $\mathcal{F} = \{1, 2, 3, 5\}$.

The data is $\mathbf{d} = [1\ 0\ 0\ 1]$



Decoding Algorithms: A Big Picture



****CRC:*** Cyclic Redundancy Check – An error detecting code

Successive Cancellation (SC)

Key idea:

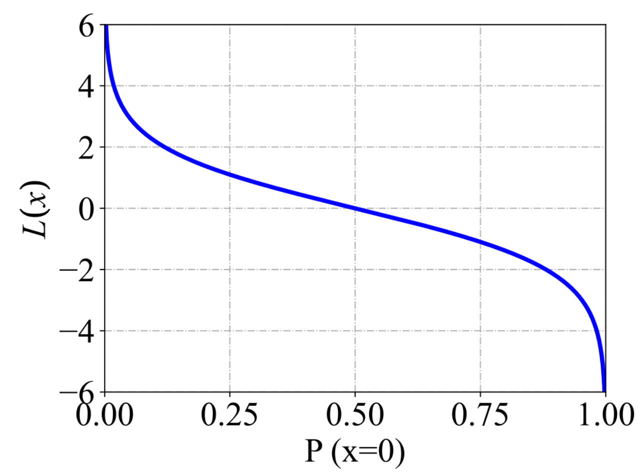
- The decoding is performed sequential. Each bit is decoded one after the other.
- The SC decoding algorithm can be seen as a reverse process of the encoder.
- The algorithm operates on the same circuit of the encoder.
- The input is **log likelihood ratio.**

Log likelihood Ratio (LLR)

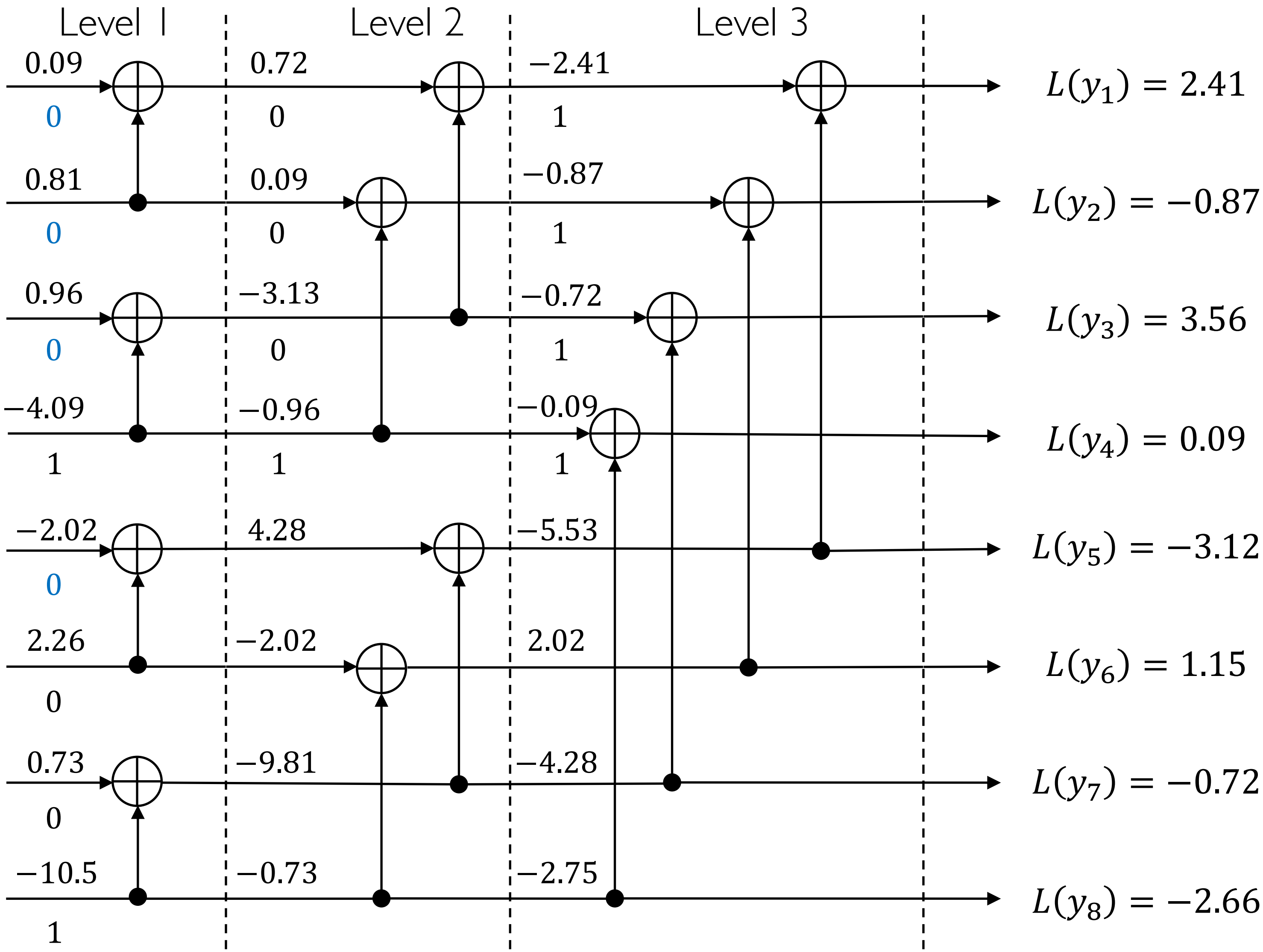
- Let x be the binary-valued random variable taking values on set {0, 1}.
- The LLR of x measures **the reliability of x** and can be computed as

$$L(x) = \ln \frac{P(x=1)}{P(x=0)}$$

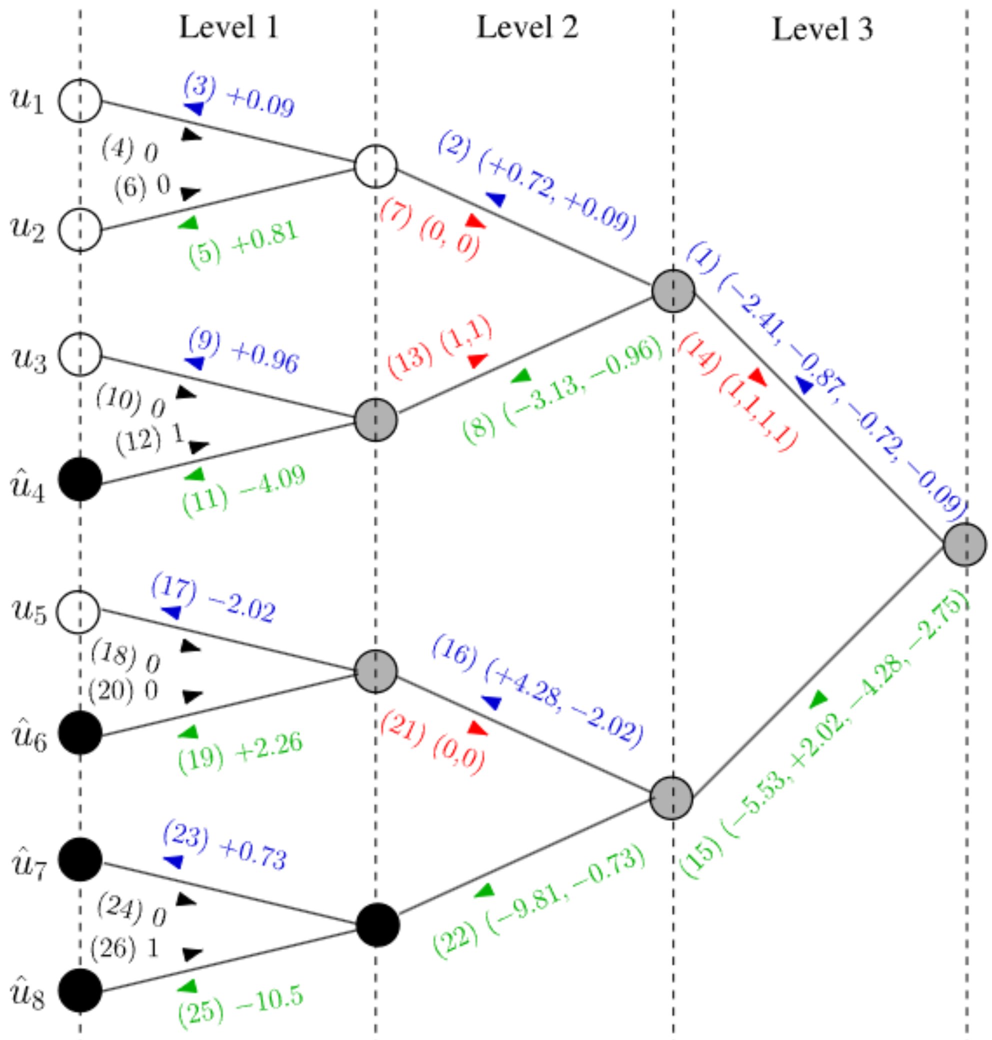
- If $P\ (x=0) \to 0, |L(x)| \to \infty$
- If $P\ (x=0) = P(x=1) = 1/2, |L(x)| \to 0$



Successive Cancellation (SC)



Successive Cancellation (SC): Information Flow



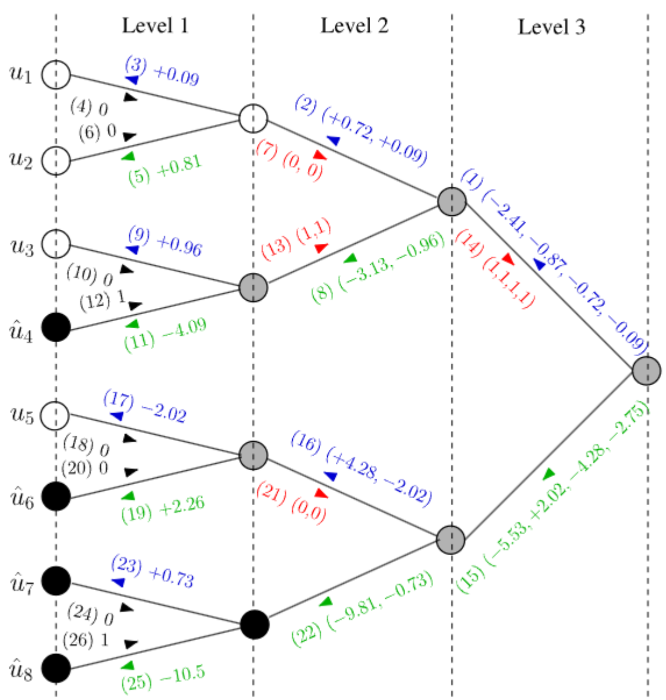
Successive Cancellation List (SCL)

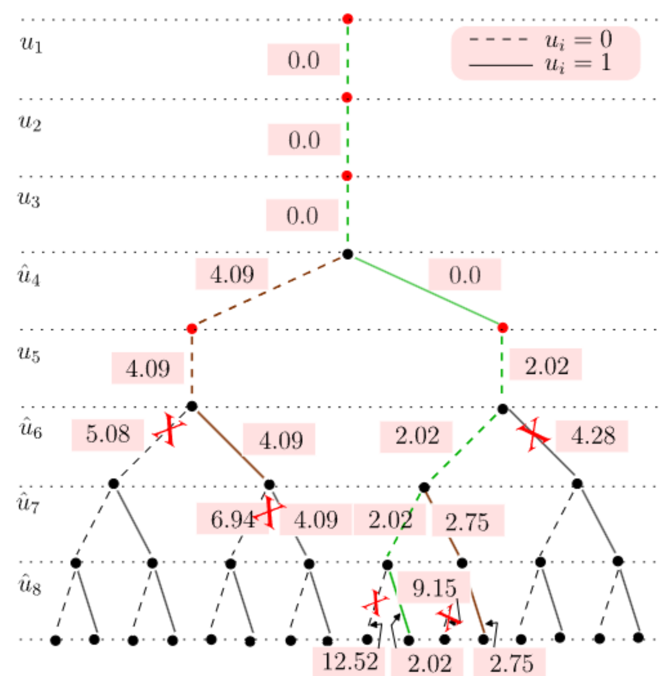
Drawbacks of SC decoding algorithm: It can only work well with a very long codeword, where the polarization effect is extreme.

Key idea to improve:

- Maintain a list of candidate paths, which is built up when the algorithm proceeds.
- Delete the worst paths and keep the maximum number of candidate paths as L.

By additionally considering the CRC, the performance of SCL decoding algorithm *can be on par with LDPC codes in short and moderate block lengths.*



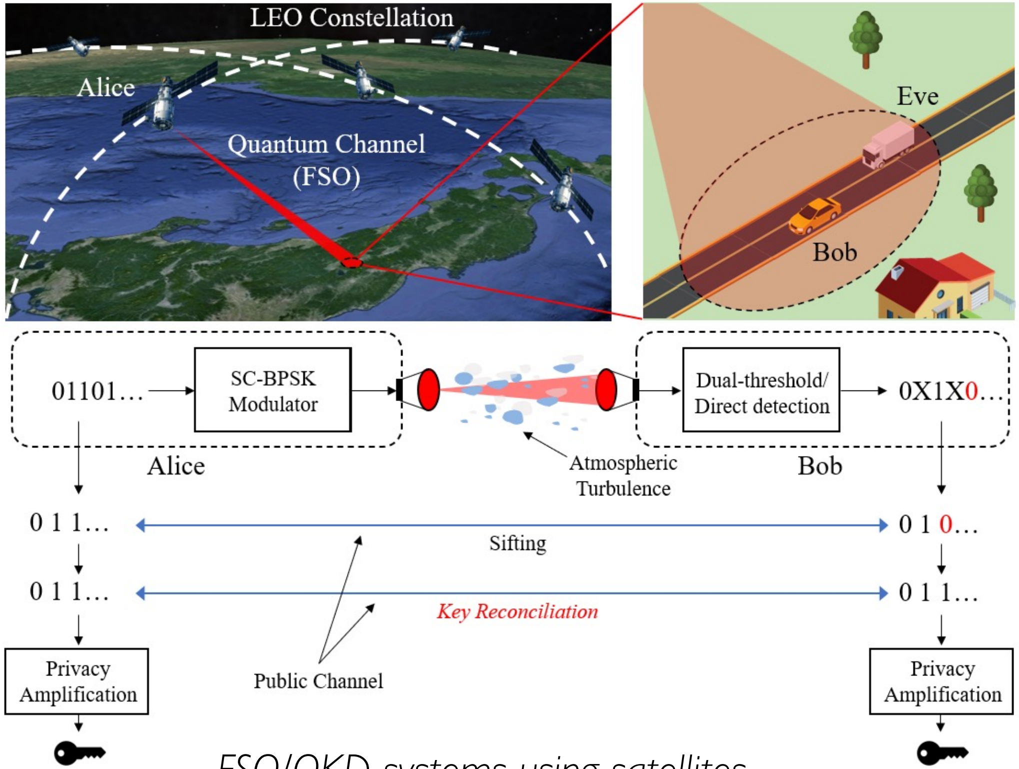


Outline

- Part I: An Introduction to Polar Codes
- Part II: Information Reconciliation with Polar Code for Satellite QKD Systems

Key Reconciliation for Satellite QKD Systems

- Wireless QKD systems using FSO
  - Support wireless/mobile applications, e.g., secure Internet of Vehicles (IoV)
- We focus on key reconciliation step in the post-processing phase
  - KR: attempt to reconcile sifted keys from both sides



FSO/QKD systems using satellites

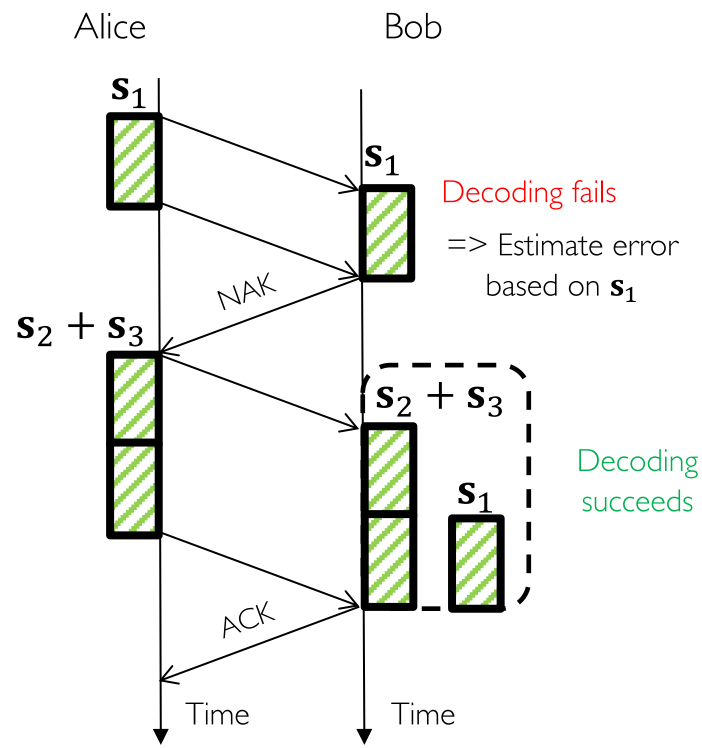
- Why is it important:
  - The uncertainty of time-varying FSO channel ⇒ Highly fluctuating quantum bit-error rate (QBER)
  - Long propagation delay of satellite communication (in order of milliseconds) ⇒ Increase the latency of the KR.

My Previous Work: Blind Reconciliation with LDPC Codes

- Key idea: Alice reveals more information after each decoding attempt until Bob can correct

- This can be done with a special family of LDPC Codes (Protograph LDPC)

- Syndrome-based error estimation is implemented to reduce the number of required communication rounds.



Flow chart of the blind reconciliation method

An Open Issue: KR for Short Blocklength

- An open issue: *In some situations, the sifted key lengths are relatively short (~ 1000 bits).*
  - Atmospheric loss reduces the arrived photon rates
  - DV-QKD protocols have low repetition rate.

⇒ *It is necessary to have a proper KR design for short block length.*

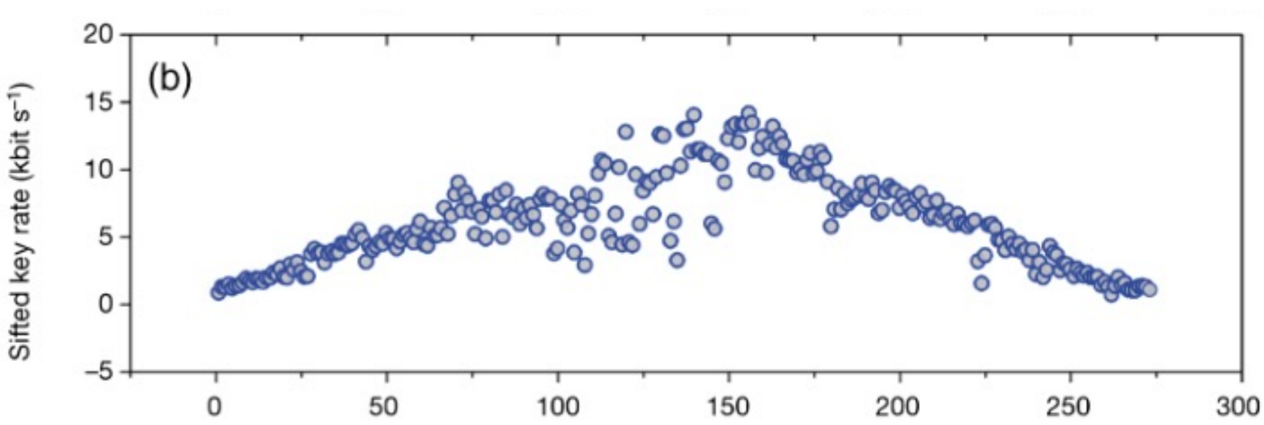


Fig. Sifted key rate versus time of the Micius quantum satellite to the ground station

Possible Solutions: *sp*-RC-LDPC Code

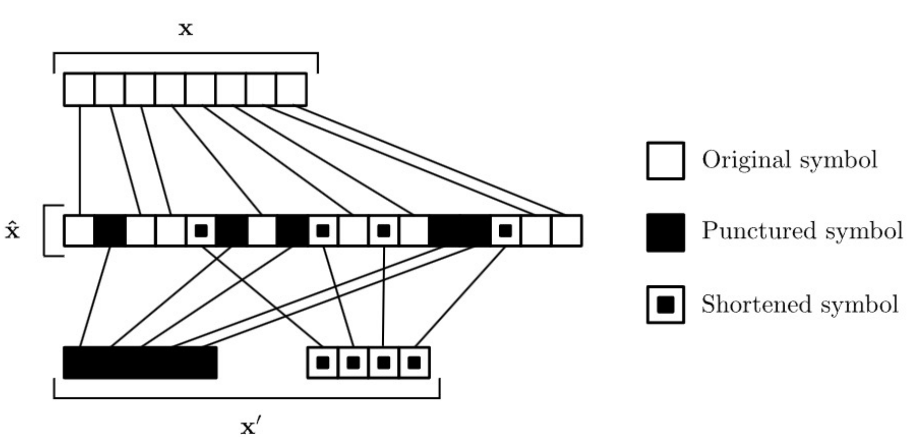
Possible coding solutions for blind reconciliation: (1) RC-LDPC with shortening and puncturing (sp), (2) protograph RC-LDPC code, and (3) polar code.

1. sp-LDPC code design

- Adding random bits to the sifted keys
- These bits are treated as puncturing and shortening bits at Bob's decoder
- When a decoding attempt fails, Alice will disclose more punctured bits to Bob.

Drawbacks: *The code rates in the family depends on the fraction of punctured bits, α*

- *If α is high => limit the highest code rate*
- *If α is small => limit the code range of the family*



$$R_{\max}^{\mathrm{LDPC}} := \frac{R_{\mathrm{base}}}{1-\alpha} \geq R \geq \frac{R_{\mathrm{base}}-\alpha}{1-\alpha} =: R_{\min}^{\mathrm{LDPC}}$$

The code rate range of the *sp*-RC-LDPC family. α denotes the fraction of punctured bits

Possible Solutions: Protograph LDPC Code

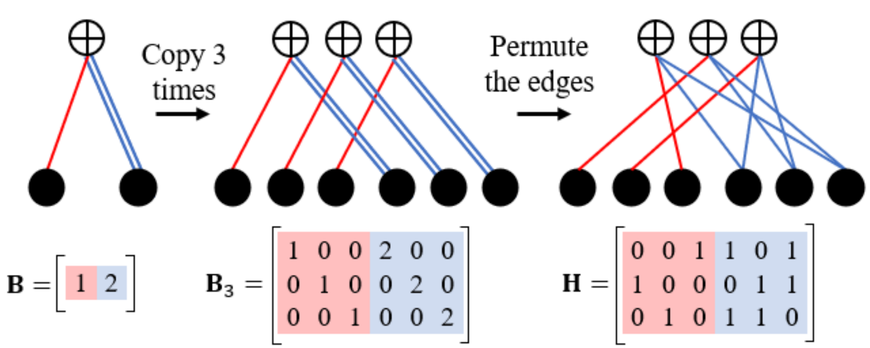
2. Protograph LDPC code

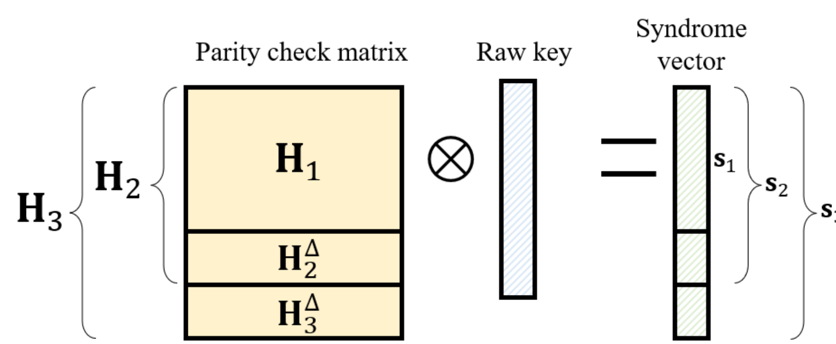
- The LDPC codes are constructed based on a small prototype, denoted as protograph.
- The construction is conducted via a "copy-and-permute" operation.
- To facilitate the operation of blind reconciliation, the below structure is required.

Drawbacks: *Ineffective design for short block length*

- *Large protographs are required to have a wide range of code rates*
- *However, this will limit the possible permuting options when lifting the protograph => introduce short cycles to the lifted matrix.*

Short-length protograph LDPC codes construction usually prefer small protograph [R1].





[R1] Van Nguyen, Thuy, and Aria Nosratinia. "Rate-compatible short-length protograph LDPC codes." *IEEE Commun. Lett.*, 2013.

Possible Solution: Polar Code

3. Polar code

- Polar code with CA-SCL decoding algorithm can achieve competitive performance in a short blocklength regime.
- Polar codes can adapt code rate by disclosing bits => No bound for low code rate

➡ *The design of blind reconciliation with polar codes for satellite-based QKD systems has not been investigated in the literature.*

Research Goals

1. Propose a design of blind reconciliation with polar codes for short length KR in satellite-based QKD systems
   - The methods focus on reducing the number of required communication rounds via the channel estimation using frozen bits.
2. Show effectiveness of the proposed design with the state-of-the-art approach in terms of KR efficiency, KR throughput, and final key rate.
3. Investigate the performance of the proposed design for the considered systems with BB84 protocols