Non-Binary LDPC Codes for Quantum Key Distribution

Lara Dolecek

Based on joint work with:
D. Mitra, L. Tauz, M. Sarihan, J. Shreekumar,
Prof. C. W. Wong, and †Prof. E. Soljanin
ECE Department, UCLA, †EE Department Rutgers University

MSCT, TUM, Germany
April 3-5, 2024

Outline

1. Background and Motivation

2. System Model

3. NB-LDPC codes for Quantum Key Distribution
   - Preliminaries
   - Channel code design
   - Sequential Decoding and Interactive Communication
   - Privacy Amplification-Aware LDPC Code Design

4. Concluding Remarks and Future Outlook

Outline

Quantum Key Distribution (QKD)

- Quantum Communication
  - Takes advantage of the laws of quantum physics to convey data
  - Rapidly growing interest and investment; 6G technology

Quantum Key Distribution (QKD)

- Quantum Communication
  - Takes advantage of the laws of quantum physics to convey data
  - Rapidly growing interest and investment; 6G technology
  - One-time-pad encryption is perfectly secure but it requires one time random key generation, which is hard to implement

Quantum Key Distribution (QKD)

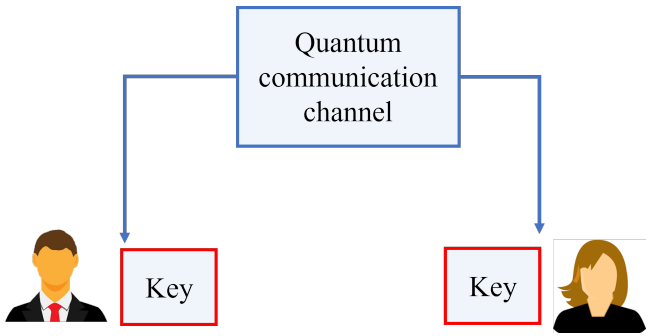
- Quantum Communication
  - Takes advantage of the laws of quantum physics to convey data
  - Rapidly growing interest and investment; 6G technology
  - One-time-pad encryption is perfectly secure but it requires one time random key generation, which is hard to implement

- Quantum Key Distribution (QKD) (Gisin '02)

Quantum Key Distribution (QKD)

- Quantum Communication
  - Takes advantage of the laws of quantum physics to convey data
  - Rapidly growing interest and investment; 6G technology
  - One-time-pad encryption is perfectly secure but it requires one time random key generation, which is hard to implement

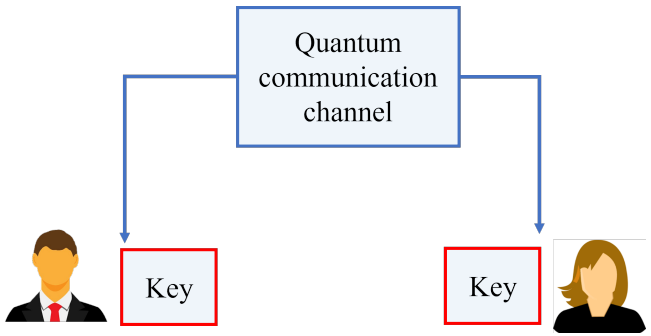
- Quantum Key Distribution (QKD) (Gisin '02)
  - Offers a physically secure way for effectively sharing an encryption key over a quantum communication channel



Quantum Key Distribution (QKD)

- Quantum Communication
  - Takes advantage of the laws of quantum physics to convey data
  - Rapidly growing interest and investment; 6G technology
  - One-time-pad encryption is perfectly secure but it requires one time random key generation, which is hard to implement

- Quantum Key Distribution (QKD) (Gisin '02)
  - Offers a physically secure way for effectively sharing an encryption key over a quantum communication channel
  - We focus on Discrete Variable (DV)-QKD



QKD Protocol

- A QKD protocol consists of two phases:

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

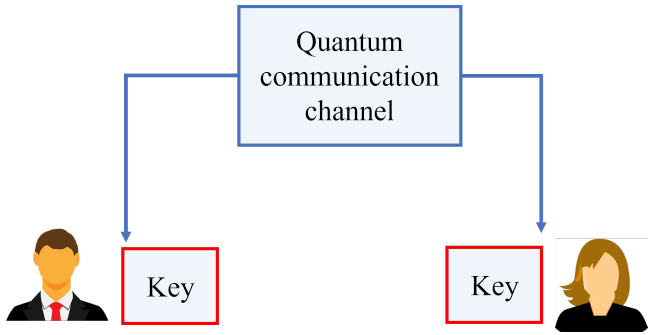
Quantum Phase: Key Generation

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:



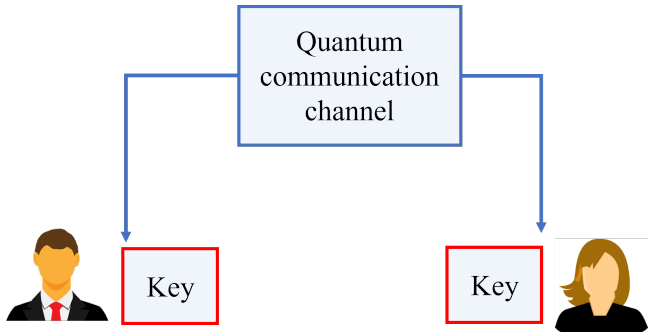
QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:
  $\rightarrow$ may disagree at certain positions

Classical Phase: Post-post processing of raw keys

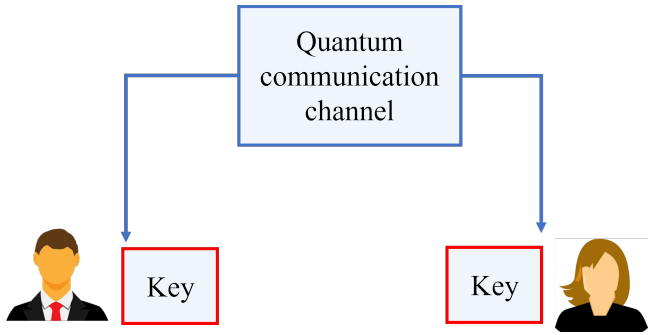


QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:
  $\rightarrow$ may disagree at certain positions



Classical Phase: Post-post processing of raw keys

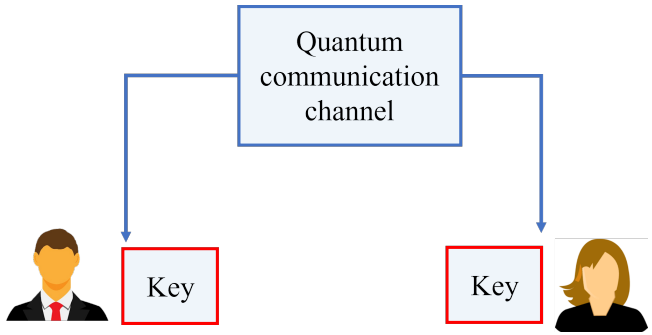
- Involves communication over a classical channel (public to everyone)

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:
  $\rightarrow$ may disagree at certain positions



Classical Phase: Post-post processing of raw keys

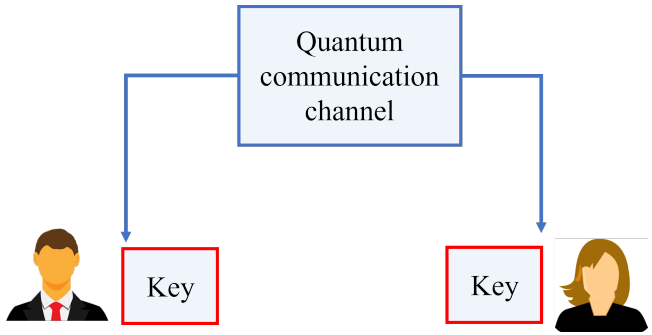
- Involves communication over a classical channel (public to everyone)
  1) **Information reconciliation:** Alice and Bob correct the errors in the raw keys via communication over the public channel

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:
  $\rightarrow$ may disagree at certain positions



Classical Phase: Post-post processing of raw keys

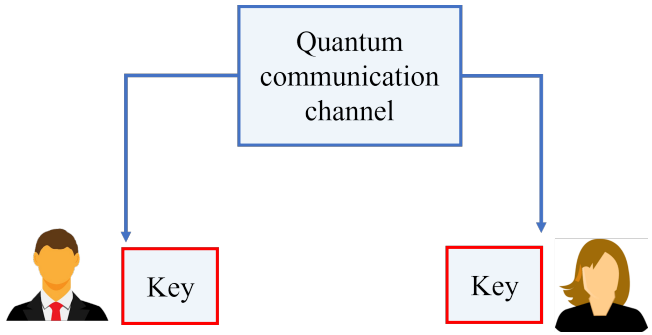
- Involves communication over a classical channel (public to everyone)
  1) **Information reconciliation:** Alice and Bob correct the errors in the raw keys via communication over the public channel
  2) **Verification**: Alice and Bob verify if the reconciled keys indeed match

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:
  $\rightarrow$ may disagree at certain positions



Classical Phase: Post-post processing of raw keys

- Involves communication over a classical channel (public to everyone)

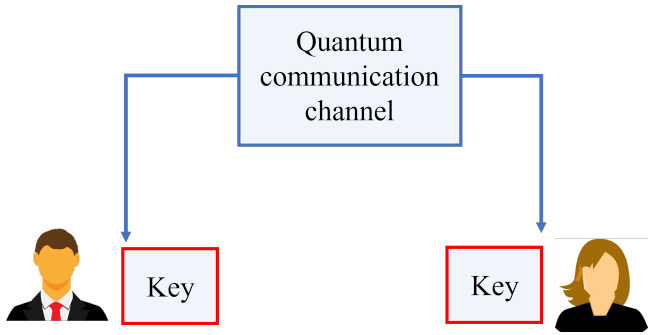
  1) **Information reconciliation:** Alice and Bob correct the errors in the raw keys via communication over the public channel
  2) **Verification**: Alice and Bob verify if the reconciled keys indeed match
  3) **Privacy Amplification**: Reduce the information obtained by eavesdropper Eve to arrive at final secret keys
  (via hashing and compression)

QKD Protocol

- A QKD protocol consists of two phases:
  1) Quantum Phase 2) Classical Phase

Quantum Phase: Key Generation

- Alice and Bob use a quantum communication channel to generate a set of raw keys:
  $\rightarrow$ may disagree at certain positions



Classical Phase: Post-post processing of raw keys

- Involves communication over a classical channel (public to everyone)

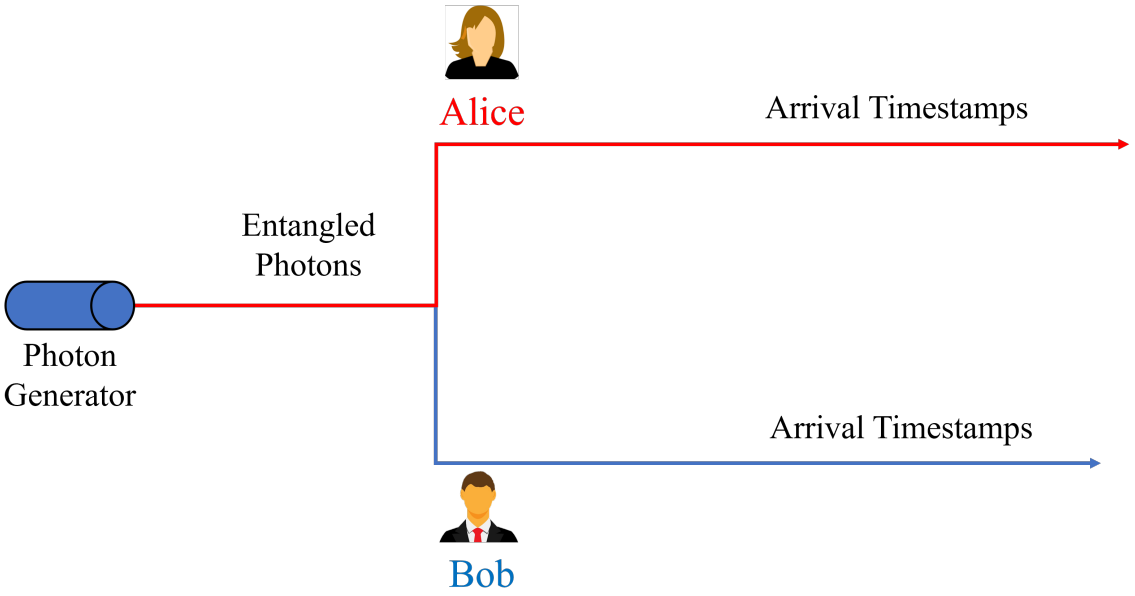
  1) **Information reconciliation:** Alice and Bob correct the errors in the raw keys via communication over the public channel
  2) **Verification**: Alice and Bob verify if the reconciled keys indeed match
  3) **Privacy Amplification**: Reduce the information obtained by eavesdropper Eve to arrive at final secret keys
  (via hashing and compression)

Error Correction Coding is applied to the information reconciliation phase.

Time-Bin QKD Protocol: Promise of High Key Rates

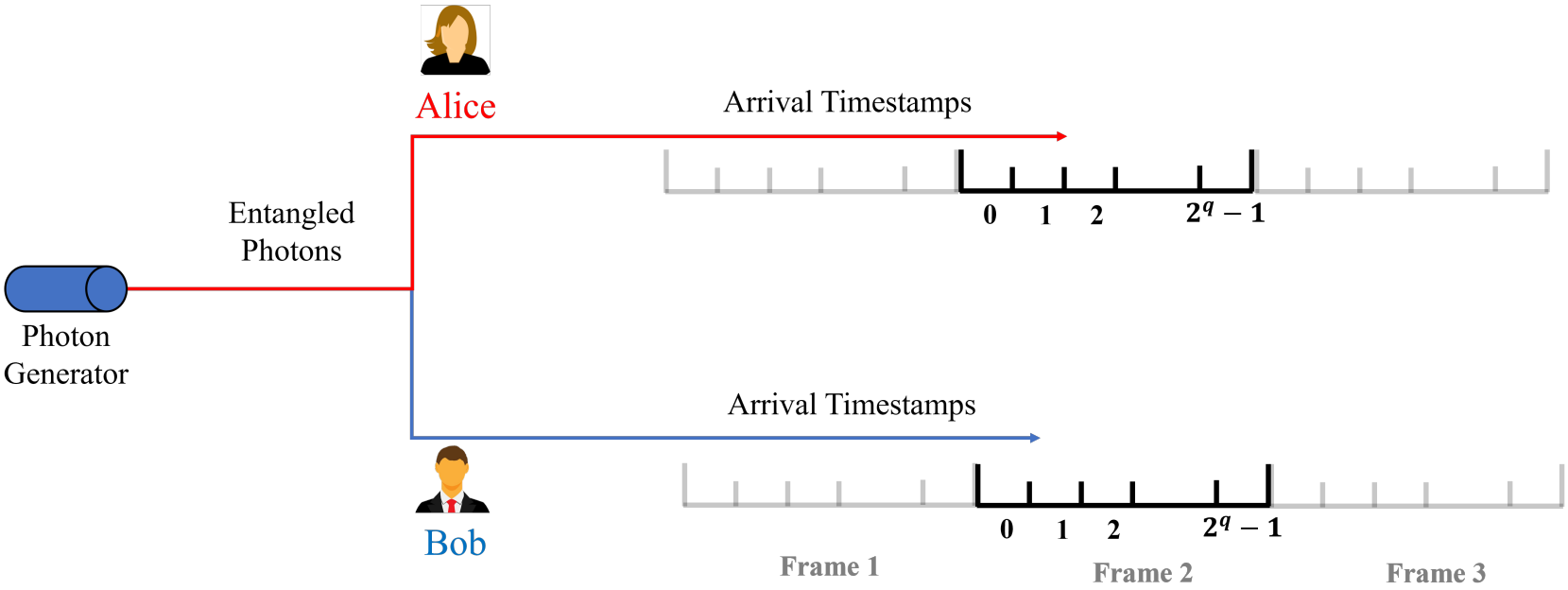
- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob

Time-Bin QKD Protocol: Promise of High Key Rates



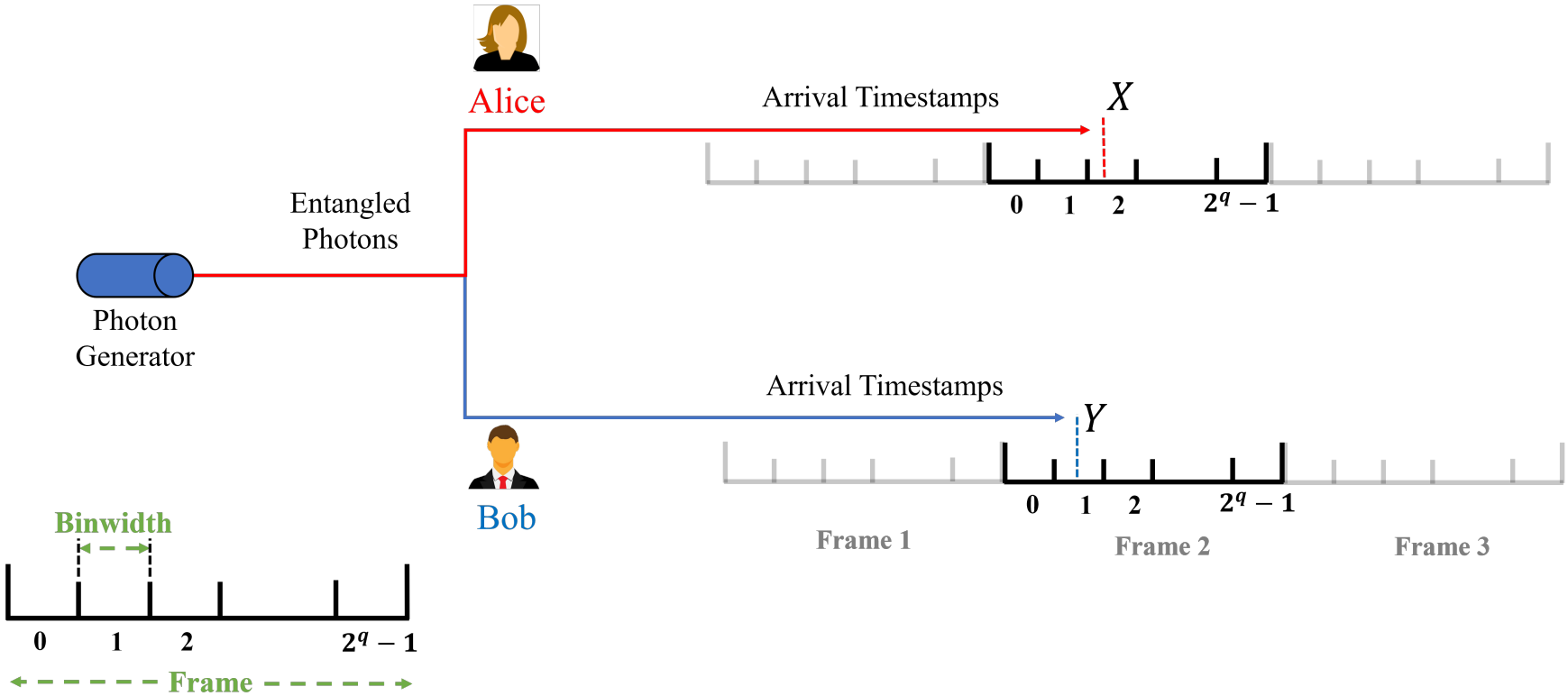
- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob

Time-Bin QKD Protocol: Promise of High Key Rates



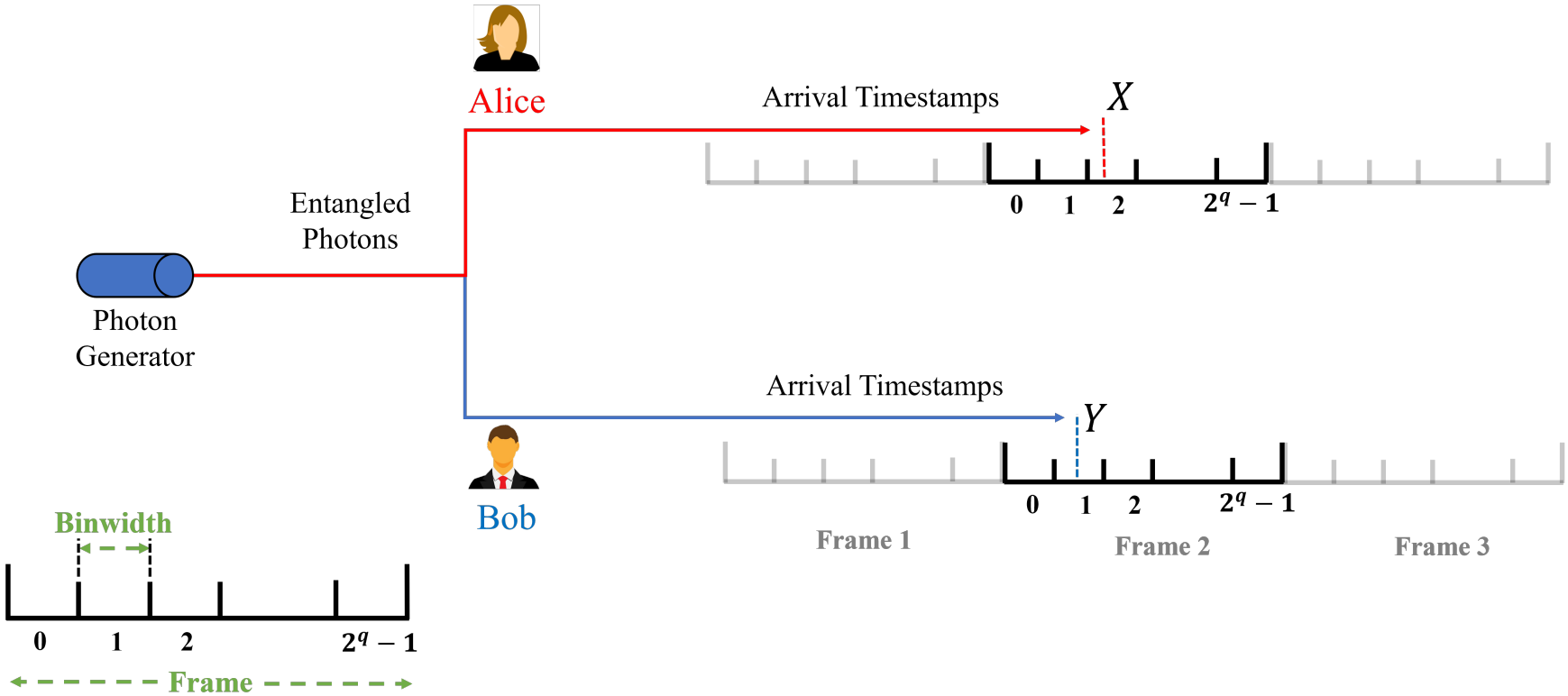
- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob

Time-Bin QKD Protocol: Promise of High Key Rates



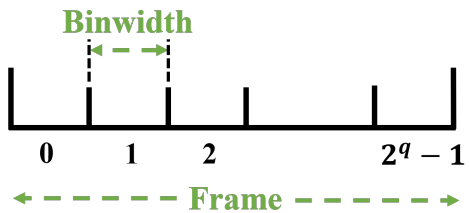
- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob
  - Alice and Bob record the quantized arrival time of photons

Time-Bin QKD Protocol: Promise of High Key Rates



- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob
  - Alice and Bob record the quantized arrival time of photons
  - Pulse Position Modulation: Each photon pair corresponds to a non-binary symbol

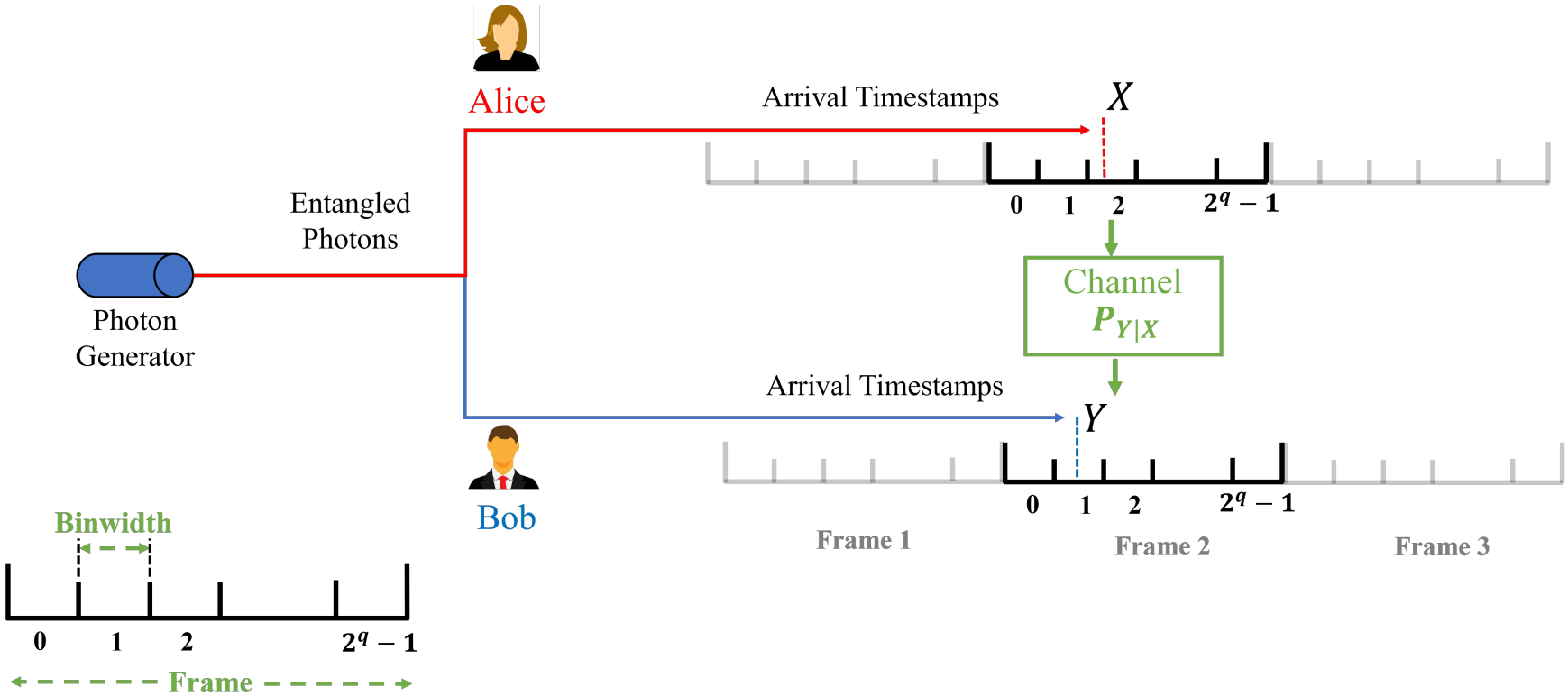
Time-Bin QKD Protocol: Promise of High Key Rates



- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob
  - Alice and Bob record the quantized arrival time of photons
  - Pulse Position Modulation: Each photon pair corresponds to a non-binary symbol

Multiple bits per entangled photon pair aim to provide a higher secure key rate.

Time-Bin QKD Protocol: Promise of High Key Rates

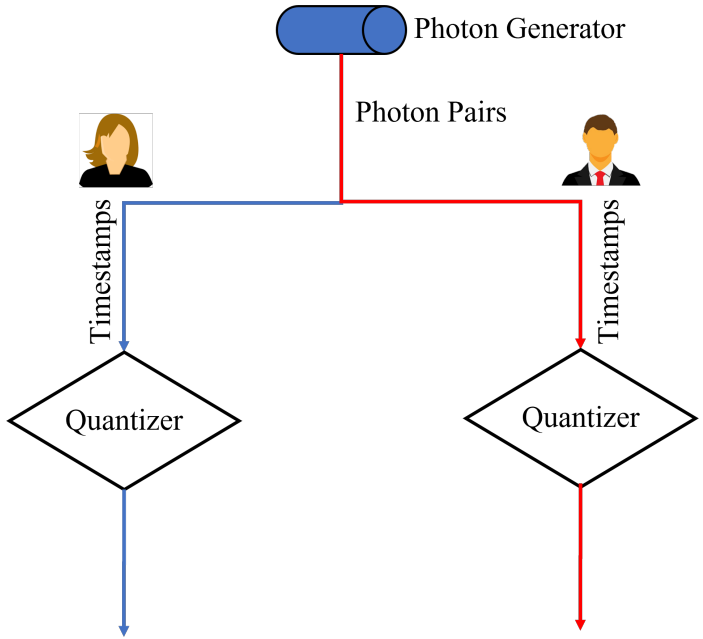


- Energy-time entangled photons are used in the quantum phase (Zhong '15)
  - Entangled photons pairs are sent to Alice and Bob
  - Alice and Bob record the quantized arrival time of photons
  - Pulse Position Modulation: Each photon pair corresponds to a non-binary symbol

Multiple bits per entangled photon pair aim to provide a higher secure key rate.

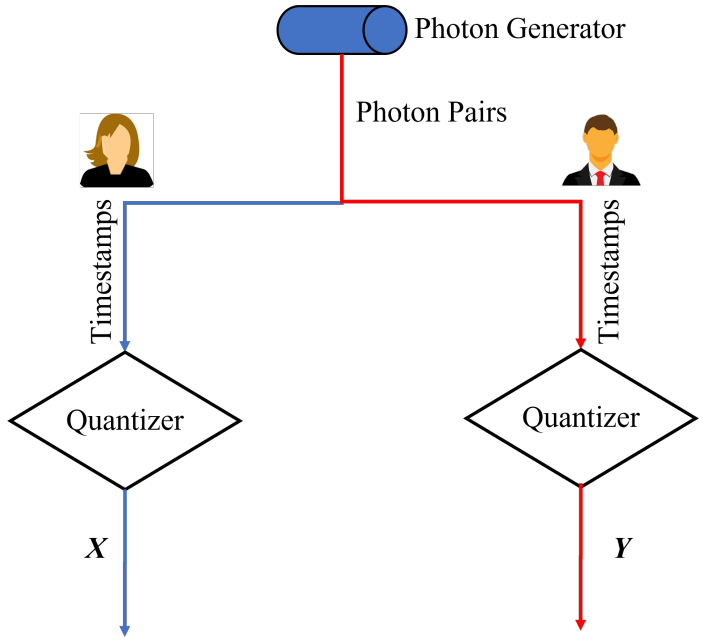
Outline

Information Reconciliation



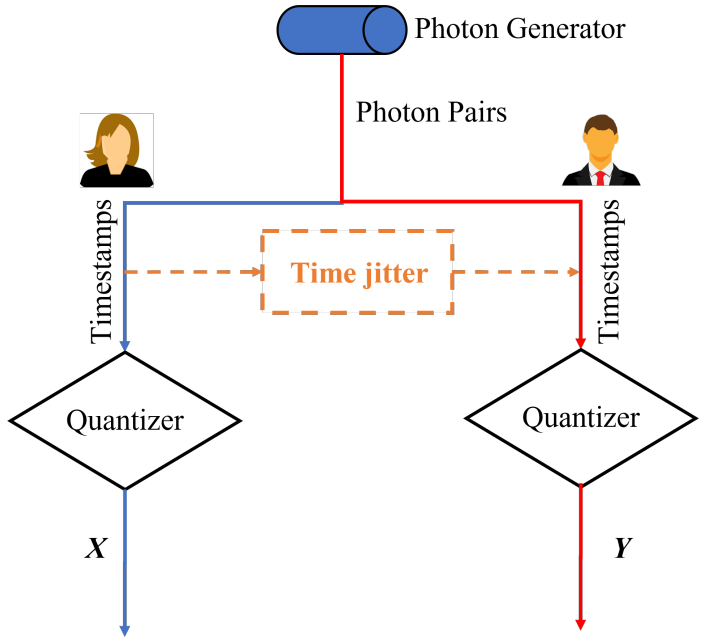
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences



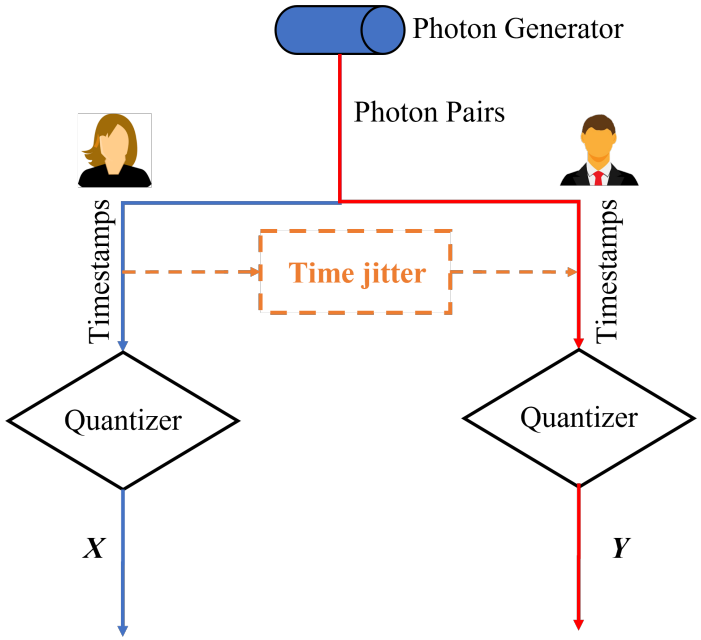
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences



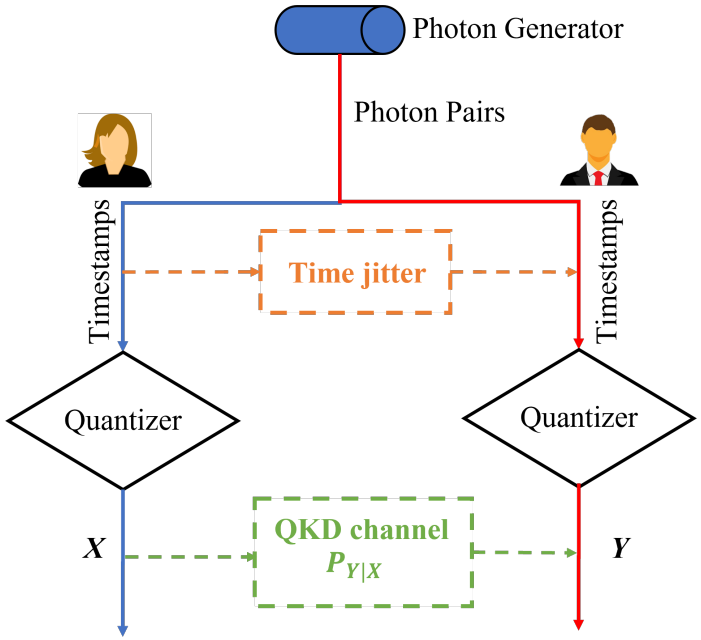
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences



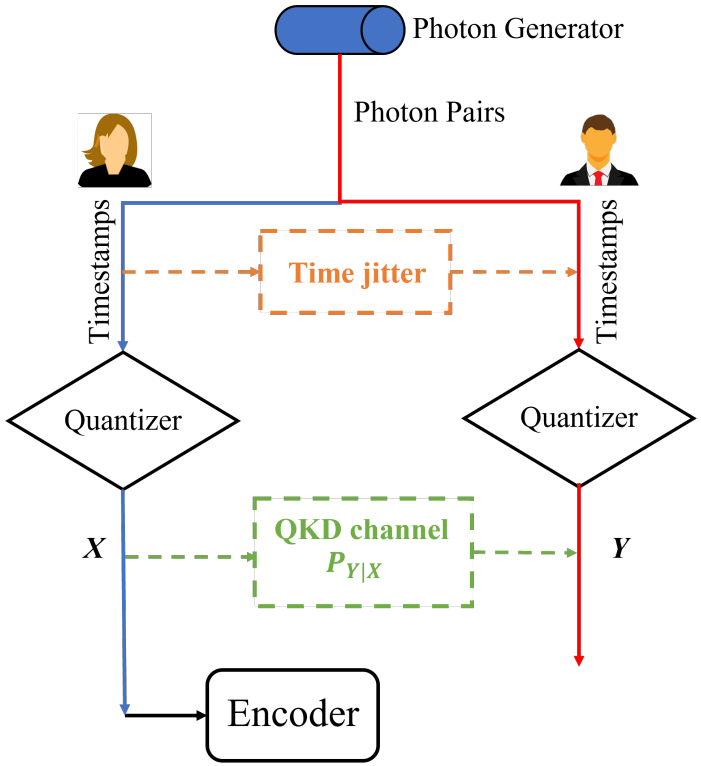
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences
  $\rightarrow$ modeled as a QKD channel and corrected using ECC



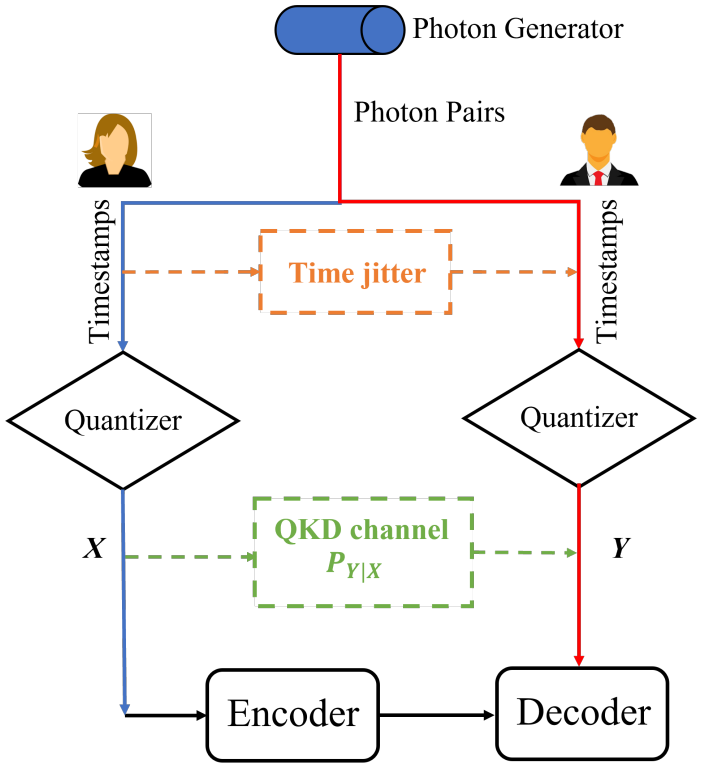
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences
  $\rightarrow$ modeled as a QKD channel and corrected using ECC
- Alice sends syndrome bits to Bob over public channel



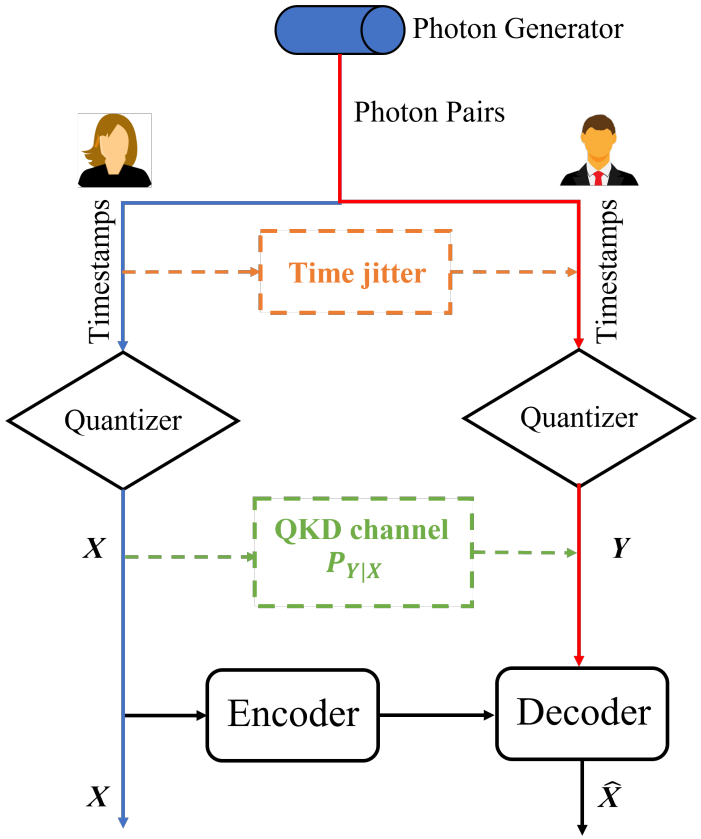
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences
  $\rightarrow$ modeled as a QKD channel and corrected using ECC
- Alice sends syndrome bits to Bob over public channel
- Bob decodes Alice's sequence from the sequence he receives and the parities from Alice using syndrome decoding.



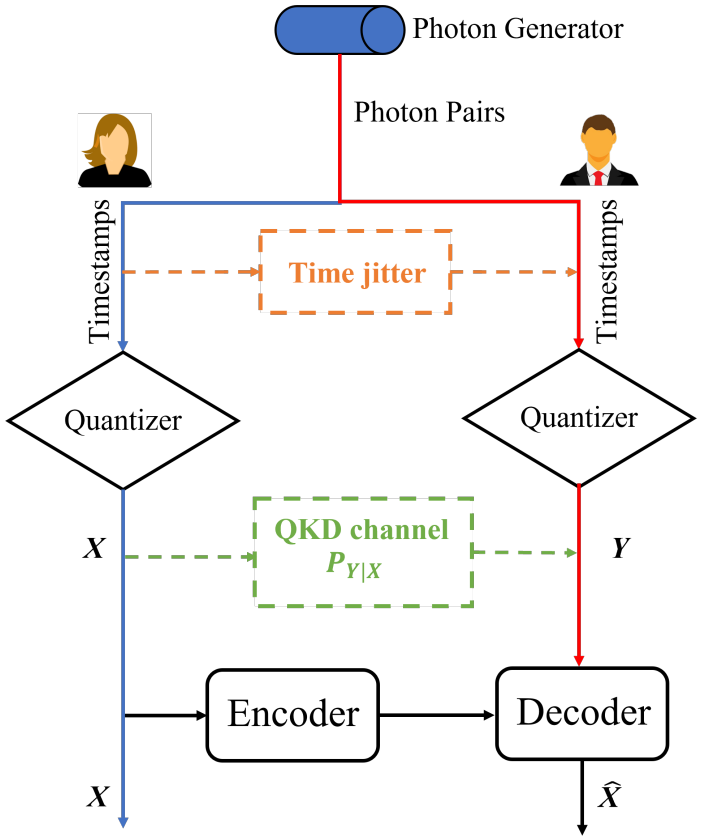
Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences
  $\rightarrow$ modeled as a QKD channel and corrected using ECC
- Alice sends syndrome bits to Bob over public channel
- Bob decodes Alice's sequence from the sequence he receives and the parities from Alice using syndrome decoding.



Information Reconciliation

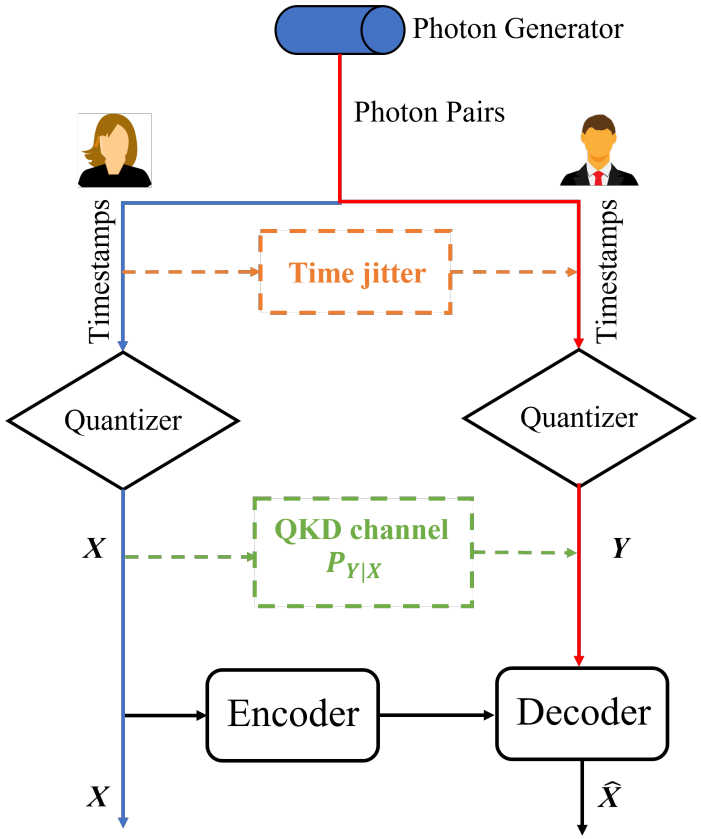
- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences
  $\rightarrow$ modeled as a QKD channel and corrected using ECC
- Alice sends syndrome bits to Bob over public channel
- Bob decodes Alice's sequence from the sequence he receives and the parities from Alice using syndrome decoding.



If decoding is successful, Alice and Bob share the same key.

Information Reconciliation

- The arrival times of photons received by Alice and Bob are quantized and can be regarded as two random sequences
- The discrepancies in the arrival times result in differences between the quantized sequences
  $\rightarrow$ modeled as a QKD channel and corrected using ECC
- Alice sends syndrome bits to Bob over public channel
- Bob decodes Alice's sequence from the sequence he receives and the parities from Alice using syndrome decoding.



If decoding is successful, Alice and Bob share the same key.

- Any information sent over the public channel is seen by Eve and will reduce the final key length (due to privacy amplification)

Earliest Reconciliation Protocol: Cascade

- One of the earliest proposed schemes for information reconciliation (binary)

Figure: https://cascade-python.readthedocs.io/en/latest/protocol.html

Earliest Reconciliation Protocol: Cascade

- One of the earliest proposed schemes for information reconciliation (binary)
- Involves multiple iterations, where each iteration corrects multiple bit errors

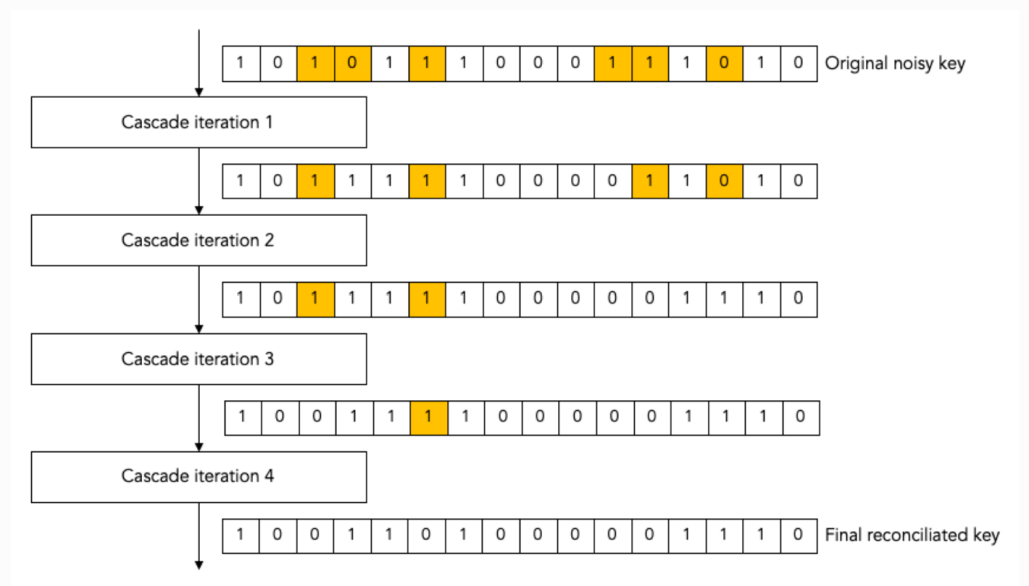
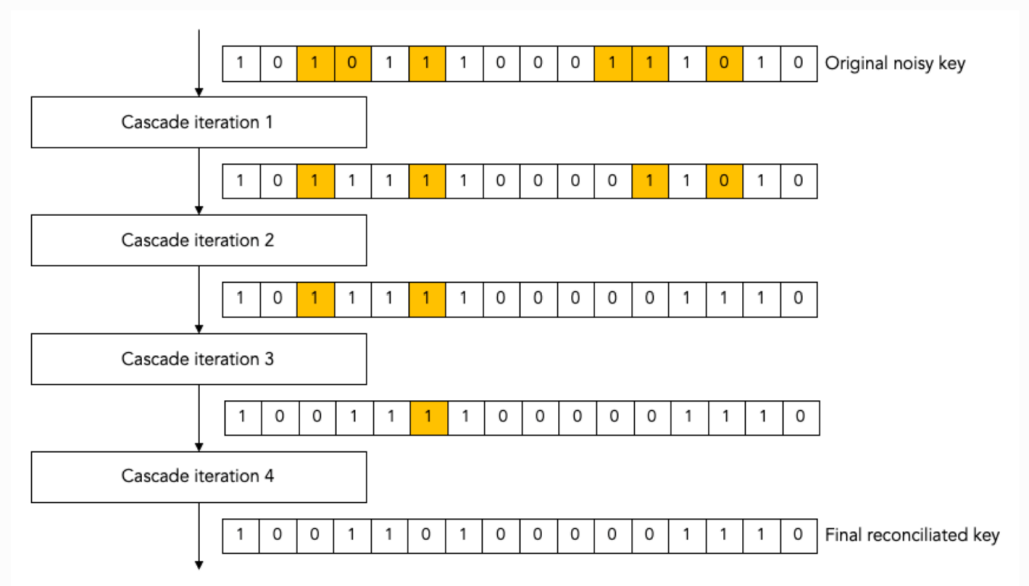


Figure: https://cascade-python.readthedocs.io/en/latest/protocol.html

Earliest Reconciliation Protocol: Cascade

- One of the earliest proposed schemes for information reconciliation (binary)
- Involves multiple iterations, where each iteration corrects multiple bit errors



- During each iteration, the raw key is shuffled and divided into top-level blocks
  - Size of the top-level block depends on the iteration number and the estimated quantum bit-error rate

Figure: https://cascade-python.readthedocs.io/en/latest/protocol.html

Cascade

- Generalizations:

Cascade

- Generalizations:
  - Use other channel codes instead of single parities, e.g., Hamming codes [Buttler '03]

Cascade

- Generalizations:
  - Use other channel codes instead of single parities, e.g., Hamming codes [Buttler '03]
  - Cascade for high-dimensional data (non-binary) [Mueller '23]

Cascade

- Generalizations:
  - Use other channel codes instead of single parities, e.g., Hamming codes [Buttler '03]
  - Cascade for high-dimensional data (non-binary) [Mueller '23]
- High reconciliation efficiency, but inefficient due to many communication rounds between Alice and Bob

Cascade

- Generalizations:
  - Use other channel codes instead of single parities, e.g., Hamming codes [Buttler '03]
  - Cascade for high-dimensional data (non-binary) [Mueller '23]
- High reconciliation efficiency, but inefficient due to many communication rounds between Alice and Bob
- Additionally, the codes do not use any properties specific to the QKD channel

Cascade

- Generalizations:
  - Use other channel codes instead of single parities, e.g., Hamming codes [Buttler '03]
  - Cascade for high-dimensional data (non-binary) [Mueller '23]
- High reconciliation efficiency, but inefficient due to many communication rounds between Alice and Bob
- Additionally, the codes do not use any properties specific to the QKD channel

Can LDPC codes cognizant of the properties of the QKD channel improve key rates ?

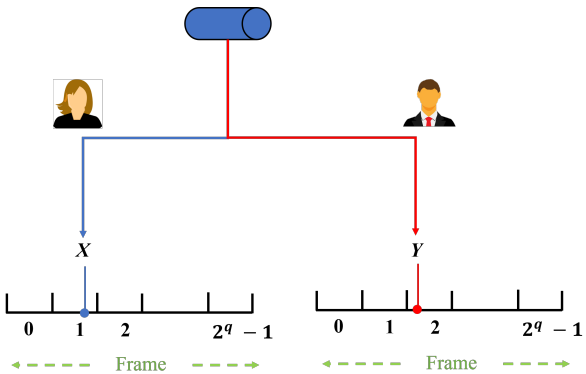
Energy time (ET)-QKD Channel: Overview

- The time domain is divided into frames, each frame contains 2^q bins: each arrival-time is represented by a q-bit symbol

- Experimental Set-up: Wong Group at UCLA.

Energy time (ET)-QKD Channel: Overview

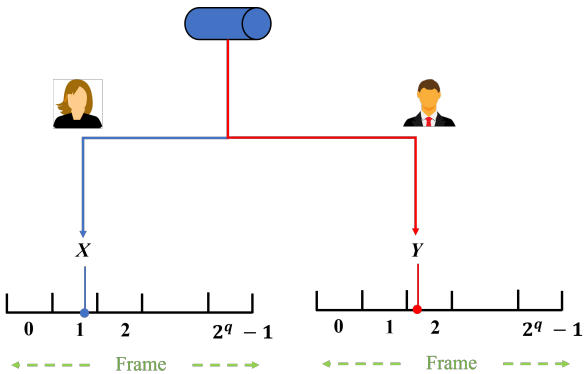
- The time domain is divided into frames, each frame contains 2^q bins: each arrival-time is represented by a q-bit symbol

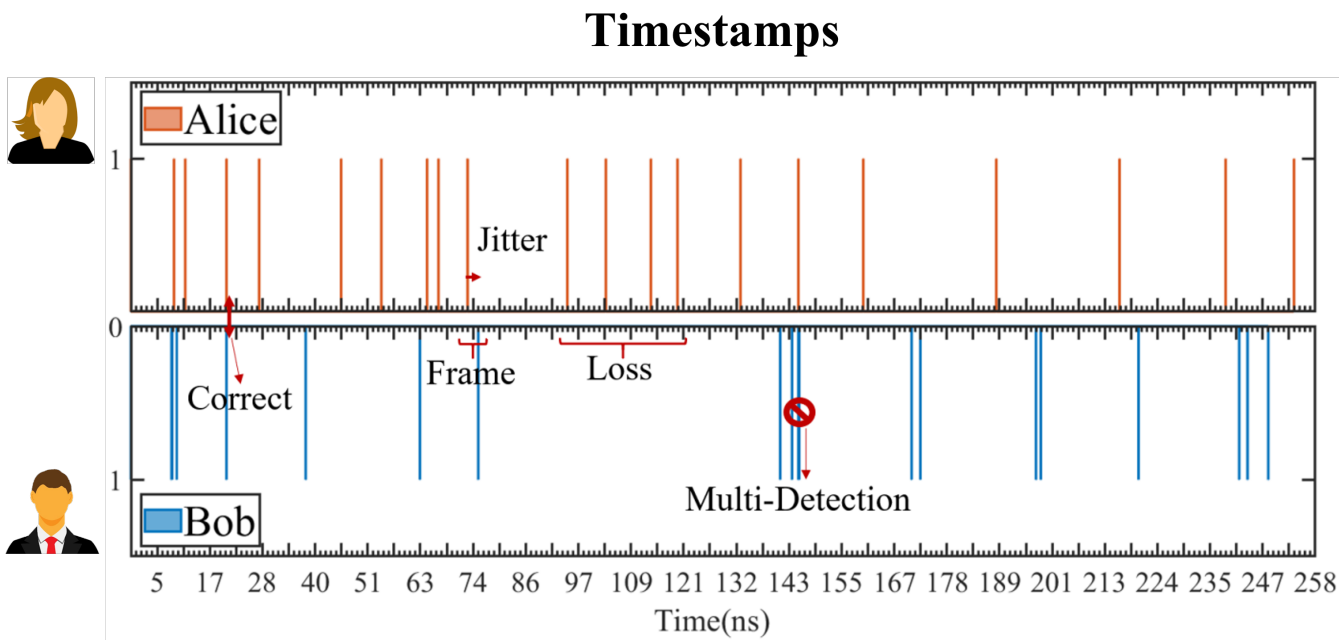


- Experimental Set-up: Wong Group at UCLA.

Energy time (ET)-QKD Channel: Overview

- The time domain is divided into frames, each frame contains 2^q bins: each arrival-time is represented by a q-bit symbol

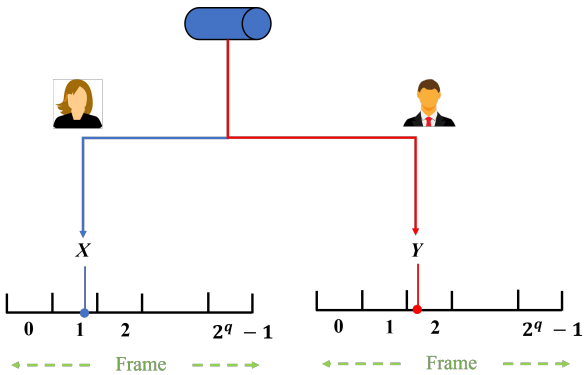


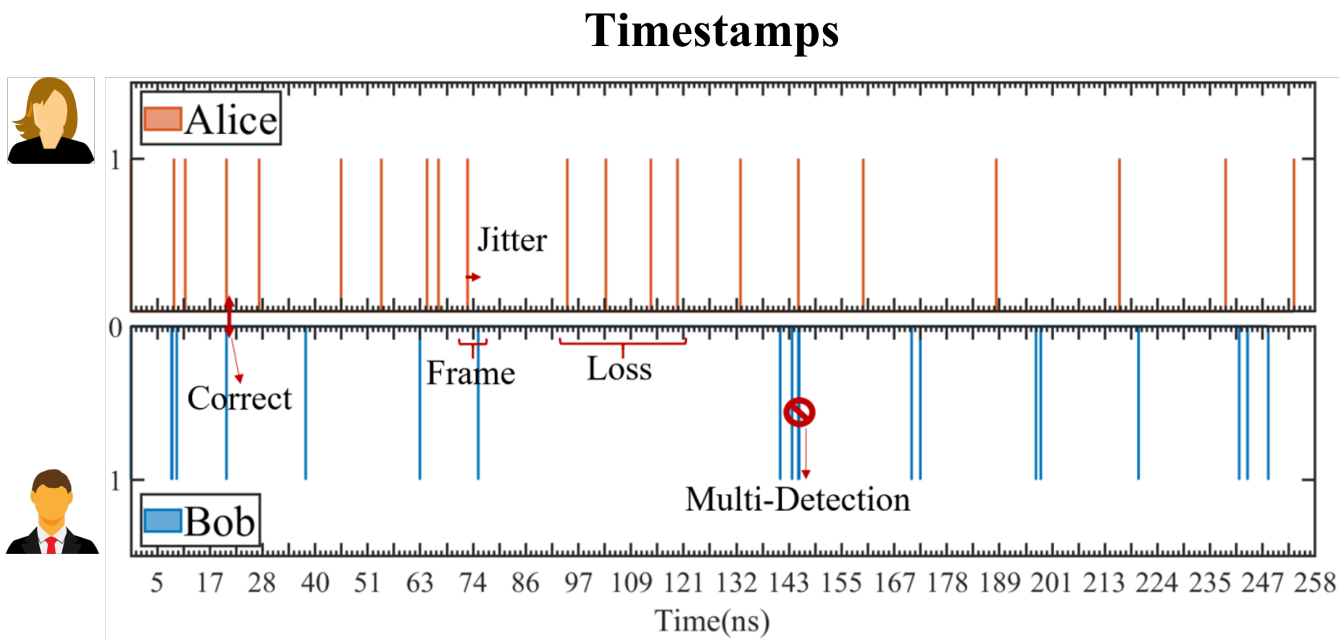


- Experimental Set-up: Wong Group at UCLA.

Energy time (ET)-QKD Channel: Overview

- The time domain is divided into frames, each frame contains 2^q bins: each arrival-time is represented by a q-bit symbol
- Only the frames where both Alice and Bob have exactly one detection are kept

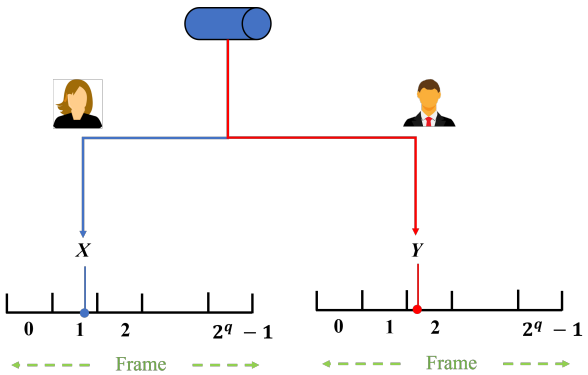


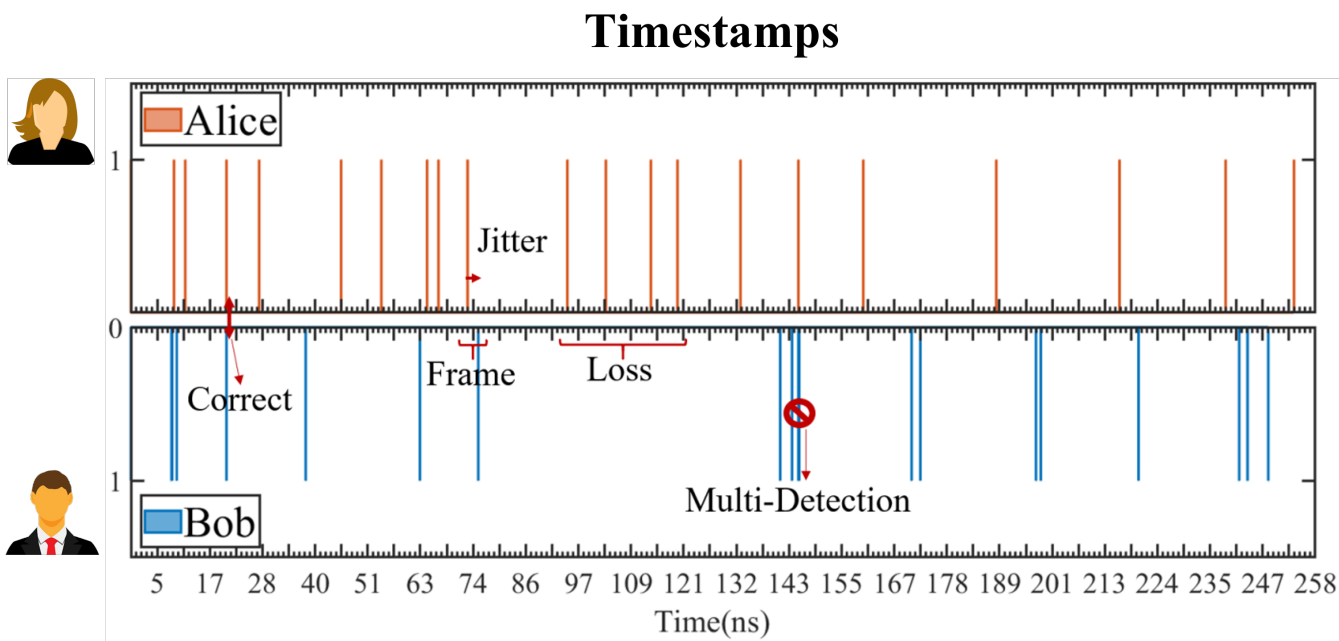


- Experimental Set-up: Wong Group at UCLA.

Energy time (ET)-QKD Channel: Overview

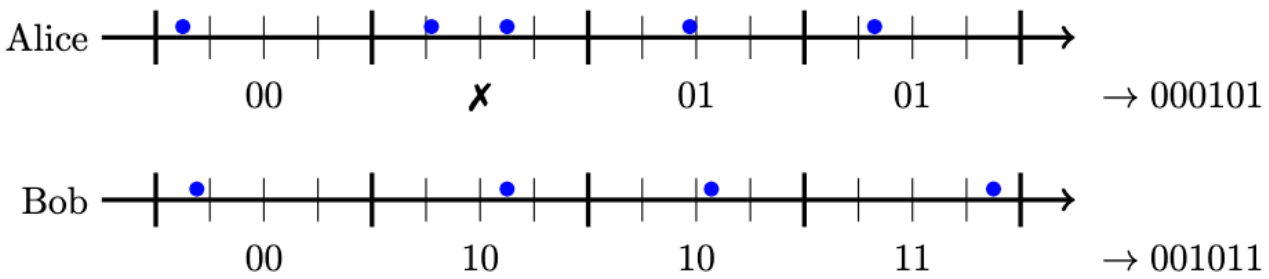
- The time domain is divided into frames, each frame contains 2^q bins: each arrival-time is represented by a q-bit symbol
- Only the frames where both Alice and Bob have exactly one detection are kept
- Complex error sources: timing jitter errors, detector downtime, dark counts, photon loss





- Experimental Set-up: Wong Group at UCLA.

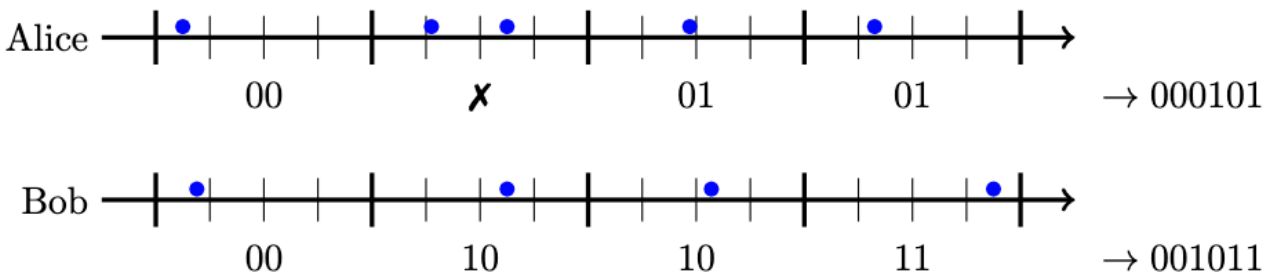
An Example



- **In the leftmost frame**, both Alice and Bob map their result to '00' (the leftmost bin is occupied in both). Bit extraction is successful despite a slight arrival jitter.

Figure credit: E. Soljanin.

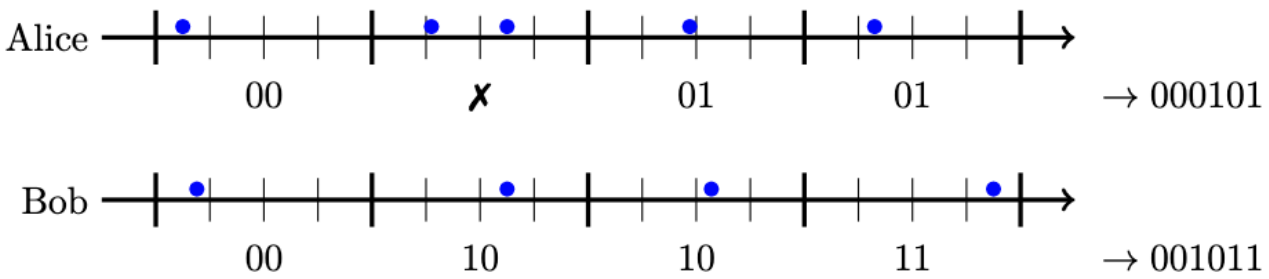
An Example



- **In the second frame**, Alice detects two arrivals, with the spurious one due to dark counts. While Bob initially can map his result to '01' for his second frame, upon receiving information from Alice that this frame is invalid, he too discards it.

Figure credit: E. Soljanin.

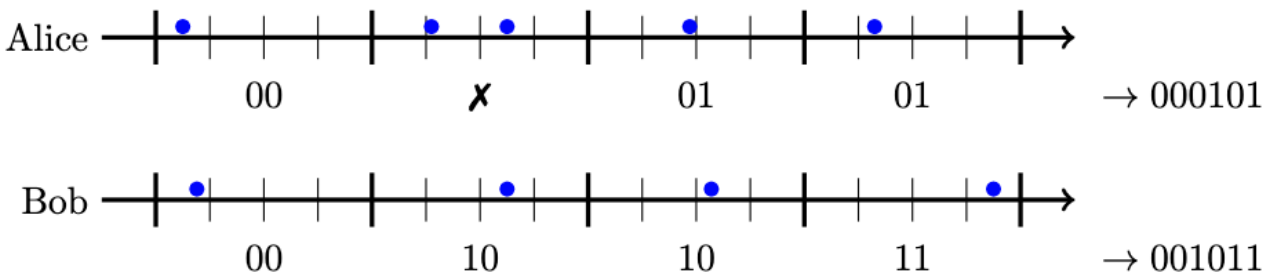
An Example



- **In the third frame**, both Alice and Bob observe a single arrival. However, due to timing jitter, the two arrivals fall into adjacent bins. Alice maps her result to '01' whereas Bob maps his to '10', resulting in a 2-bit discrepancy.

Figure credit: E. Soljanin.

An Example

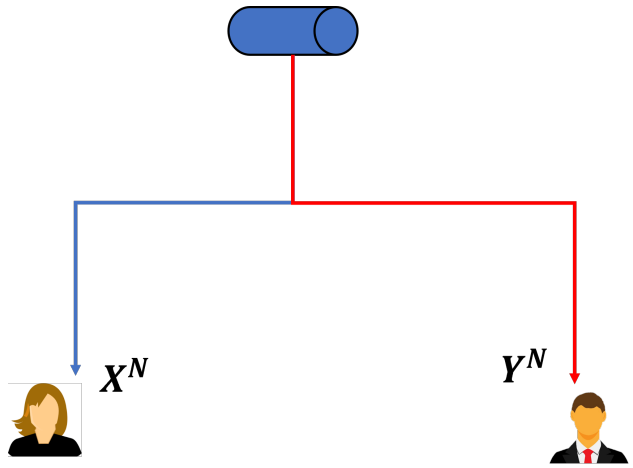


- **In the rightmost frame**, Alice and Bob each again detect a single arrival. In this example, two arrivals are due to dark counts and are uncorrelated (unbeknownst to Alice and Bob at this point). Alice maps her result to '01' and Bob his to '11'.

Figure credit: E. Soljanin.

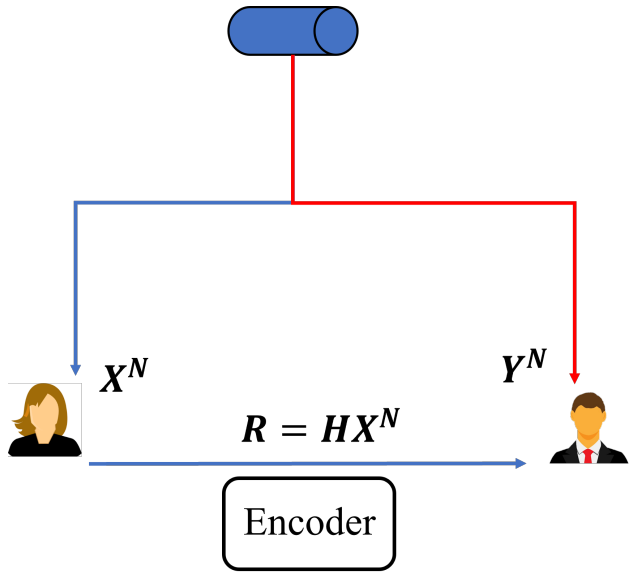
Information Reconciliation: Source Coding with Side Information (Elkouss '09)

- Encoding
  - Sequences received by Alice and Bob are X^N and Y^N respectively



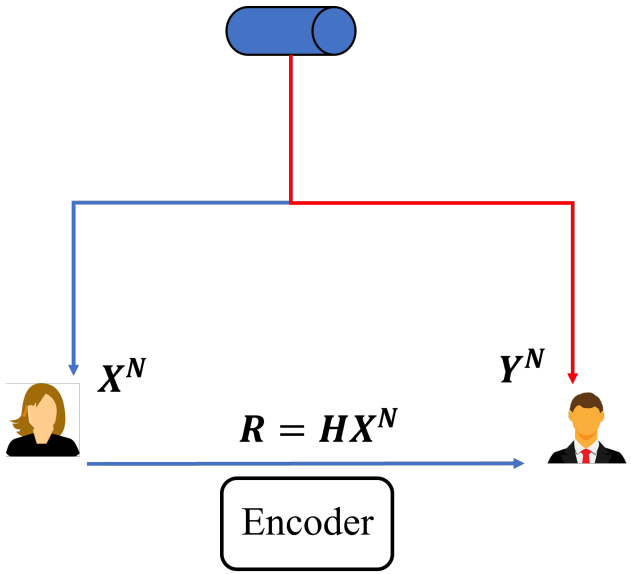
Information Reconciliation: Source Coding with Side Information (Elkouss '09)

- Encoding
  - Sequences received by Alice and Bob are X^N and Y^N respectively
  - Alice send parities $R = HX^N$ to Bob over a public channel



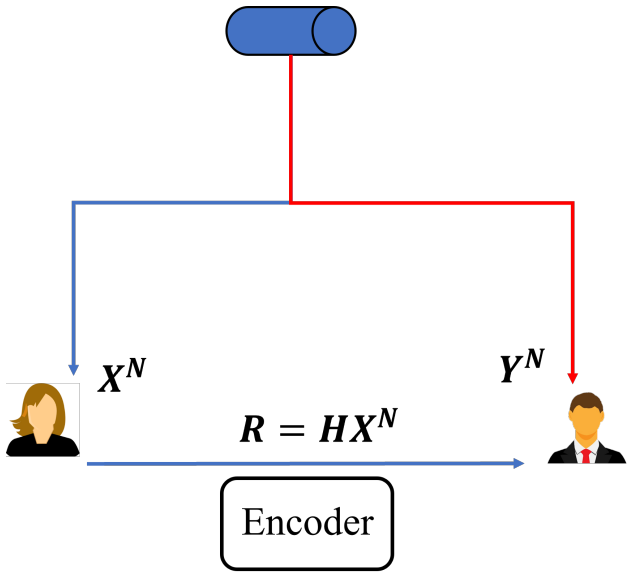
Information Reconciliation: Source Coding with Side Information (Elkouss '09)

- Encoding
  - Sequences received by Alice and Bob are X^N and Y^N respectively
  - Alice send parities $R = HX^N$ to Bob over a public channel
  - H is a parity check matrix of an LDPC code



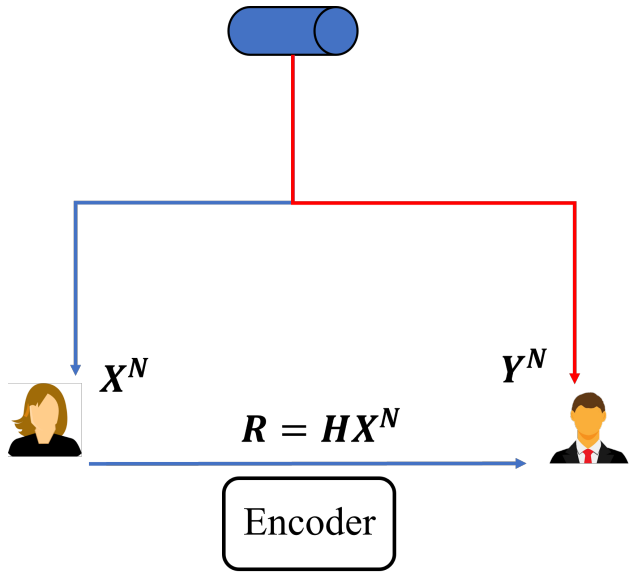
Information Reconciliation: Source Coding with Side Information (Elkouss '09)

- Encoding
  - Sequences received by Alice and Bob are X^N and Y^N respectively
  - Alice send parities $R = HX^N$ to Bob over a public channel
  - H is a parity check matrix of an LDPC code
- Decoding at Bob's Side



Information Reconciliation: Source Coding with Side Information (Elkouss '09)

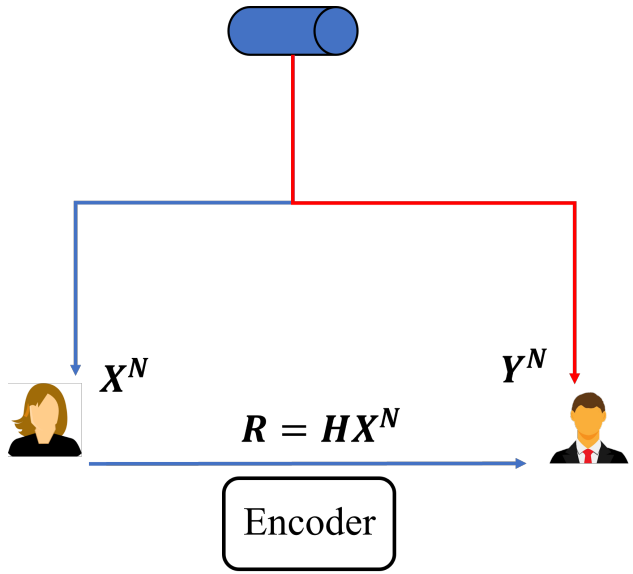
- Encoding
  - Sequences received by Alice and Bob are X^N and Y^N respectively
  - Alice send parities $R = HX^N$ to Bob over a public channel
  - H is a parity check matrix of an LDPC code



- Decoding at Bob's Side
  - The syndrome $S = HY^N - R = H(Y^N - X^N) = H\Delta$ should be zero if $X^N = Y^N$, which can be used to decode Y^N by belief propagation

Information Reconciliation: Source Coding with Side Information (Elkouss '09)

- Encoding
  - Sequences received by Alice and Bob are X^N and Y^N respectively
  - Alice send parities $R = HX^N$ to Bob over a public channel
  - H is a parity check matrix of an LDPC code



- Decoding at Bob's Side
  - The syndrome $S = HY^N - R = H(Y^N - X^N) = H\Delta$ should be zero if $X^N = Y^N$, which can be used to decode Y^N by belief propagation

Parity bits are visible to Eve.
Need to balance code rate and its error correction capability.

Prior related work

Classical design approaches

- LDPC coding (Kasai '10, Mao '19, Milicevic '17, 18, Muller '23), Polar coding (Jouguet '14, Fang '22)
- Optimization centers on high-noise $\rightarrow$ low code rate for canonical noise channels

Prior related work

Classical design approaches

- LDPC coding (Kasai '10, Mao '19, Milicevic '17, 18, Muller '23), Polar coding (Jouguet '14, Fang '22)
- Optimization centers on high-noise $\rightarrow$ low code rate for canonical noise channels

QKD channel-aware approach

- Multilevel binary LDPC codes (Zhou '13)
  - Implemented and tested in experimental systems (Zhong '15, Chang '23, Chang '24)
  - Random code constructions

Prior related work

Classical design approaches

- LDPC coding (Kasai '10, Mao '19, Milicevic '17, 18, Muller '23), Polar coding (Jouguet '14, Fang '22)
- Optimization centers on high-noise $\rightarrow$ low code rate for canonical noise channels

QKD channel-aware approach

- Multilevel binary LDPC codes (Zhou '13)
  - Implemented and tested in experimental systems (Zhong '15, Chang '23, Chang '24)
  - Random code constructions

Next: Information Reconciliation using LDPC codes designed based on the properties of the QKD channel

ET-QKD Channel: Details

QKD Channel:

- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$

ET-QKD Channel: Details

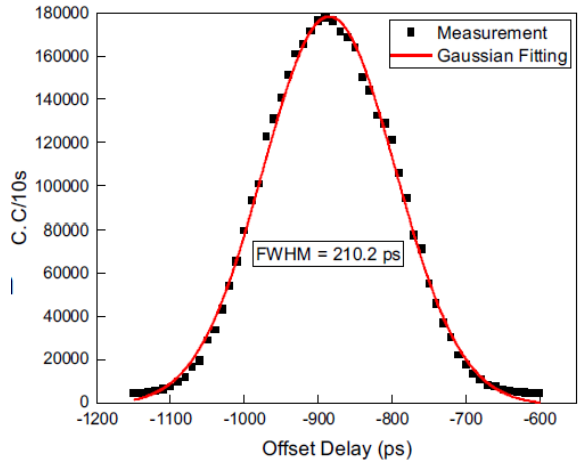
QKD Channel:

- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments

ET-QKD Channel: Details

QKD Channel:

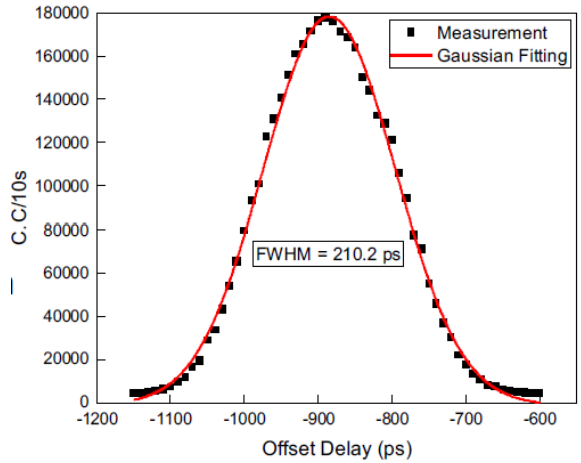
- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments
- Mixture of Gaussian and uniform noise



ET-QKD Channel: Details

QKD Channel:

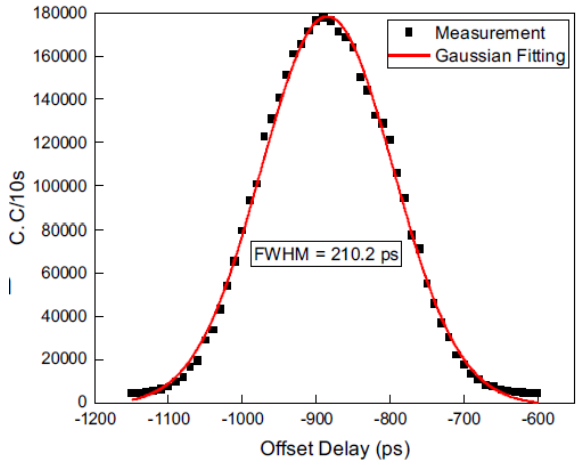
- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments
- Mixture of Gaussian and uniform noise
  - Local errors: Gaussian distribution



ET-QKD Channel: Details

QKD Channel:

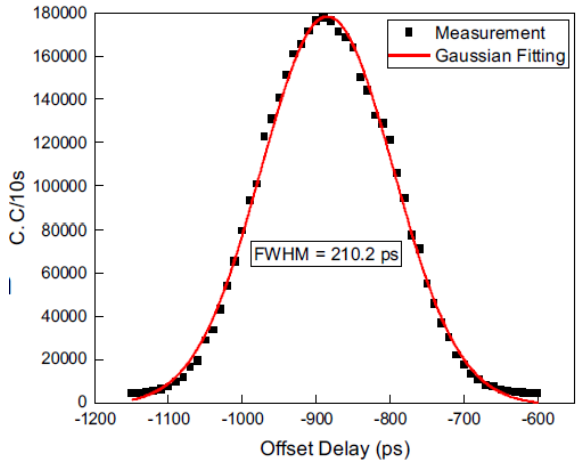
- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments
- Mixture of Gaussian and uniform noise
  - Local errors: Gaussian distribution
    - due to timing jitters and synchronization errors in photon detection.



ET-QKD Channel: Details

QKD Channel:

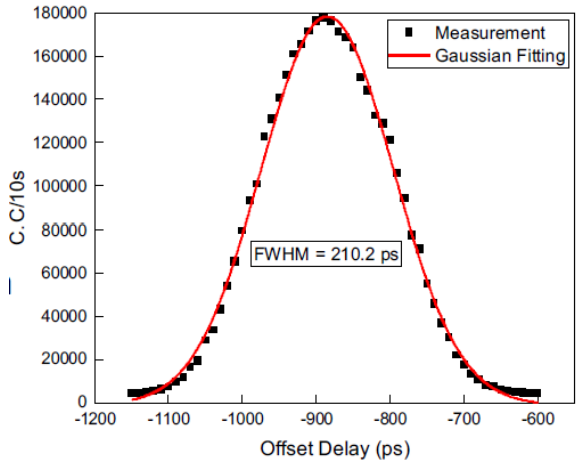
- $P_{Y|X}(y|x)$: $x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments
- Mixture of Gaussian and uniform noise
  - Local errors: Gaussian distribution
    - due to timing jitters and synchronization errors in photon detection.
  - Global errors: Uniform distribution



ET-QKD Channel: Details

QKD Channel:

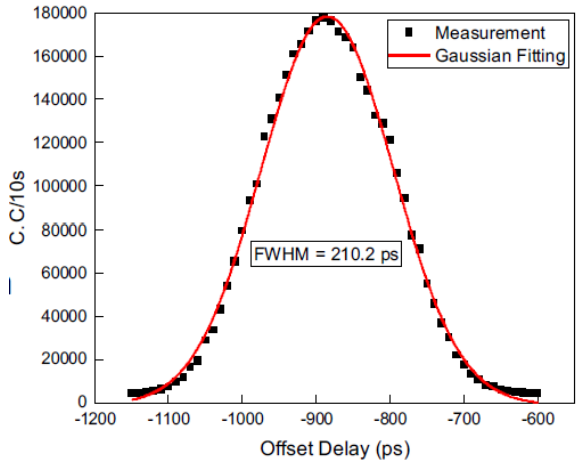
- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments
- Mixture of Gaussian and uniform noise
  - Local errors: Gaussian distribution
    - due to timing jitters and synchronization errors in photon detection.
  - Global errors: Uniform distribution
    - due to channel losses, and accidental concurrent detections of stray photons



ET-QKD Channel: Details

QKD Channel:

- $P_{Y|X}(y|x): \ x, y \in \{0, 1, \ldots q-1\}$
- Can be derived from experiments
- Mixture of Gaussian and uniform noise
  - Local errors: Gaussian distribution
    - due to timing jitters and synchronization errors in photon detection.
  - Global errors: Uniform distribution
    - due to channel losses, and accidental concurrent detections of stray photons
- The SNR in practice is very low resulting in high error rates



Outline

1. Background and Motivation

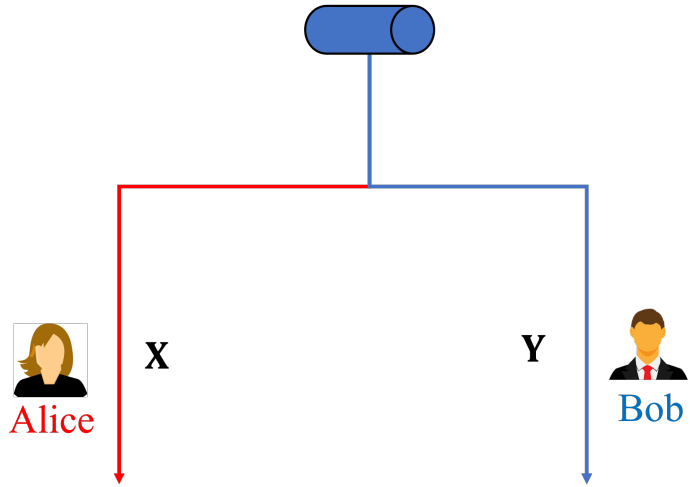
2. System Model

3. NB-LDPC codes for Quantum Key Distribution
   - Preliminaries
   - Channel code design
   - Sequential Decoding and Interactive Communication
   - Privacy Amplification-Aware LDPC Code Design

4. Concluding Remarks and Future Outlook

Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

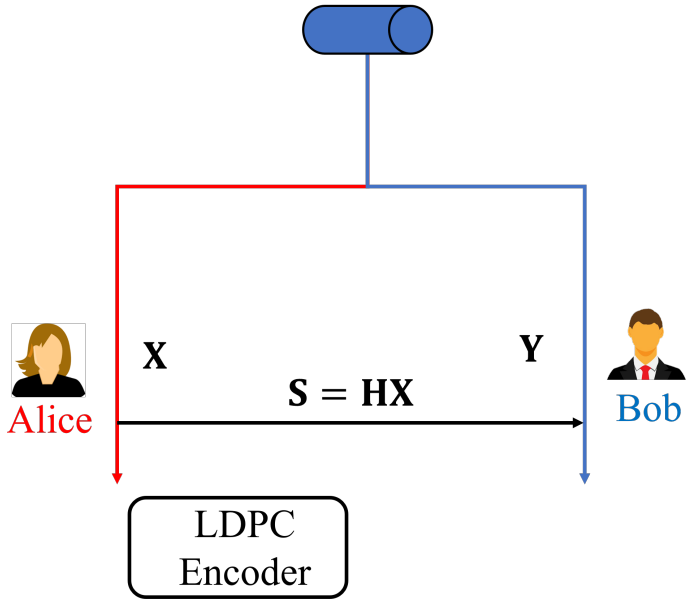
Alice:



Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

Alice:

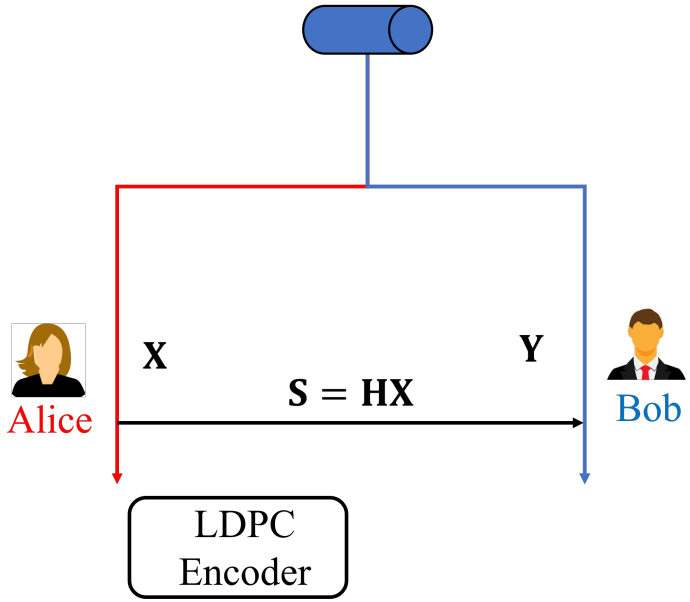
- Send syndromes $\mathbf{S} = \mathbf{HX}$ to Bob



Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

Alice:

- Send syndromes $\mathbf{S} = \mathbf{HX}$ to Bob
- $\mathbf{H}$ is a parity check matrix of a Non-Binary LDPC code in $\mathbb{GF}(2^q)^{M \times N}$



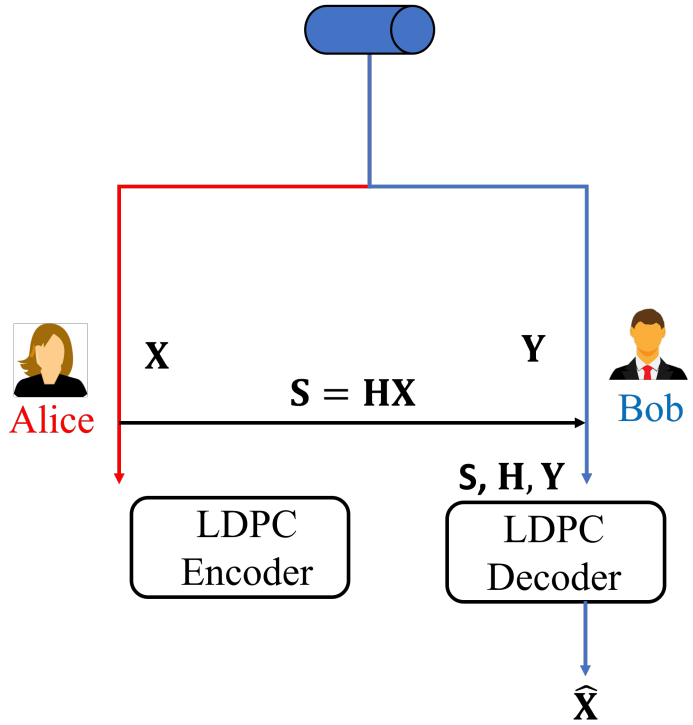
Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

Alice:

- Send syndromes $\mathbf{S} = \mathbf{HX}$ to Bob
- $\mathbf{H}$ is a parity check matrix of a Non-Binary LDPC code in $\mathbb{GF}(2^q)^{M \times N}$

Bob:

- Bob decodes $\mathbf{X}$ using $\mathbf{S}, \mathbf{H}$, side information $\mathbf{Y}$ and QKD channel $P_{Y|X}$



Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

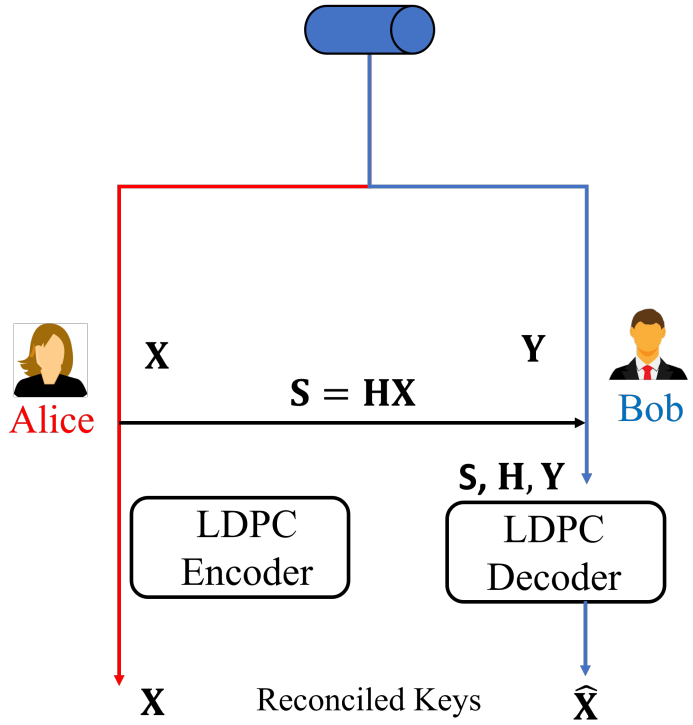
Alice:

- Send syndromes $\mathbf{S} = \mathbf{HX}$ to Bob
- $\mathbf{H}$ is a parity check matrix of a Non-Binary LDPC code in $\mathbb{GF}(2^q)^{M \times N}$

Bob:

- Bob decodes $\mathbf{X}$ using $\mathbf{S}, \mathbf{H}$, side information $\mathbf{Y}$ and QKD channel $P_{Y|X}$

Reconciled Keys: $\mathbf{X}$ and $\widehat{\mathbf{X}}$



Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

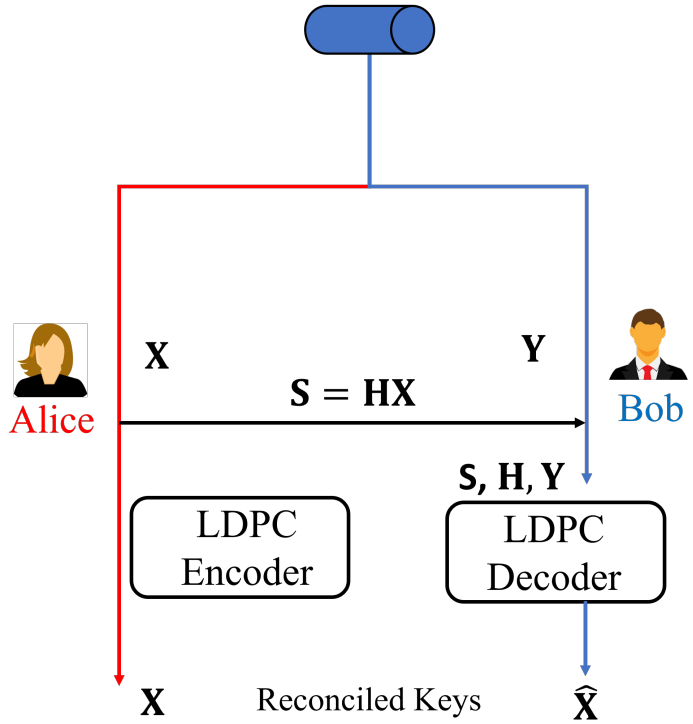
Alice:

- Send syndromes $\mathbf{S} = \mathbf{HX}$ to Bob
- $\mathbf{H}$ is a parity check matrix of a Non-Binary LDPC code in $\mathbb{GF}(2^q)^{M \times N}$

Bob:

- Bob decodes $\mathbf{X}$ using $\mathbf{S}, \mathbf{H}$, side information $\mathbf{Y}$ and QKD channel $P_{Y|X}$

Reconciled Keys: $\mathbf{X}$ and $\widehat{\mathbf{X}}$



$$\text{IR rate} = q(1 - FER)\frac{N-M}{N}$$

Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

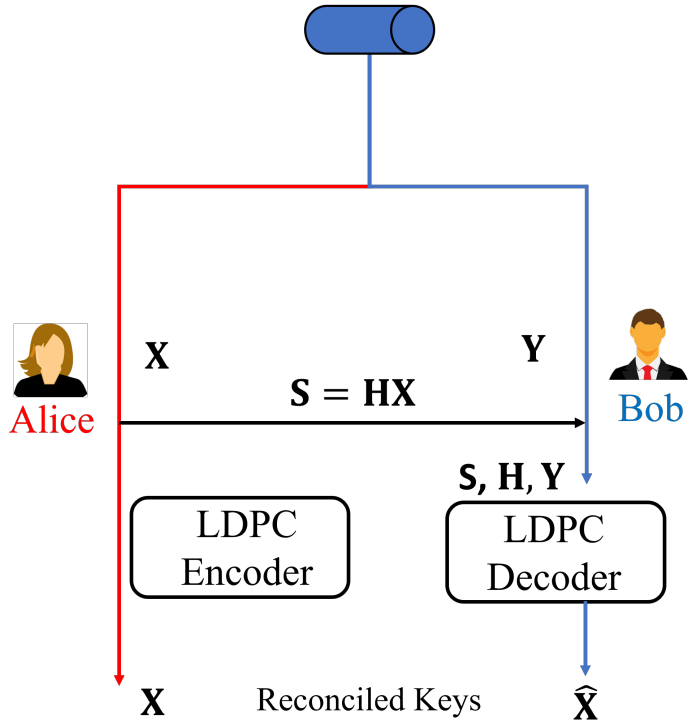
Alice:

- Send syndromes $\mathbf{S} = \mathbf{HX}$ to Bob
- $\mathbf{H}$ is a parity check matrix of a Non-Binary LDPC code in $\mathbb{GF}(2^q)^{M \times N}$

Bob:

- Bob decodes $\mathbf{X}$ using $\mathbf{S}, \mathbf{H}$, side information $\mathbf{Y}$ and QKD channel $P_{Y|X}$

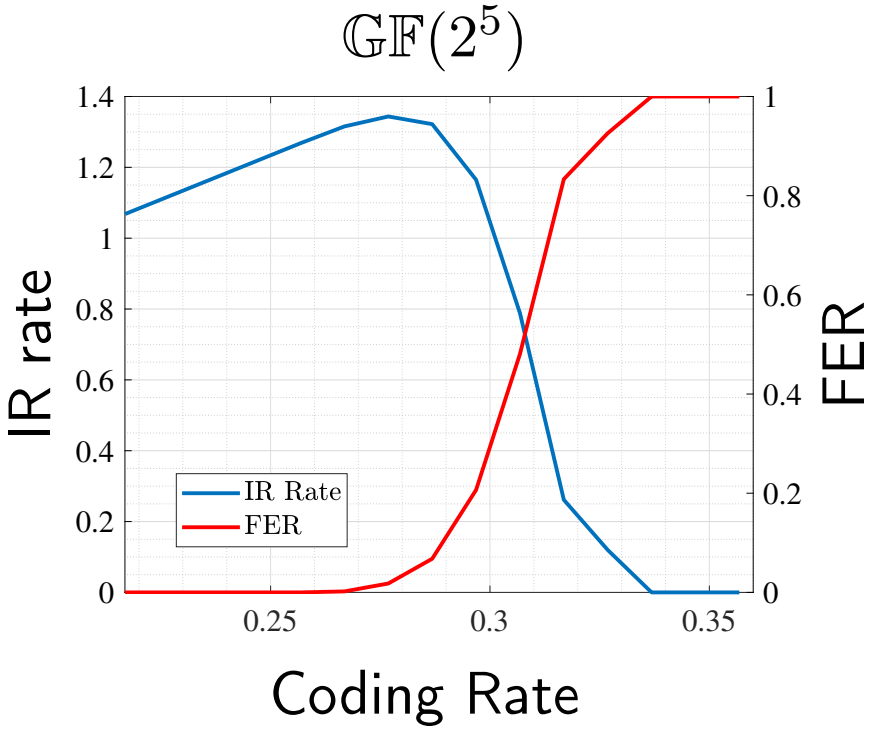
Reconciled Keys: $\mathbf{X}$ and $\widehat{\mathbf{X}}$

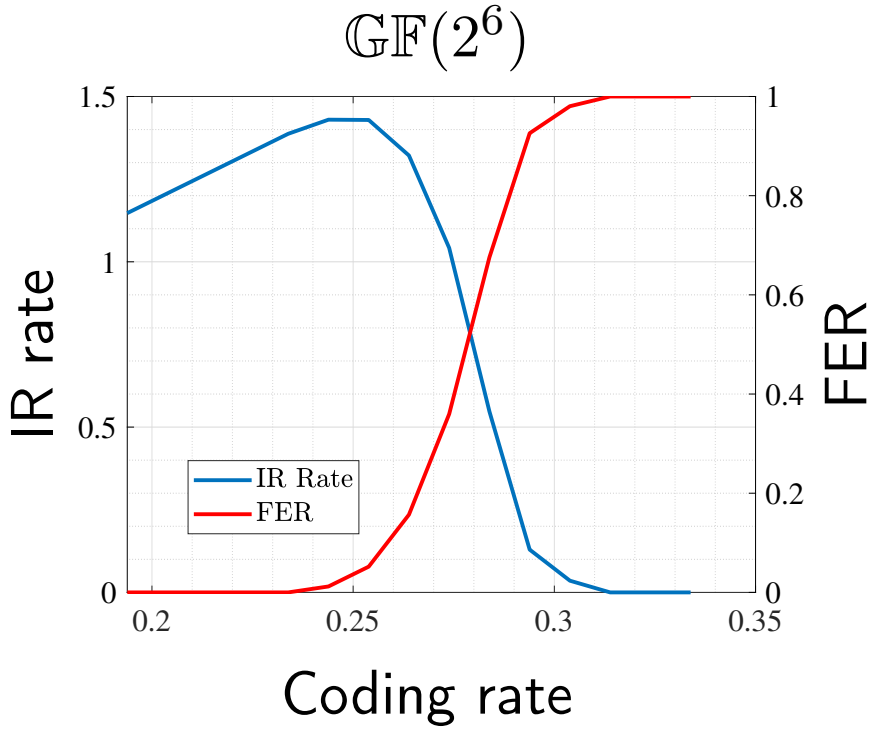


$$\text{IR rate} = q(1 - FER)\frac{N-M}{N}$$

- IR rate depends on both the coding rate ($\frac{N-M}{N}$) and FER of the code

Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR

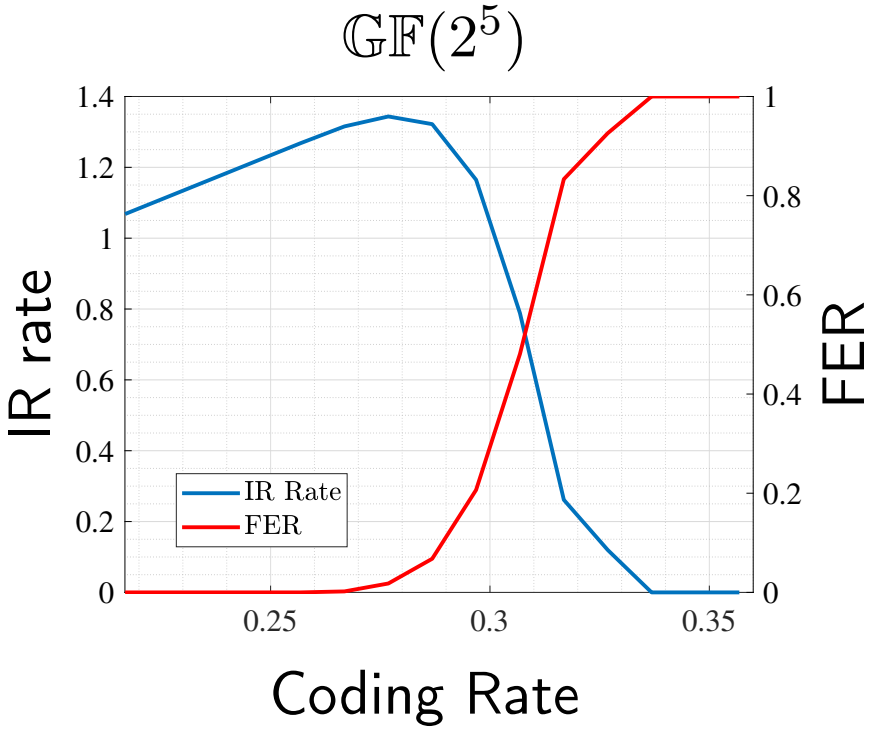


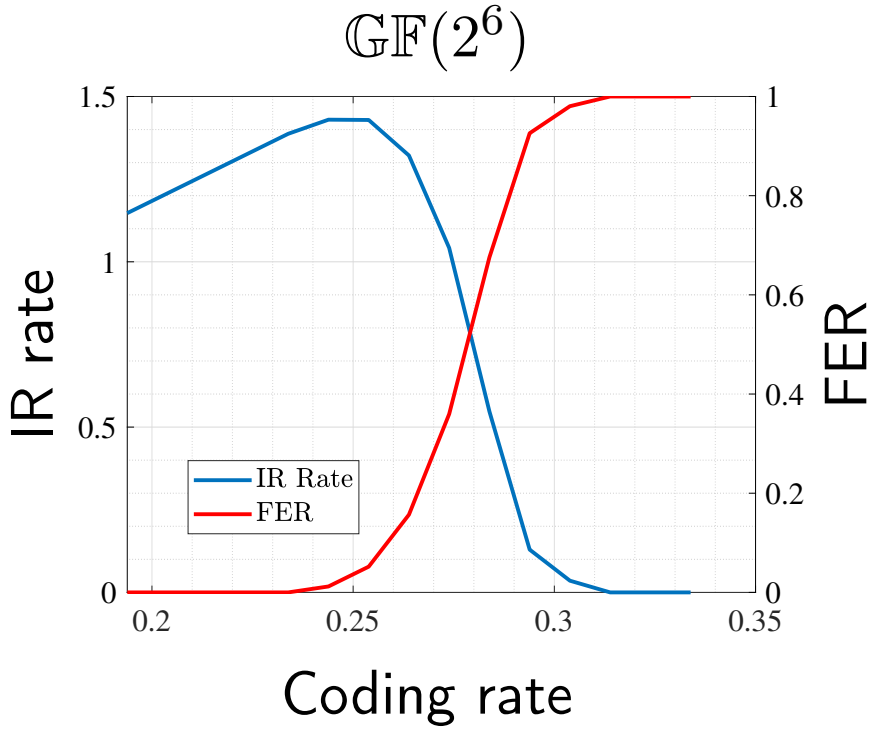


$$\text{IR rate} = q(1 - FER)\frac{N-M}{N}$$

- IR rate depends on both the coding rate ($\frac{N-M}{N}$) and FER of the code

Towards a New Solution: Fully Non-Binary (FNB) Protocol for IR





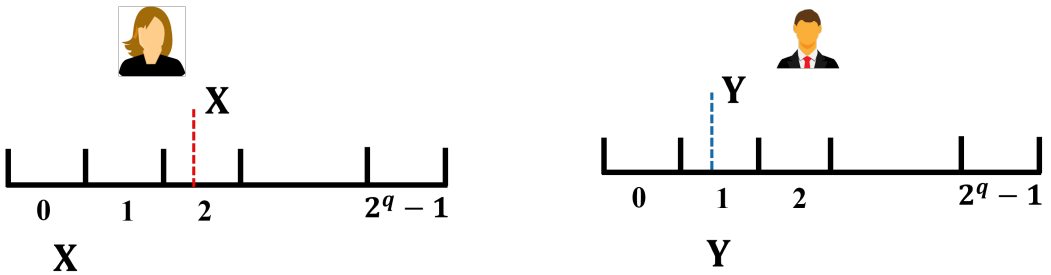
$$\text{IR rate} = q(1 - FER)\frac{N-M}{N}$$

- IR rate depends on both the coding rate ($\frac{N-M}{N}$) and FER of the code
- Maximum in the IR rate occurs for a relatively large value of FER ($\sim 1 - 10\%$)

Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

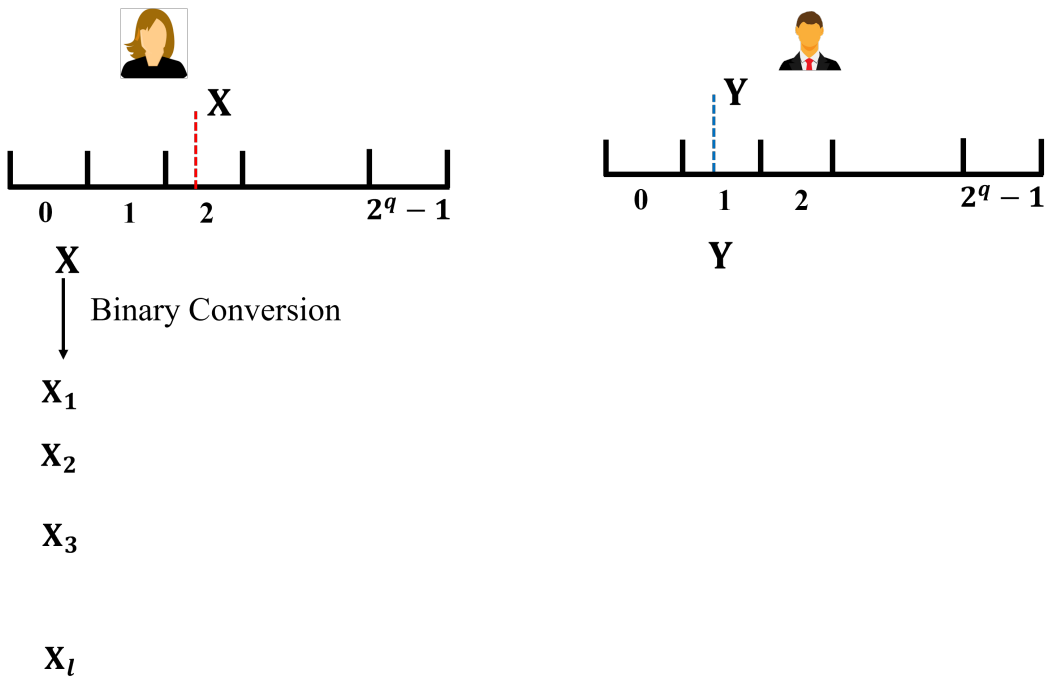
- Multi-Level Coding (MLC) (Zhou '13):



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

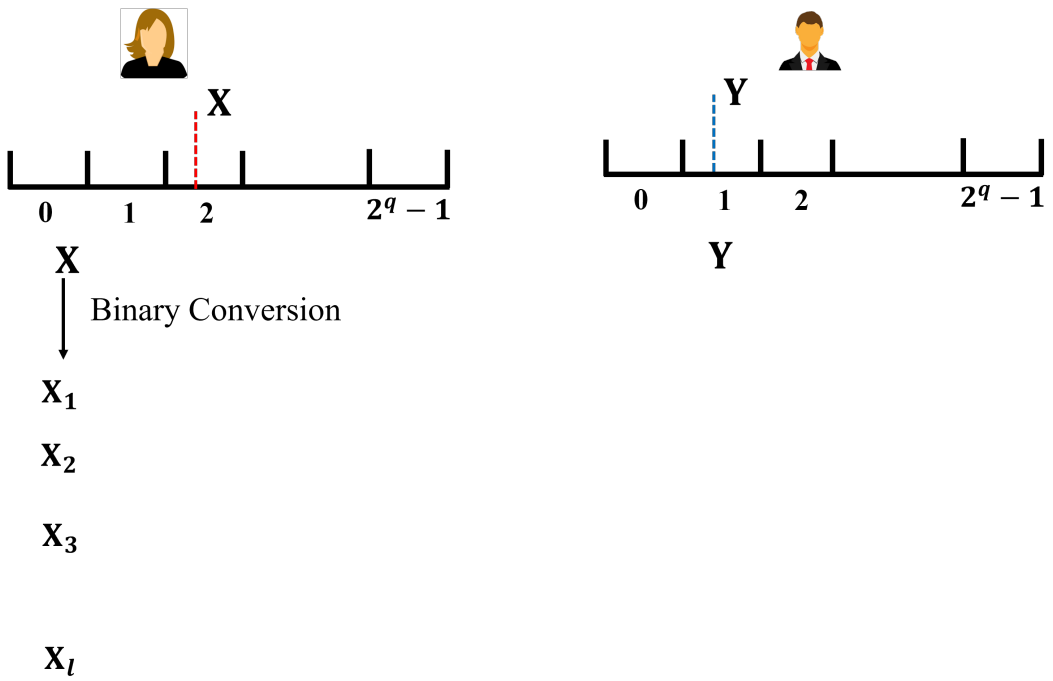
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

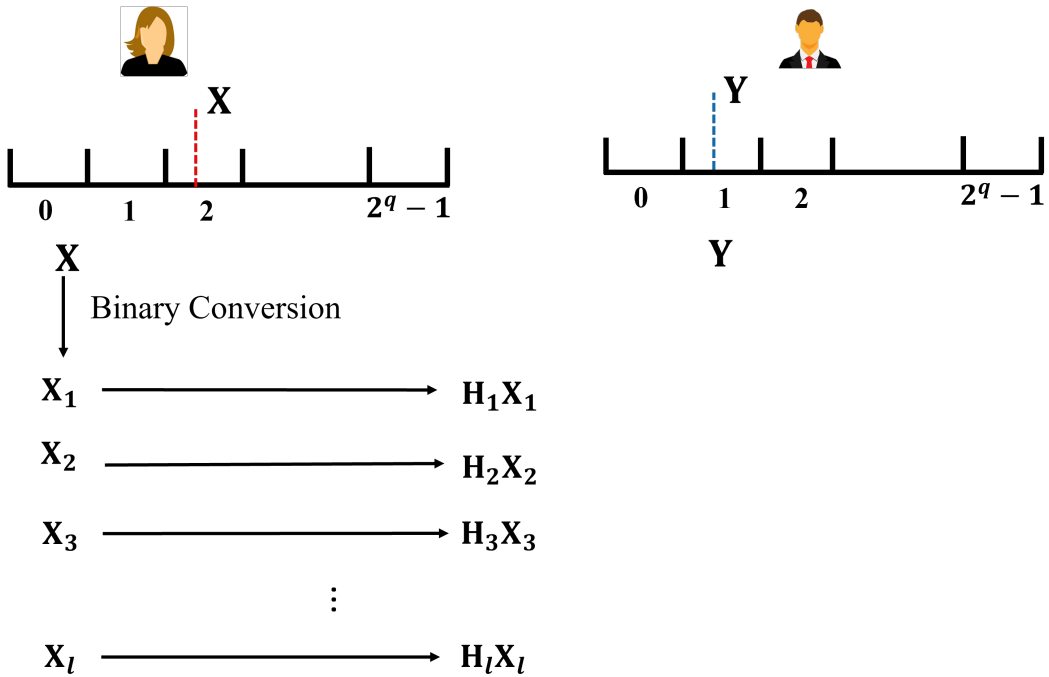
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

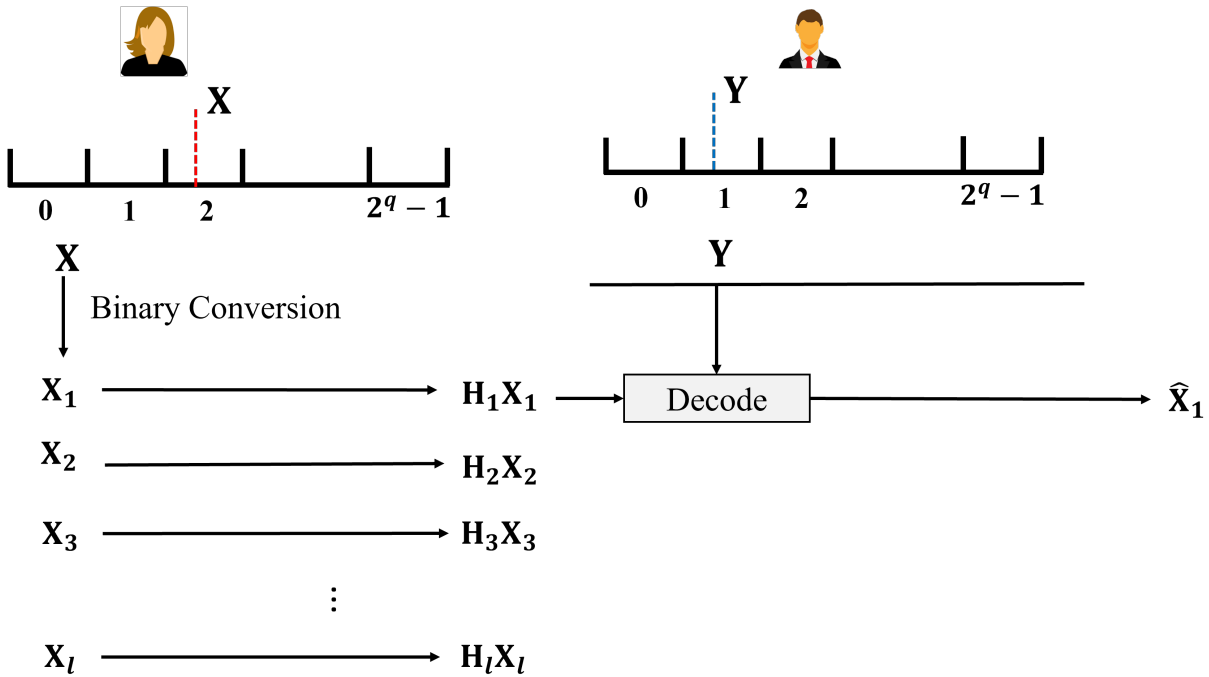
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

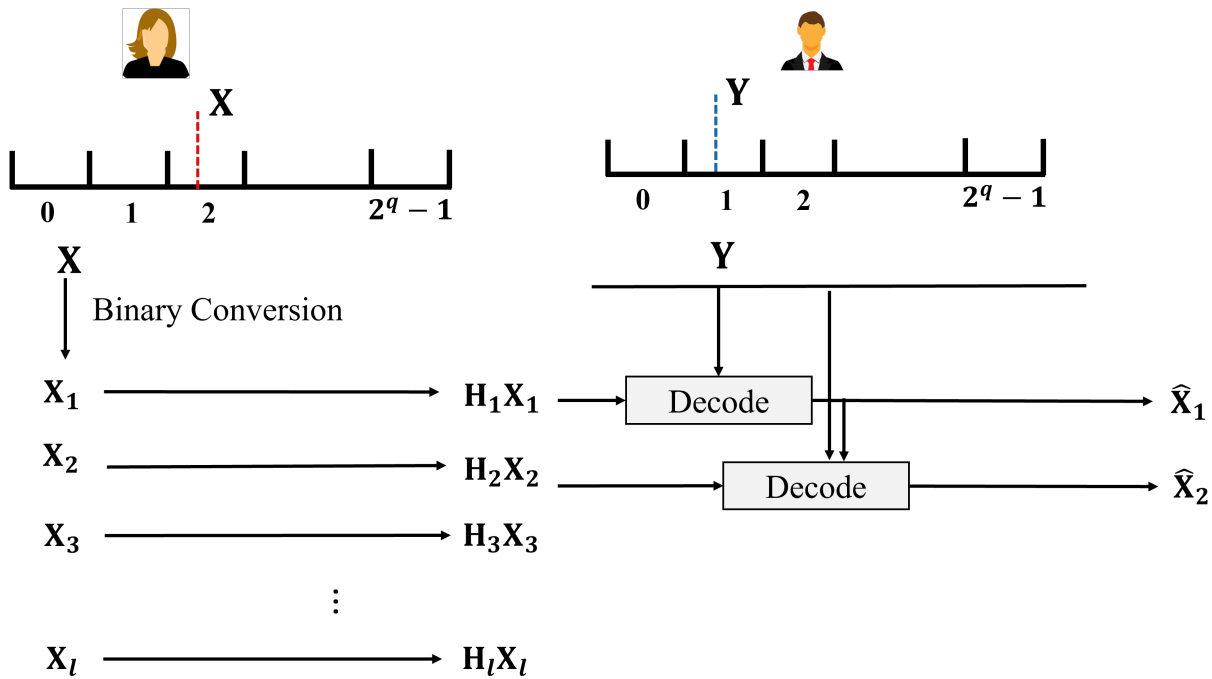
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

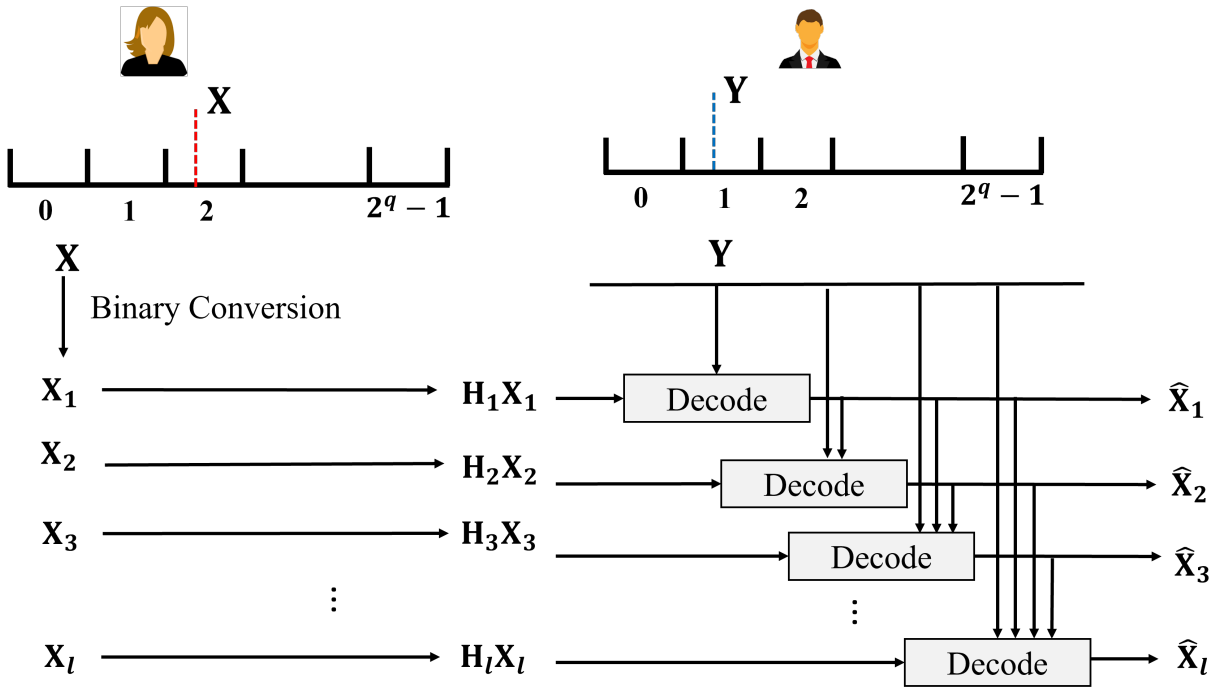
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

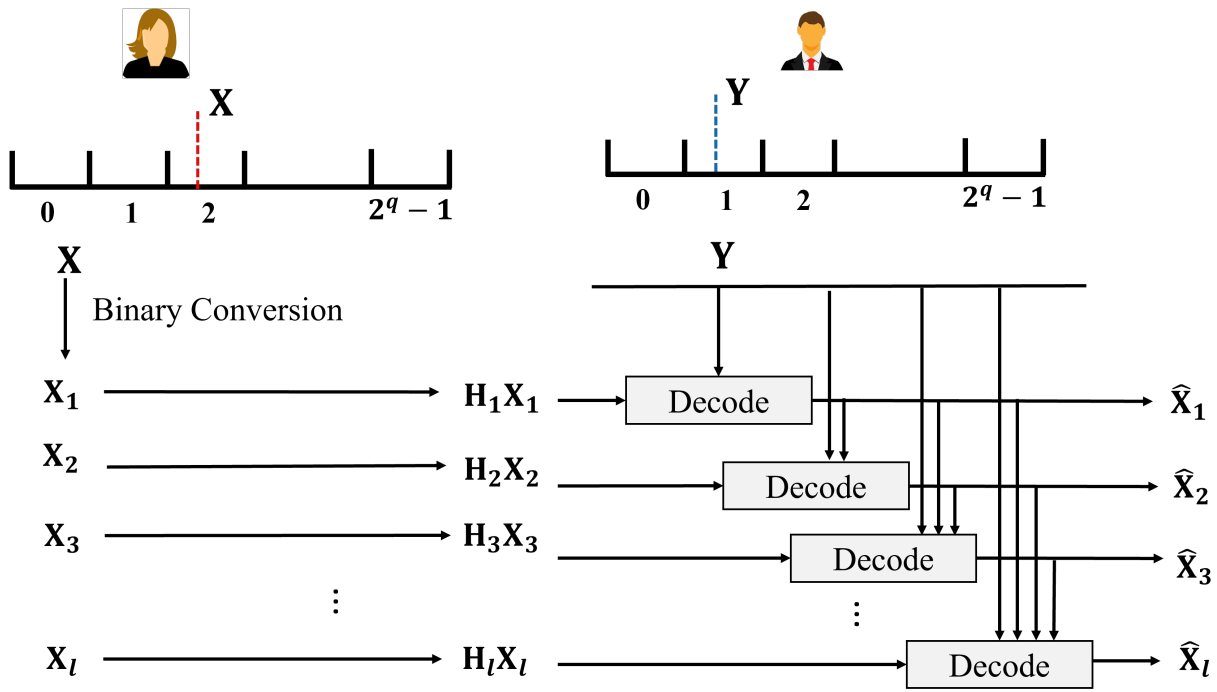
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

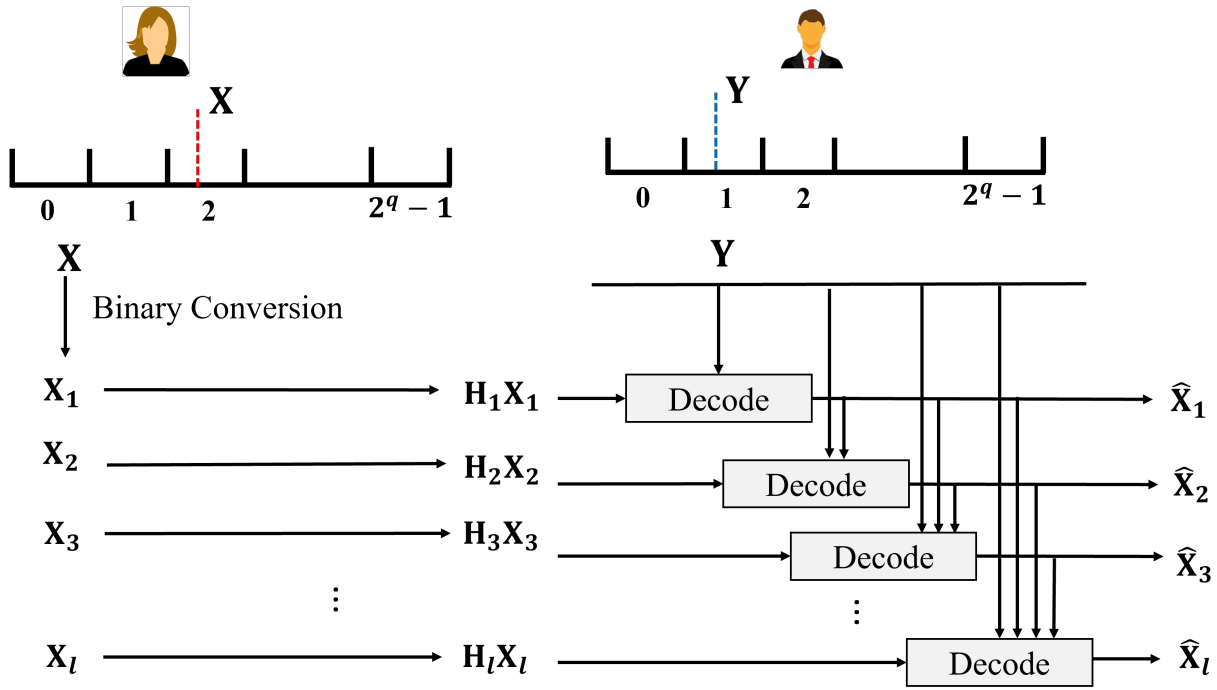
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

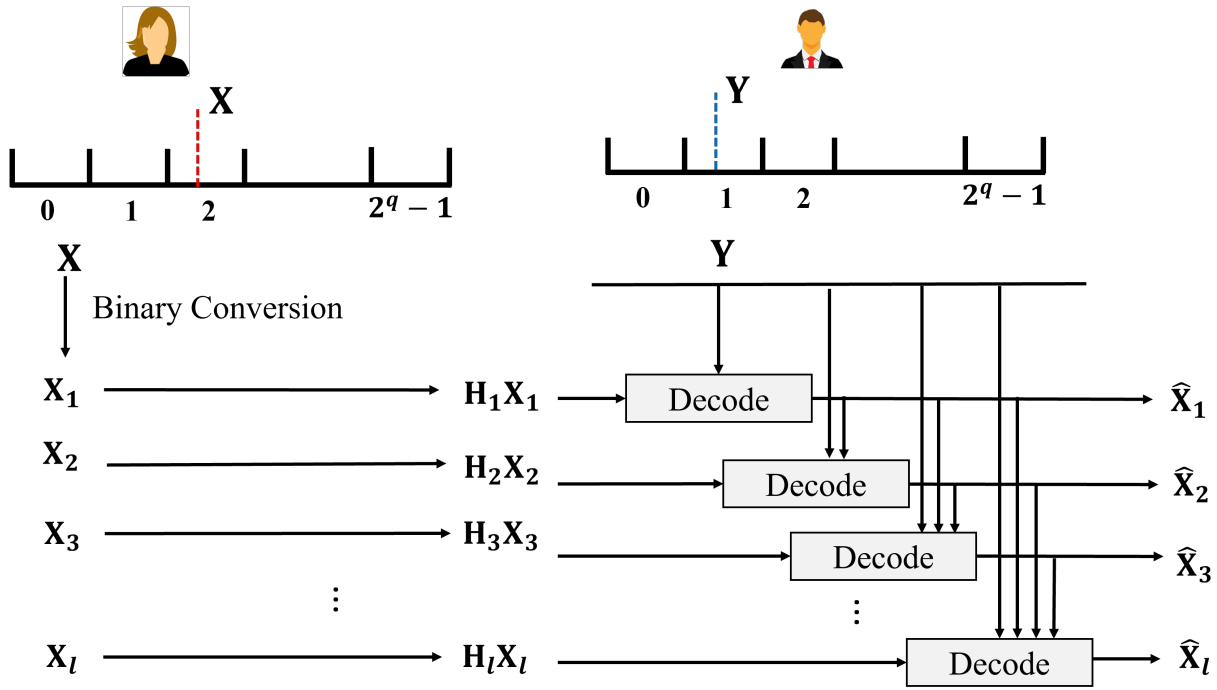
- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers



Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes

Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes

- Have higher IR rates due to stronger NB-LDPC codes

Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes

- Have higher IR rates due to stronger NB-LDPC codes
- High complexity of decoding when the symbol sizes are large

Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes

- Have higher IR rates due to stronger NB-LDPC codes
- High complexity of decoding when the symbol sizes are large

Our work:
1. Flexible protocol for IR called Non-Binary Multi-Level Coding $\texttt{NB-MLC}(a)$, which is parameterized by an integer $a > 0$

Binary vs. Non-Binary LDPC codes

Binary LDPC codes:

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes

- Have higher IR rates due to stronger NB-LDPC codes
- High complexity of decoding when the symbol sizes are large

Our work:
1. Flexible protocol for IR called Non-Binary Multi-Level Coding $\texttt{NB-MLC}(a)$, which is parameterized by an integer $a > 0$

- Utilizes specialized NB-LDPC codes in $\mathbb{GF}(2^a)$, $1 \leq a \leq q$

Binary vs. Non-Binary LDPC codes

Binary LDPC codes: | $a = 1$

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes

- Have higher IR rates due to stronger NB-LDPC codes
- High complexity of decoding when the symbol sizes are large

Our work:
1. Flexible protocol for IR called Non-Binary Multi-Level Coding $\texttt{NB-MLC}(a)$, which is parameterized by an integer $a > 0$

- Utilizes specialized NB-LDPC codes in $\mathbb{GF}(2^a)$, $1 \leq a \leq q$

Binary vs. Non-Binary LDPC codes

Binary LDPC codes: | $a = 1$

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

FNB protocol: Non-Binary LDPC codes | $a = q$

- Have higher IR rates due to stronger NB-LDPC codes
- High complexity of decoding when the symbol sizes are large

Our work:
1. Flexible protocol for IR called Non-Binary Multi-Level Coding $\texttt{NB-MLC}(a)$, which is parameterized by an integer $a > 0$

- Utilizes specialized NB-LDPC codes in $\mathbb{GF}(2^a)$, $1 \leq a \leq q$

Binary vs. Non-Binary LDPC codes

Binary LDPC codes: | $a = 1$

- Multi-Level Coding (MLC) (Zhou '13): Split symbols into bit layers
- Reconcile each layer using binary LDPC codes
- Low complexity and fast decoding algorithms
- Low complexity for key generation
- Sequential decoding among layers

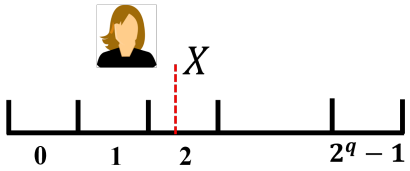
FNB protocol: Non-Binary LDPC codes | $a = q$

- Have higher IR rates due to stronger NB-LDPC codes
- High complexity of decoding when the symbol sizes are large

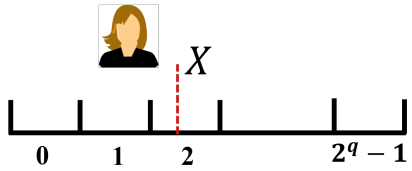
Our work:
1. Flexible protocol for IR called Non-Binary Multi-Level Coding $\texttt{NB-MLC}(a)$, which is parameterized by an integer $a > 0$
2. Interleaved decoding among layers to improve IR rates

- Utilizes specialized NB-LDPC codes in $\mathbb{GF}(2^a)$, $1 \leq a \leq q$

NB–MLC(a) Protocol



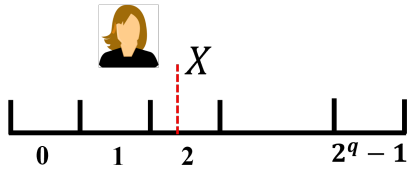
NB–MLC(a) Protocol



$\mathbb{GF}(2^q)$ { X

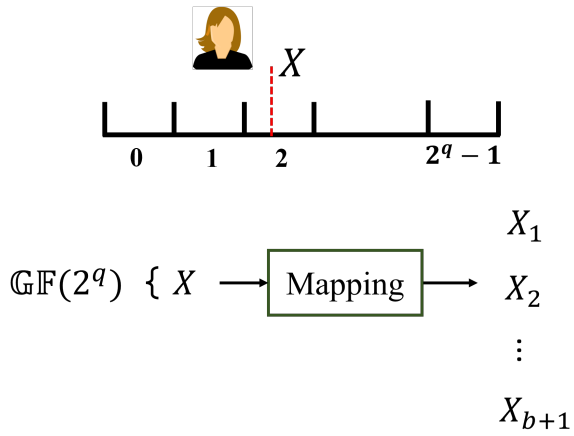
NB–MLC(a) Protocol

- For given a, let $q = ab + r$, $r < a$



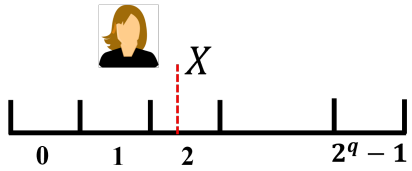
$\mathbb{GF}(2^q)$ { X

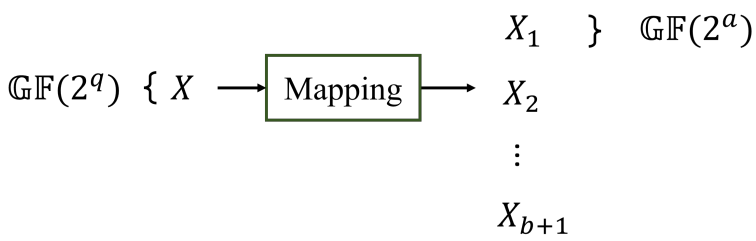
NB–MLC(a) Protocol



- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$

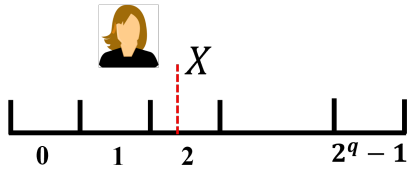
NB–MLC(a) Protocol

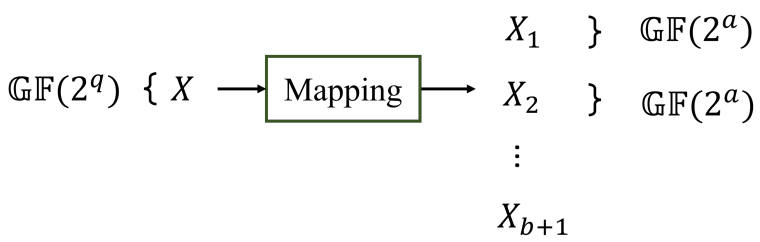




- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$

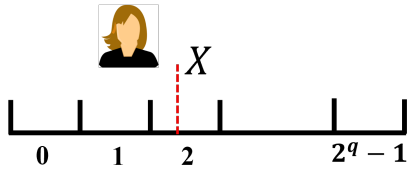
NB–MLC(a) Protocol

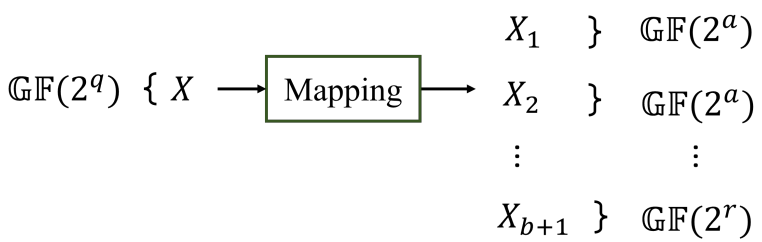




- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$

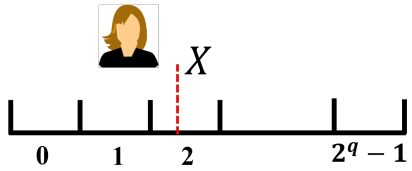
NB–MLC(a) Protocol

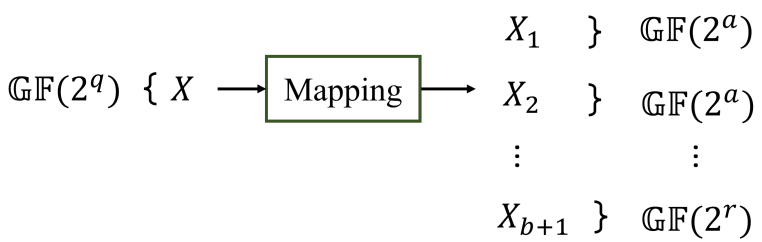




- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$

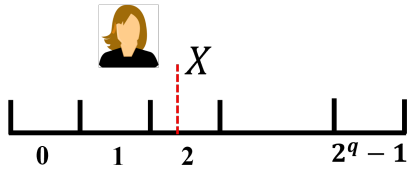
NB–MLC(a) Protocol

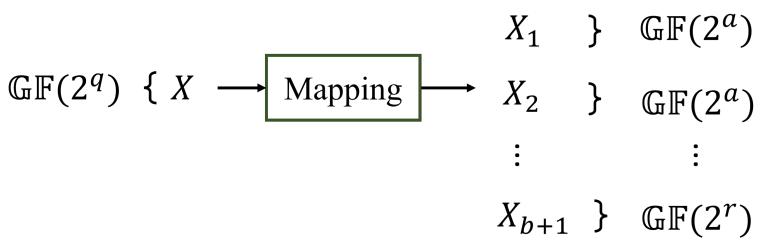


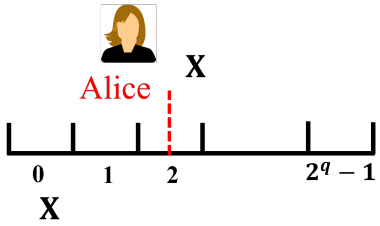


- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols

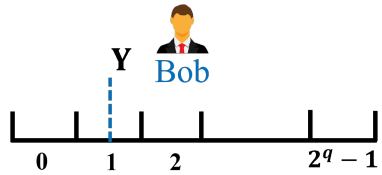
NB–MLC(a) Protocol



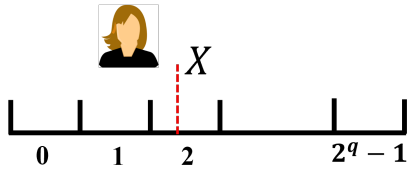


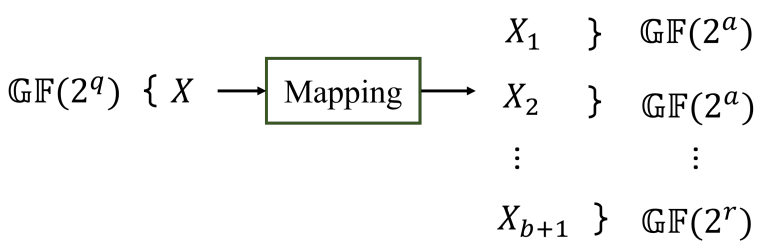


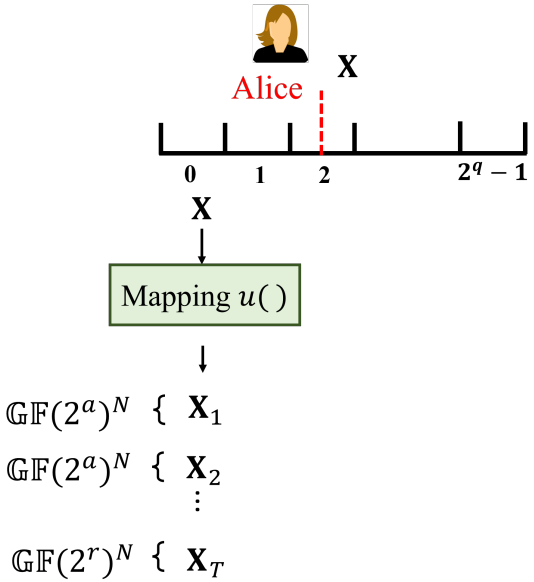
- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \leq i \leq b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.



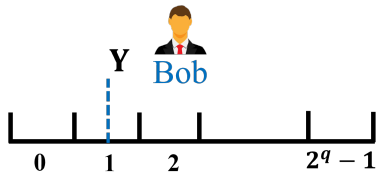
NB–MLC(a) Protocol



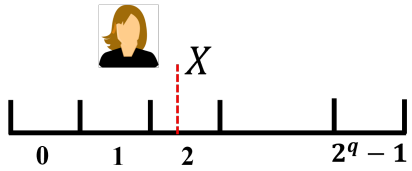


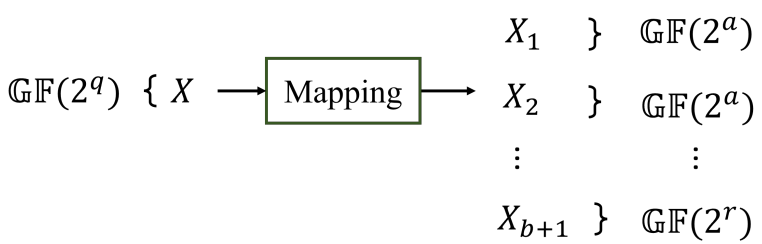


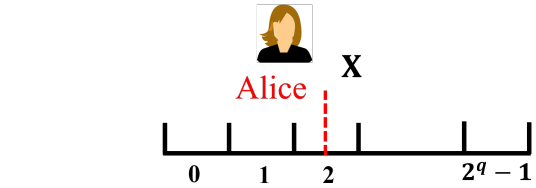
- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \le i \le b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.

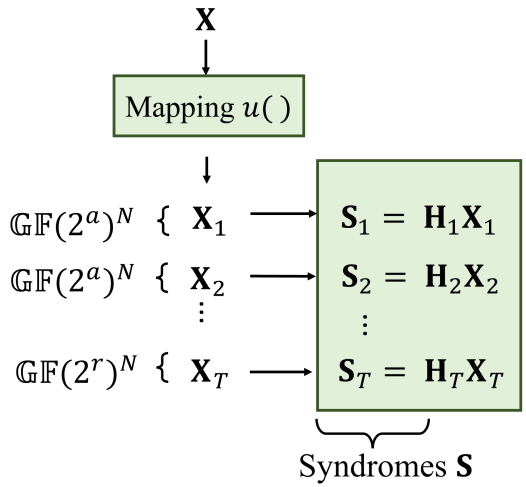


NB–MLC(a) Protocol

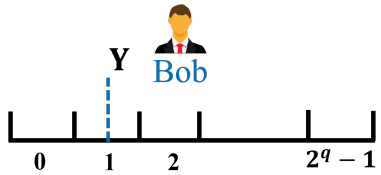




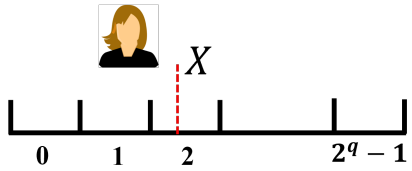


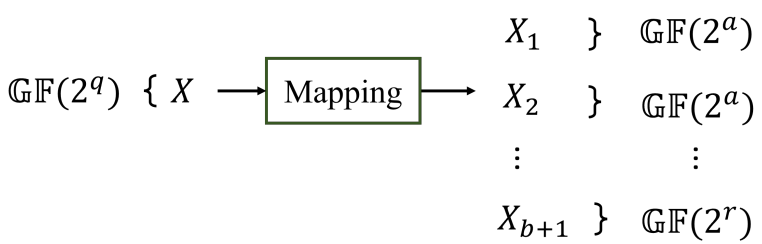


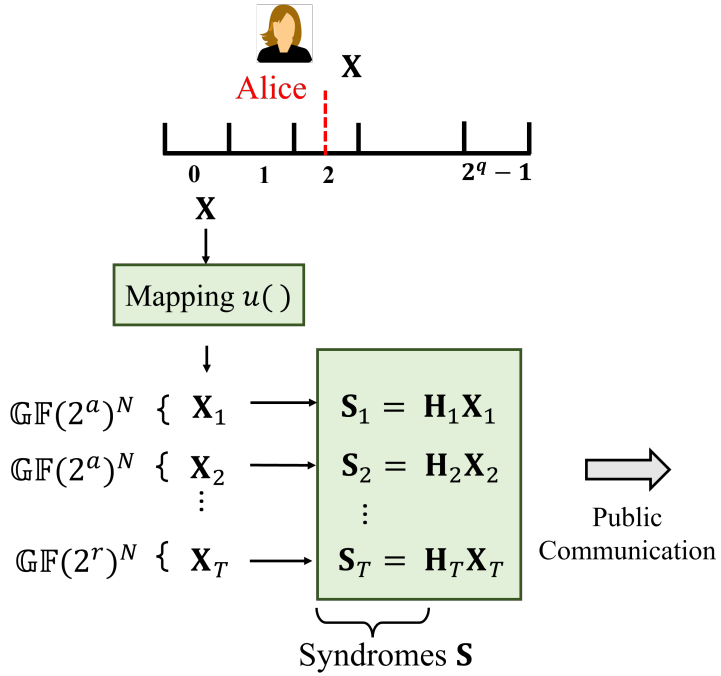
- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \leq i \leq b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.



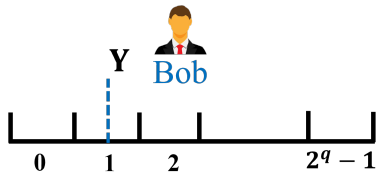
NB–MLC(a) Protocol



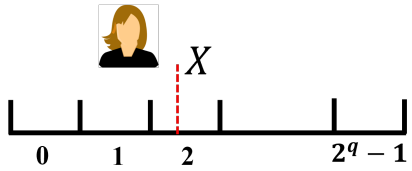


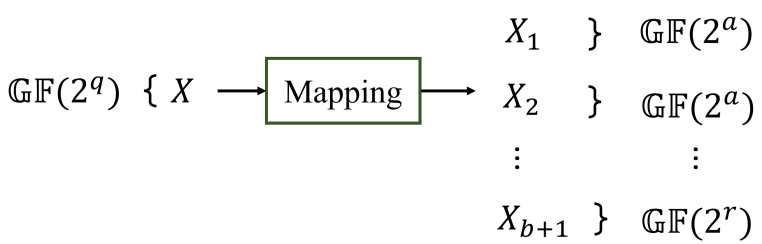


- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \le i \le b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.

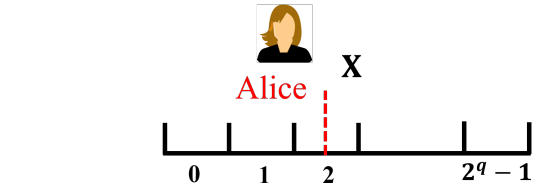


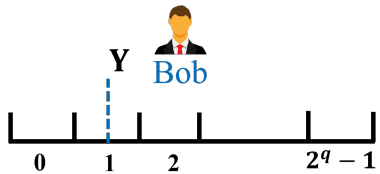
NB–MLC(a) Protocol

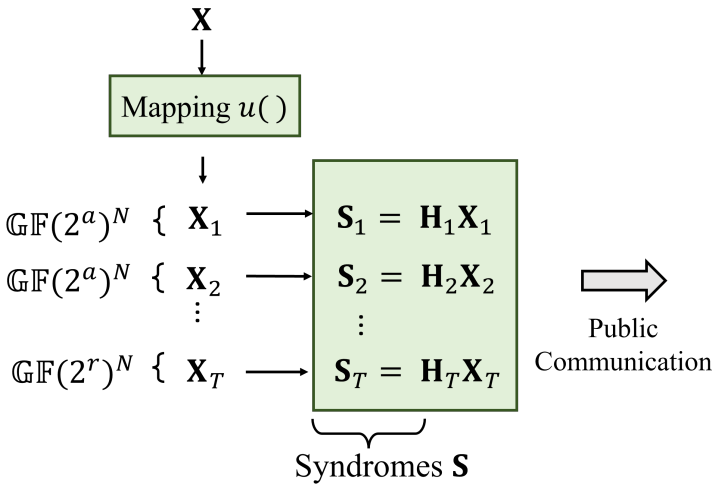


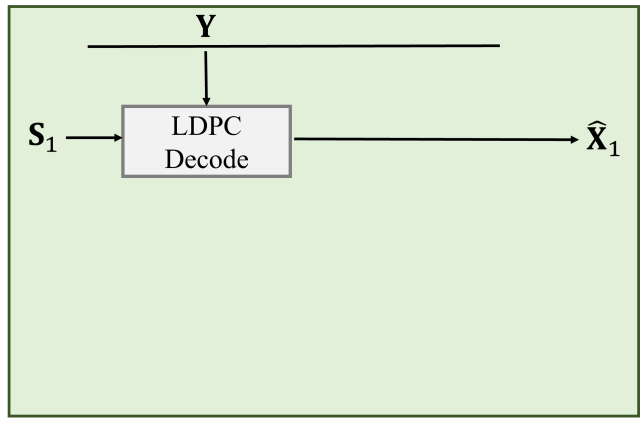


- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \leq i \leq b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.

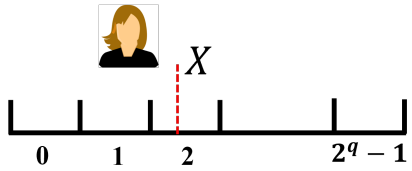


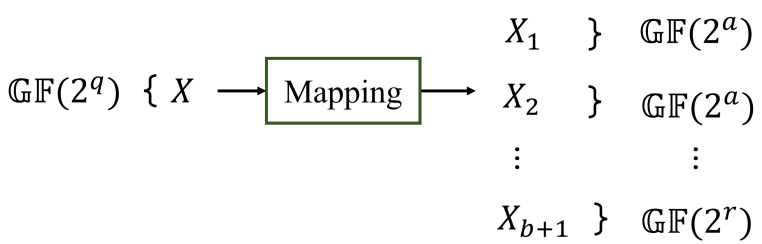




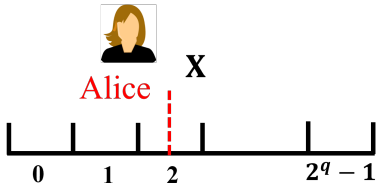


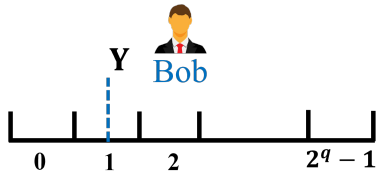
NB–MLC(a) Protocol

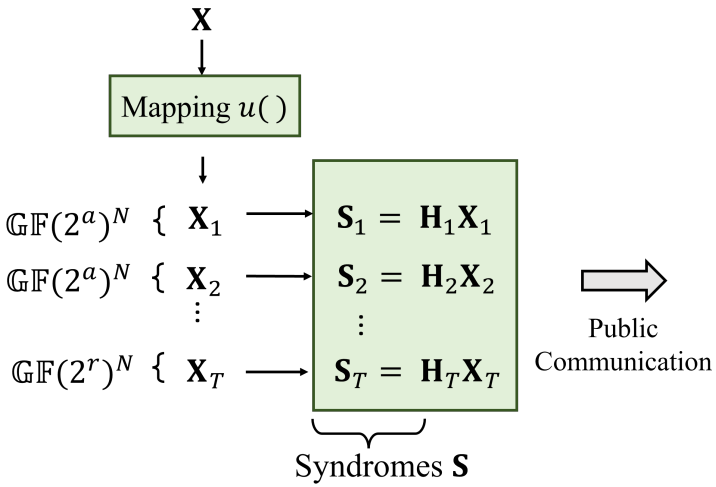


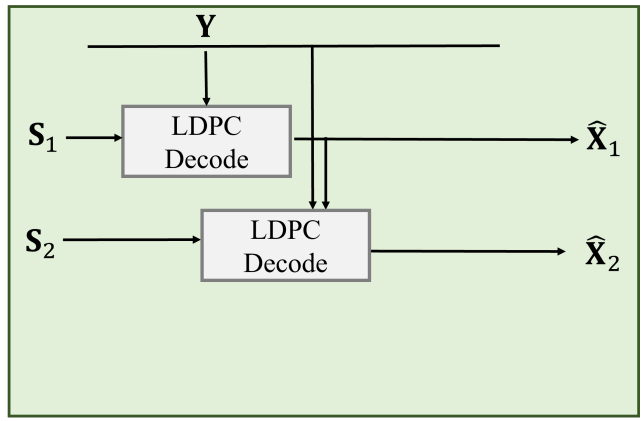


- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \le i \le b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.

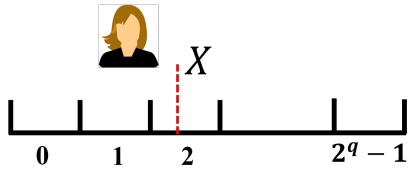


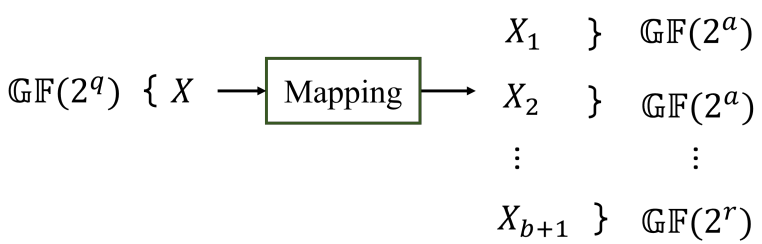




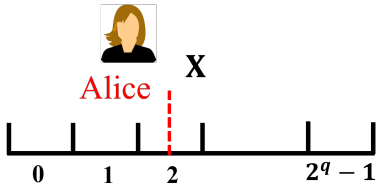


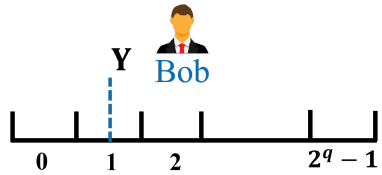
NB–MLC(a) Protocol

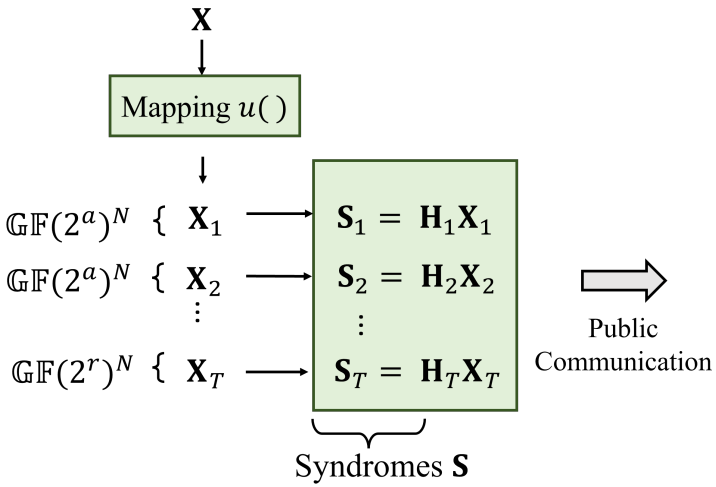


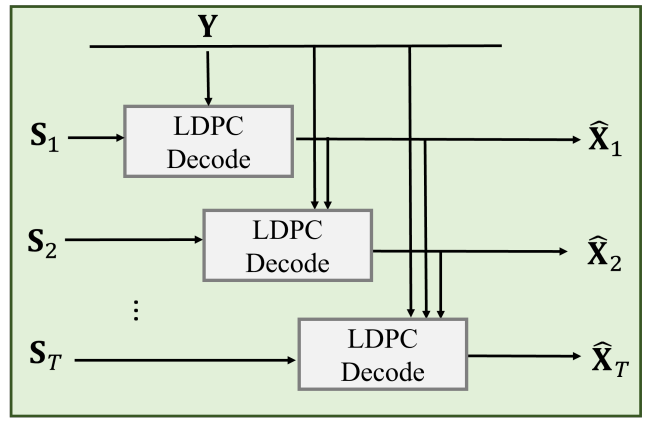


- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \le i \le b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.







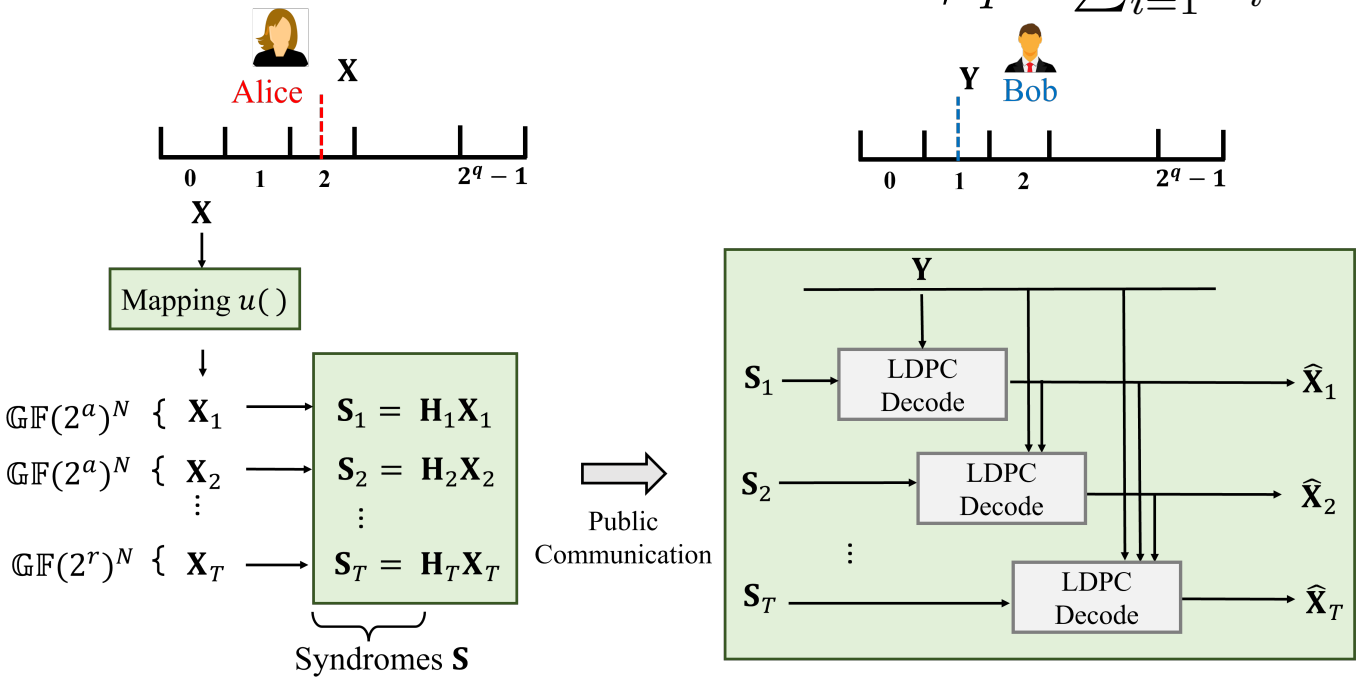


NB–MLC(a) Protocol

- The IR rate is the sum IR rate across all the layers

$$\text{IR rate} = \sum_{i=1}^{T}(1-FER_i) * Rate_i * \alpha_i$$

- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \leq i \leq b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.

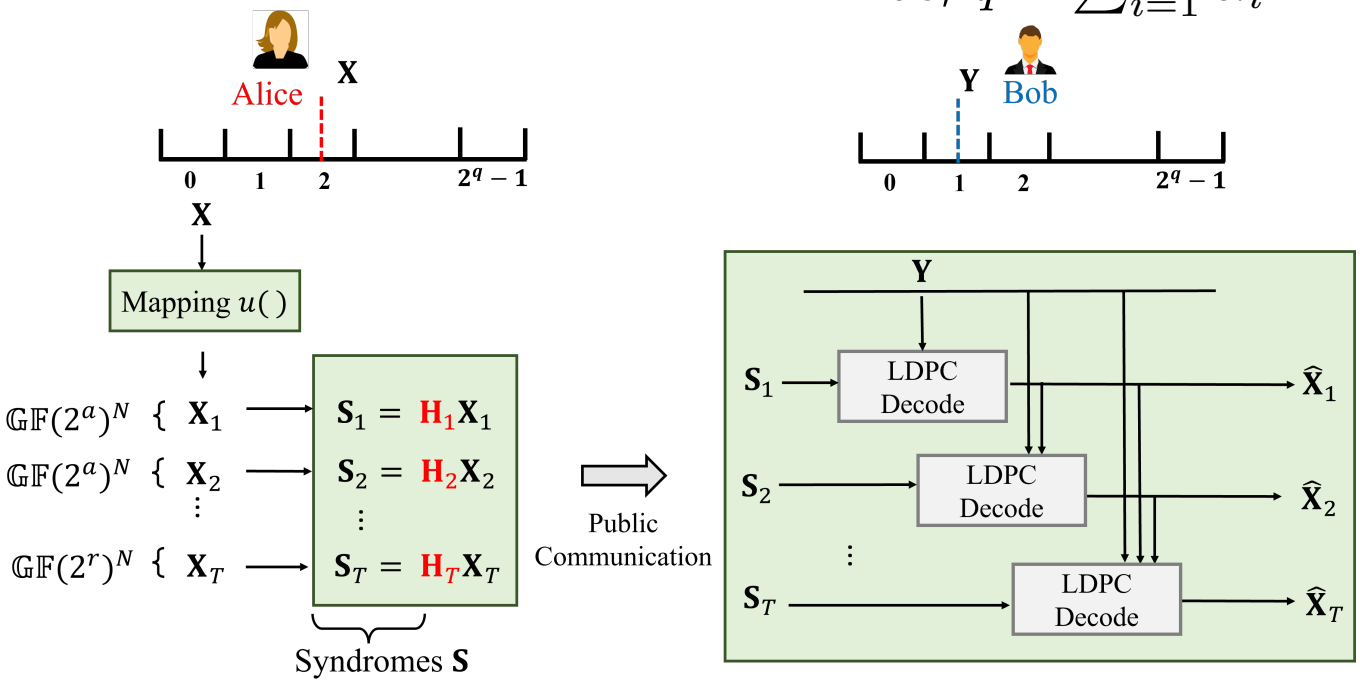


NB–MLC(a) Protocol

- The IR rate is the sum IR rate across all the layers

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$

- For given a, let $q = ab + r$, $r < a$
- Split X into b symbols in $\mathbb{GF}(2^a)$ and 1 symbol in $\mathbb{GF}(2^r)$
- Apply layered reconciliation on the split symbols
- Let number of layers $T = \lceil \frac{q}{a} \rceil$. Bitsize of each layer $\alpha_i = a, 1 \leq i \leq b$ and $\alpha_{b+1} = r$. Thus, $q = \sum_{i=1}^{T} \alpha_i$.



NB-LDPC Code design

Irregular LDPC codes

- Improves the FER performance of the code
- Can be characterized using their VN and CN degree distributions $L(x)$ and $P(x)$, respectively

$$L(x) = \sum_d L_d x^d \qquad P(x) = \sum_d P_d x^d$$

NB-LDPC Code design

Irregular LDPC codes

- Improves the FER performance of the code
- Can be characterized using their VN and CN degree distributions $L(x)$ and $P(x)$, respectively

$$L(x) = \sum_d L_d x^d \qquad P(x) = \sum_d P_d x^d$$

  - L_d: fraction of VNs of degree d, P_d: fraction of CNs of degree d

NB-LDPC Code design

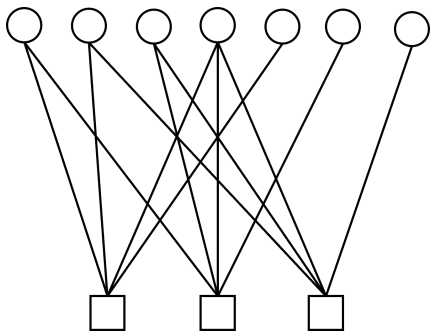
Irregular LDPC codes

- Improves the FER performance of the code
- Can be characterized using their VN and CN degree distributions $L(x)$ and $P(x)$, respectively

$$L(x) = \sum_d L_d x^d \qquad P(x) = \sum_d P_d x^d$$

  - L_d: fraction of VNs of degree d, P_d: fraction of CNs of degree d

Example:



- $L(x) = \frac{3}{7}x + \frac{3}{7}x^2 + \frac{1}{7}x^3$
- $P(x) = x^4$

NB-LDPC Code design

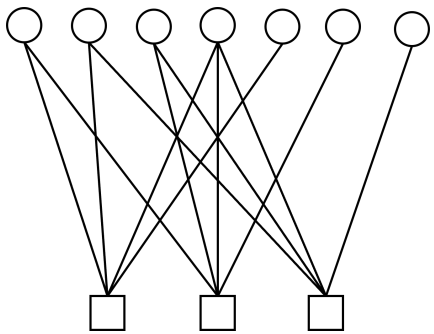
Irregular LDPC codes

- Improves the FER performance of the code
- Can be characterized using their VN and CN degree distributions $L(x)$ and $P(x)$, respectively

$$L(x) = \sum_d L_d x^d \qquad P(x) = \sum_d P_d x^d$$

  - L_d: fraction of VNs of degree d, P_d: fraction of CNs of degree d

Example:



- $L(x) = \frac{3}{7}x + \frac{3}{7}x^2 + \frac{1}{7}x^3$
- $P(x) = x^4$
- Code Rate $R = 1 - \frac{L'(1)}{R'(1)}$

NB-LDPC Code design

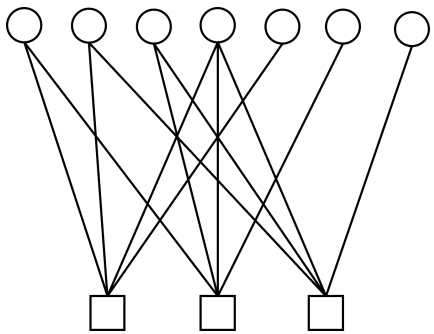
Irregular LDPC codes

- Improves the FER performance of the code
- Can be characterized using their VN and CN degree distributions $L(x)$ and $P(x)$, respectively

$$L(x) = \sum_d L_d x^d \qquad P(x) = \sum_d P_d x^d$$

  - L_d: fraction of VNs of degree d, P_d: fraction of CNs of degree d

Example:



- $L(x) = \frac{3}{7}x + \frac{3}{7}x^2 + \frac{1}{7}x^3$
- $P(x) = x^4$
- Code Rate $R = 1 - \frac{L'(1)}{R'(1)}$

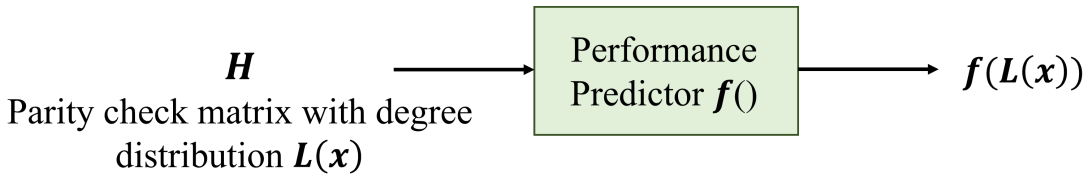
Our work: we optimize degree distribution $L(x), P(x)$ for the QKD channel to result in large IR rates

Degree Distribution Optimization using Differential Evolution

- General procedure to optimize degree distribution (Shokrollahi '00):

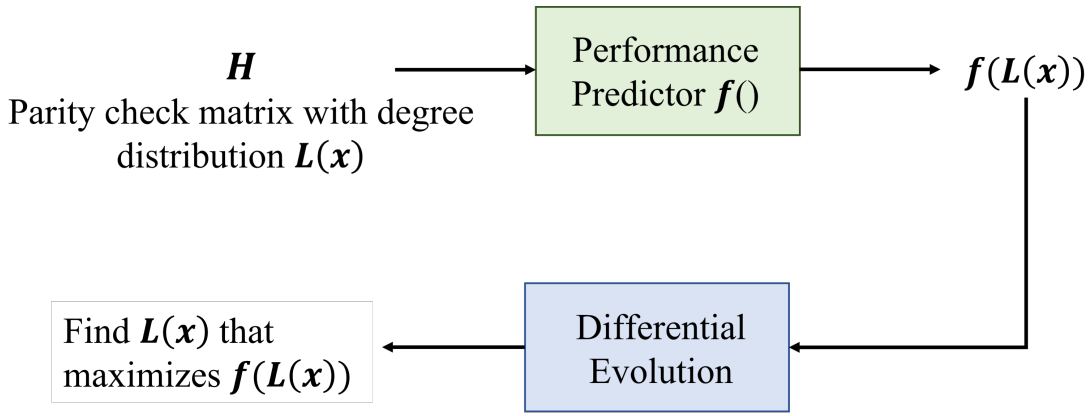
Degree Distribution Optimization using Differential Evolution

- General procedure to optimize degree distribution (Shokrollahi '00):



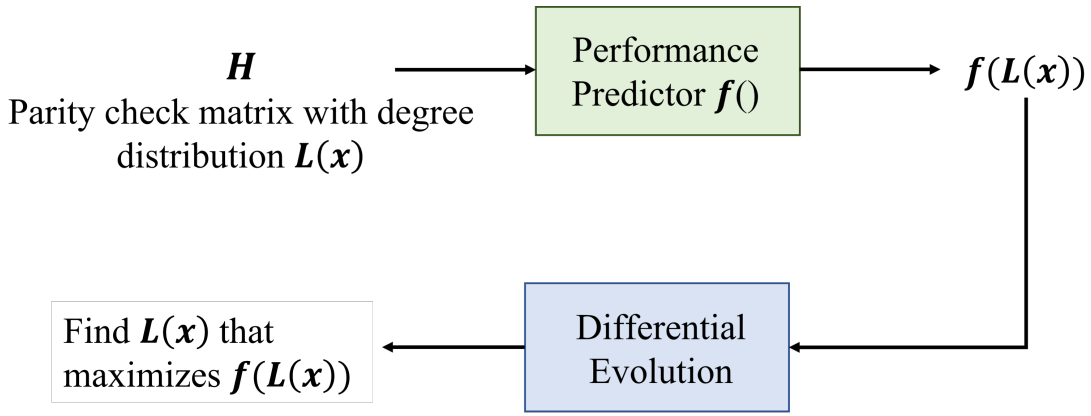
Degree Distribution Optimization using Differential Evolution

- General procedure to optimize degree distribution (Shokrollahi '00):



Degree Distribution Optimization using Differential Evolution

- General procedure to optimize degree distribution (Shokrollahi '00):

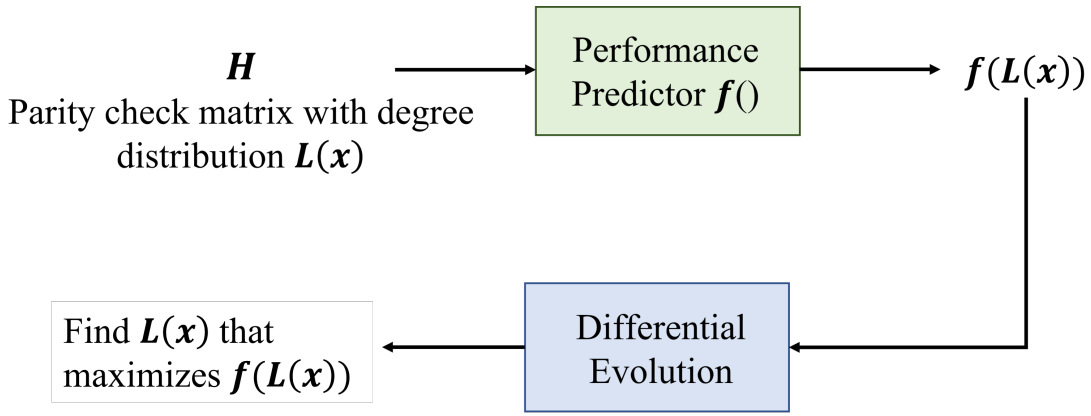


Generally

- The performance predictor is the code threshold (low complexity to compute)

Degree Distribution Optimization using Differential Evolution

- General procedure to optimize degree distribution (Shokrollahi '00):

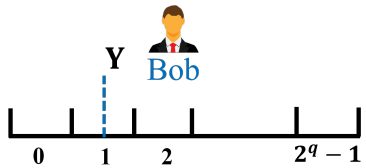


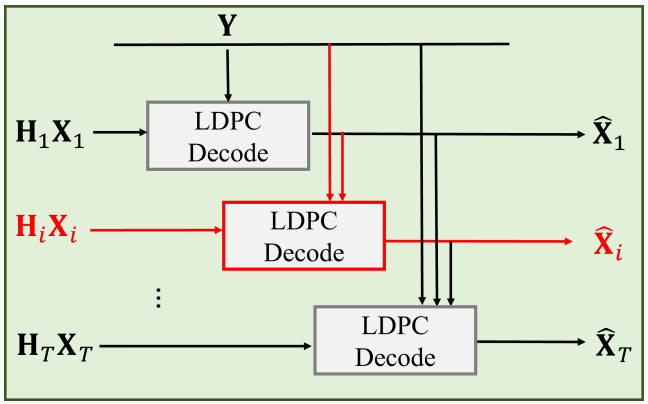
Generally

- The performance predictor is the code threshold (low complexity to compute)
- $L(x)$ is optimized for a fixed code rate R

Joint Rate and Degree Distribution Optimization (JRDO)

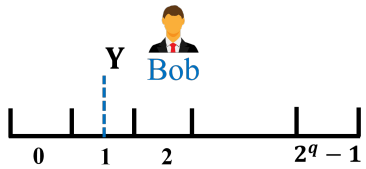
$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$

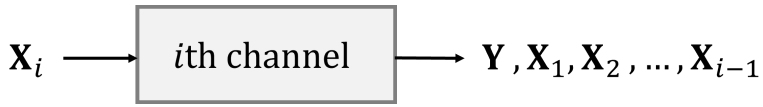


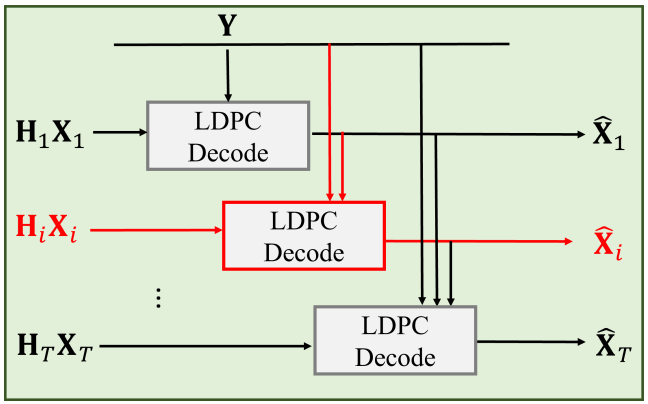


Joint Rate and Degree Distribution Optimization (JRDO)

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$

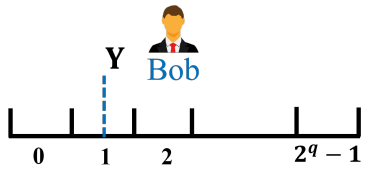


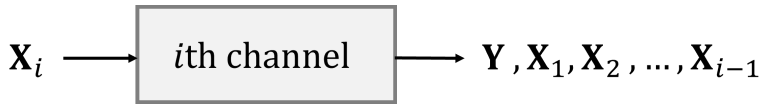


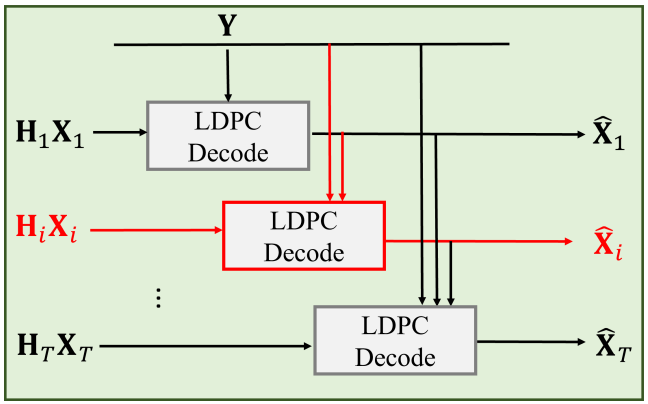


Joint Rate and Degree Distribution Optimization (JRDO)

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$



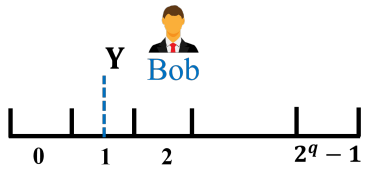


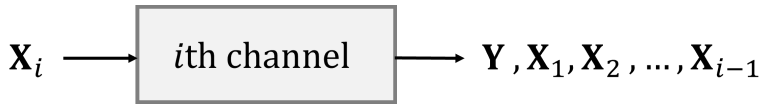


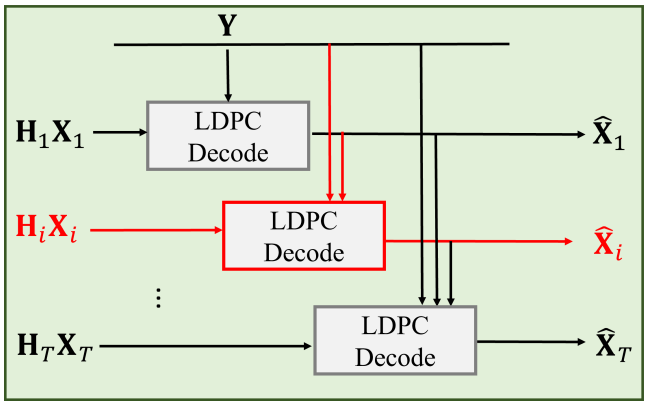
- $\gamma_i = P(Y = y, X_1 = x_1, \ldots, X_{i-1} = x_{i-1} | X_i = x_i)$

Joint Rate and Degree Distribution Optimization (JRDO)

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$



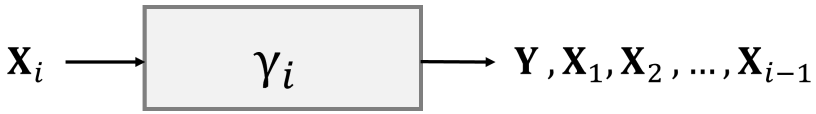


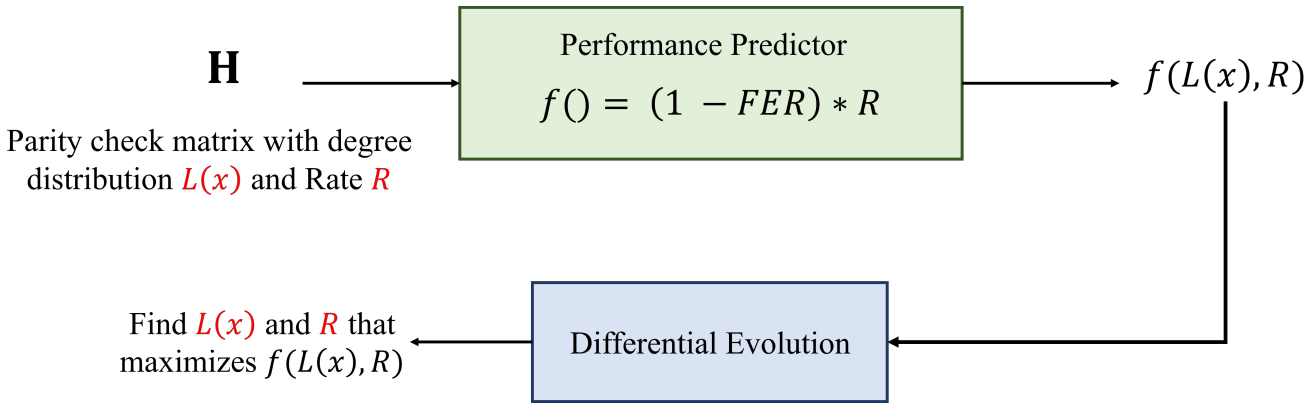


- $\gamma_i = P(Y = y, X_1 = x_1, \ldots, X_{i-1} = x_{i-1} | X_i = x_i)$
- Can be derived from the QKD channel $P_{Y|X}(Y = y|X = x)$

Joint Rate and Degree Distribution Optimization (JRDO)

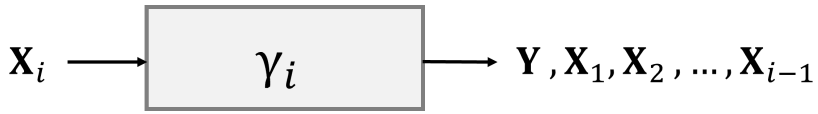
$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$

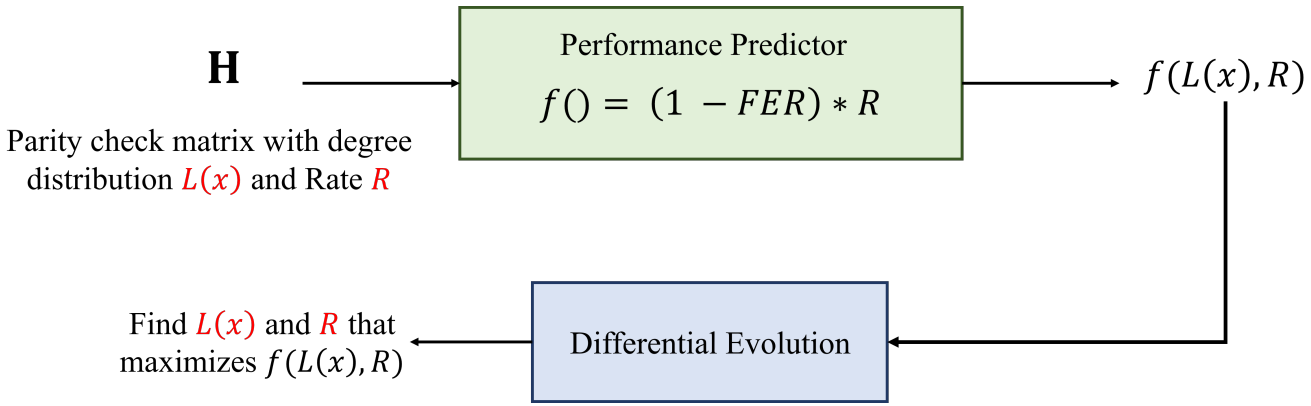




Joint Rate and Degree Distribution Optimization (JRDO)

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$

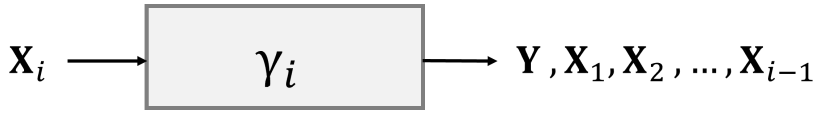


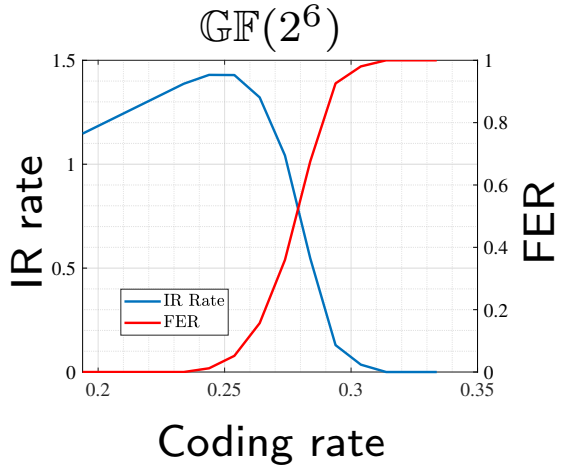


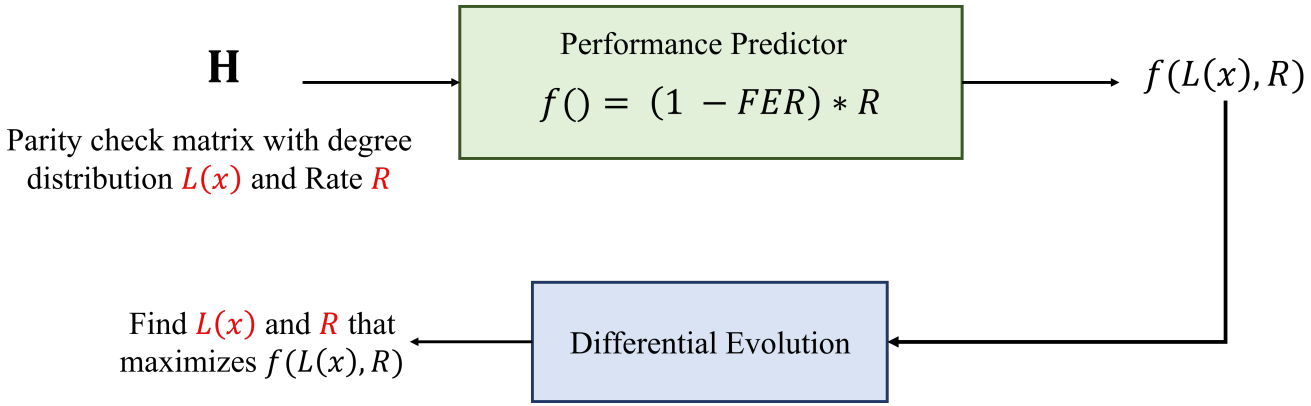
- FER is the frame error rate encountered on channel γ_i

Joint Rate and Degree Distribution Optimization (JRDO)

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$



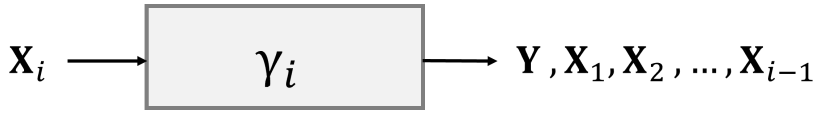


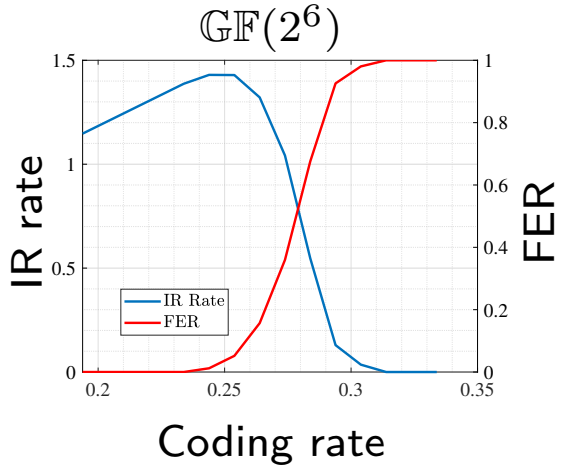


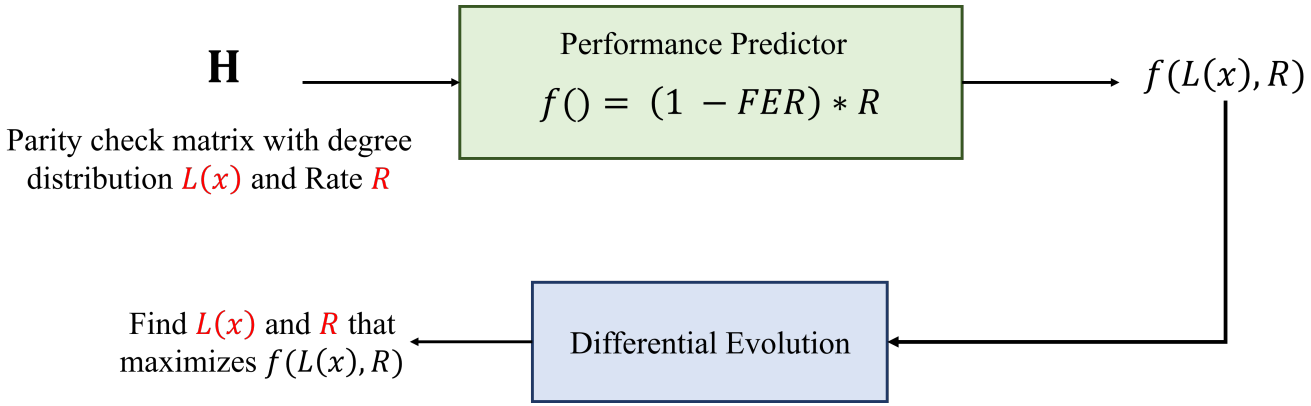
- FER is the frame error rate encountered on channel γ_i
- FER can be obtained with low complexity by Monte-Carlo simulation of a small number of codewords

Joint Rate and Degree Distribution Optimization (JRDO)

$$\text{IR rate} = \sum_{i=1}^{T}(1 - FER_i) * Rate_i * \alpha_i$$

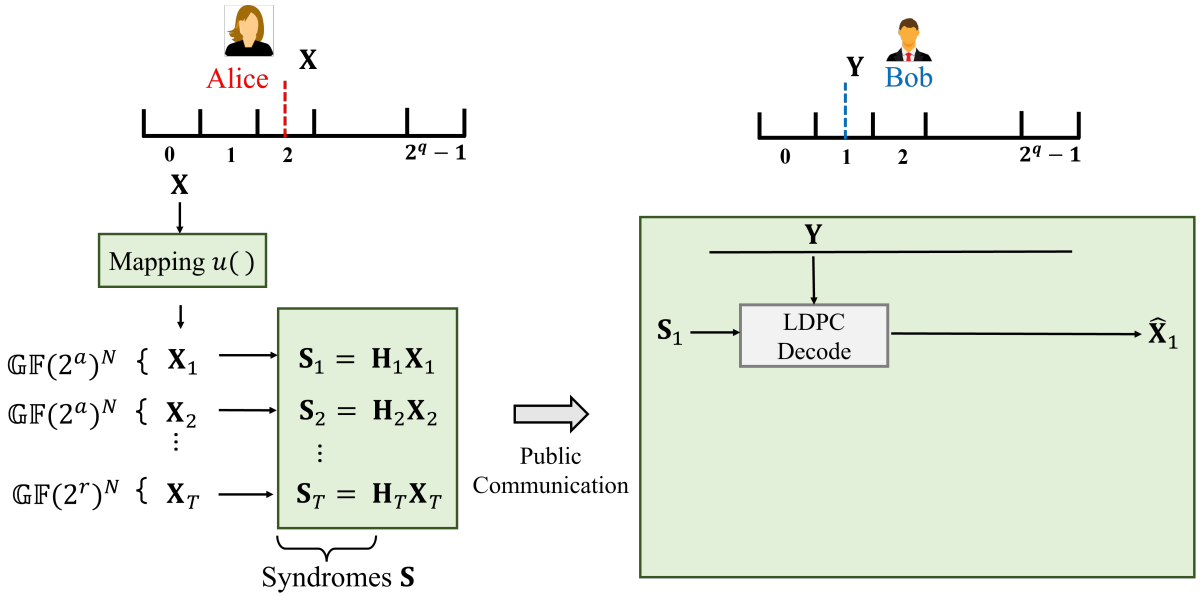






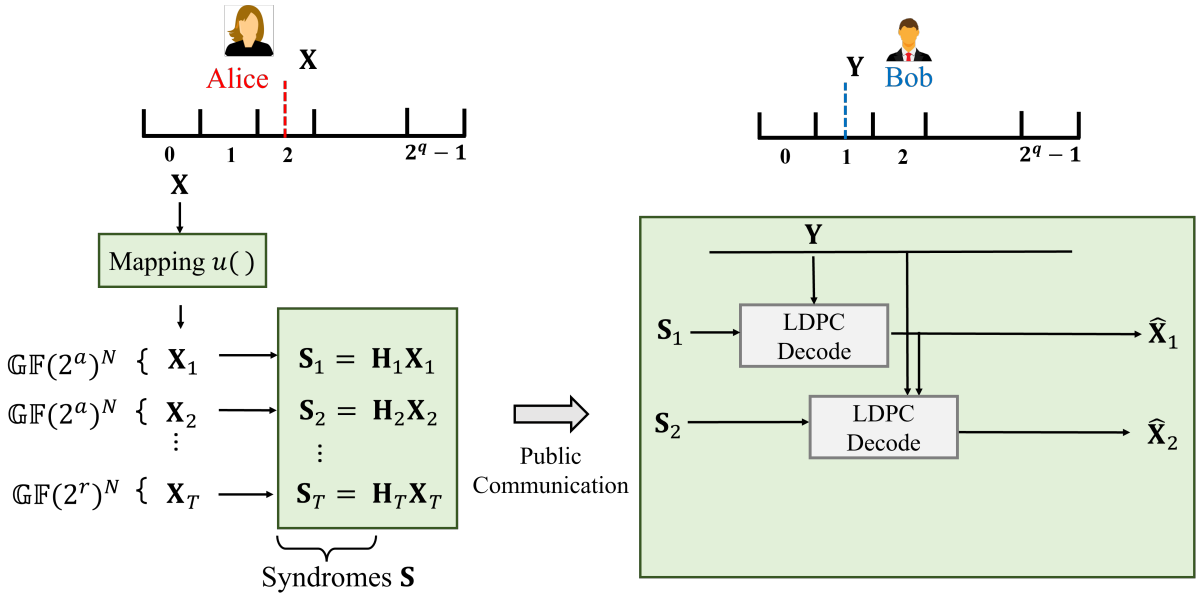
- FER is the frame error rate encountered on channel γ_i
- Can jointly optimize the degree distribution $L(x)$ and rate R to get high IR rates

Sequential Decoding and Interactive Communication



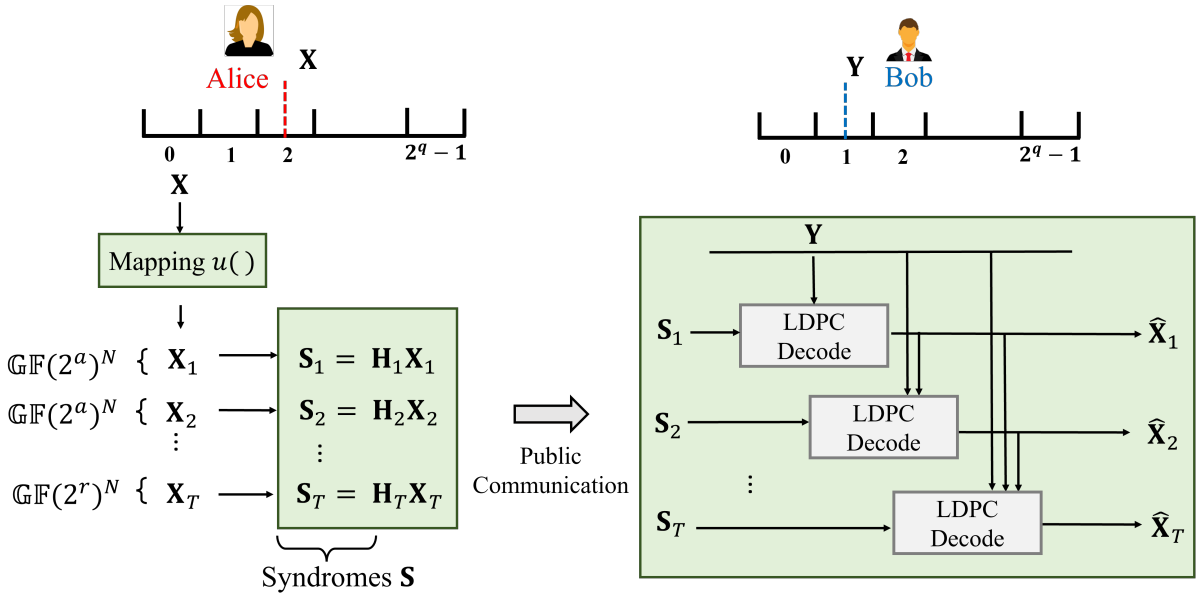
Error propagation and current remedy:

Sequential Decoding and Interactive Communication



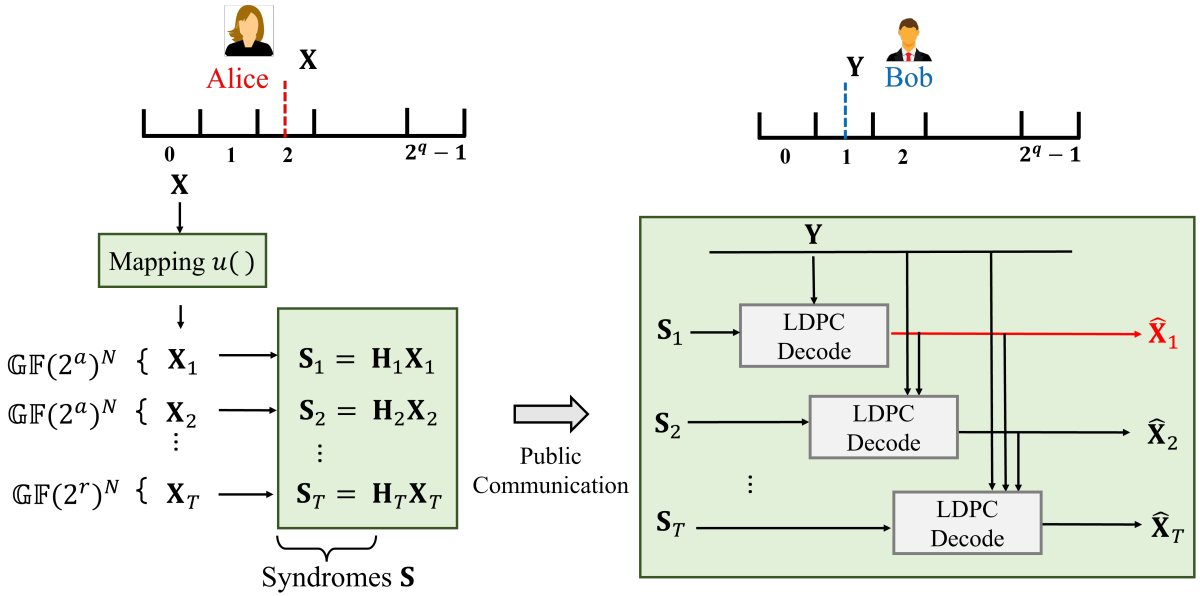
Error propagation and current remedy:

Sequential Decoding and Interactive Communication



Error propagation and current remedy:

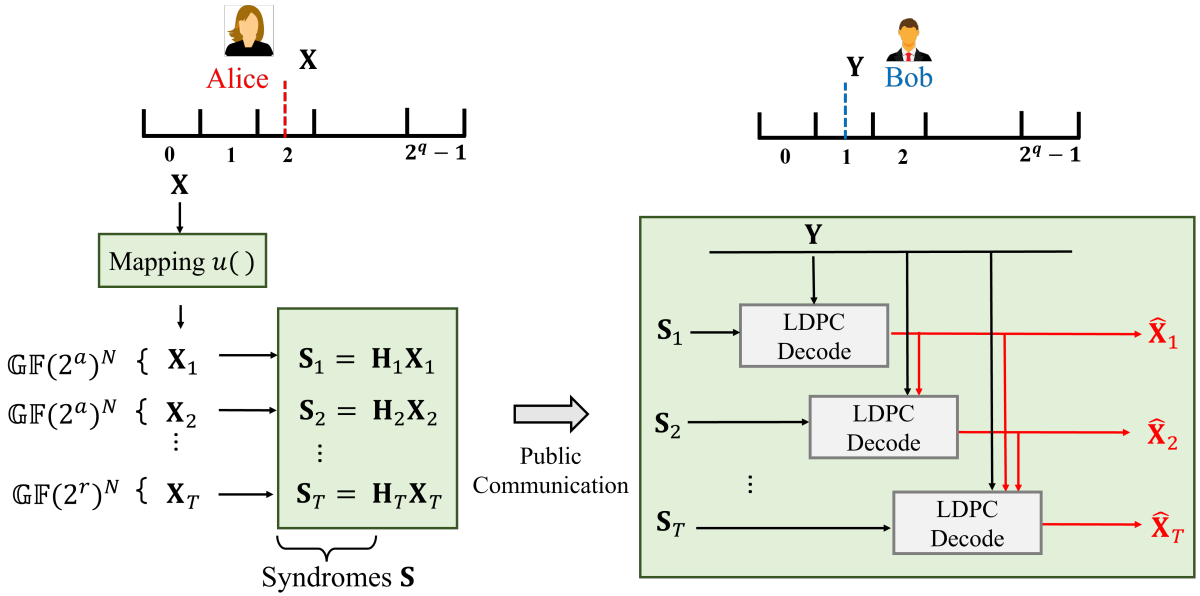
Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers

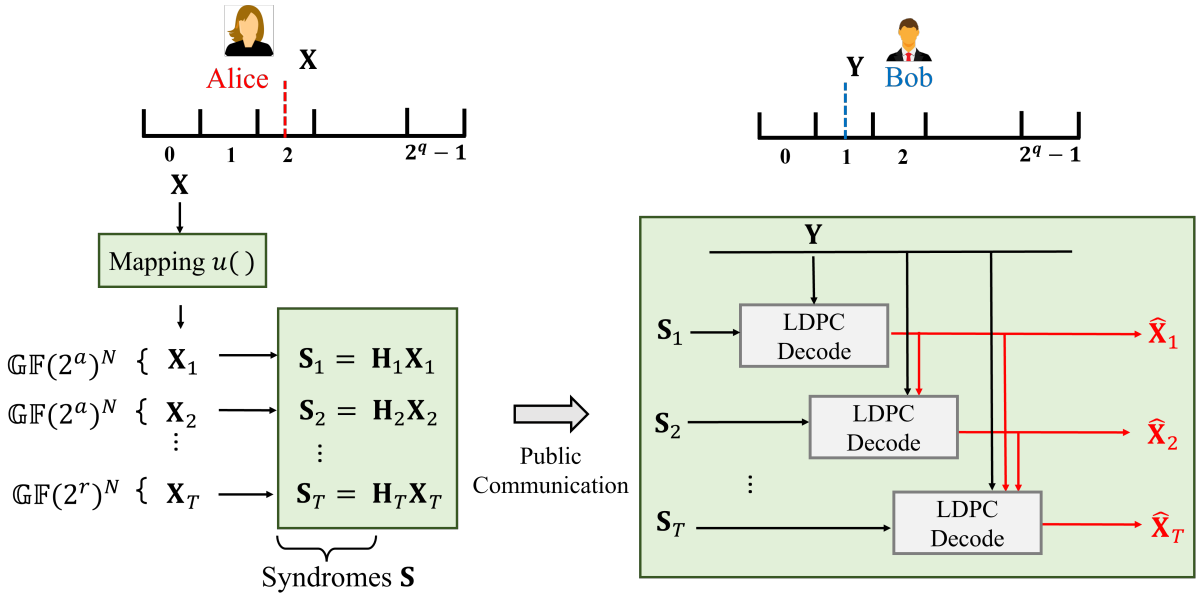
Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers

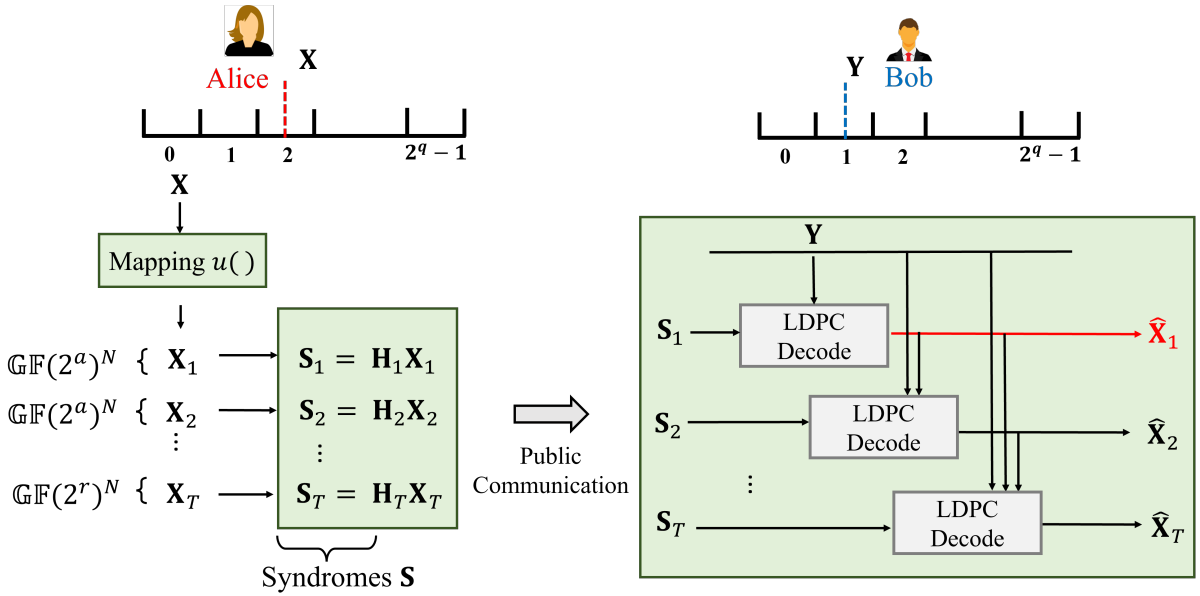
Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers
- Interactive communication used to mitigate error propagation (Zhou '13)

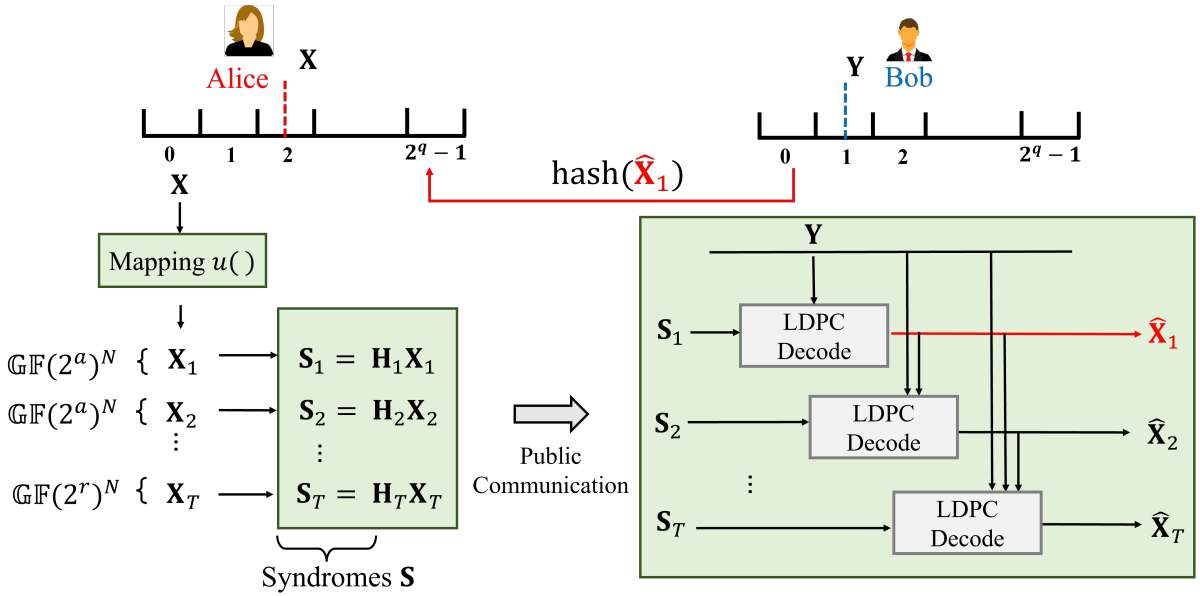
Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers
- Interactive communication used to mitigate error propagation (Zhou '13)

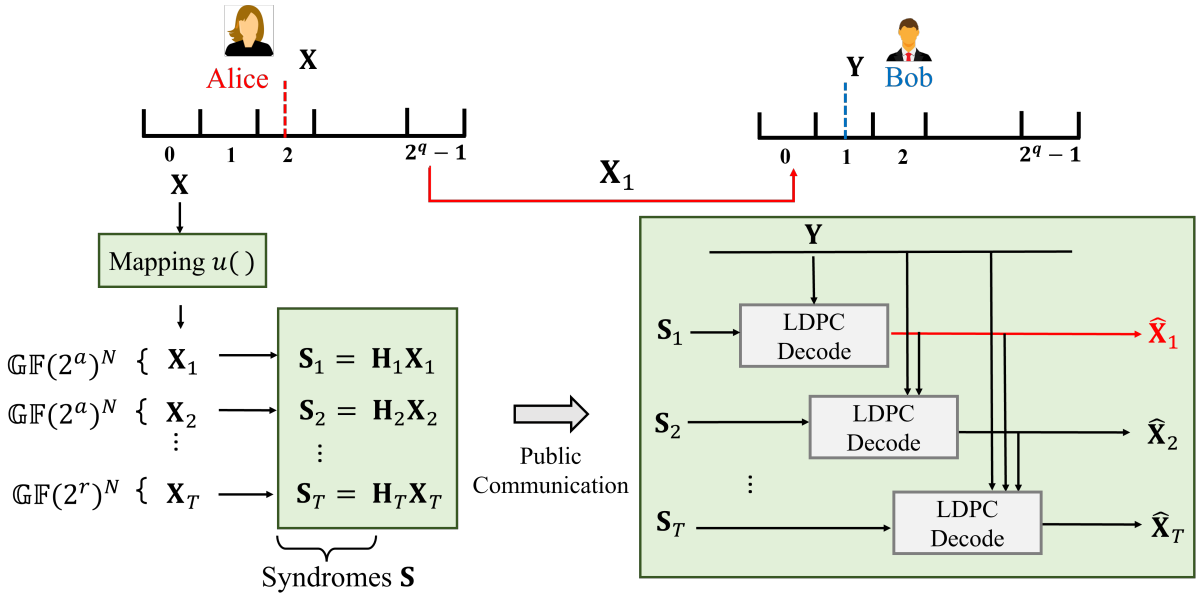
Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers
- Interactive communication used to mitigate error propagation (Zhou '13)
- Verify decoded output using hashes (Federov '18)

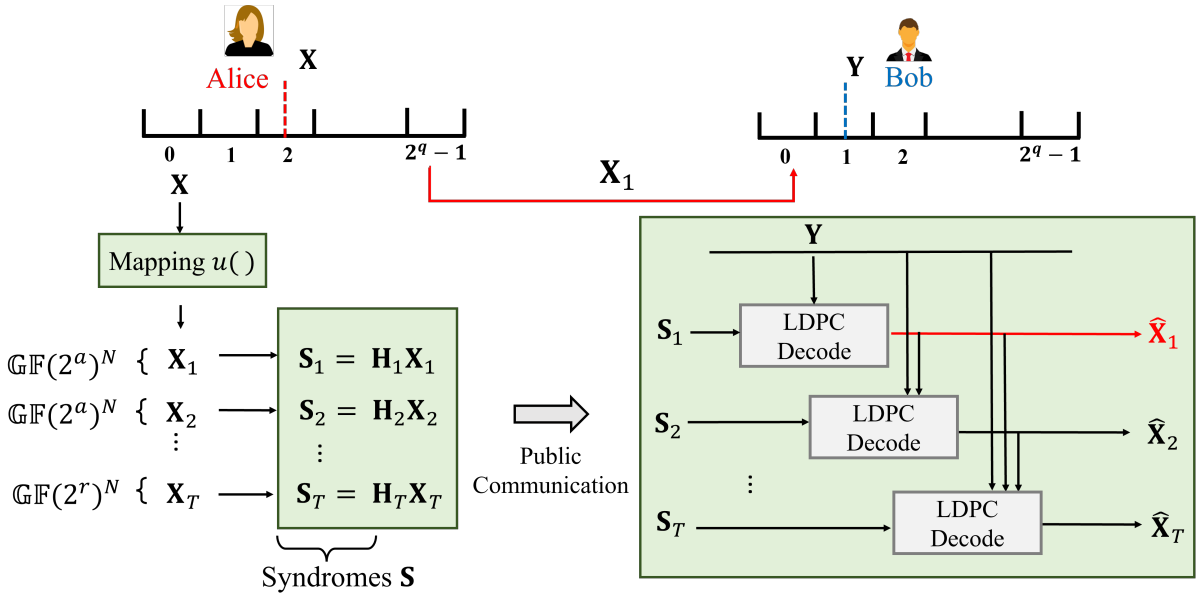
Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers
- Interactive communication used to mitigate error propagation (Zhou '13)
- Verify decoded output using hashes (Federov '18)
- Verification fails $\rightarrow$ Alice sends Bob the actual symbol for subsequent decoding

Sequential Decoding and Interactive Communication



Error propagation and current remedy:

- A decoding error in one layer $\rightarrow$ decoding error in subsequent layers
- Interactive communication used to mitigate error propagation (Zhou '13)
- Verify decoded output using hashes (Federov '18)
- Verification fails $\rightarrow$ Alice sends Bob the actual symbol for subsequent decoding

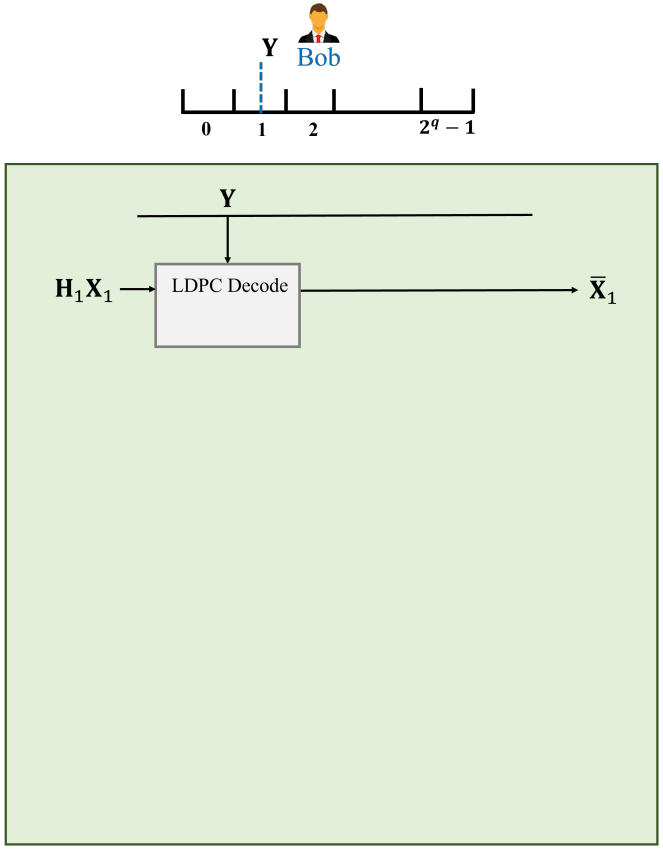
Decoding and interactive communication is sequential

Interleaved Decoding and Communication (IDC)

Idea: Use interactive communication of the later layers to decode previous layers

Interleaved Decoding and Communication (IDC)

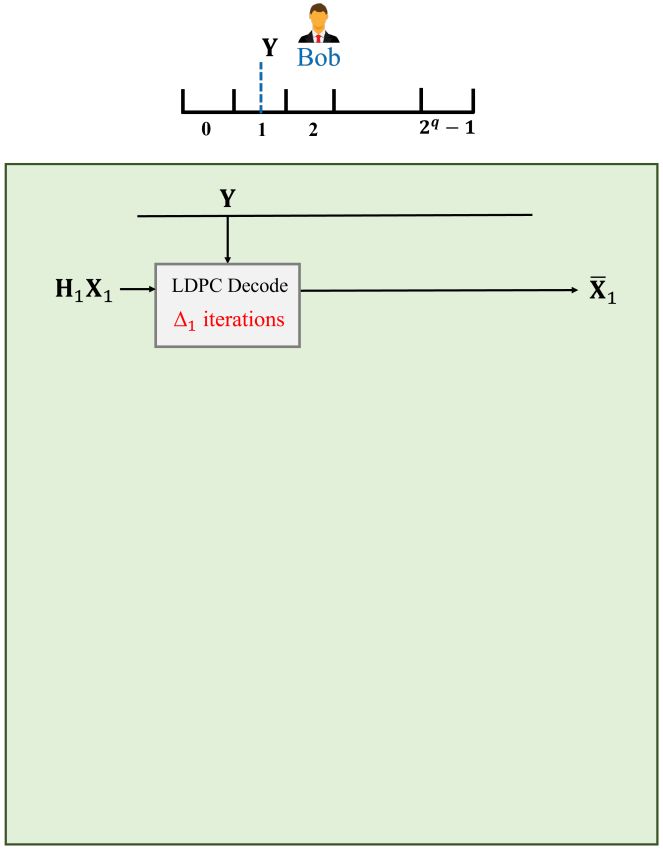
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ,

Interleaved Decoding and Communication (IDC)

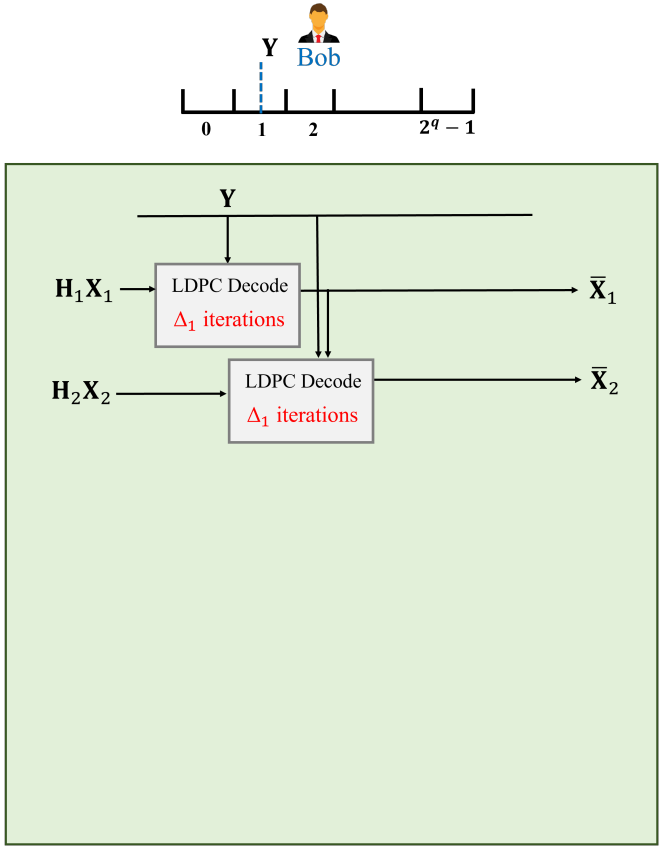
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$

Interleaved Decoding and Communication (IDC)

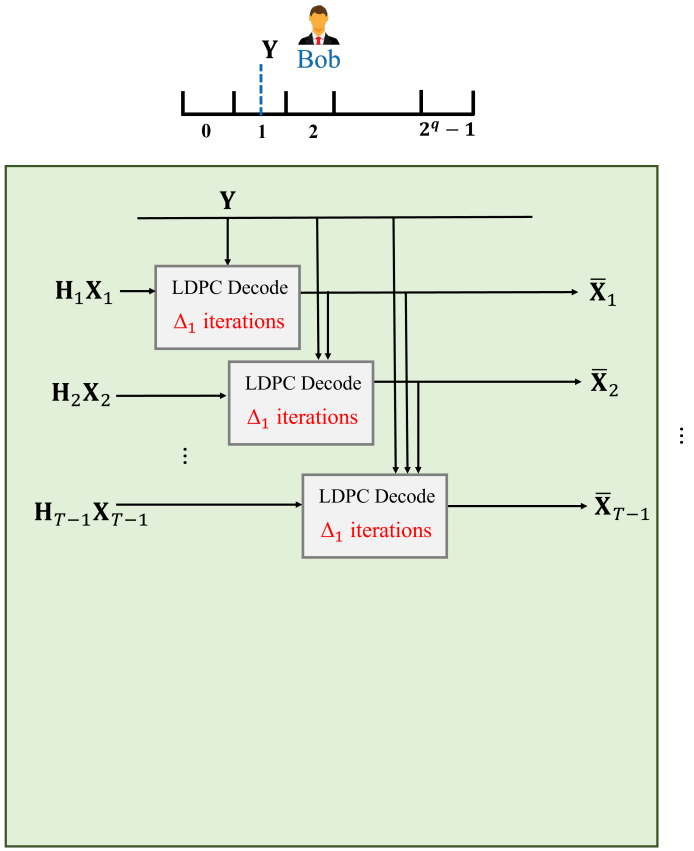
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$

Interleaved Decoding and Communication (IDC)

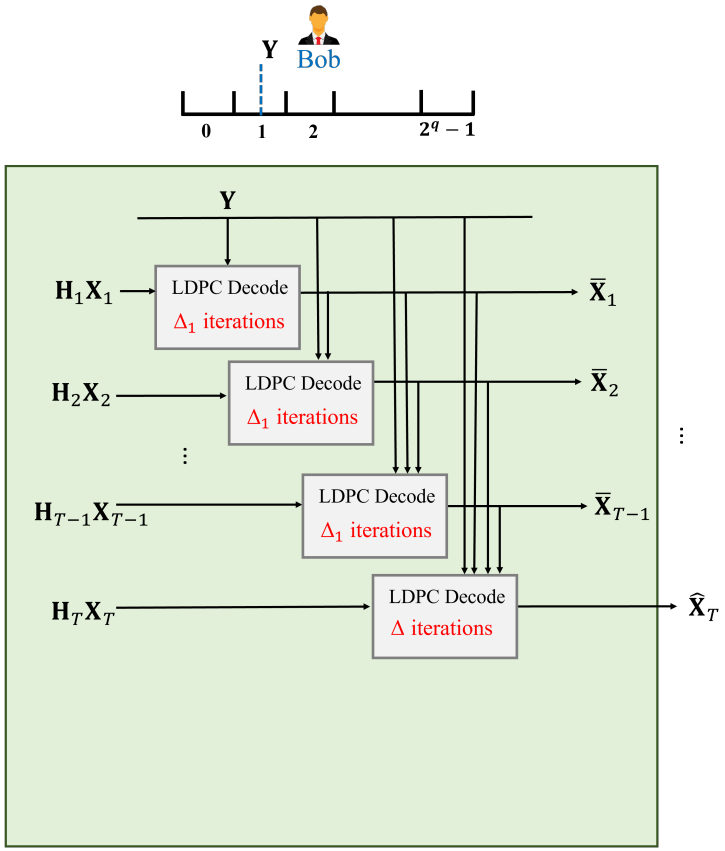
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$

Interleaved Decoding and Communication (IDC)

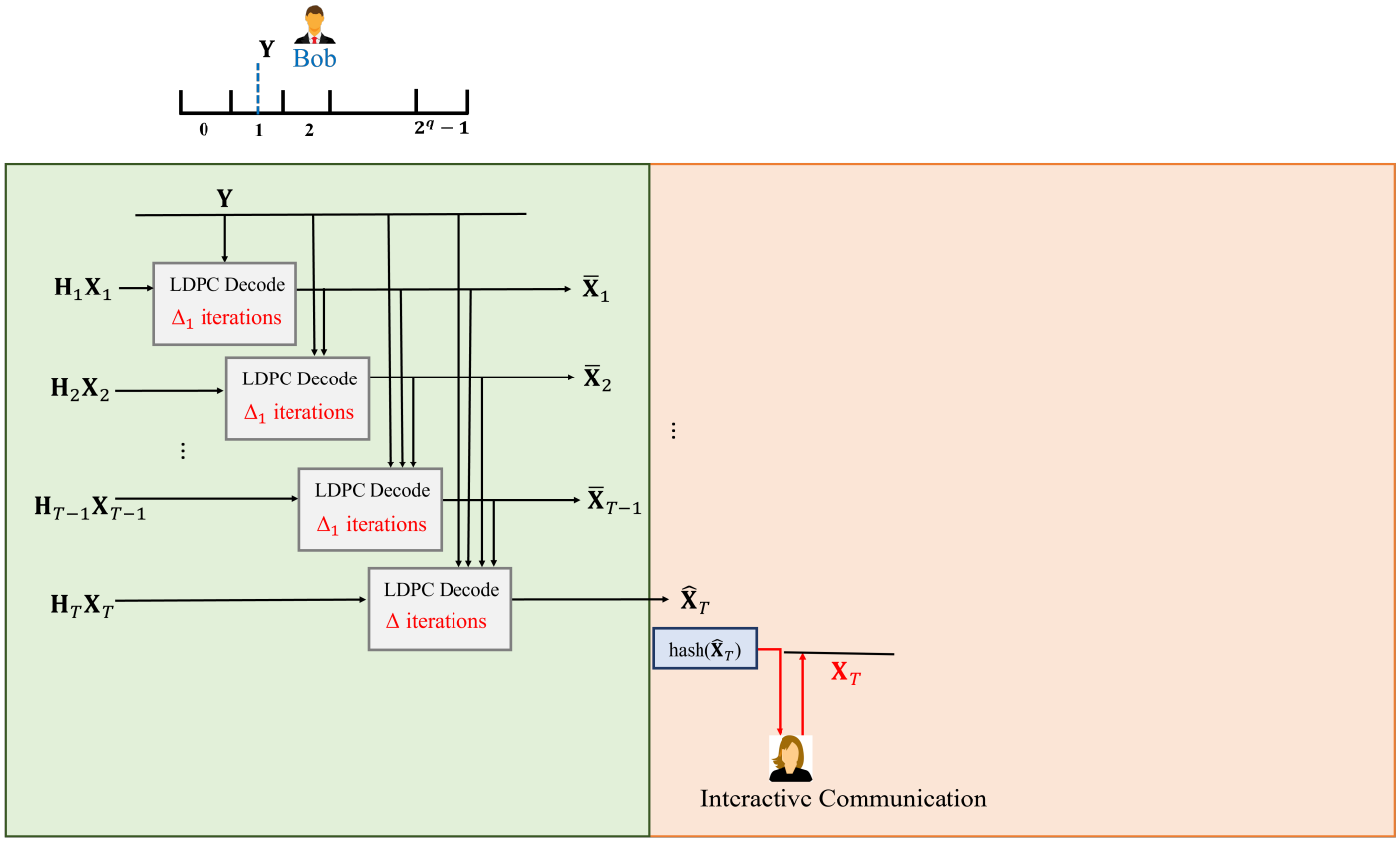
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$

Interleaved Decoding and Communication (IDC)

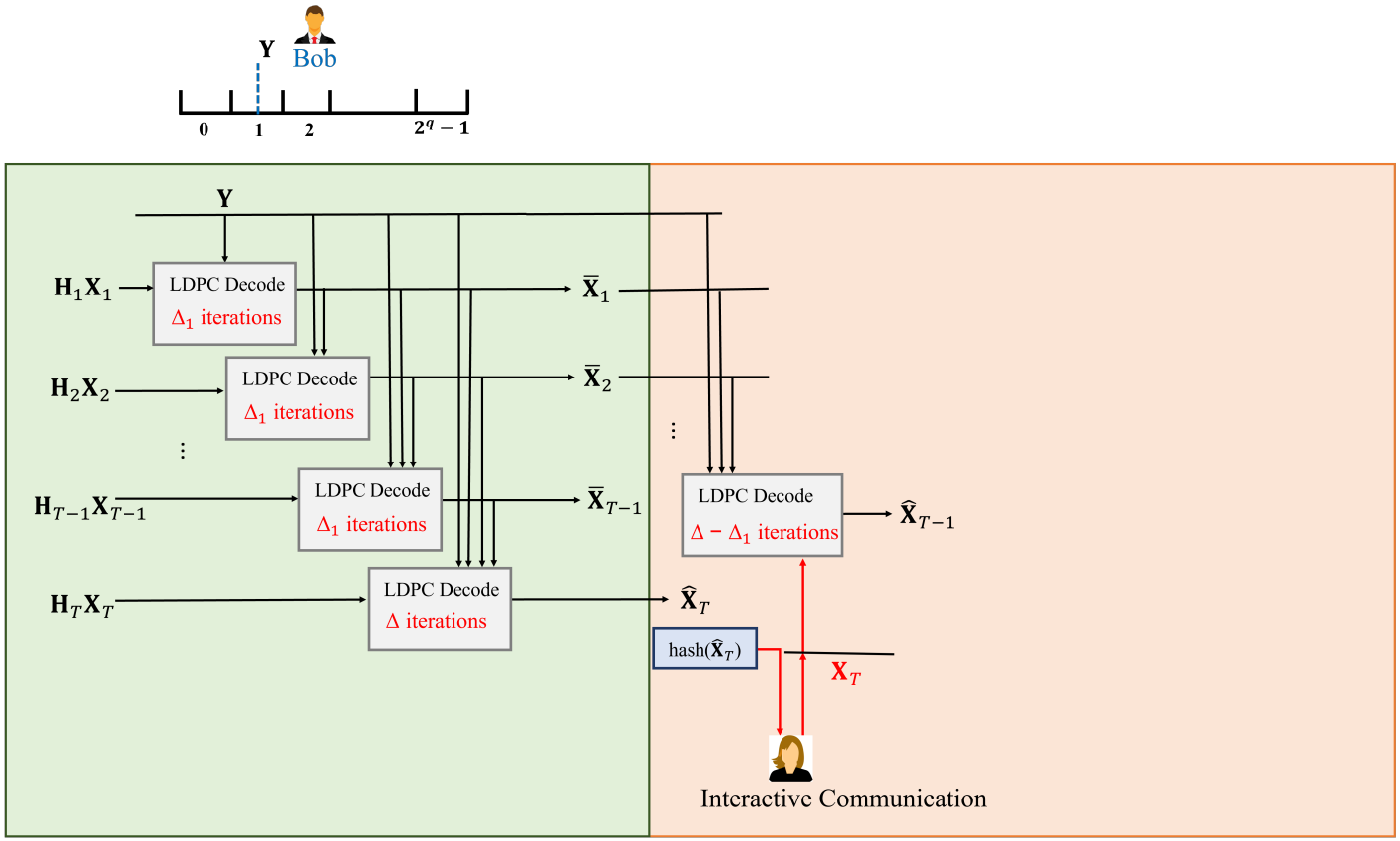
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\Delta_1 \leq \Delta$

Interleaved Decoding and Communication (IDC)

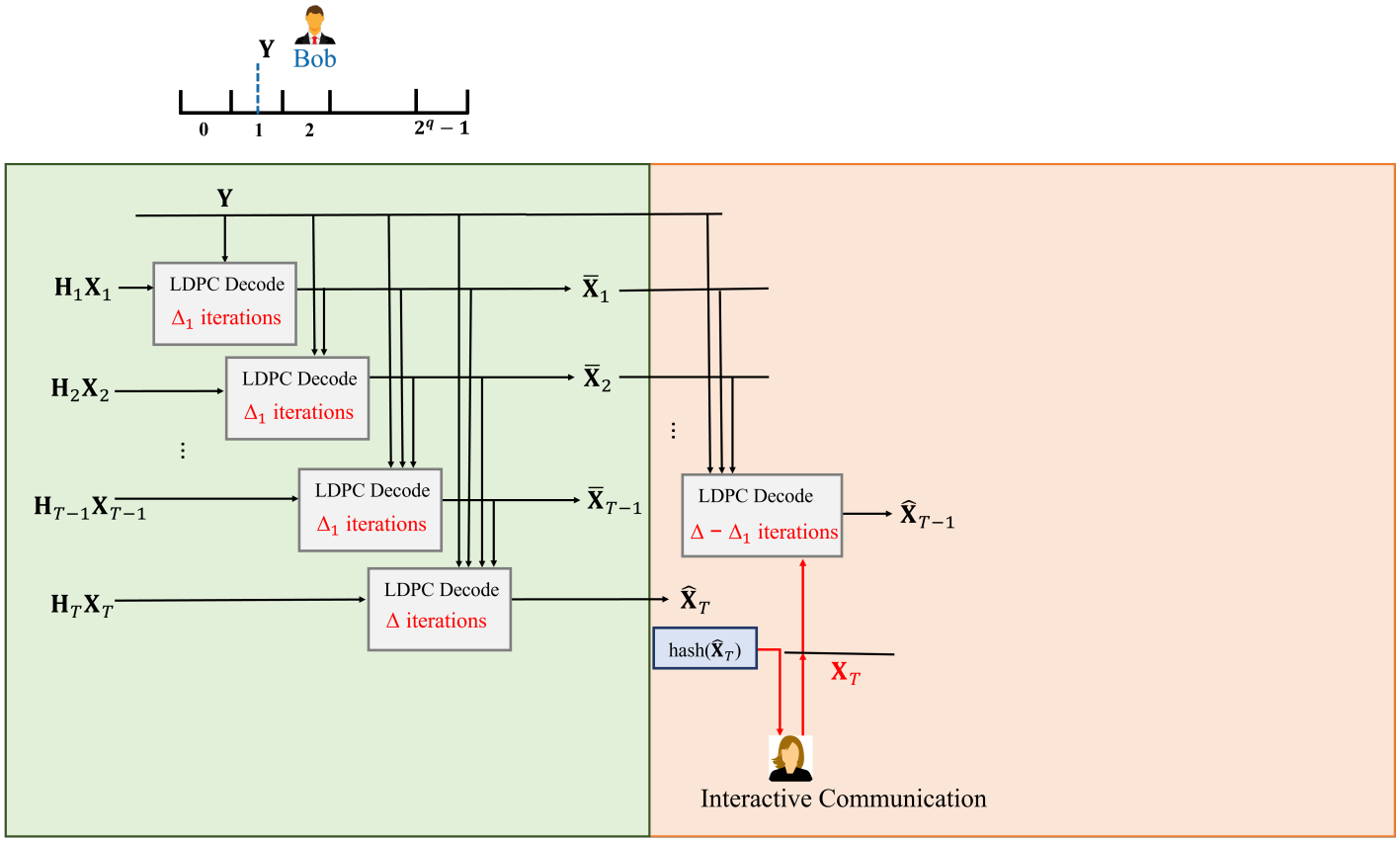
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\Delta_1 \leq \Delta$

Interleaved Decoding and Communication (IDC)

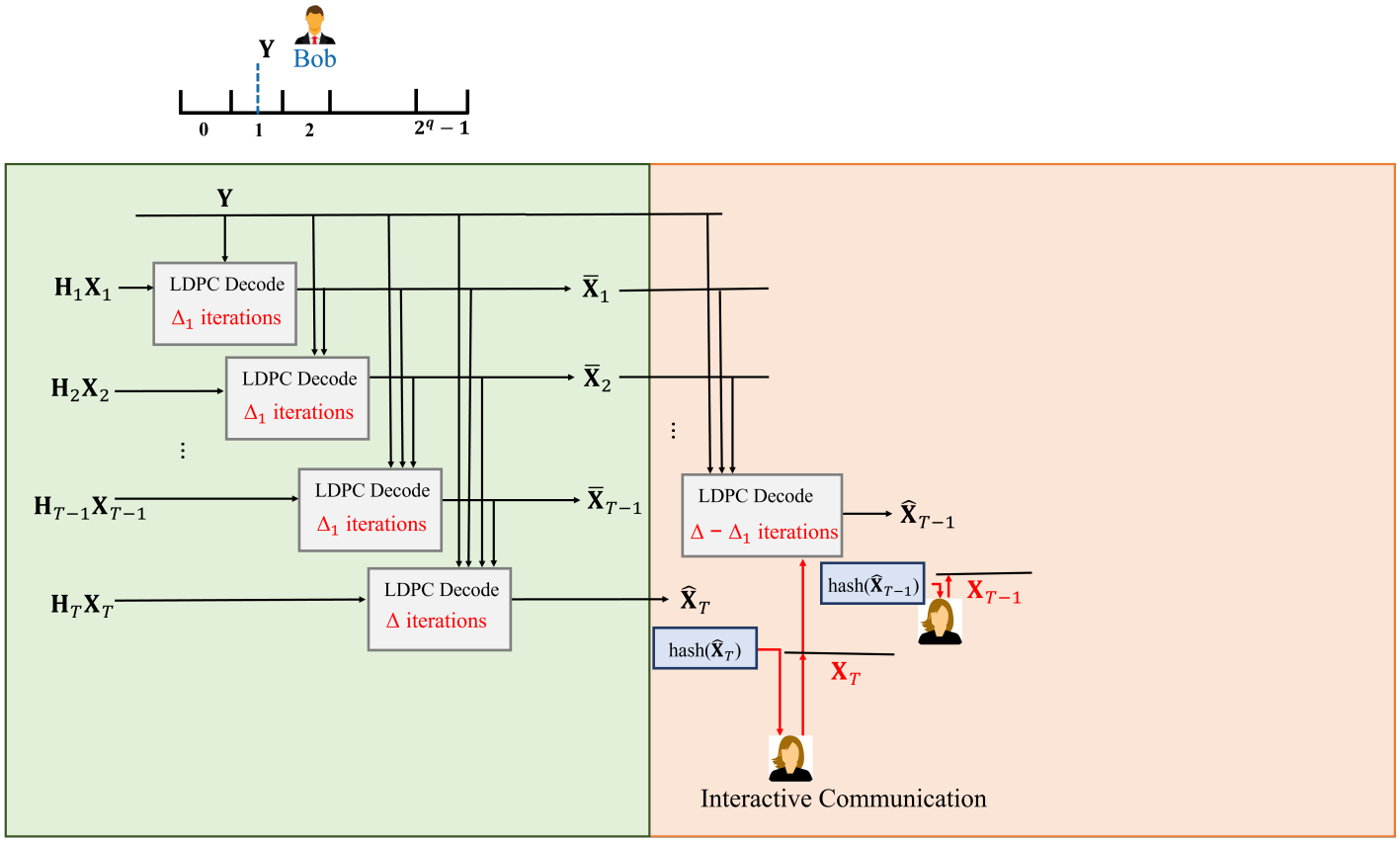
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$
- Additional side information aids decoding and help improve the IR rate (even with error propagation)

Interleaved Decoding and Communication (IDC)

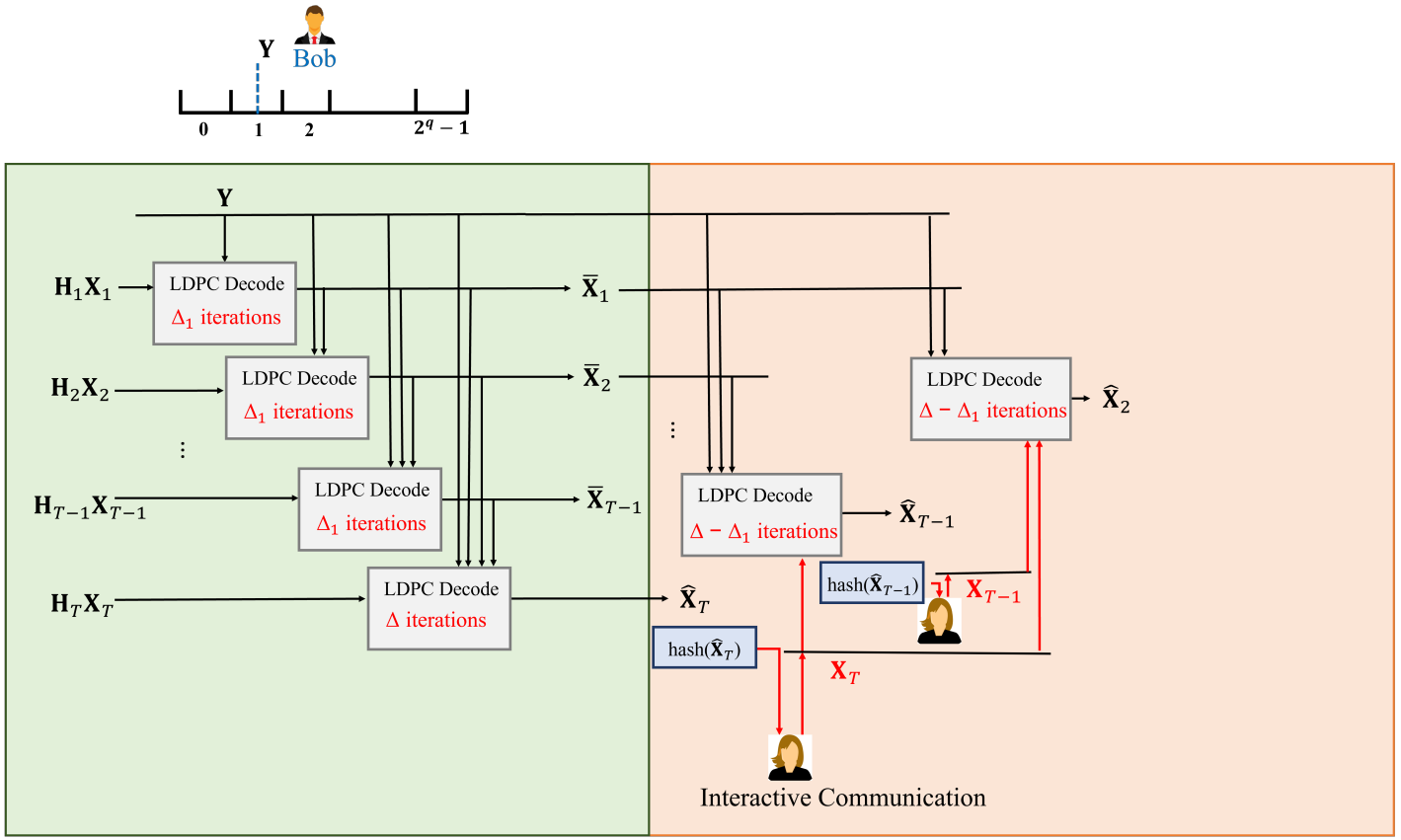
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$
- Additional side information aids decoding and help improve the IR rate (even with error propagation)

Interleaved Decoding and Communication (IDC)

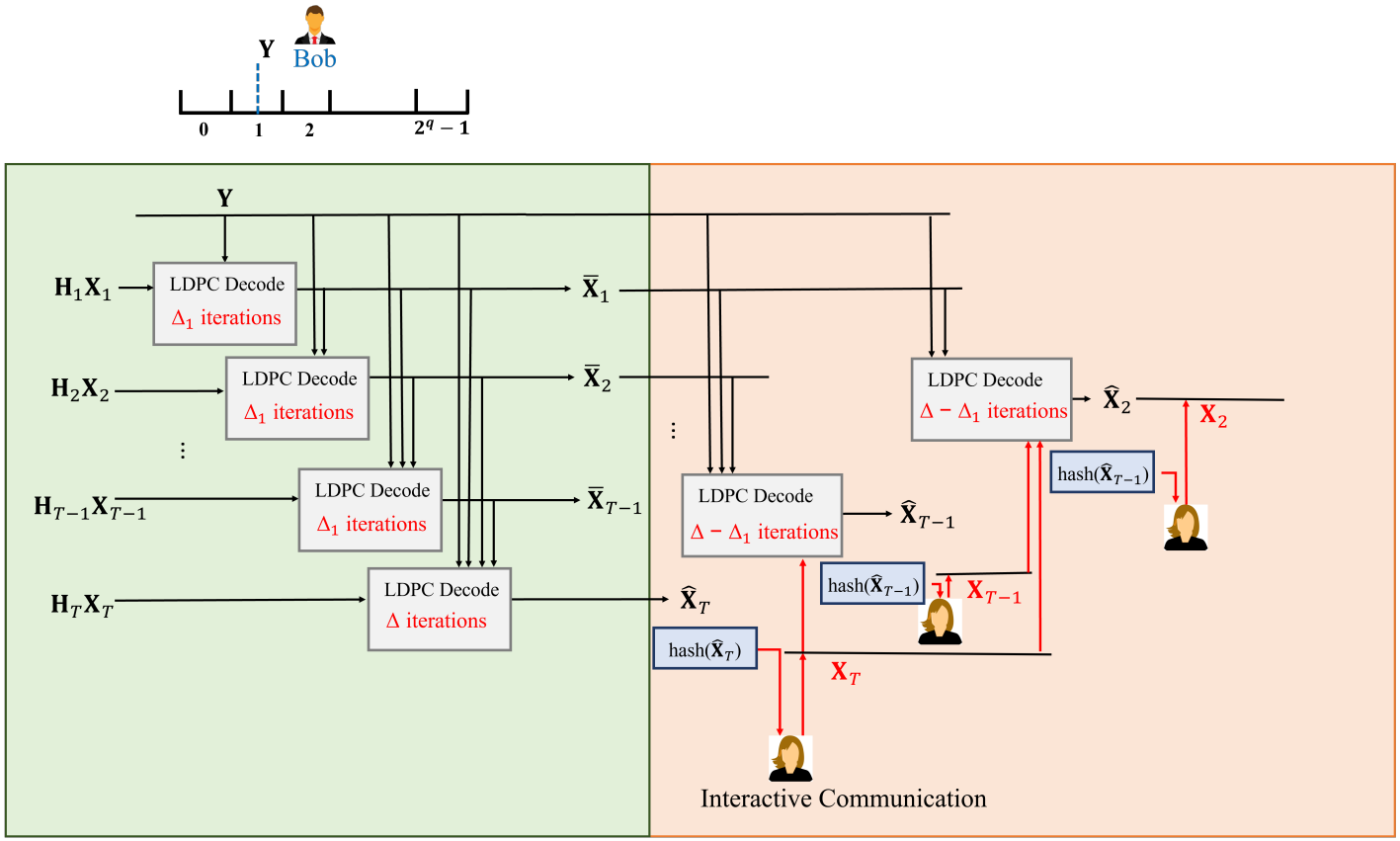
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$
- Additional side information aids decoding and help improve the IR rate (even with error propagation)

Interleaved Decoding and Communication (IDC)

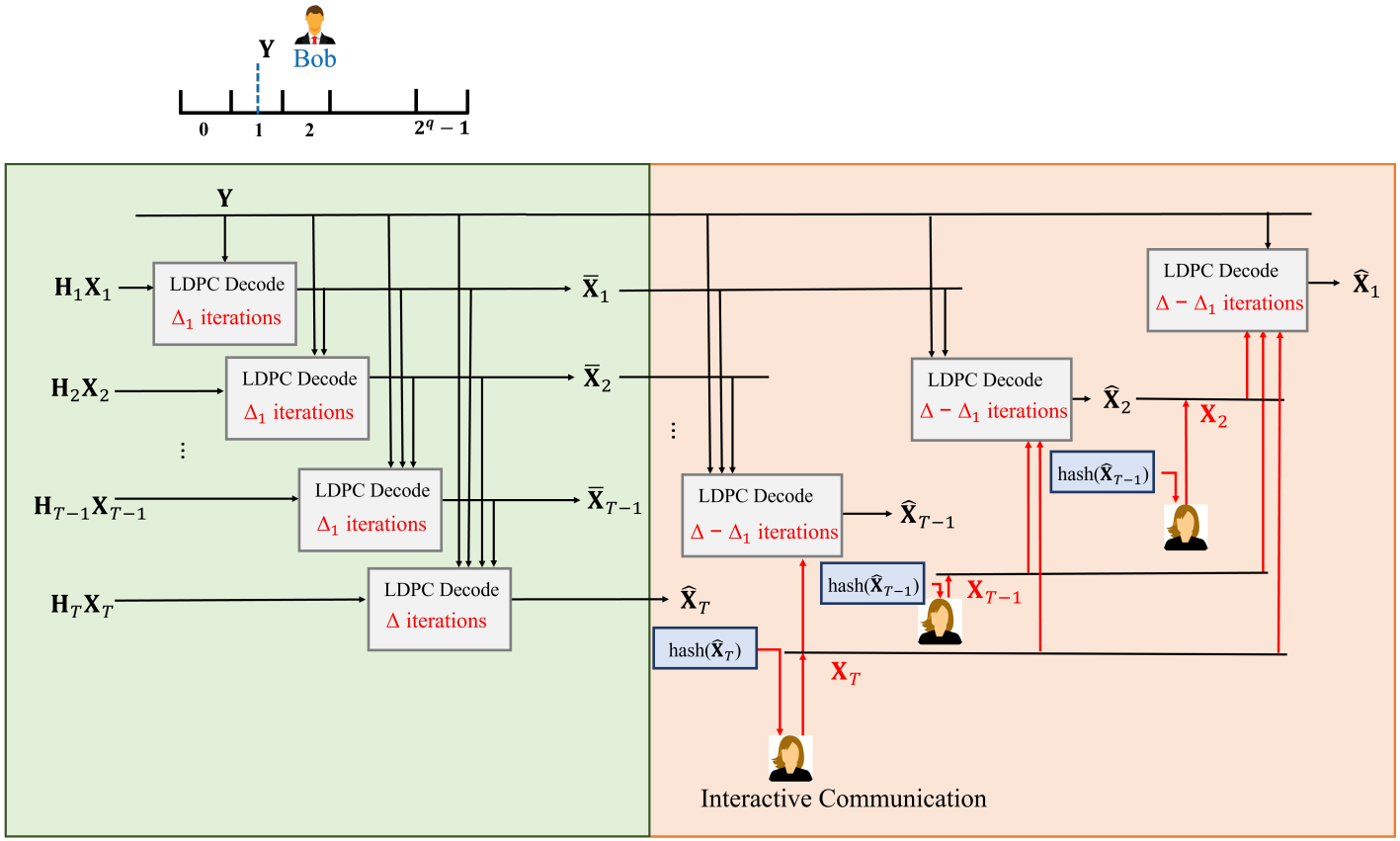
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$
- Additional side information aids decoding and help improve the IR rate (even with error propagation)

Interleaved Decoding and Communication (IDC)

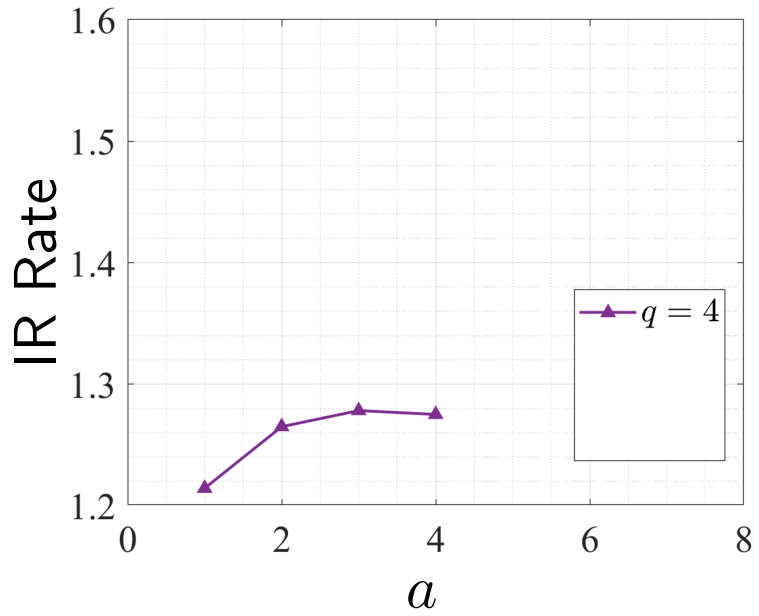
Idea: Use interactive communication of the later layers to decode previous layers



- Maximum number of decoding iterations: Δ, $\quad \Delta_1 \leq \Delta$
- Additional side information aids decoding and help improve the IR rate (even with error propagation)

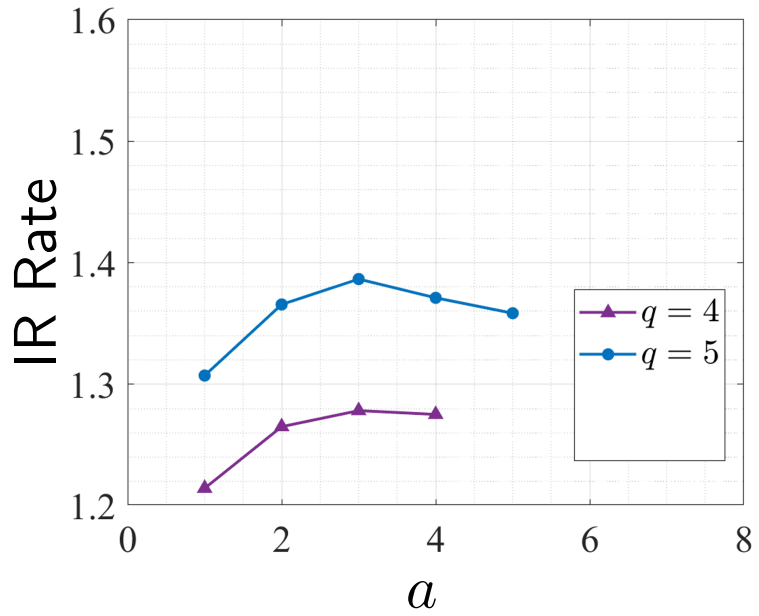
Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.



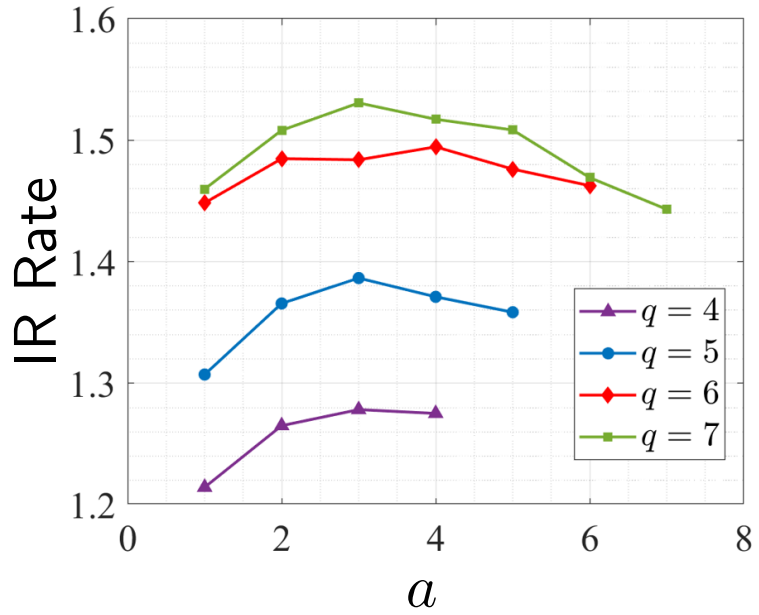
Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.



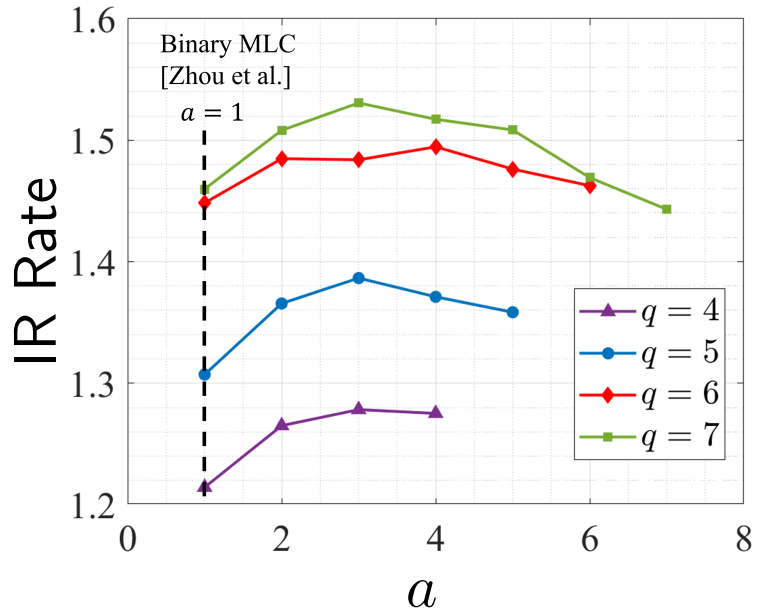
Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.



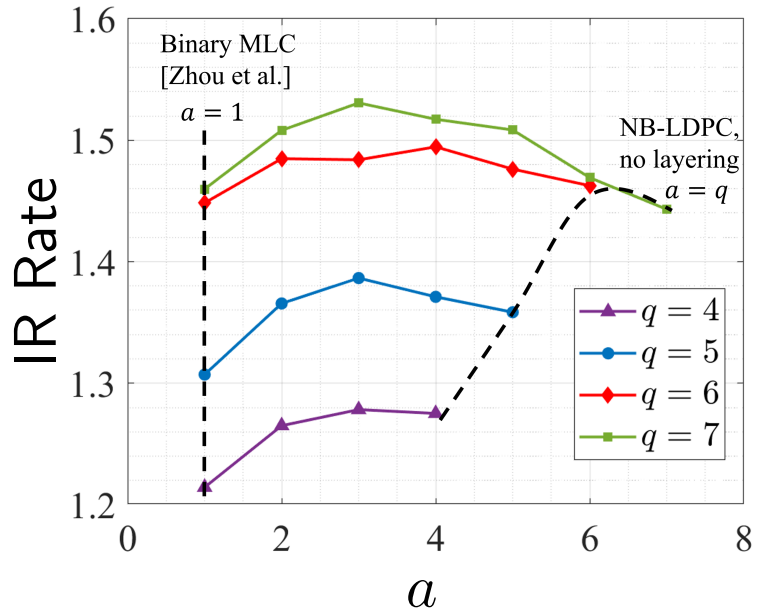
Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.



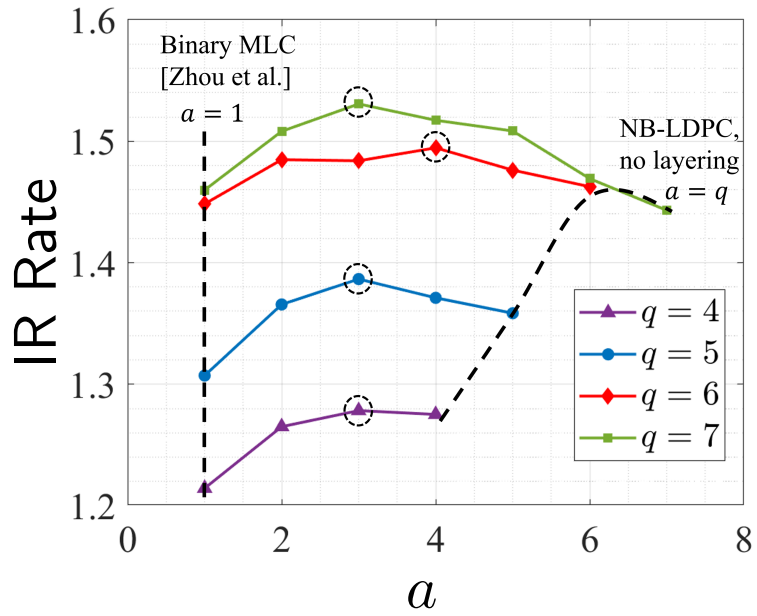
Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.



Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.

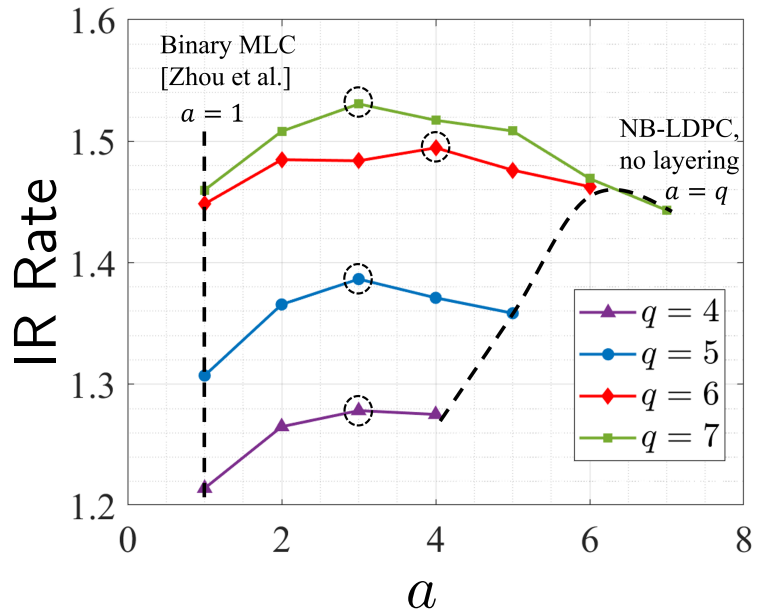


q	best a
4	3
5	3
6	4
7	3

- The IR rate is non-monotonic in a and has a maximum when a is strictly between 1 and q.

Simulation Results: IR vs. latency as a choice of parameter a

- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.

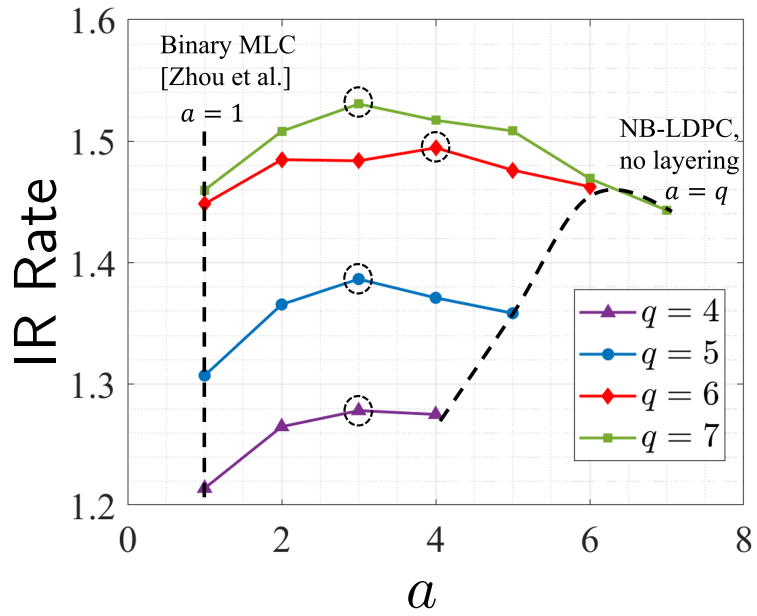


q	best a
4	3
5	3
6	4
7	3

- The IR rate is non-monotonic in a and has a maximum when a is strictly between 1 and q.
- Large $a \implies$ stronger NB-LDPC codes $\implies$ lower FER and better IR rate

Simulation Results: IR vs. latency as a choice of parameter a

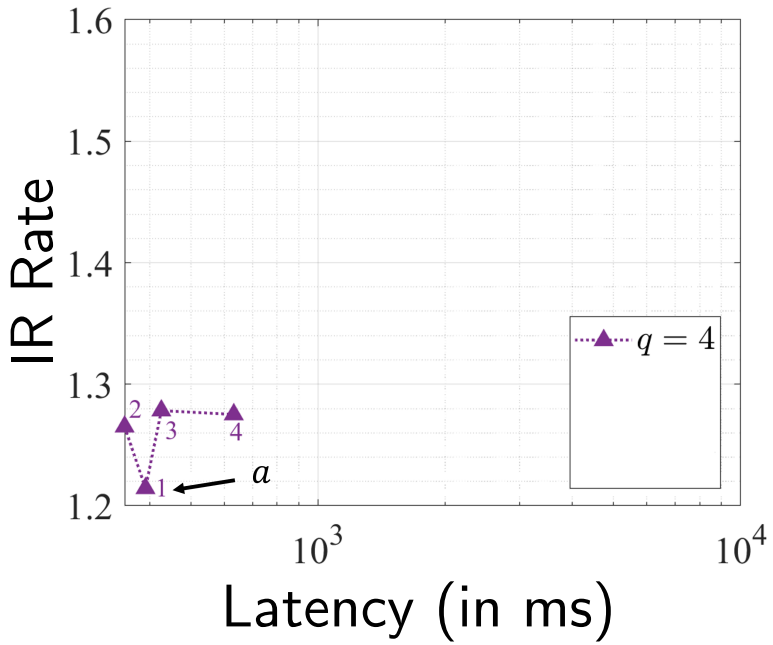
- Set-up: Wong Group @ UCLA. 2000 postprocessed frames.



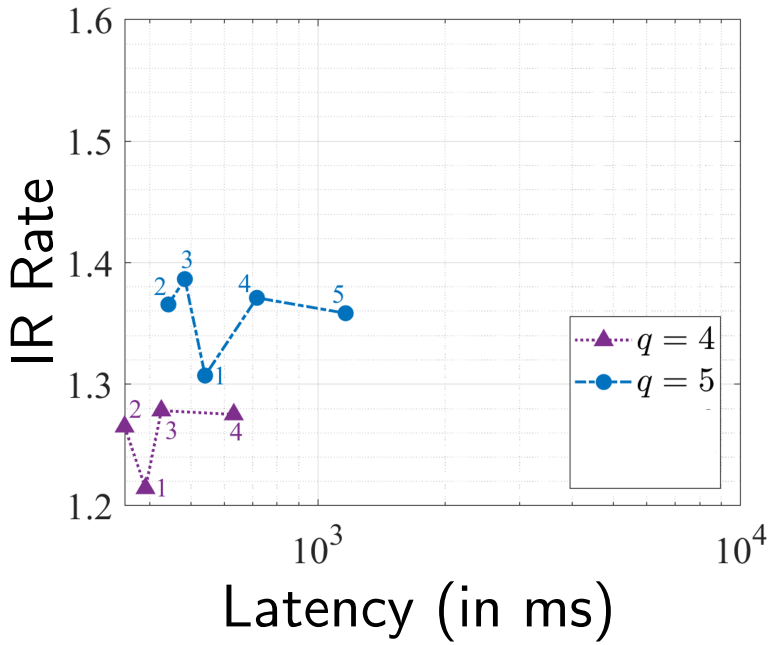
q	best a
4	3
5	3
6	4
7	3

- The IR rate is non-monotonic in a and has a maximum when a is strictly between 1 and q.
- Large a $\implies$ stronger NB-LDPC codes $\implies$ lower FER and better IR rate
- Small a $\implies$ more layers $\implies$ larger IR rate due to sum IR rate formula

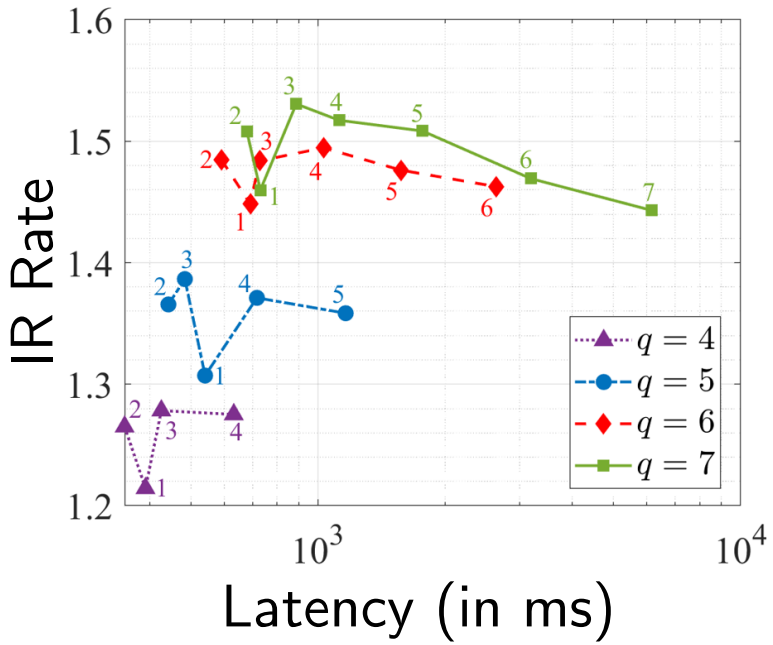
Simulation Results: IR vs. latency as the choice of parameter a



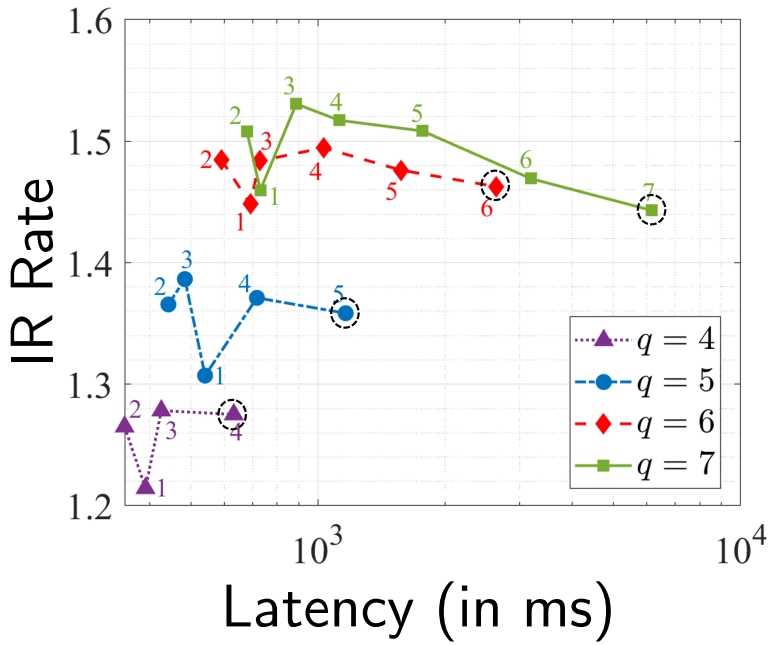
Simulation Results: IR vs. latency as the choice of parameter a



Simulation Results: IR vs. latency as the choice of parameter a

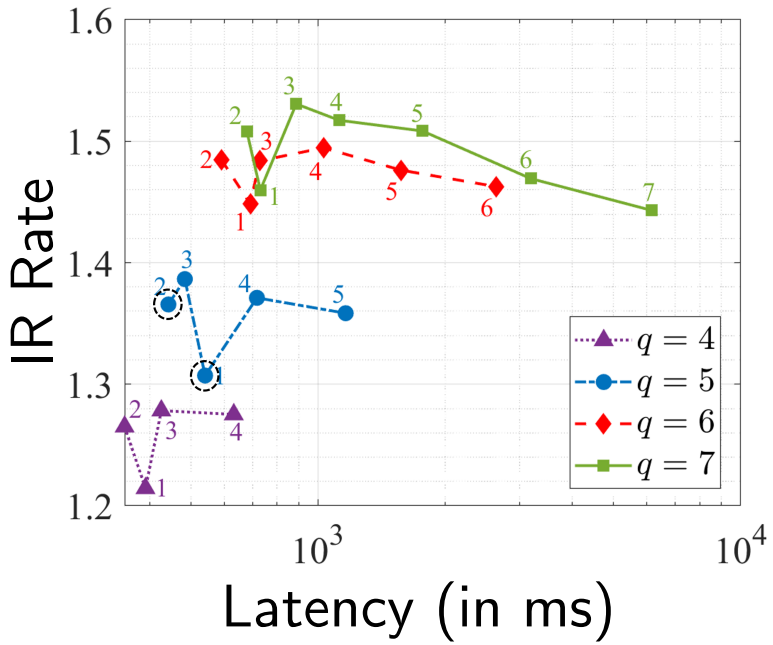


Simulation Results: IR vs. latency as the choice of parameter a



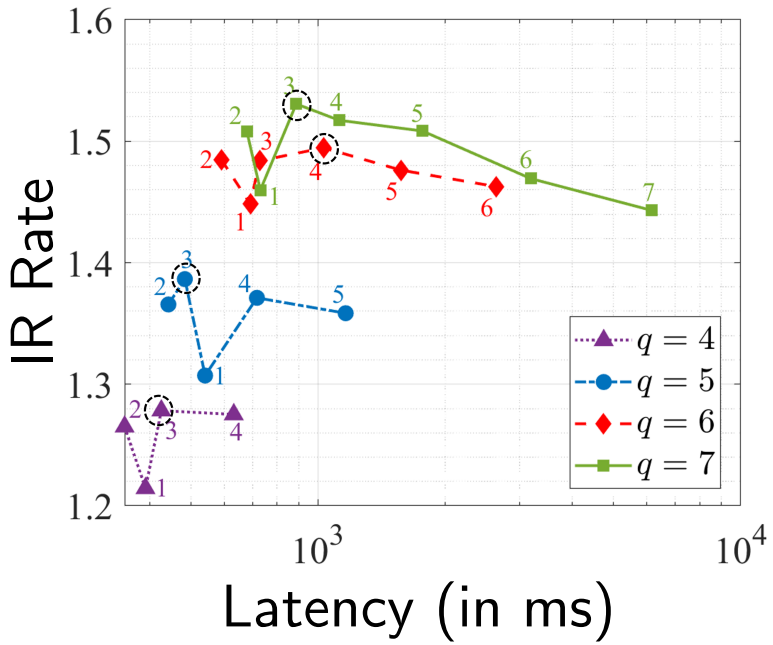
- Latency becomes significantly large as a becomes large (close to q)

Simulation Results: IR vs. latency as the choice of parameter a



- Latency becomes significantly large as a becomes large (close to q)
- Latency is non-monotonic in a: since as a increases, the increase in decoding complexity is offset by the decrease in the number of layers

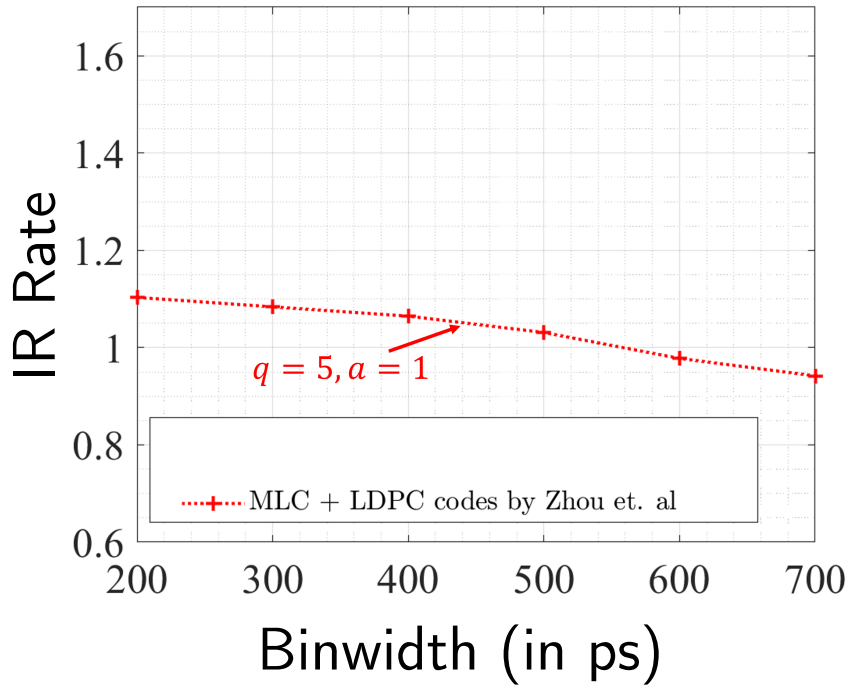
Simulation Results: IR vs. latency as the choice of parameter a



- Latency becomes significantly large as a becomes large (close to q)
- Latency is non-monotonic in a: since as a increases, the increase in decoding complexity is offset by the decrease in the number of layers
- Best trade-off between IR rate and latency is obtained for a small value of a (3 or 4)

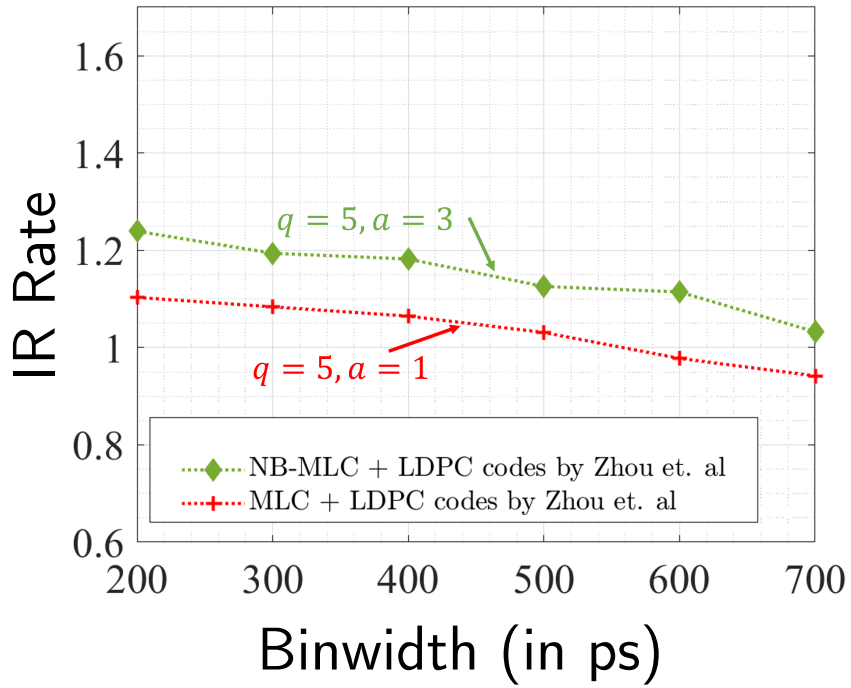
Simulation Results: Comparison with Classical Schemes

- 32 bins per frame $\rightarrow q = 5$.



Simulation Results: Comparison with Classical Schemes

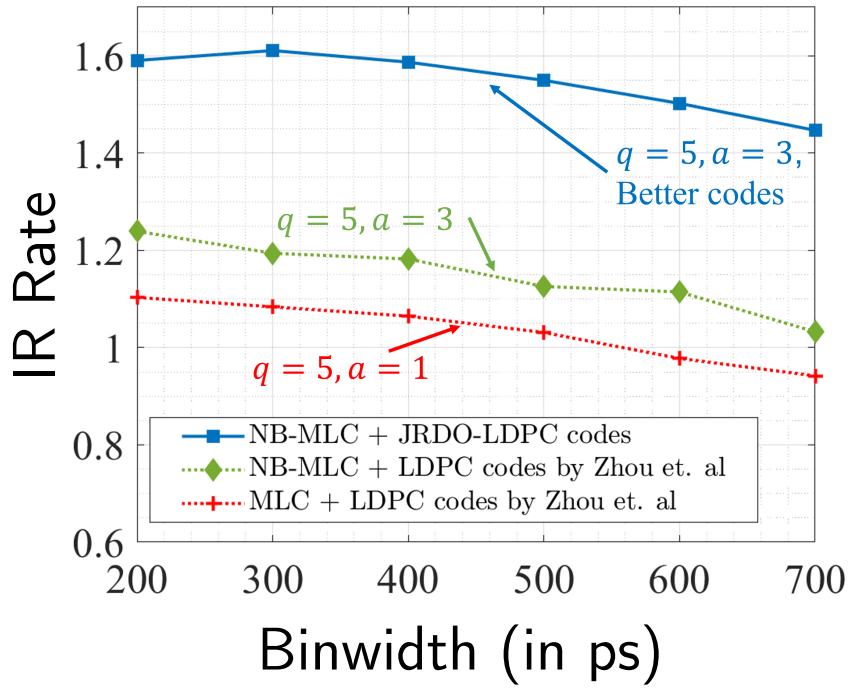
- 32 bins per frame $\rightarrow q = 5$.



- Improvement due to $a = 1 \rightarrow a = 3$

Simulation Results: Comparison with Classical Schemes

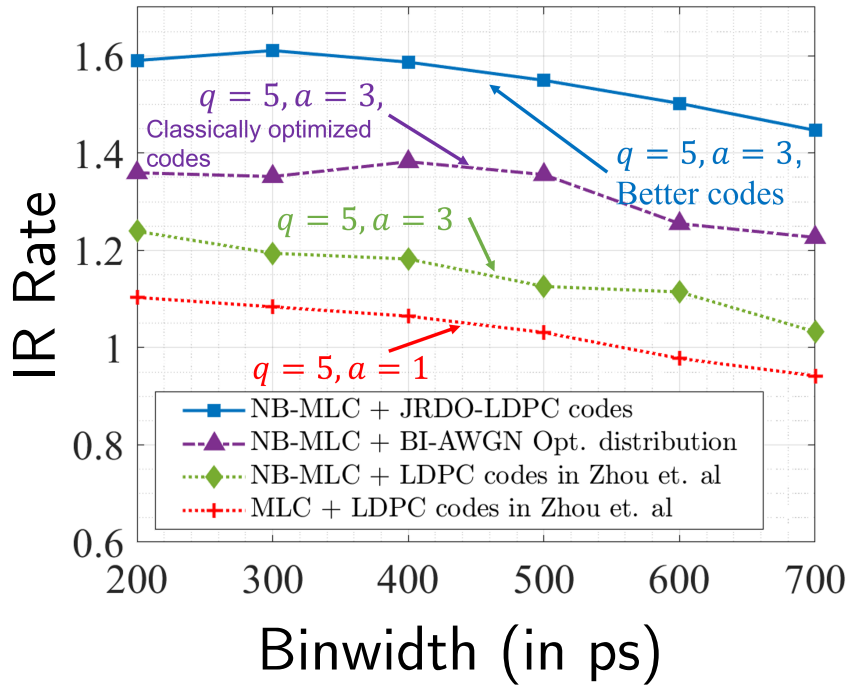
- 32 bins per frame $\rightarrow q = 5$.



- Improvement due to $a = 1 \rightarrow a = 3$
- Improvement due to using JRDO-LDPC codes

Simulation Results: Comparison with Classical Schemes

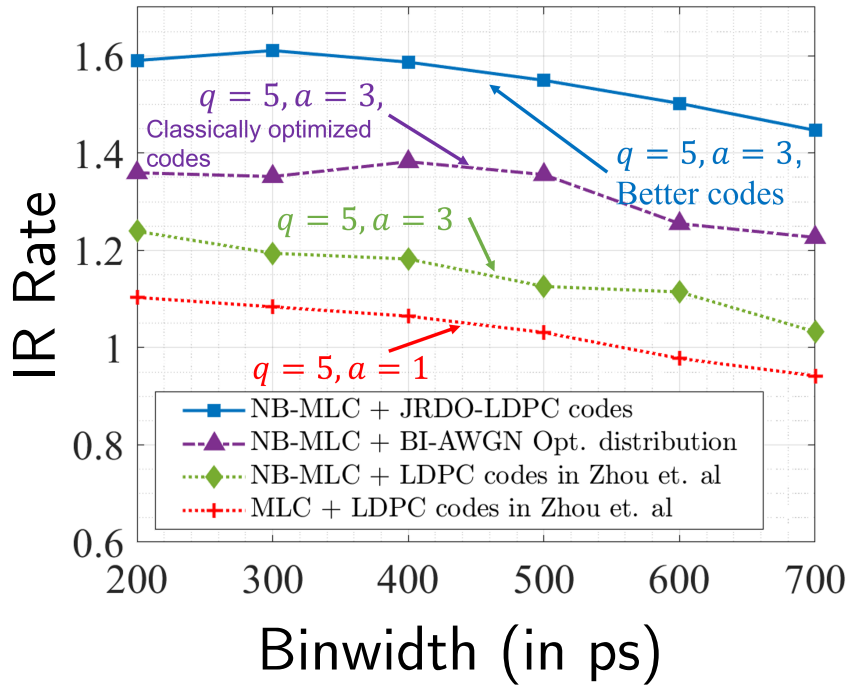
- 32 bins per frame $\rightarrow q = 5$.



- Improvement due to $a = 1 \rightarrow a = 3$
- Improvement due to using JRDO-LDPC codes

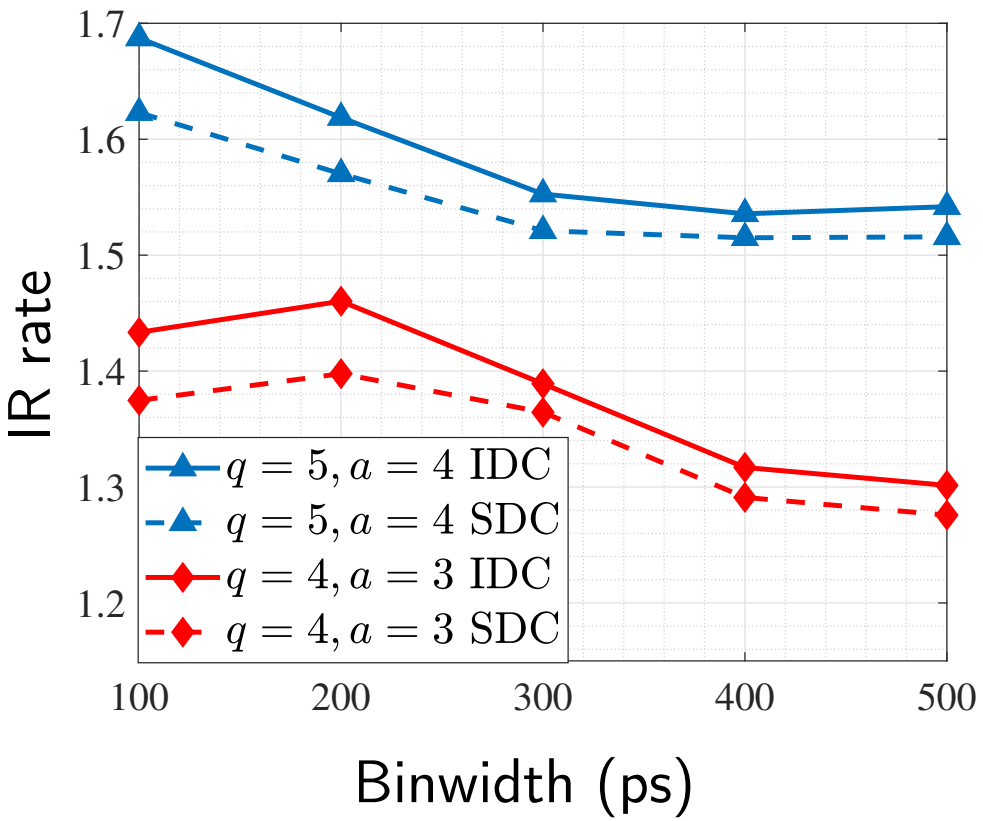
Simulation Results: Comparison with Classical Schemes

- 32 bins per frame $\rightarrow q = 5$.



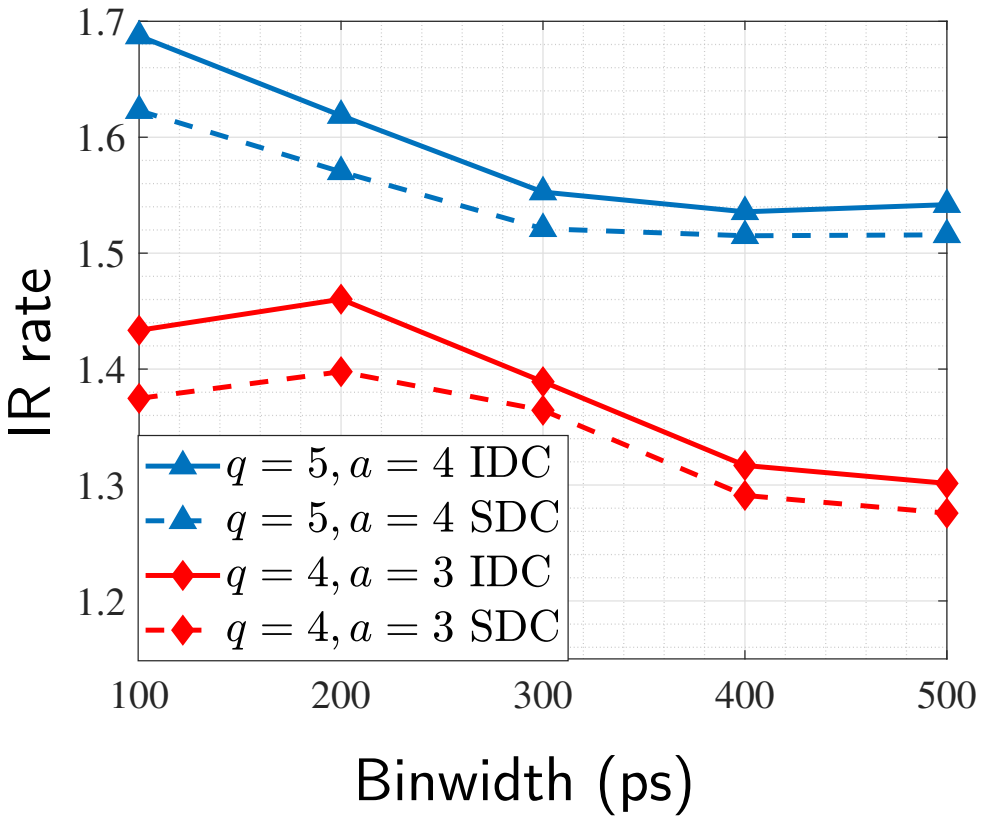
- Improvement due to $a = 1 \rightarrow a = 3$
- Improvement due to using JRDO-LDPC codes
- Overall, JRDO-LDPC codes combined with NB-MLC with a small a result in the largest IR rates (effectively uses one code over $GF(8)$ and one code over $GF(4)$)

Performance Comparison: Benefits of Interleaved Decoding



- IDC: Interleaved Decoding and Communication
- SDC: Sequential Decoding and Communication

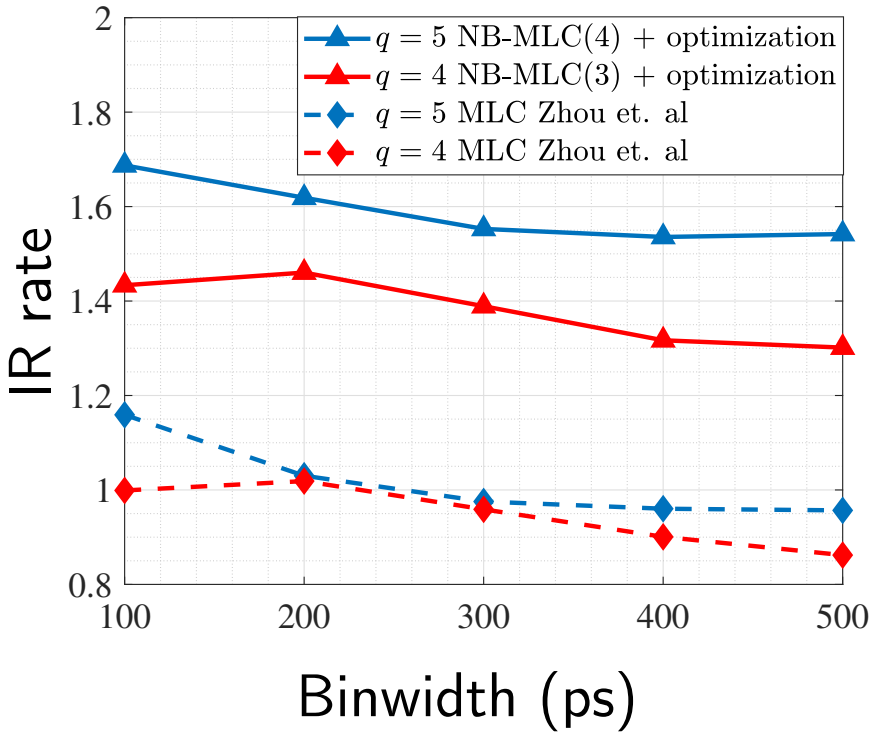
Performance Comparison: Benefits of Interleaved Decoding



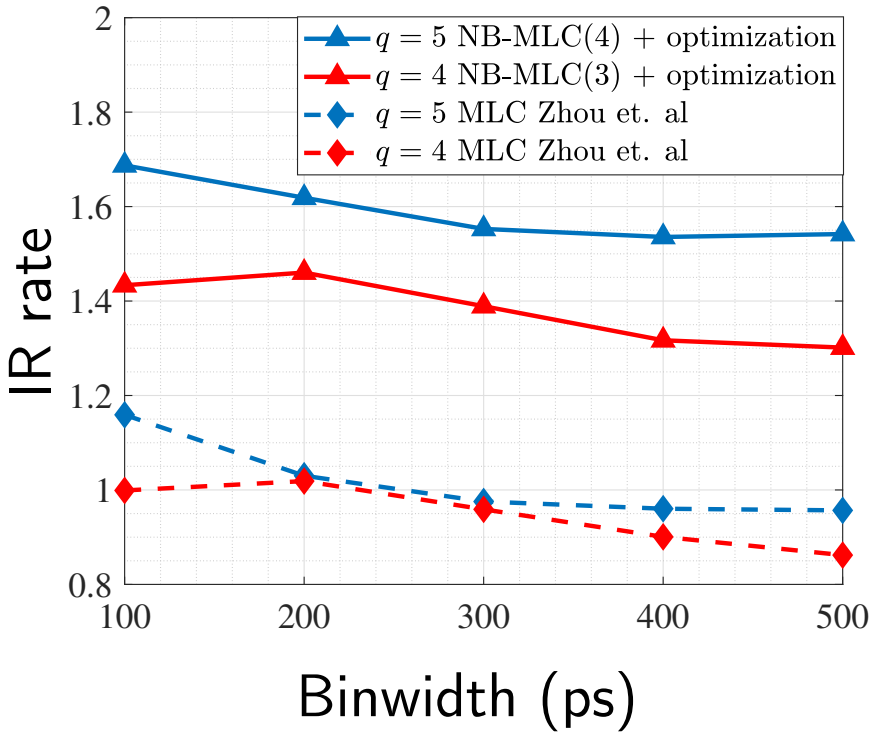
- IDC: Interleaved Decoding and Communication
- SDC: Sequential Decoding and Communication

- IDC protocol results in higher IR rates compared to the conventional SDC protocol

The Overall Comparison



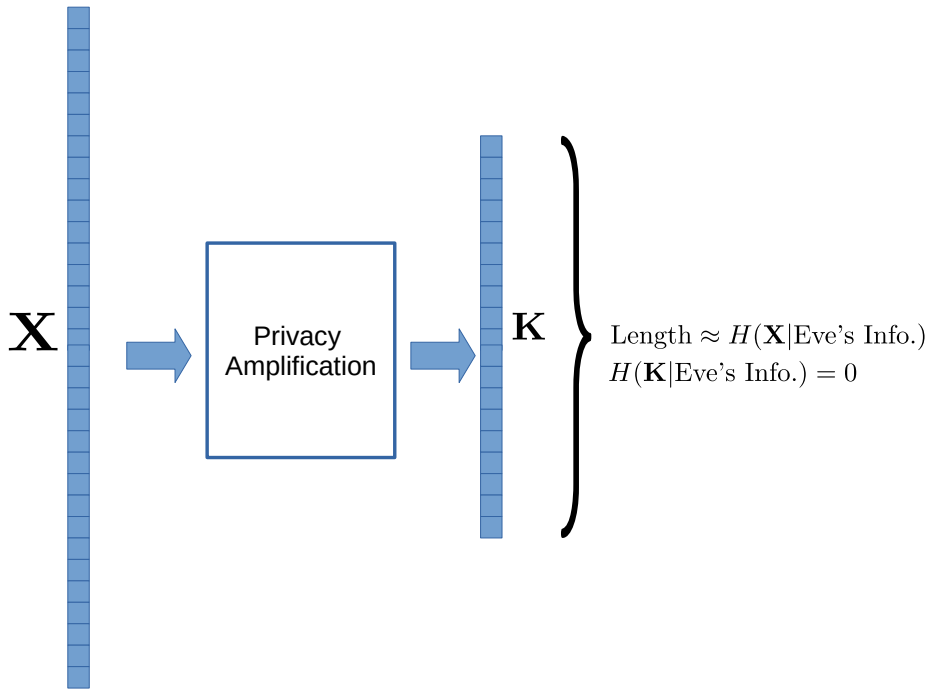
The Overall Comparison



- Overall, our techniques result in around $40 - 60\%$ improvement in IR rates compared to the MLC scheme (prior state of the art).
- Asymptotic limit of a simplified (better) channel is around 2.1 for $q = 5$ and 1.8 for $q = 4$.

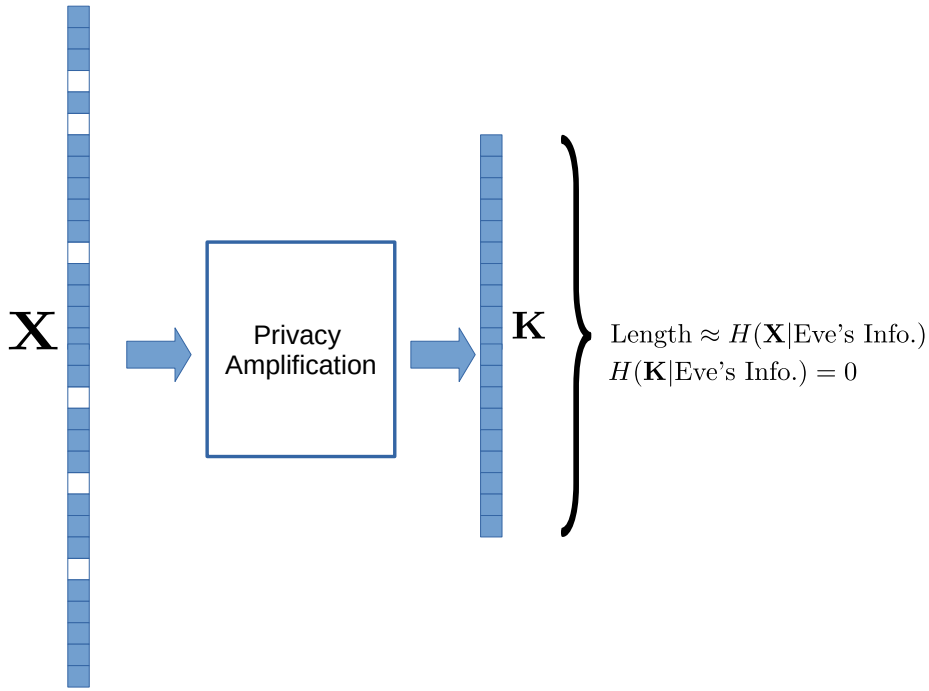
Privacy Amplification-Aware LDPC Code Design

- Privacy Amplification compresses the common string between Alice and Bob whose length is dependent on the information Eve has (Bennet '88)



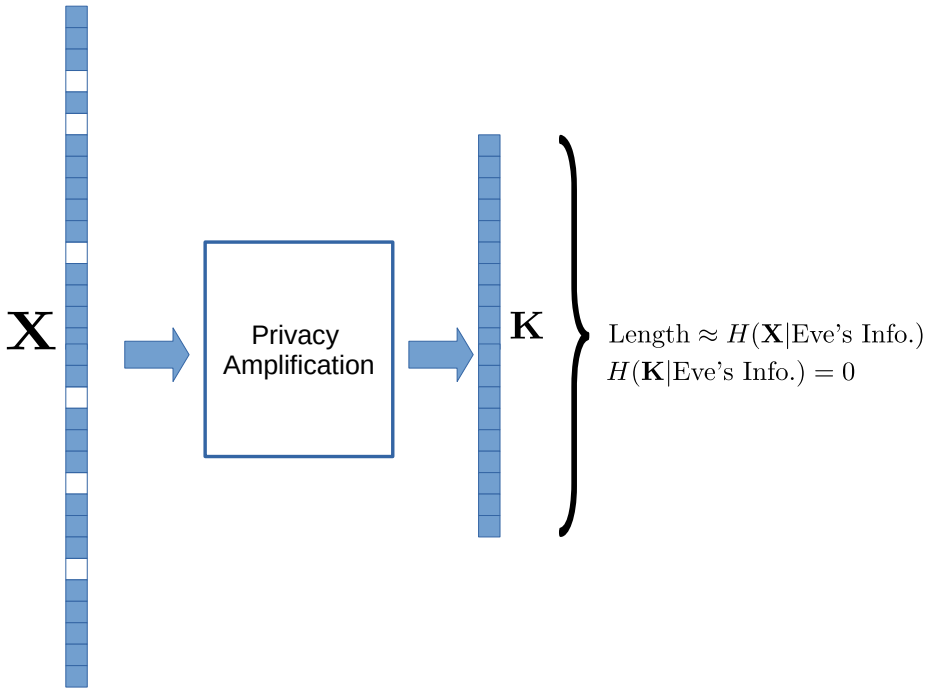
Privacy Amplification-Aware LDPC Code Design

- Privacy Amplification compresses the common string between Alice and Bob whose length is dependent on the information Eve has (Bennet '88)
- Question: Depending on the information Eve has, do we need all of $\mathbf{X}$ in order to extract $\mathbf{K}$?



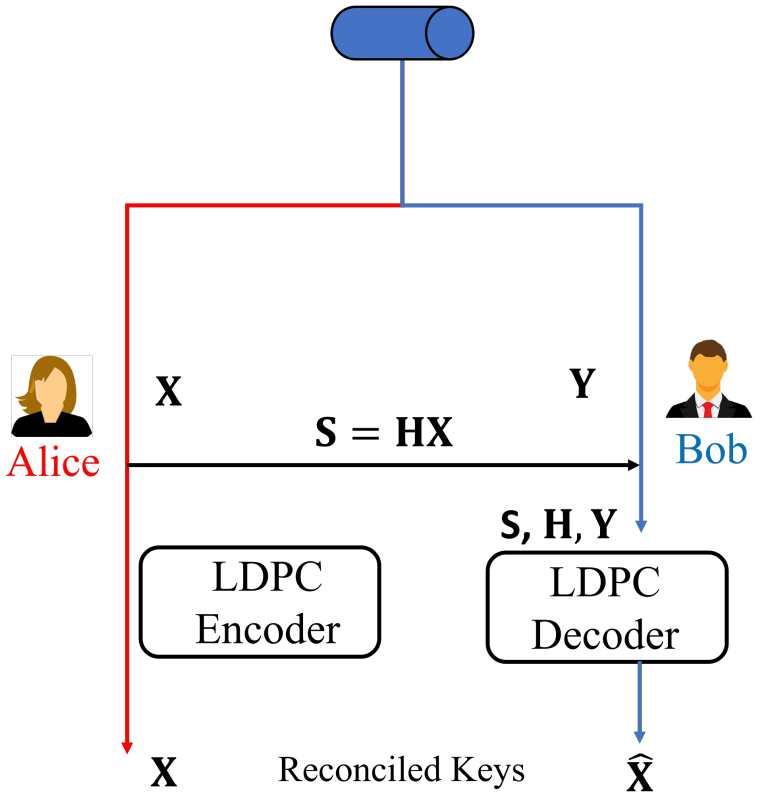
Privacy Amplification-Aware LDPC Code Design

- Privacy Amplification compresses the common string between Alice and Bob whose length is dependent on the information Eve has (Bennet '88)
- Question: Depending on the information Eve has, do we need all of $\mathbf{X}$ in order to extract $\mathbf{K}$?
  No



Revisit the Full Non-Binary Example

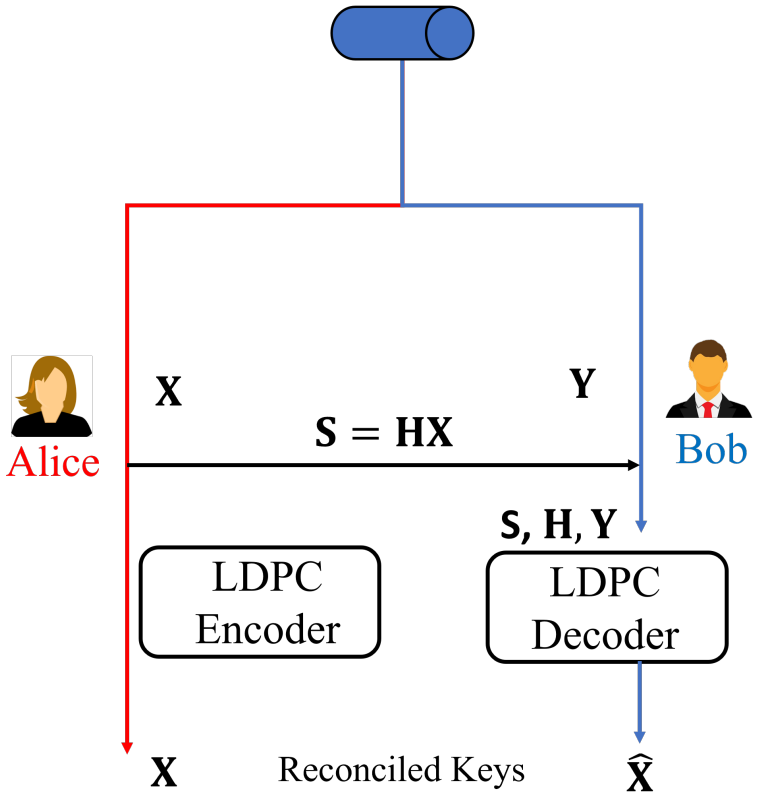
- Assume that $\mathbf{H}$ can be partitioned into two sub-matrices $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2]$ such that $\mathbf{H}_2$ is $m \times m$ and is full rank.



Revisit the Full Non-Binary Example

- Assume that $\mathbf{H}$ can be partitioned into two sub-matrices $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2]$ such that $\mathbf{H}_2$ is $m \times m$ and is full rank.
- Then,

$$\mathbf{S} = \mathbf{HX} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{H}_2\mathbf{X}_2$$
$$\implies \mathbf{X}_2 = (\mathbf{H}_2)^{-1}(\mathbf{S} - \mathbf{H}_1\mathbf{X}_1)$$

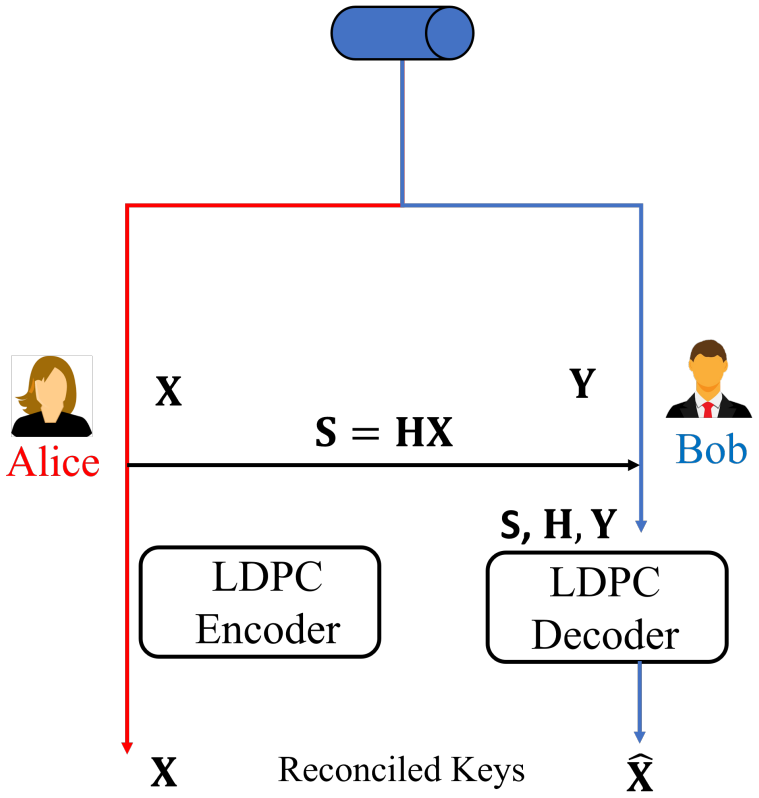


Revisit the Full Non-Binary Example

- Assume that $\mathbf{H}$ can be partitioned into two sub-matrices $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2]$ such that $\mathbf{H}_2$ is $m \times m$ and is full rank.
- Then,

$$\mathbf{S} = \mathbf{HX} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{H}_2\mathbf{X}_2$$
$$\implies \mathbf{X}_2 = (\mathbf{H}_2)^{-1}(\mathbf{S} - \mathbf{H}_1\mathbf{X}_1)$$

- Since $\mathbf{X}_2$ is a function of $\mathbf{X}_1$, $H(\mathbf{X}|S) = H(\mathbf{X}_1|S)$.

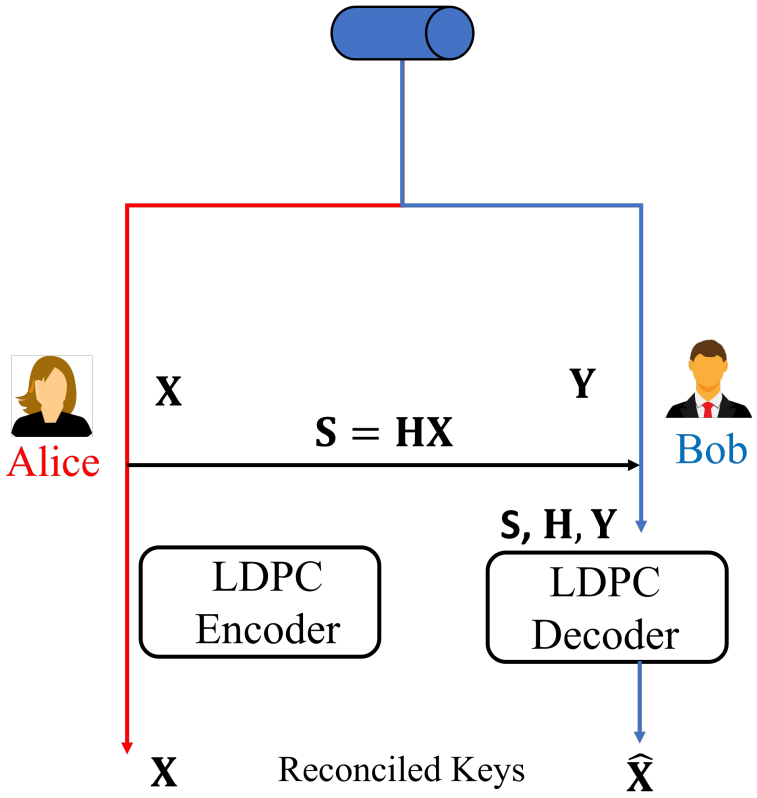


Revisit the Full Non-Binary Example

- Assume that $\mathbf{H}$ can be partitioned into two sub-matrices $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2]$ such that $\mathbf{H}_2$ is $m \times m$ and is full rank.
- Then,

$$\mathbf{S} = \mathbf{HX} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{H}_2\mathbf{X}_2$$
$$\implies \mathbf{X}_2 = (\mathbf{H}_2)^{-1}(\mathbf{S} - \mathbf{H}_1\mathbf{X}_1)$$

- Since $\mathbf{X}_2$ is a function of $\mathbf{X}_1$, $H(\mathbf{X}|S) = H(\mathbf{X}_1|S)$.



Key Observations

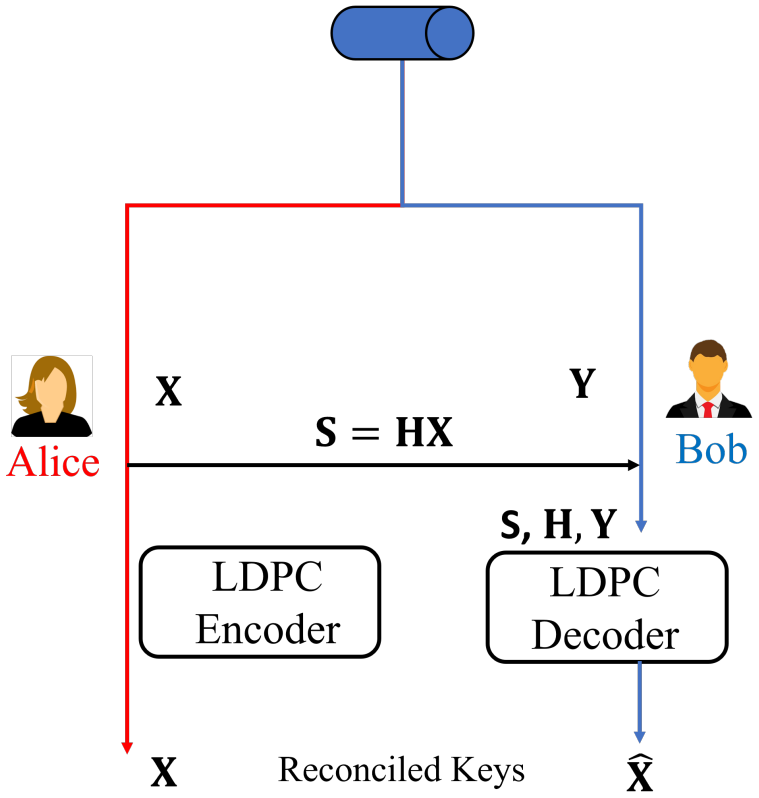
- We only need to decode $\mathbf{X}_1$ successfully to do Privacy Amplification and get $\mathbf{K}$.

Revisit the Full Non-Binary Example

- Assume that $\mathbf{H}$ can be partitioned into two sub-matrices $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2]$ such that $\mathbf{H}_2$ is $m \times m$ and is full rank.
- Then,

$$\mathbf{S} = \mathbf{HX} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{H}_2\mathbf{X}_2$$
$$\implies \mathbf{X}_2 = (\mathbf{H}_2)^{-1}(\mathbf{S} - \mathbf{H}_1\mathbf{X}_1)$$

- Since $\mathbf{X}_2$ is a function of $\mathbf{X}_1$, $H(\mathbf{X}|S) = H(\mathbf{X}_1|S)$.



Key Observations

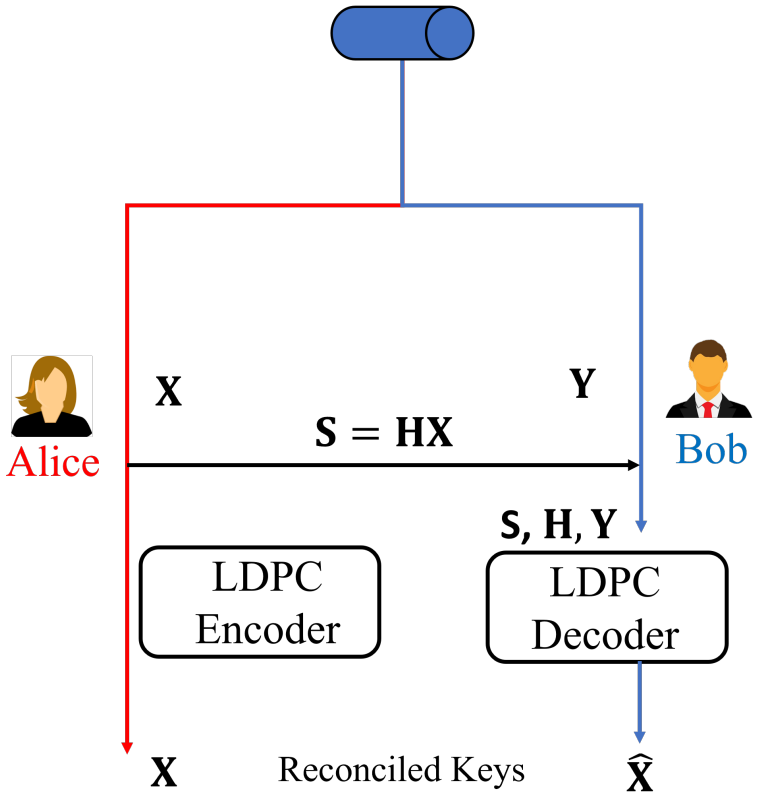
- We only need to decode $\mathbf{X}_1$ successfully to do Privacy Amplification and get $\mathbf{K}$. (Similar to Systematic Decoding)

Revisit the Full Non-Binary Example

- Assume that $\mathbf{H}$ can be partitioned into two sub-matrices $\mathbf{H} = [\mathbf{H}_1, \mathbf{H}_2]$ such that $\mathbf{H}_2$ is $m \times m$ and is full rank.
- Then,

$$\mathbf{S} = \mathbf{HX} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{H}_2\mathbf{X}_2$$
$$\implies \mathbf{X}_2 = (\mathbf{H}_2)^{-1}(\mathbf{S} - \mathbf{H}_1\mathbf{X}_1)$$

- Since $\mathbf{X}_2$ is a function of $\mathbf{X}_1$, $H(\mathbf{X}|S) = H(\mathbf{X}_1|S)$.



Key Observations

- We only need to decode $\mathbf{X}_1$ successfully to do Privacy Amplification and get $\mathbf{K}$. (Similar to Systematic Decoding)
- There may be multiple subsets that satisfy this property.

Utilizing Subset Decoding

- **MDS codes**:

Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets

Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets
  - **Cons:** Requires finite fields that scale with code length and have complex soft-decoding algorithms

Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets
  - **Cons:** Requires finite fields that scale with code length and have complex soft-decoding algorithms
- **LDPC codes**:

Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets
  - **Cons:** Requires finite fields that scale with code length and have complex soft-decoding algorithms
- **LDPC codes**:
  - **Pros:** Efficient soft-decoding algorithms and fixed finite field size

Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets
  - **Cons:** Requires finite fields that scale with code length and have complex soft-decoding algorithms
- **LDPC codes**:
  - **Pros:** Efficient soft-decoding algorithms and fixed finite field size
  - **Cons:** Determining subsets in the code that satisfy desired property can be difficult

Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets
  - **Cons:** Requires finite fields that scale with code length and have complex soft-decoding algorithms
- **LDPC codes**:
  - **Pros:** Efficient soft-decoding algorithms and fixed finite field size
  - **Cons:** Determining subsets in the code that satisfy desired property can be difficult
- Our Solution - **Block-MDS (BMDS) QC-LDPC codes**:

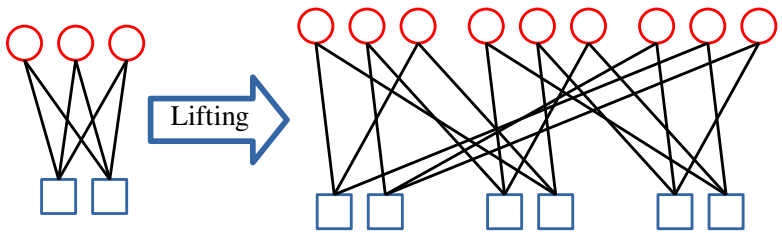
Utilizing Subset Decoding

Possible Coding Schemes

- **MDS codes**:
  - **Pros:** Can select a lot of subsets
  - **Cons:** Requires finite fields that scale with code length and have complex soft-decoding algorithms
- **LDPC codes**:
  - **Pros:** Efficient soft-decoding algorithms and fixed finite field size
  - **Cons:** Determining subsets in the code that satisfy desired property can be difficult
- Our Solution - **Block-MDS (BMDS) QC-LDPC codes**:
  - Structured code construction that guarantees the required subsets on a block matrix level while still having the benefits of LDPC codes

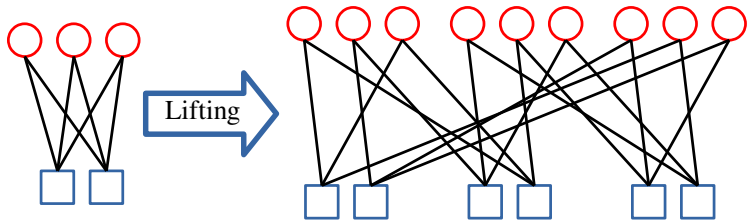
Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

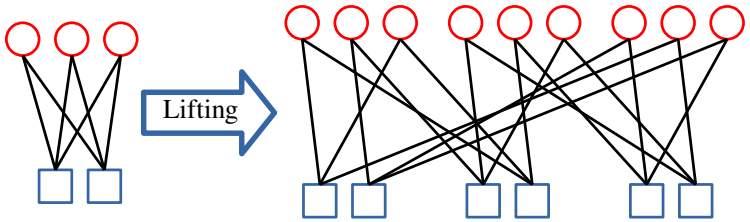


$$\mathbf{H}_1 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix} \qquad \mathbf{H}_2 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

$$\mathbf{H}_3 = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

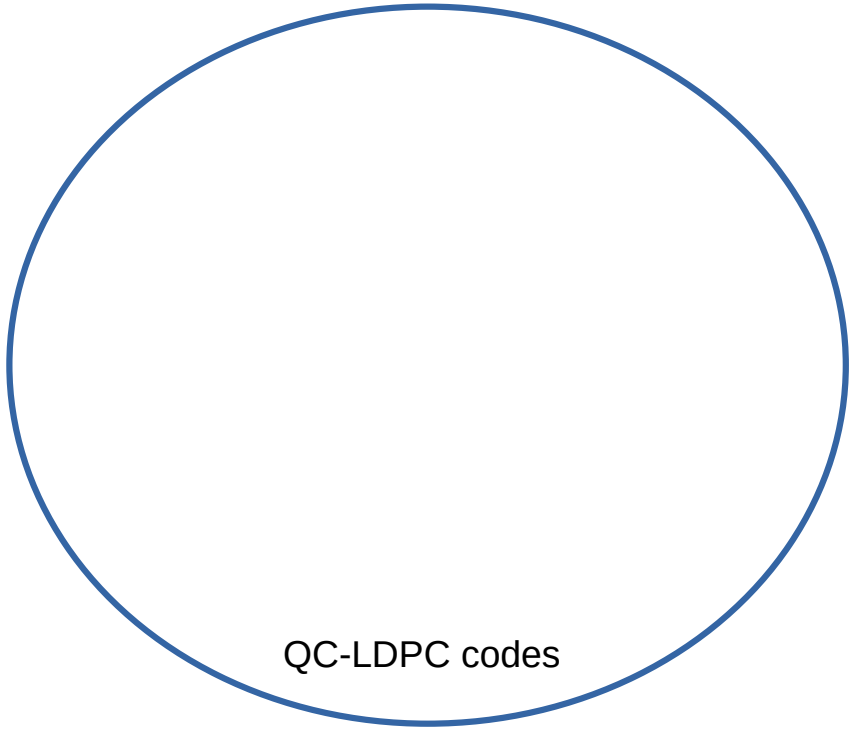
Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



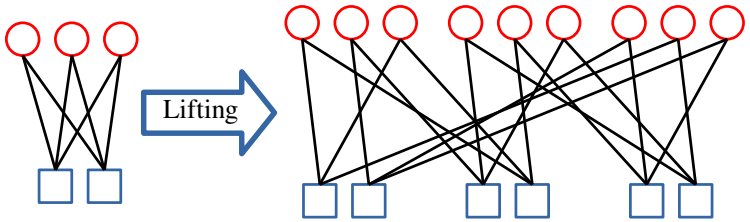
$$\mathbf{H}_1 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix} \qquad \mathbf{H}_2 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

$$\mathbf{H}_3 = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



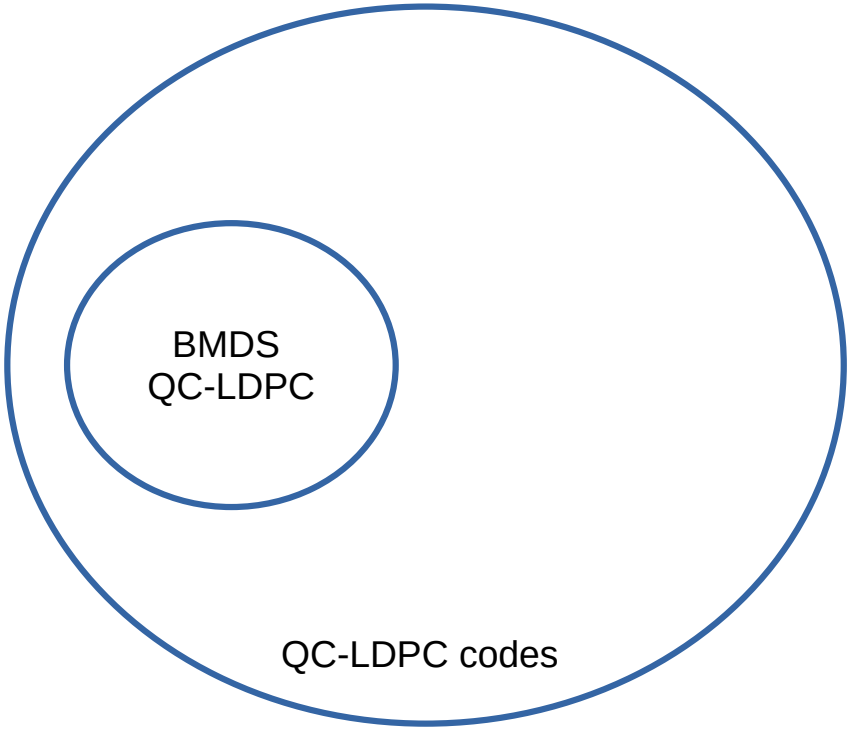
Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



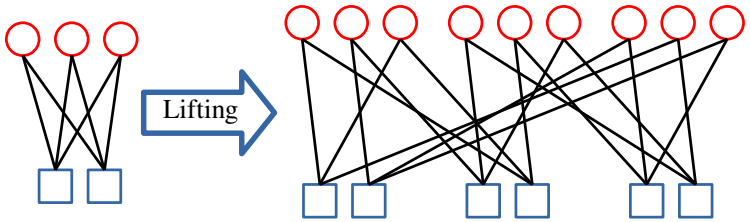
$$\mathbf{H}_1 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix} \qquad \mathbf{H}_2 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

$$\mathbf{H}_3 = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



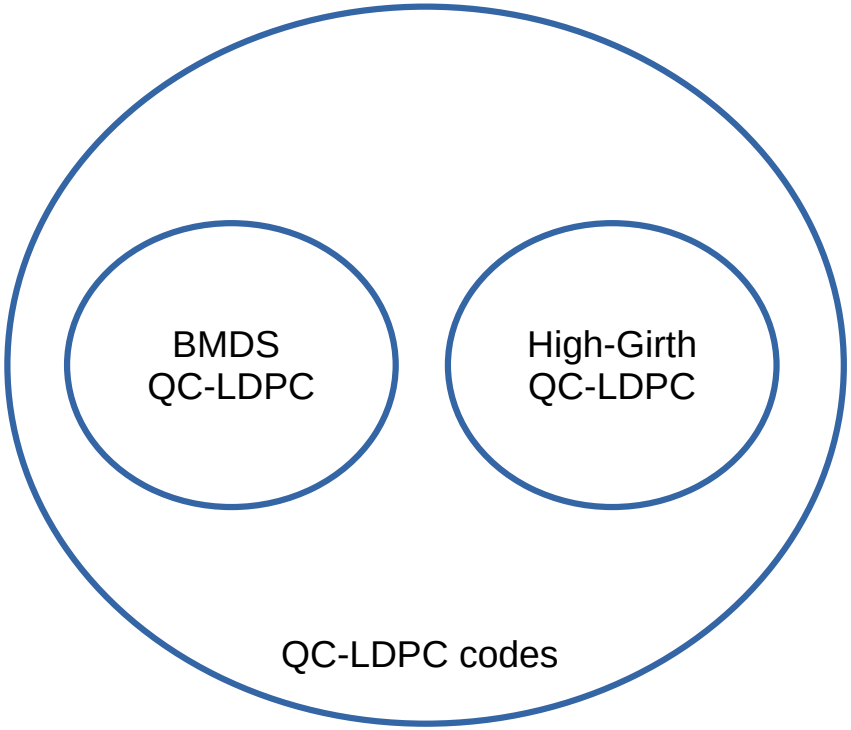
Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



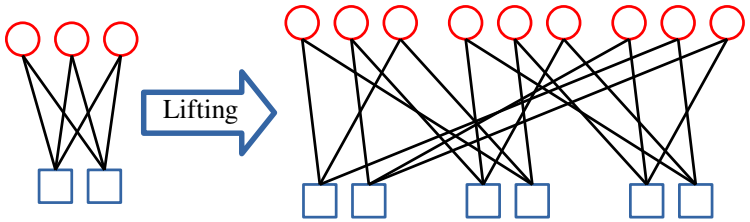
$$\mathbf{H}_1 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix} \qquad \mathbf{H}_2 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

$$\mathbf{H}_3 = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



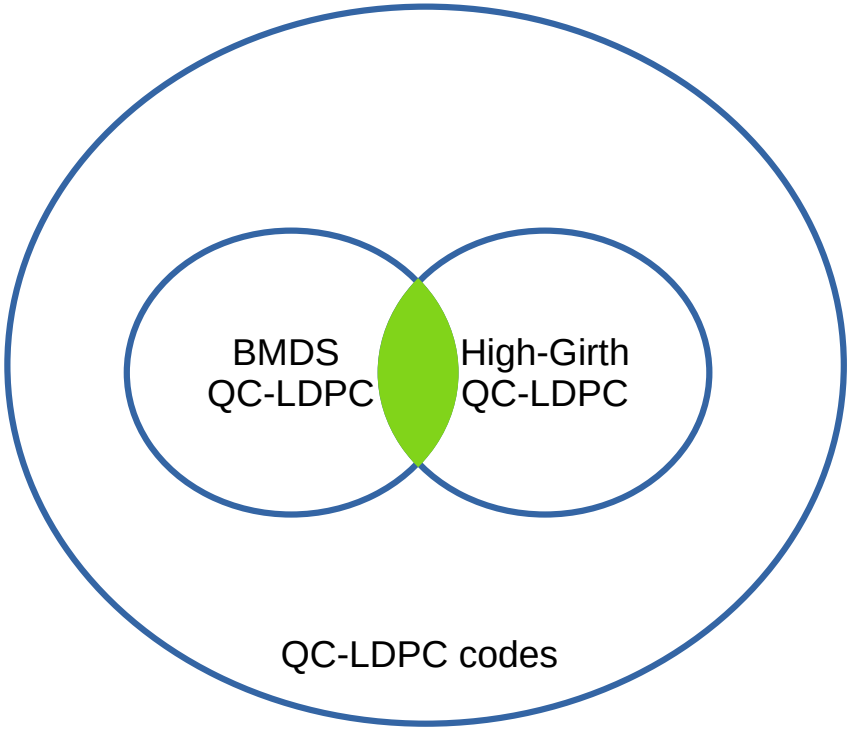
Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



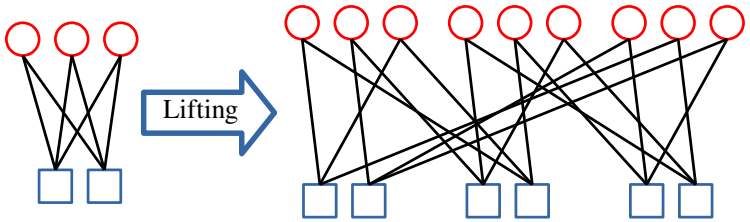
$$\mathbf{H}_1 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix} \qquad \mathbf{H}_2 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

$$\mathbf{H}_3 = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



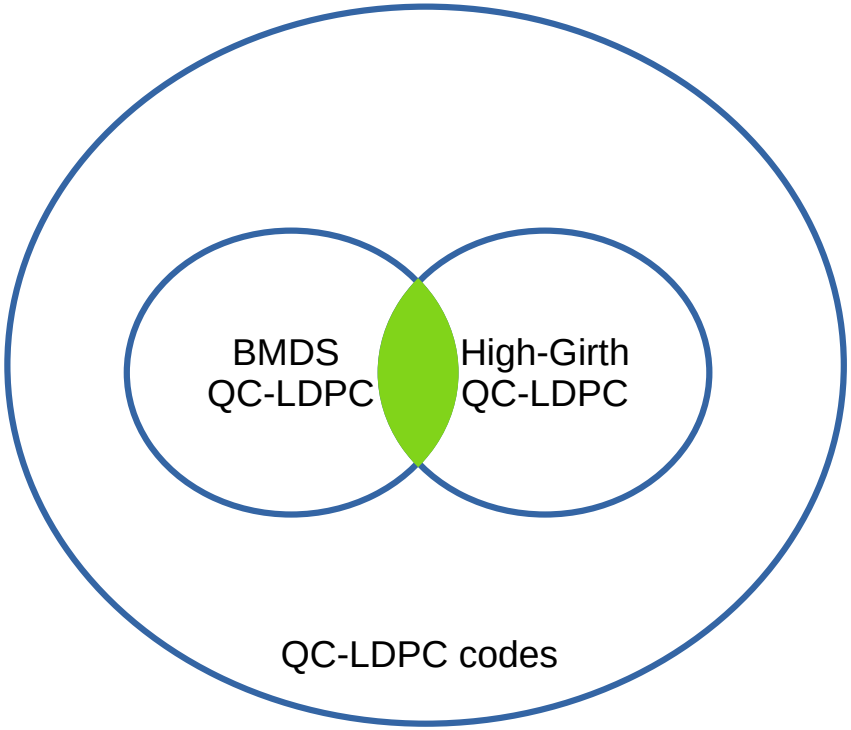
Construction of BMDS QC-LDPC codes

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$



$$\mathbf{H}_1 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,2}\mathbf{C}^{p_{1,2}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,2}\mathbf{C}^{p_{2,2}} \end{bmatrix} \qquad \mathbf{H}_2 = \begin{bmatrix} s_{1,1}\mathbf{C}^{p_{1,1}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,1}\mathbf{C}^{p_{2,1}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

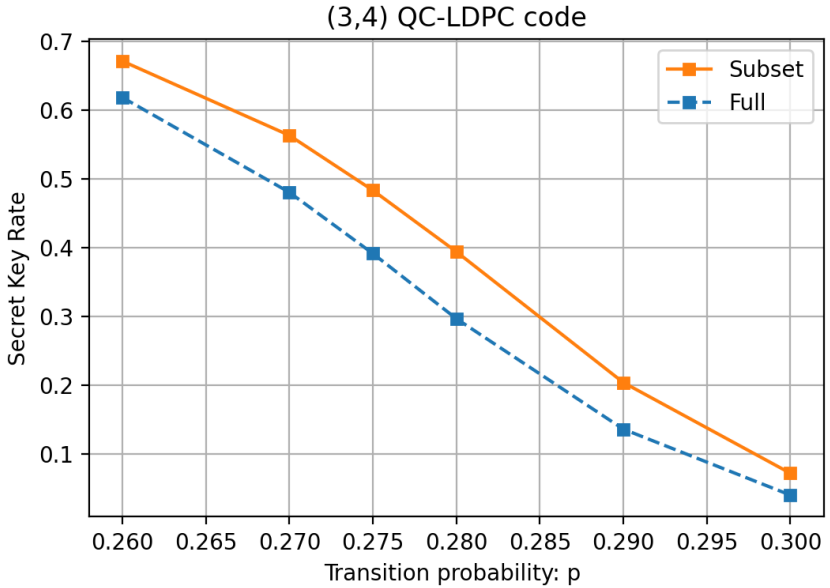
$$\mathbf{H}_3 = \begin{bmatrix} s_{1,2}\mathbf{C}^{p_{1,2}} & s_{1,3}\mathbf{C}^{p_{1,3}} \\ s_{2,2}\mathbf{C}^{p_{2,2}} & s_{2,3}\mathbf{C}^{p_{2,3}} \end{bmatrix}$$

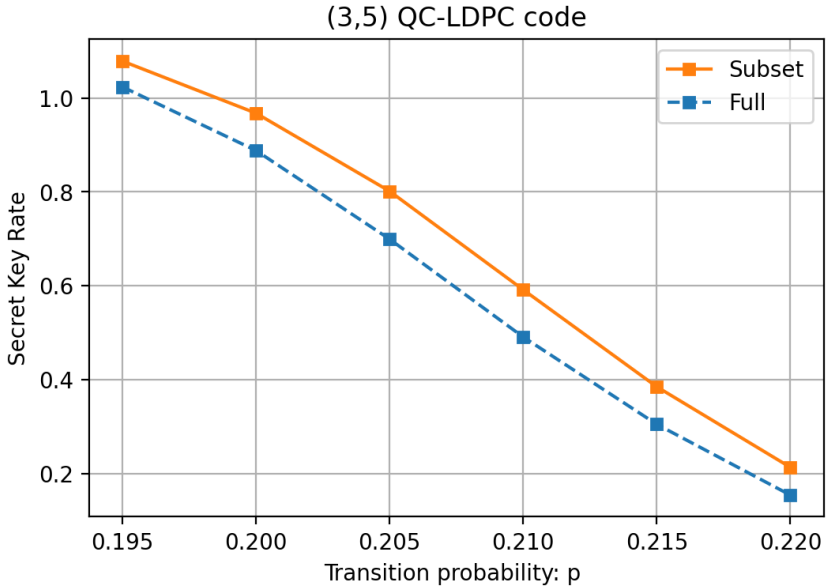


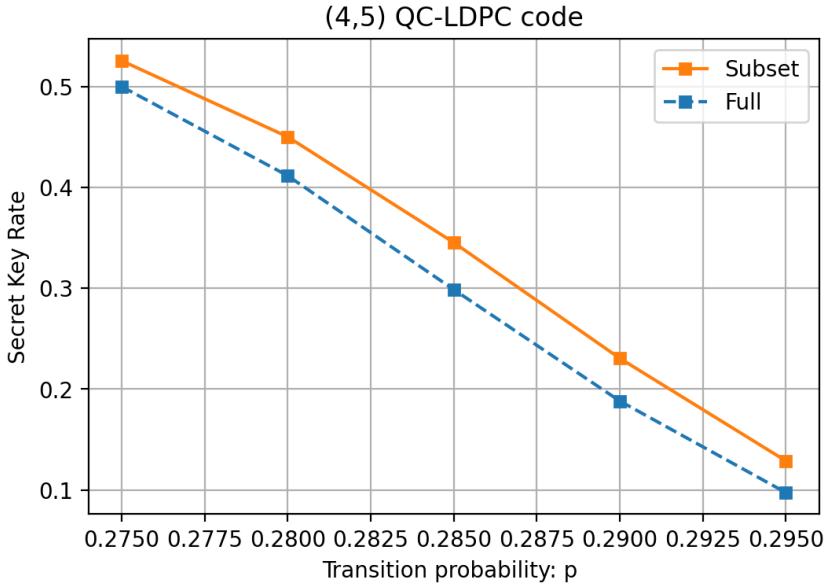
Main Result

A binary regular QC-LDPC code with column weight γ, row weight κ, and girth $\gamma + 2$ can be transformed into a non-binary BMDS code with finite field size at least κ, for a particular prime choice of the lifting factor.

Full Codeword Decoding vs Subset Decoding Simulations







- All codes have girth 10, length of approximately 2000, and perform operations in $\mathbb{GF}(8)$
- Channel is a q-ary symmetric channel with transition probability p

Outline

1. Background and Motivation

2. System Model

3. NB-LDPC codes for Quantum Key Distribution
   - Preliminaries
   - Channel code design
   - Sequential Decoding and Interactive Communication
   - Privacy Amplification-Aware LDPC Code Design

4. Concluding Remarks and Future Outlook

Key Takeaways

Quantum Communications

- High-dimensional QKD solutions are becoming critical to quantum communications, also for 6G

Key Takeaways

Quantum Communications

- High-dimensional QKD solutions are becoming critical to quantum communications, also for 6G

- Challenge: Physical constraints, high noise, presence of eavesdroppers.

Key Takeaways

Quantum Communications

- High-dimensional QKD solutions are becoming critical to quantum communications, also for 6G

- Challenge: Physical constraints, high noise, presence of eavesdroppers.
- Key Insights: Novel code design strategies using source coding with side information of graph codes.
  - Tools based on well-understood set-ups e.g., data storage, do not apply.
  - Code designs that operate in a low SNR regime; refined channel model
  - Domain-specific metrics lead to new theoretical insights

Key Takeaways

Quantum Communications

- High-dimensional QKD solutions are becoming critical to quantum communications, also for 6G

- Challenge: Physical constraints, high noise, presence of eavesdroppers.
- Key Insights: Novel code design strategies using source coding with side information of graph codes.
  - Tools based on well-understood set-ups e.g., data storage, do not apply.
  - Code designs that operate in a low SNR regime; refined channel model
  - Domain-specific metrics lead to new theoretical insights
- Key Result: Novel non-binary codes (Mitra '24, Tauz '24)
  - Research supported by NSF-QuIC-TAQS no. 2137984 and NSF-FET no. 2008728.

Advances in Technology and Suggested Research Directions

- High-dimensional energy-time QKD promises unprecedented key rates. To reach this promise, and in tandem with experimental advances, it will be necessary to investigate:
  - Design of codes tailored to the specifics of the QKD channels (this work)

- Special issue on Quantum Information Science, 2023, including L. Dolecek and E. Soljanin: a primer on time-bin QKD

Advances in Technology and Suggested Research Directions

- High-dimensional energy-time QKD promises unprecedented key rates. To reach this promise, and in tandem with experimental advances, it will be necessary to investigate:
  - Design of codes tailored to the specifics of the QKD channels (this work)
  - Alternative coding solutions (spatial, polar etc.); low-latency decoding algorithms.

- Special issue on Quantum Information Science, 2023, including L. Dolecek and E. Soljanin: a primer on time-bin QKD

Advances in Technology and Suggested Research Directions

- High-dimensional energy-time QKD promises unprecedented key rates. To reach this promise, and in tandem with experimental advances, it will be necessary to investigate:
  - Design of codes tailored to the specifics of the QKD channels (this work)
  - Alternative coding solutions (spatial, polar etc.); low-latency decoding algorithms.
  - Careful mathematical modeling of the appropriate channel models, and relevant capacity-style bounds and finite-length analysis (cf. Boutros and Soljanin '23).

- Special issue on Quantum Information Science, 2023, including L. Dolecek and E. Soljanin: a primer on time-bin QKD

Advances in Technology and Suggested Research Directions

- High-dimensional energy-time QKD promises unprecedented key rates. To reach this promise, and in tandem with experimental advances, it will be necessary to investigate:
  - Design of codes tailored to the specifics of the QKD channels (this work)
  - Alternative coding solutions (spatial, polar etc.); low-latency decoding algorithms.
  - Careful mathematical modeling of the appropriate channel models, and relevant capacity-style bounds and finite-length analysis (cf. Boutros and Soljanin '23).
  - Practical joint modulation and coding schemes (cf. Karimi '20)

- Special issue on Quantum Information Science, 2023, including L. Dolecek and E. Soljanin: a primer on time-bin QKD

Advances in Technology and Suggested Research Directions

- High-dimensional energy-time QKD promises unprecedented key rates. To reach this promise, and in tandem with experimental advances, it will be necessary to investigate:
  - Design of codes tailored to the specifics of the QKD channels (this work)
  - Alternative coding solutions (spatial, polar etc.); low-latency decoding algorithms.
  - Careful mathematical modeling of the appropriate channel models, and relevant capacity-style bounds and finite-length analysis (cf. Boutros and Soljanin '23).
  - Practical joint modulation and coding schemes (cf. Karimi '20)
  - Relevant attack models and security proofs for them.

- Special issue on Quantum Information Science, 2023, including L. Dolecek and E. Soljanin: a primer on time-bin QKD

Advances in Technology and Suggested Research Directions

- **Frequency Combs.** Due to their frequency scaling and long-term coherence, they offer a new, more robust platform for photon generation, (Lee '18).

Advances in Technology and Suggested Research Directions

- **Frequency Combs.** Due to their frequency scaling and long-term coherence, they offer a new, more robust platform for photon generation, (Lee '18).
- **Hyper-entanglement based QKD.** Information is represented on multiple bases (in addition to the single basis of the time bin QKD, also polarization and angular momentum), (Chang '21).

Advances in Technology and Suggested Research Directions

- **Frequency Combs.** Due to their frequency scaling and long-term coherence, they offer a new, more robust platform for photon generation, (Lee '18).
- **Hyper-entanglement based QKD.** Information is represented on multiple bases (in addition to the single basis of the time bin QKD, also polarization and angular momentum), (Chang '21).
- **Hybrid QKD schemes.** Simultaneously uses both discrete variable and continuous variable QKD, (Djordjevic '20).

Advances in Technology and Suggested Research Directions

- **Frequency Combs.** Due to their frequency scaling and long-term coherence, they offer a new, more robust platform for photon generation, (Lee '18).
- **Hyper-entanglement based QKD.** Information is represented on multiple bases (in addition to the single basis of the time bin QKD, also polarization and angular momentum), (Chang '21).
- **Hybrid QKD schemes.** Simultaneously uses both discrete variable and continuous variable QKD, (Djordjevic '20).
- **Quantum networks.** Secure multi-party communication using efficient conference key agreement multi-party protocol, (Proietti '21).

Advances in Technology and Suggested Research Directions

- **Frequency Combs.** Due to their frequency scaling and long-term coherence, they offer a new, more robust platform for photon generation, (Lee '18).
- **Hyper-entanglement based QKD.** Information is represented on multiple bases (in addition to the single basis of the time bin QKD, also polarization and angular momentum), (Chang '21).
- **Hybrid QKD schemes.** Simultaneously uses both discrete variable and continuous variable QKD, (Djordjevic '20).
- **Quantum networks.** Secure multi-party communication using efficient conference key agreement multi-party protocol, (Proietti '21).

Each of these technologies will benefit from new studies in channel coding and related disciplines.

Selected References on Coding and Modulation for QKD

- (Mitra '24) D. Mitra et al., "Efficient Information Reconciliation in Quantum Key Distribution Systems Using Informed Design of Non-Binary LDPC Codes," *QIP*, 2024.
- (Dolecek & Soljanin '23) L. Dolecek and E. Soljanin "QKD Based on Time-Entangled Photons and its Key-Rate Promise," *IEEE BITS Magazine*, 2023.
- (Tauz '24) L. Tauz, D. Mitra, J. Shreekumar, M. C. Sarihan, C. W. Wong, and L. Dolecek, "Block-MDS QC-LDPC Codes for Information Reconciliation in Key Distribution," in review.
- (Birnie '23) C. Birnie, C. Chang, and E. Soljanin, "Information Rates With Non Ideal Photon Detectors in Time-Entanglement Based QKD," *IEEE Trans. on Communications*, 2023.
- (Soljanin '20) E. Soljanin, "Quantum Information Processing: An Essential Primer", *IEEE JSAIT*, 2020.
- (Boutros and Soljanin ' 23) J. Boutros and E. Soljanin, "Time-Entanglement QKD: Secret Key Rates and Information Reconciliation Coding," *IEEE Trans. on Communincations*.
- (Elkouss '09) D. Elkouss et al., "Efficient reconciliation protocol for discrete-variable quantum key distribution," *IEEE ISIT*, 2009.

Selected Background References

- (Gisin '02) N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002), "Quantum cryptography", *Reviews of Modern Physics,* vol. 74, pp. 145-195, 2002.
- (Zhong '15) T. Zhong, *et. al*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding", *New Journal of Physics*, vol. 7, pp. 022002, 2015.
- (Zhou '13) H. Zhou, L. Wang and G. Wornell, "Layered schemes for large-alphabet secret key distribution," *Information Theory and Applications Workshop*, Feb. 2013.
- (Shokrollahi '00) A. Shokrollahi and R. Storn, "Design of efficient erasure codes with differential evolution," *IEEE International Symposium on Information Theory*, Jun. 2000.
- (Federov '18) A. K. Fedorov, E. O. Kiktenko, and A. S. Trushechkin, "Symmetric Blind Information Reconciliation and Hash-function-based Verification for Quantum Key Distribution" *Lobachevskii J Math 39*, 2018.
- (Bennet '88) C.H. Bennett , G. Brassard, and J.M. Robert. "Privacy amplification by public discussion." *SIAM journal on Computing*, vol 17, no.2 , pp. 210-229, Apr. 1988.
- (Lee '18) S. K. Lee et al,. "Frequency comb single-photon interferometry," *Communications Physics*, 2018.
- (Chang '21) K.-C. Chang et al., "648 Hilbertspace dimensionality in a biphoton frequency comb: entanglement of formation and Schmidt mode decomposition," *npj Quantum Information*, 2021.
- (Djordjevic '20) I. B. Djordjevic, "Hybrid QKD protocol outperforming both DV- and CV-QKD protocols," *IEEE Photonics Journal*, 2020.
- (Proietti '21) M. Proietti et al. "Experimental quantum conference key agreement," *Science Advances* 2021.

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

$X = 10\ 10\ 01\ 11\ 00\ 10\ 11$

$p = 7$
$\lfloor \log_2 p \rfloor = 2$
$\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$
$k = 3$

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

$X = 10\ 10\ 01\ 11\ 00\ 10\ 11$

$p = 7$
$\lfloor \log_2 p \rfloor = 2$
$\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$
$k = 3$

- p is prime number

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

$X = 10\ 10\ 01\ 11\ 00\ 10\ 11$

$p = 7$
$\lfloor \log_2 p \rfloor = 2$
$\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$
$k = 3$

- p is prime number
- $\mathbb{F} = \{0, 1, \ldots, p-1\}$

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

$X = 10\ 10\ 01\ 11\ 00\ 10\ 11$

$p = 7$
$\lfloor \log_2 p \rfloor = 2$
$\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$
$k = 3$

- p is prime number
- $\mathbb{F} = \{0, 1, \ldots, p-1\}$
- k is a random element of $\mathbb{F}$

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

$X = 10\|10\|01\|11\|00\|10\|11$

$p = 7$
$\lfloor \log_2 p \rfloor = 2$
$\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$
$k = 3$

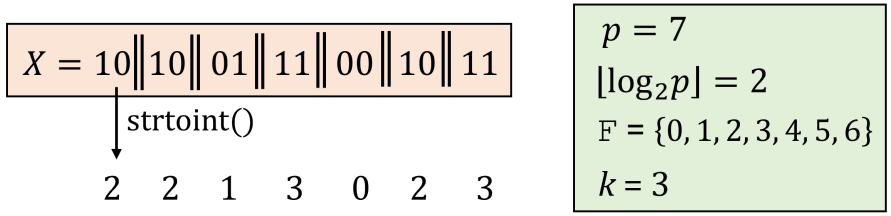
- Partition X into substrings of length $\lfloor \log_2 p \rfloor$

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

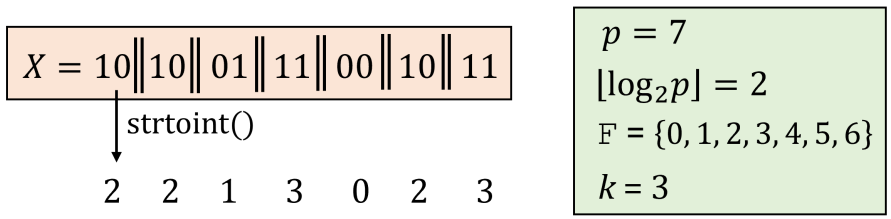


Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:



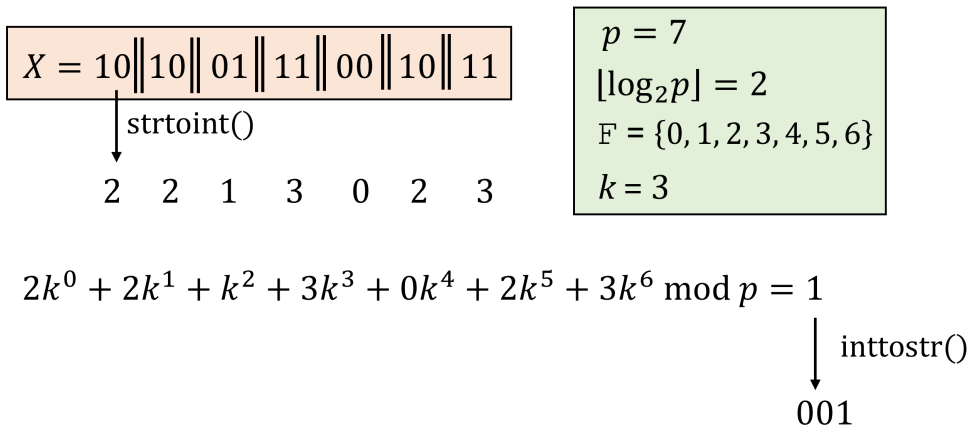
$$2k^0 + 2k^1 + k^2 + 3k^3 + 0k^4 + 2k^5 + 3k^6 \bmod p = 1$$

Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

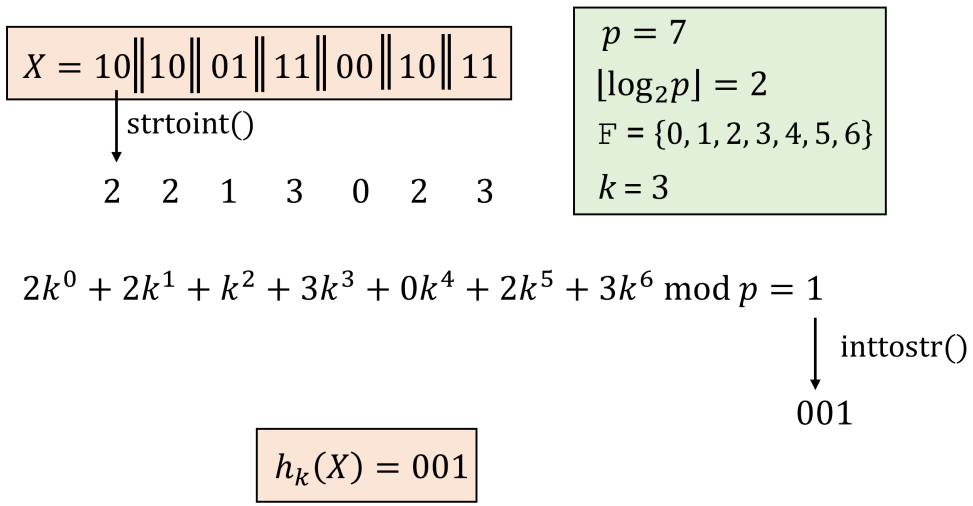


Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:

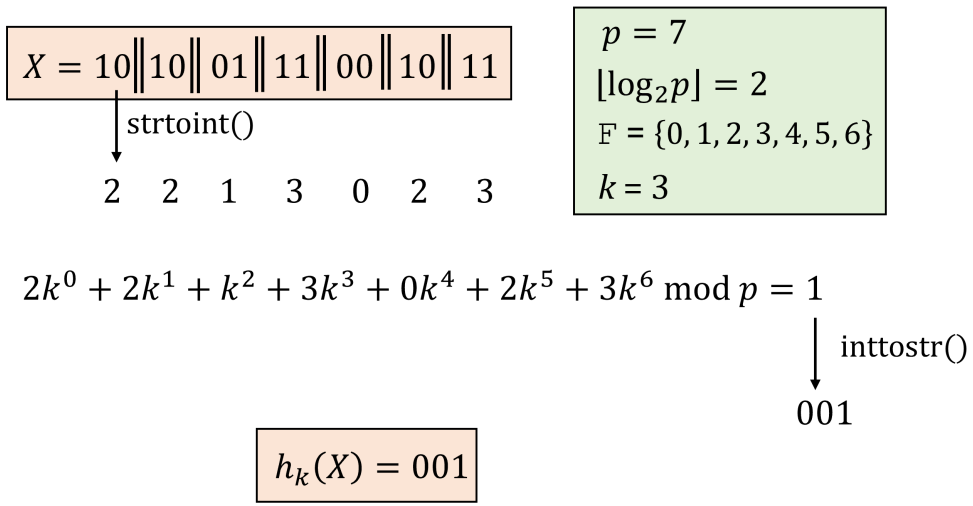


Verification after Information Reconciliation

- The verification protocol is based on the following hash function [Federov '18]:

$$h_k(X) = \text{inttostr}\left[\sum_{i=1}^{n} \text{strtoint}(x_i)k^{i-1} \mod p\right]$$

Example:



- Verification is achieved by matching the hash of the string X at Alice and decoded (reconciled) string $\widehat{X}$ at Bob