Privacy-Preserving Outsourced Media Search Using Secure Sparse Ternary Codes

Behrooz Razeghi and Slava Voloshynovskiy

Stochastic Information Processing Group
University of Geneva
Switzerland

April 2018

Outline

Introduction

Proposed Framework
- Main Idea
- Sparse Data Representation
- Ambiguization
- Privacy-Preserving Search

Results

Introduction

Privacy-preserving content search

- Biometrics
- Physical object recognition and security
- Medical/clinical applications
- Privacy-sensitive multimedia records

Introduction

Privacy-preserving content search

- Biometrics
- Physical object recognition and security
- Medical/clinical applications
- Privacy-sensitive multimedia records

Recent Trends

Big Data & Distributed Applications

Services on outsourced cloud-based systems

Introduction

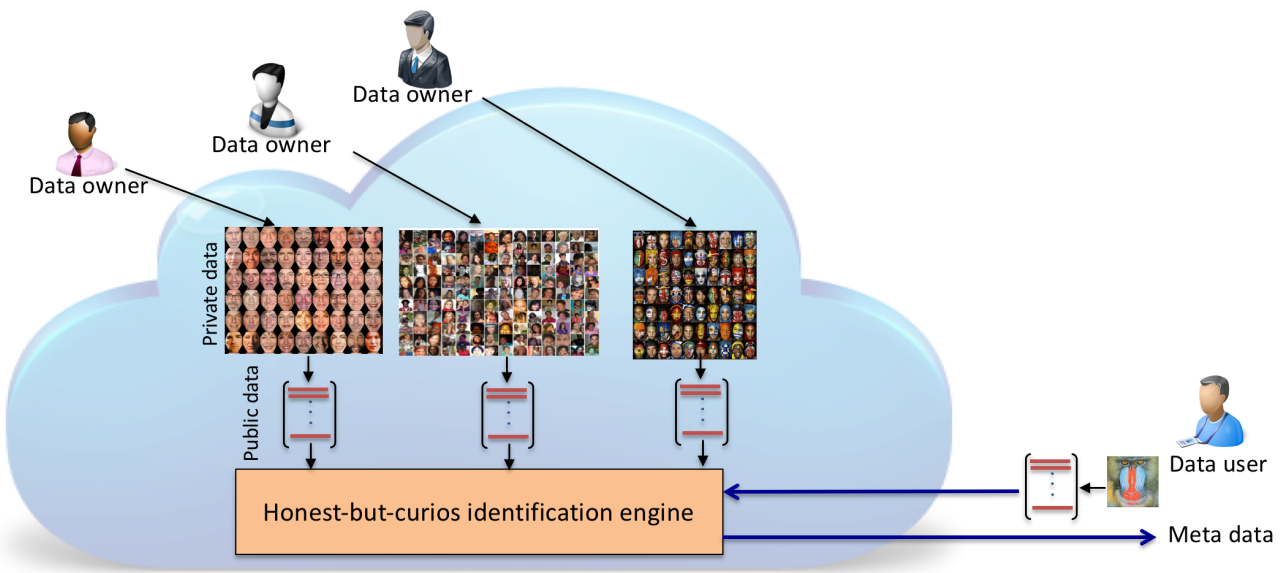
Privacy-preserving content search

- Biometrics
- Physical object recognition and security
- Medical/clinical applications
- Privacy-sensitive multimedia records

Recent Trends

Big Data & Distributed Applications

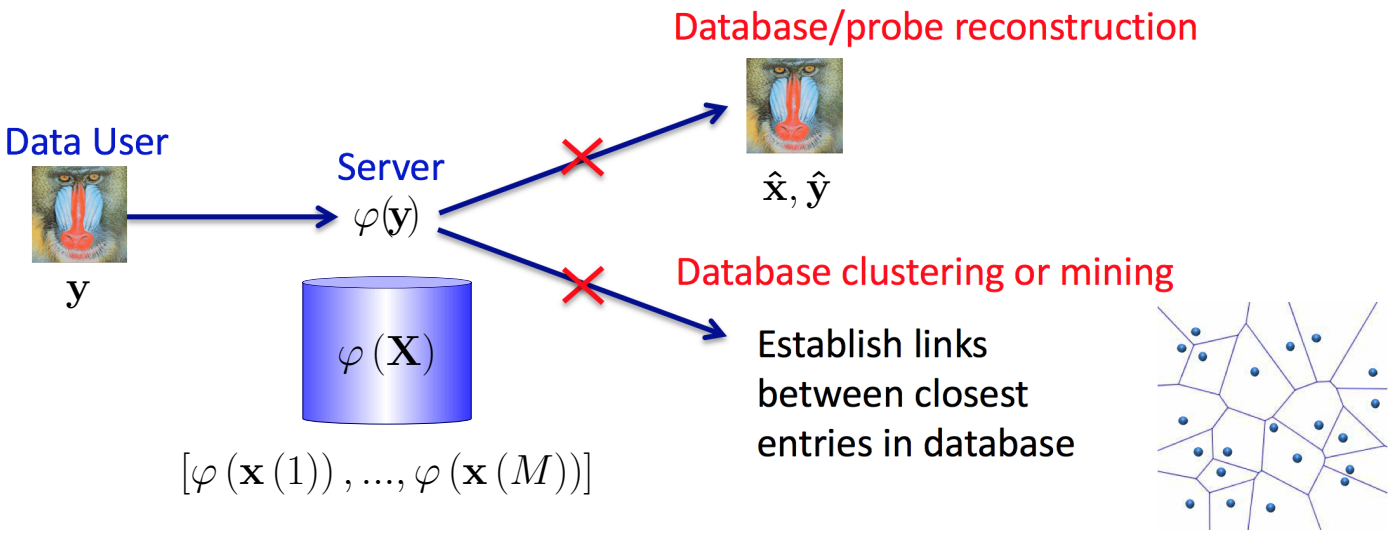
Services on outsourced cloud-based systems



Introduction

Problem Formulation

Goal of privacy protection in outsourced services



Introduction

state-of-the-art

- **Cryptographic Methods - Homomorphic Encryption**
  - **Main Idea:** Similarity search in the encrypted domain
    - Brute force identification $\Longrightarrow$ huge complexity
- **Robust Hashing - a single hash from the whole content / local descriptors / last layer of CNN**
  - **Main Idea:** $\mathbf{x} \longrightarrow (011011100110)$ and believed non-invertability
    - Loss in performance due to binarization
    - Unauthorized database clustering

Introduction

state-of-the-art

- **Cryptographic Methods - Homomorphic Encryption**
  - **Main Idea:** Similarity search in the encrypted domain
    - Brute force identification $\Longrightarrow$ huge complexity
- **Robust Hashing - a single hash from the whole content / local descriptors / last layer of CNN**
  - **Main Idea:** $\mathbf{x} \longrightarrow (011011100110)$ and believed non-invertability
    - Loss in performance due to binarization
    - Unauthorized database clustering
- **Group Testing / Memory Vectors**
  - **Main Idea:** Group testing by measuring the proximity to the group representative
    - Group representatives (memory vectors) should be stored in memory

Introduction

state-of-the-art

- **Cryptographic Methods - Homomorphic Encryption**
  - **Main Idea:** Similarity search in the encrypted domain
    - Brute force identification $\Longrightarrow$ huge complexity
- **Robust Hashing - a single hash from the whole content / local descriptors / last layer of CNN**
  - **Main Idea:** $\mathbf{x} \longrightarrow (011011100110)$ and believed non-invertability
    - Loss in performance due to binarization
    - Unauthorized database clustering
- **Group Testing / Memory Vectors**
  - **Main Idea:** Group testing by measuring the proximity to the group representative
    - Group representatives (memory vectors) should be stored in memory

Introduction

state-of-the-art

- **Proposed approach: 3 key elements**
  - Sparsification
  - Ambiguization
  - Search / Identification
- **Advantages:**
  - Fast search / memory efficient
  - Difficult to accurately reconstruct from probe
  - Server cannot reveal a structure of the database

Introduction

state-of-the-art

- **Proposed approach: 3 key elements**
  - Sparsification
  - Ambiguization
  - Search / Identification
- **Advantages:**
  - Fast search / memory efficient
  - Difficult to accurately reconstruct from probe
  - Server cannot reveal a structure of the database
- **Main concerns addressed in our study:**
  - Performance
  - Memory (database) / complexity (identification)
  - Privacy-preserving with respect to:
    - database $\mathcal{A}$
    - probe $\mathbf{y}$

Introduction

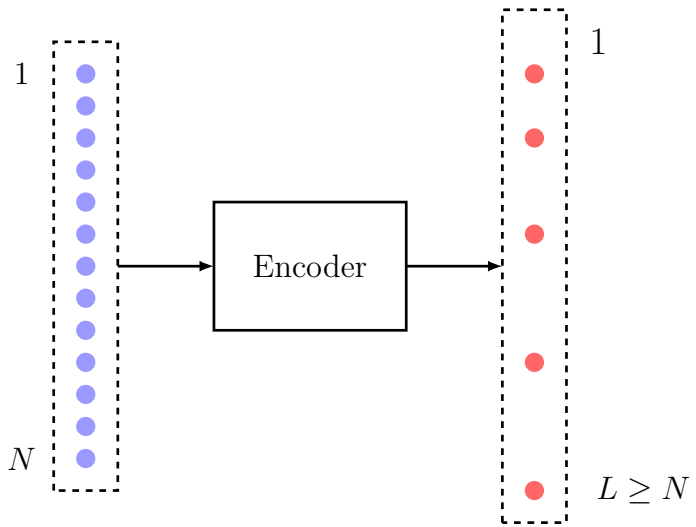
state-of-the-art

- **Proposed approach: 3 key elements**
  - Sparsification
  - Ambiguization
  - Search / Identification
- **Advantages:**
  - Fast search / memory efficient
  - Difficult to accurately reconstruct from probe
  - Server cannot reveal a structure of the database
- **Main concerns addressed in our study:**
  - Performance
  - Memory (database) / complexity (identification)
  - Privacy-preserving with respect to:
    - database $\mathcal{A}$
    - probe $\mathbf{y}$

Part 1:
Sparse Data Representation

Sparsification

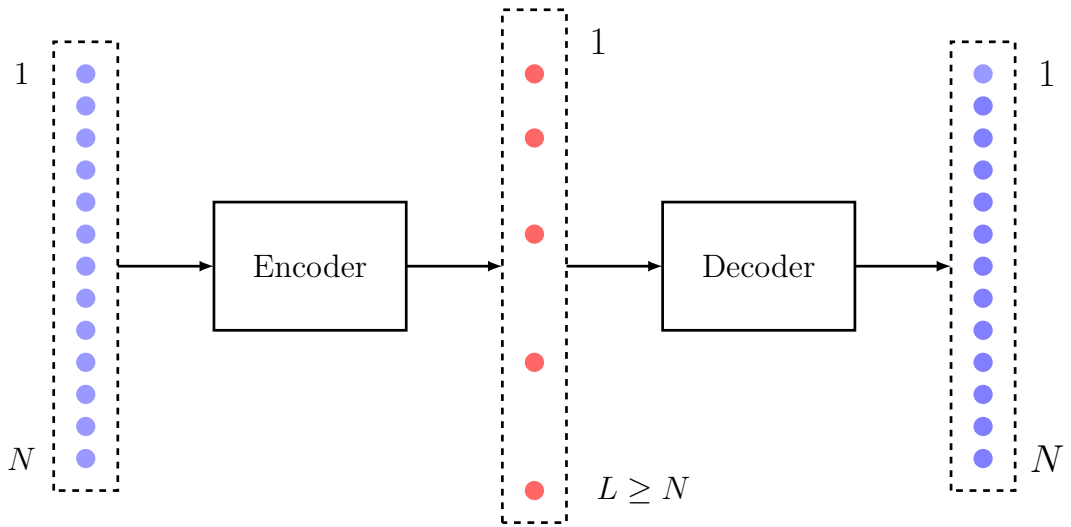
Main Idea



- $\mathbf{x}(m) \in \mathbb{R}^N$
- $\mathbf{x}(m) \sim p(\mathbf{x})$
- $\mathbf{a}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{a}(m)\|_0 \leq S_x$
- Rate: $R = \frac{1}{L} \log_2 \left(\binom{L}{S_x} 2^{S_x} \right)$

Sparsification

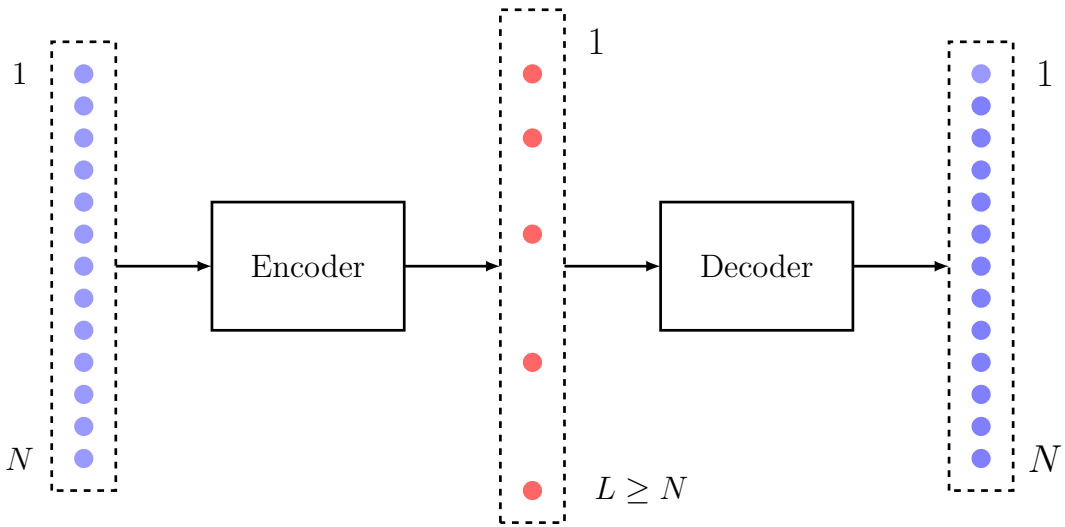
Main Idea

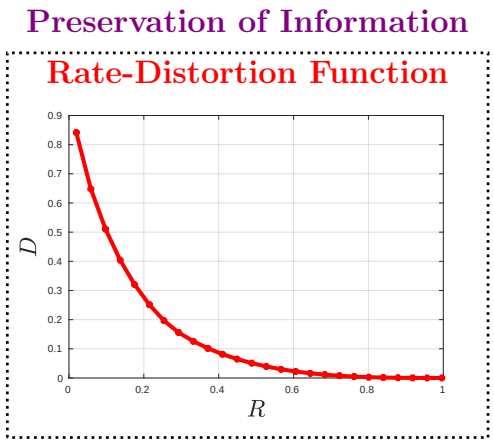


- $\mathbf{x}(m) \in \mathbb{R}^N$
- $\mathbf{x}(m) \sim p(\mathbf{x})$
- $\mathbf{a}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{a}(m)\|_0 \leq S_x$
- Rate: $R = \frac{1}{L} \log_2 \left(\binom{L}{S_x} 2^{S_x} \right)$
- $\hat{\mathbf{x}}(m) \in \mathbb{R}^N$
- Distortion : $\frac{1}{N} \|\mathbf{x}(m) - \hat{\mathbf{x}}(m)\|_2^2 \leq D$

Sparsification

Main Idea



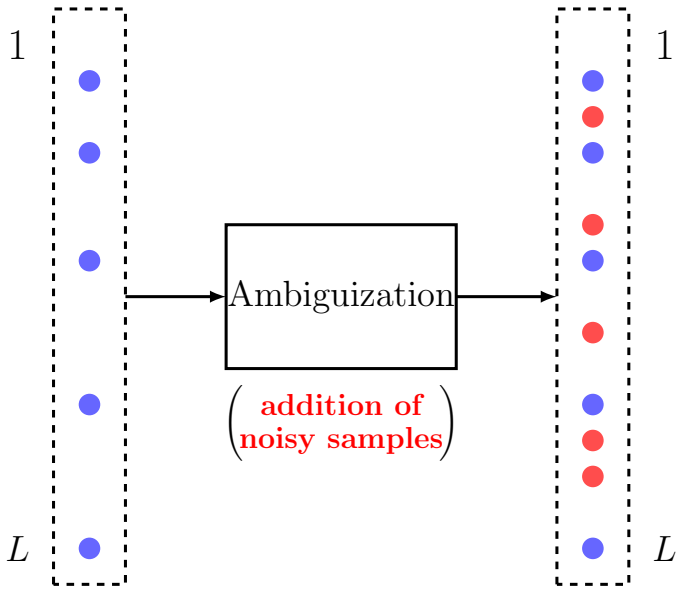


- $\mathbf{x}(m) \in \mathbb{R}^N$
- $\mathbf{x}(m) \sim p(\mathbf{x})$
- $\mathbf{a}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{a}(m)\|_0 \leq S_x$
- Rate: $R = \frac{1}{L} \log_2 \left(\binom{L}{S_x} 2^{S_x} \right)$
- $\hat{\mathbf{x}}(m) \in \mathbb{R}^N$
- Distortion : $\frac{1}{N} \|\mathbf{x}(m) - \hat{\mathbf{x}}(m)\|_2^2 \leq D$

Part 2:
Ambiguization

Ambiguization

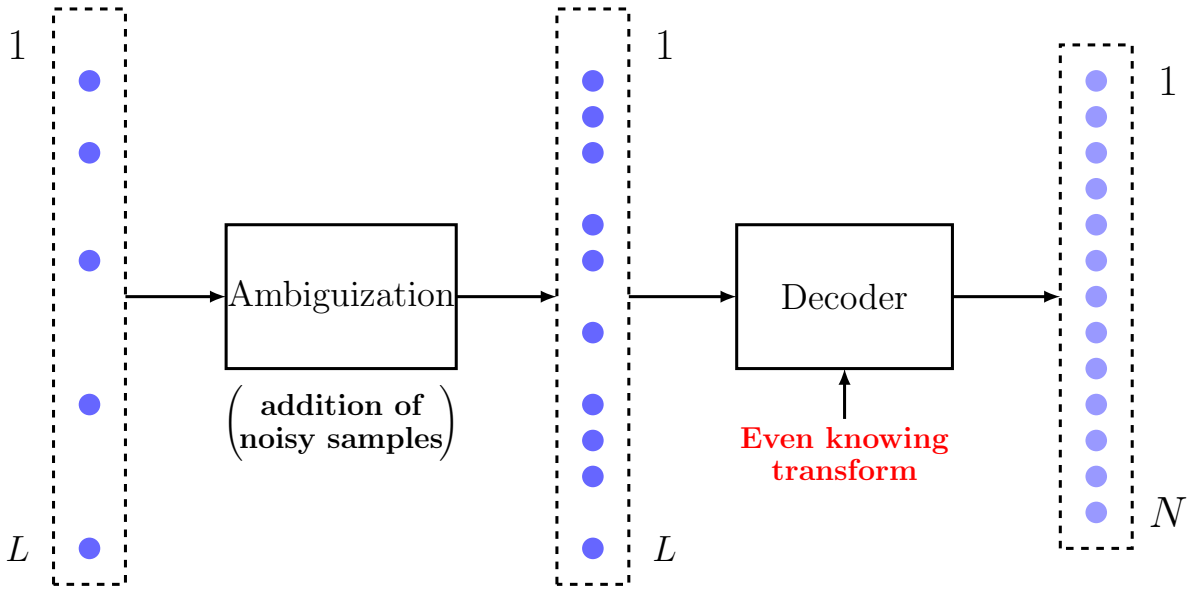
Main Idea



- $\mathbf{a}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{a}(m)\|_0 \leq S_x$
- **Public Domain**
- $\mathbf{a}(m) \bigoplus \mathbf{n}$

Ambiguization

Main Idea



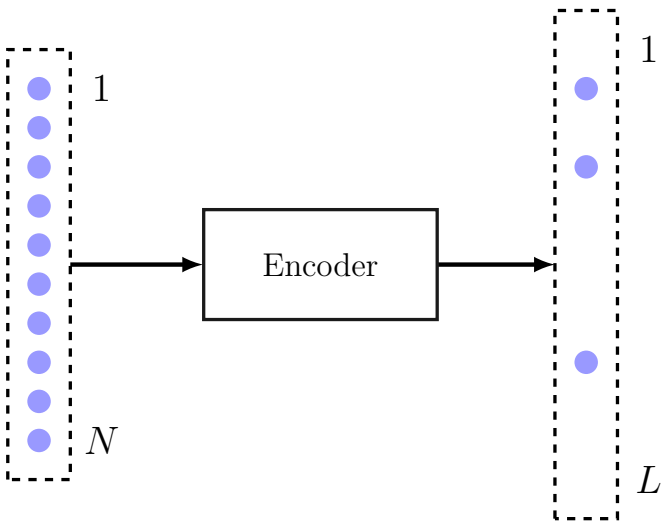
- $\mathbf{a}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{a}(m)\|_0 \leq S_x$
- **Public Domain**
- $\mathbf{a}(m) \bigoplus \mathbf{n}$
- $\hat{\mathbf{x}}(m) \in \mathbb{R}^N$
- $\|\mathbf{x}(m) - \hat{\mathbf{x}}(m)\|_2^2 \to \simeq 2N\sigma_{\mathbf{x}}^2$

- Prevent reconstruction from $\mathbf{a}(m) \bigoplus \mathbf{n}$ and from probe $\mathbf{y}$
- Preclude server from discovering the structure of the database $\mathcal{A}$

Part 3:
Privacy-Preserving Search

Privacy-Preserving Search: Private Search

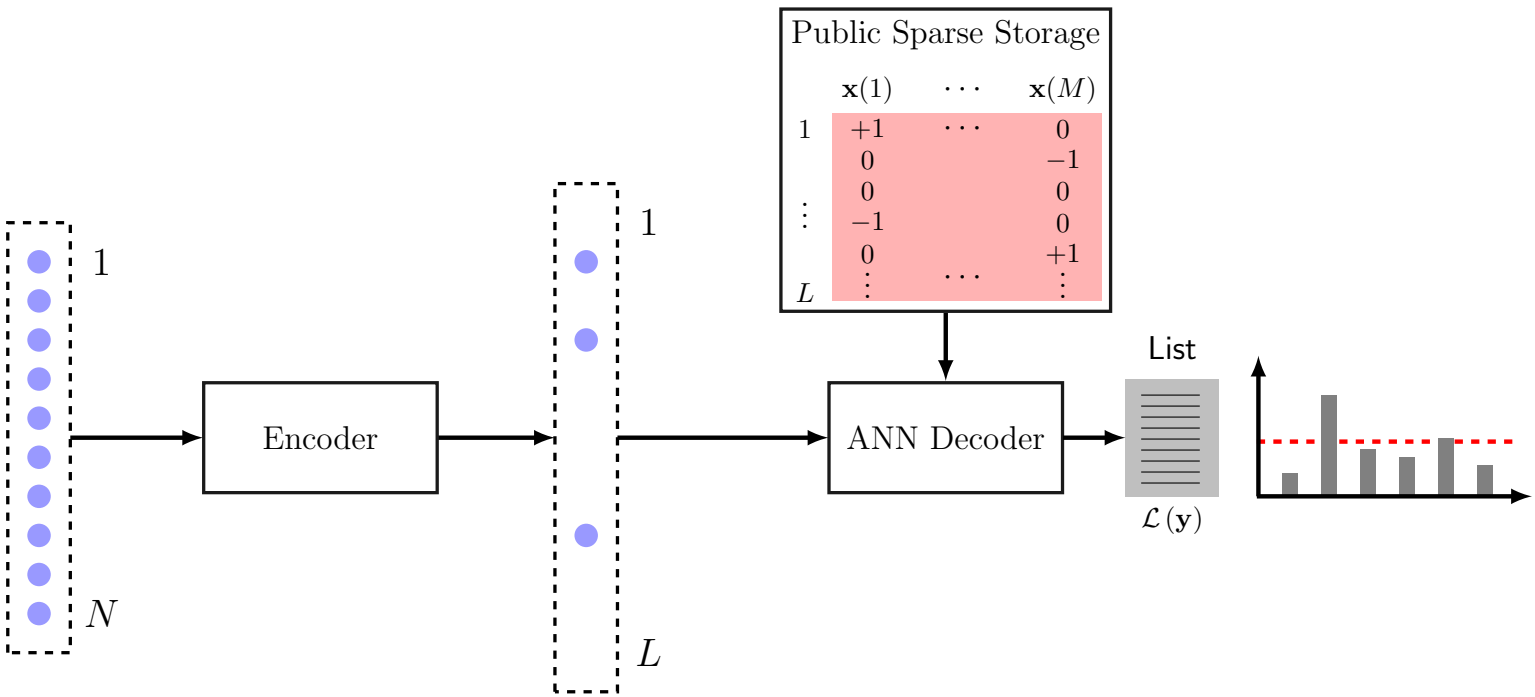
Main Idea: User discloses his probe completely



- $\mathbf{y} \in \mathbb{R}^N$
- $\mathbf{b} \in \{-1, 0, +1\}^L$
- $\|\mathbf{b}\|_0 \leq S_y$

Privacy-Preserving Search: Private Search

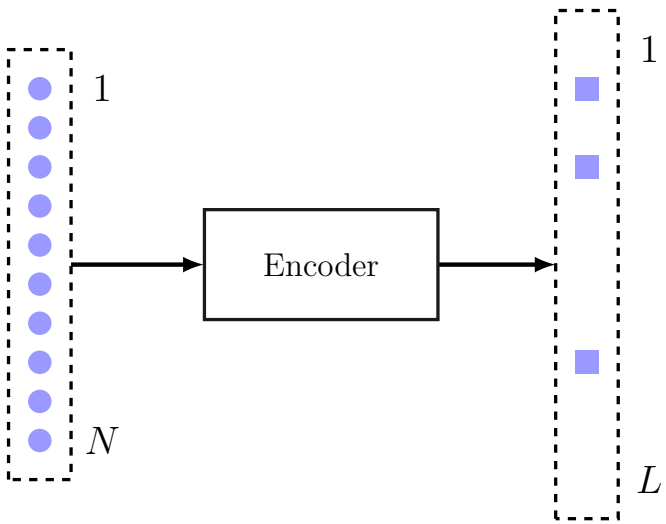
Main Idea: User discloses his probe completely



- $\mathbf{y} \in \mathbb{R}^N$
- $\mathbf{b} \in \{-1, 0, +1\}^L$
- $\|\mathbf{b}\|_0 \leq S_y$

Privacy-Preserving Search: Public Search

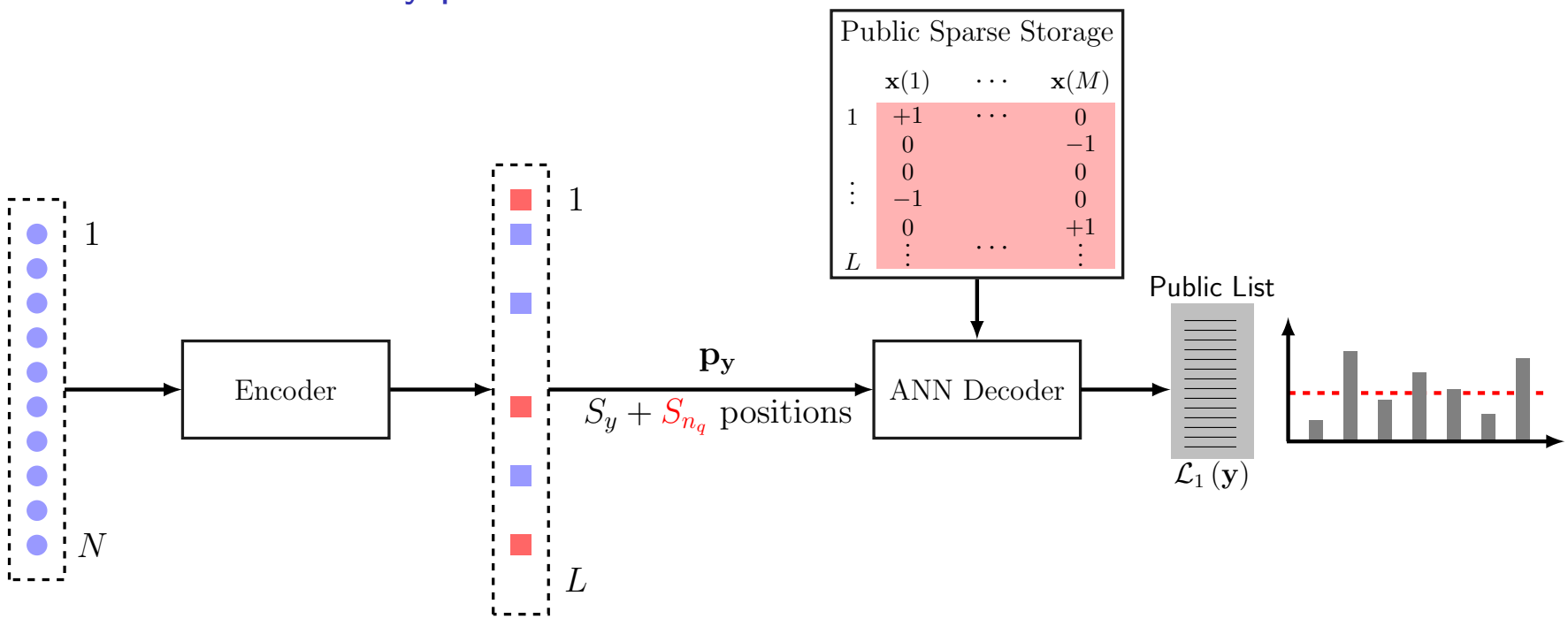
Main Idea: User sends only positions of interest



- $\mathbf{y} \in \mathbb{R}^N$
- $\mathbf{b} \in \{-1, 0, +1\}^L$
- $\|\mathbf{b}\|_0 \leq S_y$

Privacy-Preserving Search: Public Search

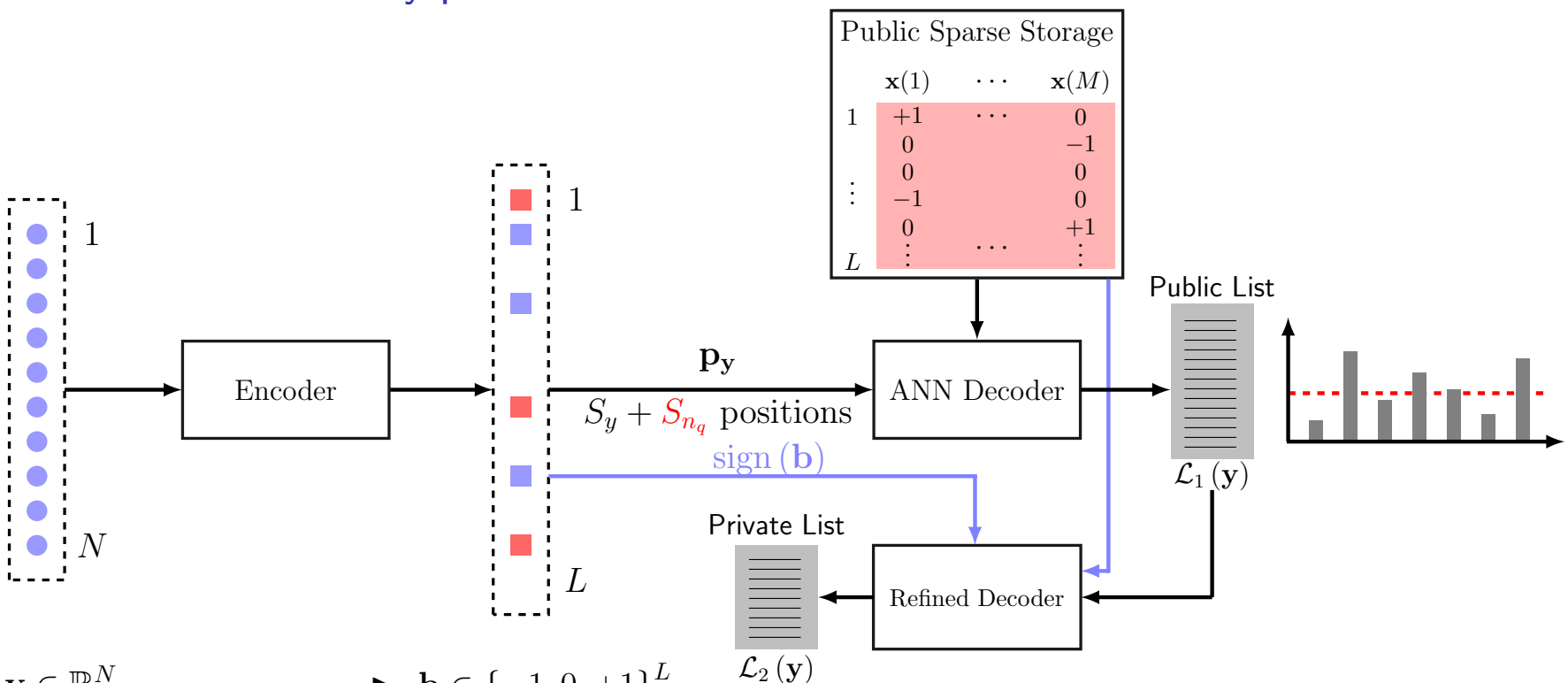
Main Idea: User sends only positions of interest



- $\mathbf{y} \in \mathbb{R}^N$
- $\mathbf{b} \in \{-1, 0, +1\}^L$
- $\|\mathbf{b}\|_0 \leq S_y$
- Add S_{n_q} random positions

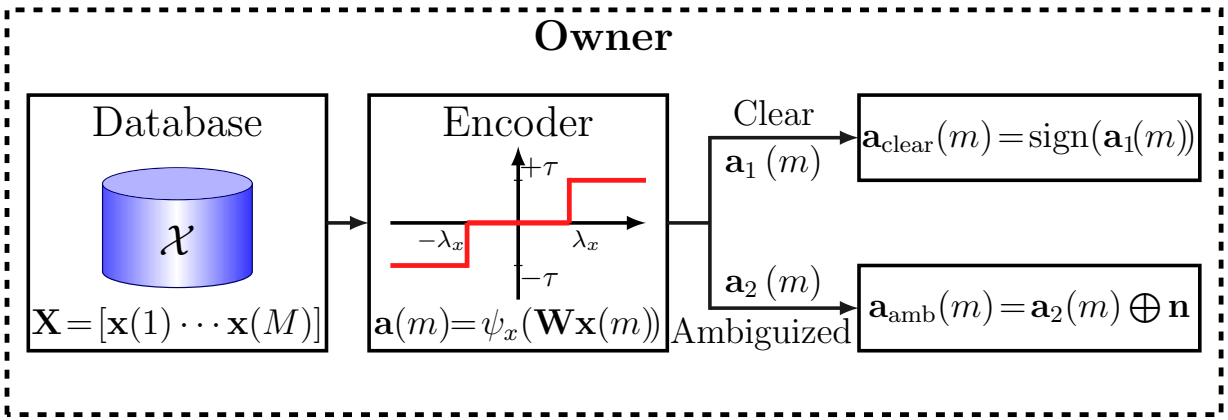
Privacy-Preserving Search: Public Search

Main Idea: User sends only positions of interest

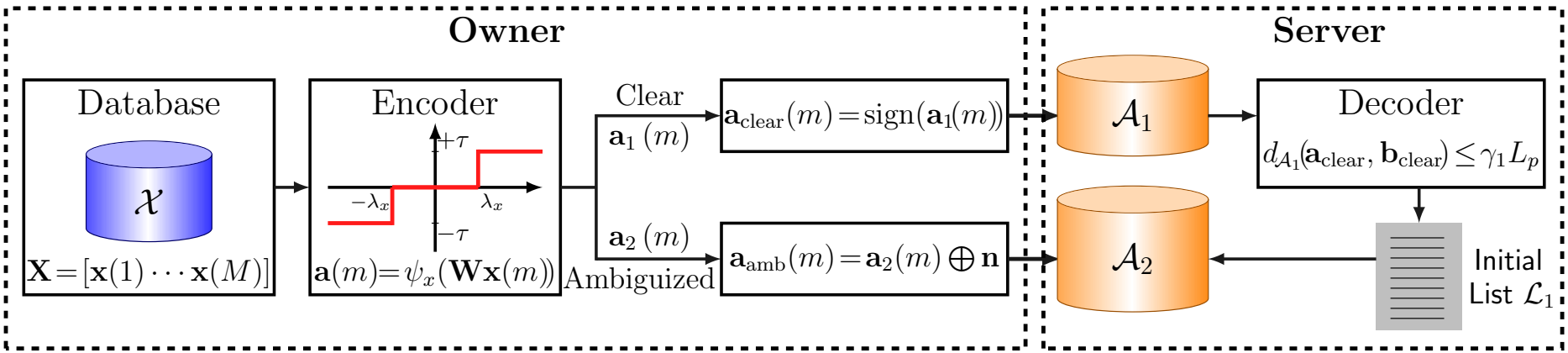


- $\mathbf{y} \in \mathbb{R}^N$
- $\mathbf{b} \in \{-1, 0, +1\}^L$
- $\|\mathbf{b}\|_0 \leq S_y$
- Add S_{n_q} random positions

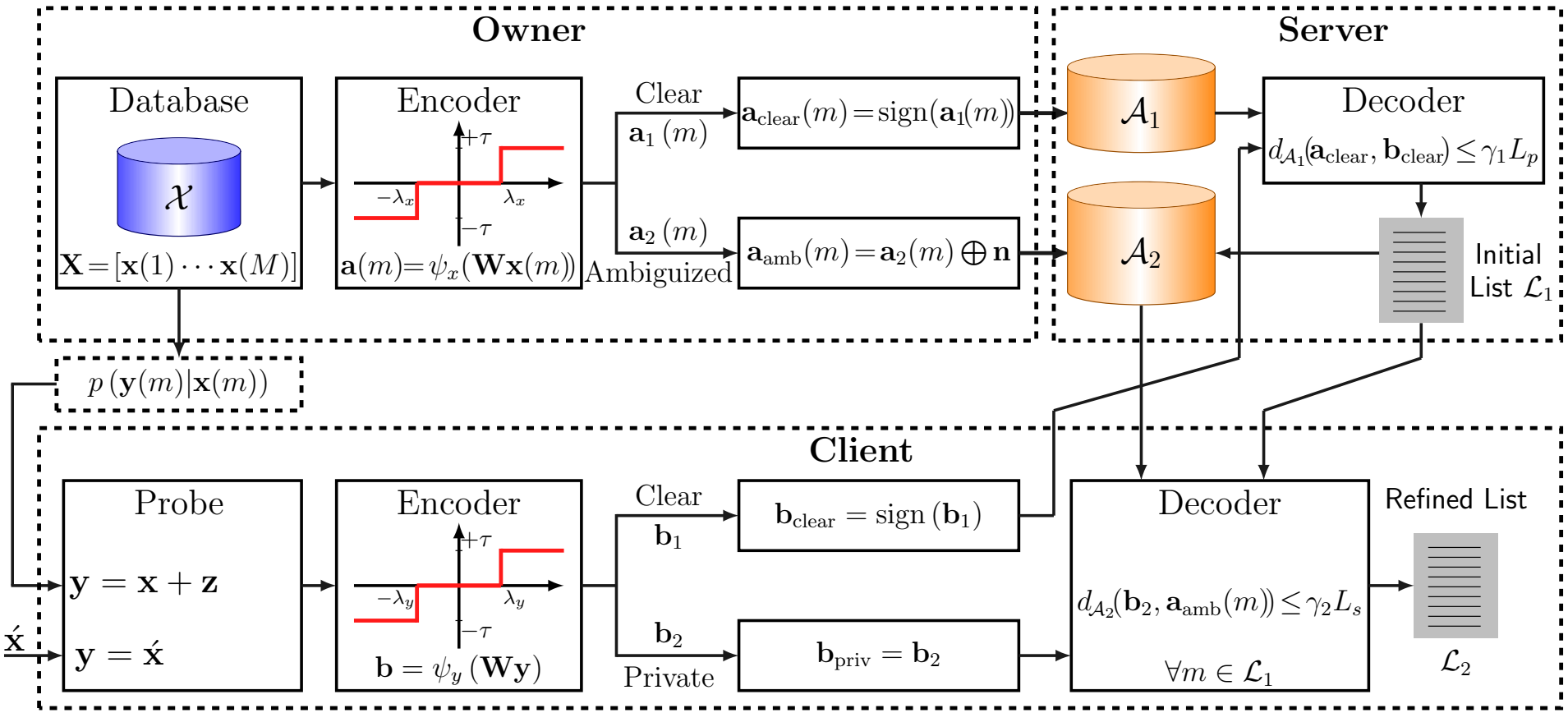
Main idea behind the proposed solution



Main idea behind the proposed solution

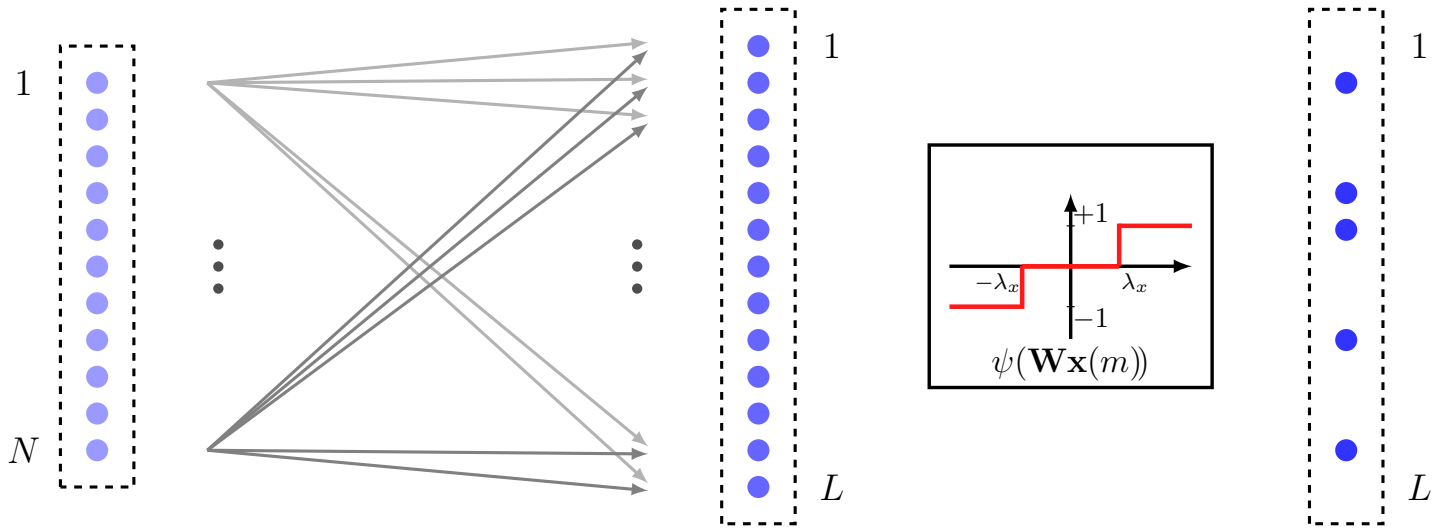


Main idea behind the proposed solution



Sparsifying Transform

A Schematic Idea



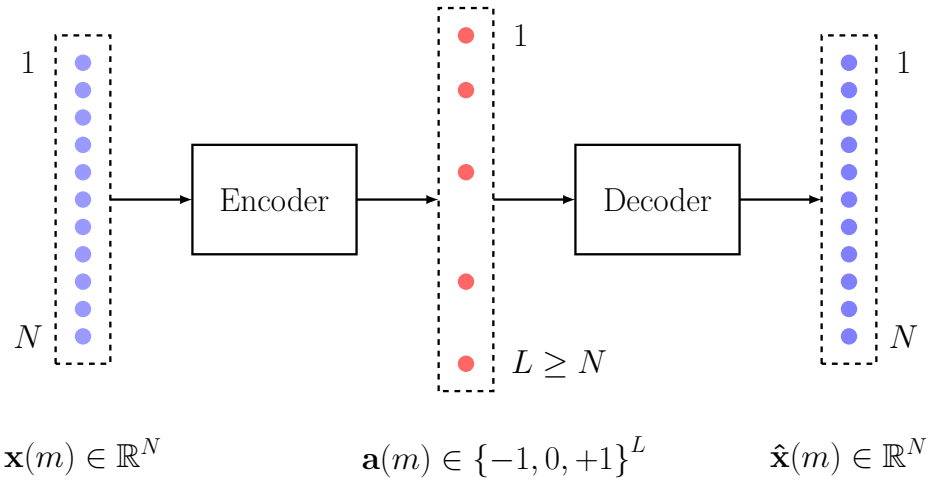
Linear Mapping Element-wise Non-linearity

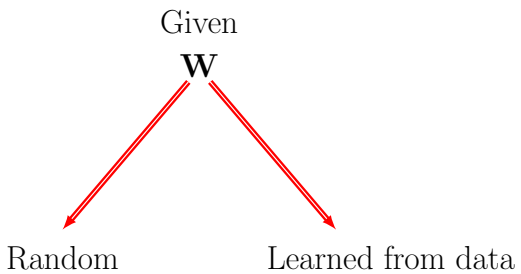
$$\mathbf{x}(m) \in \mathbb{R}^N \xrightarrow{\mathbf{W}} \mathbf{W}\mathbf{x}(m) \in \mathbb{R}^L \xrightarrow{\psi(.)} \mathbf{a}(m) \in \{-1, 0, +1\}^L$$

$$\varphi(.)$$

Sparsifying Transform

General Problem Formulation





- **Encoder:**

$$\hat{\mathbf{a}}(m) = \psi(\mathbf{W}\mathbf{x}(m))$$

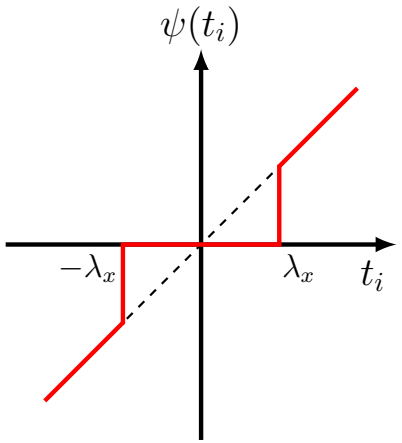
- **Decoder:**

$$\hat{\mathbf{x}}(m) = \boldsymbol{\tau} \odot \mathbf{W}^{\dagger}\hat{\mathbf{a}}(m)$$

Encoder: as a projection problem (for a fixed $\mathbf{W}$)

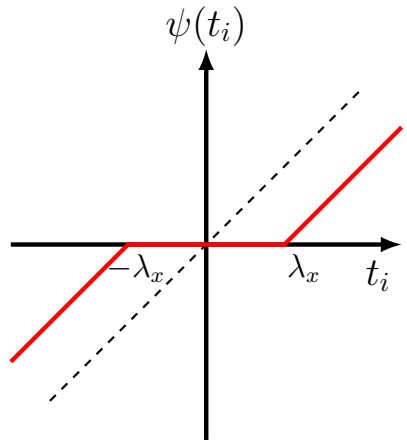
$$\widehat{\mathbf{a}}(m) = \underset{\mathbf{a}(m)\in\mathcal{A}^L}{\arg\min} \|\mathbf{W}\mathbf{x}(m) - \mathbf{a}(m)\|_2^2 + \beta\Omega\left(\mathbf{a}(m)\right), \forall m \in [M]$$

- $\mathbf{W} \in \mathbb{R}^{L\times N}$, $\mathbf{x}(m) \in \mathbb{R}^N$, $\mathbf{a}(m) \in \mathbb{R}^L$
- Closed-form solution for: $\Omega(.) = \|.\|_0$ and $\Omega(.) = \|.\|_1$



Hard-thresholding operator

$\Omega(.) = \|.\|_0$



Soft-thresholding operator

$\Omega(.) = \|.\|_1$

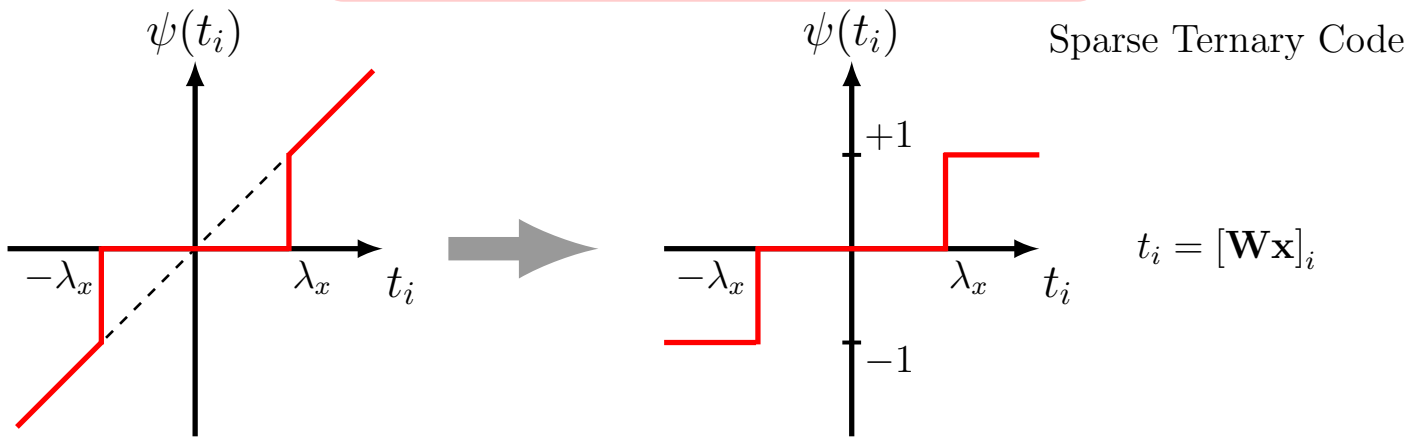
$$t_i = [\mathbf{W}\mathbf{x}]_i$$

$$\hat{\mathbf{a}}(m) = \psi\left(\mathbf{W}\mathbf{x}(m)\right)$$

Encoder: Extra constraint on the alphabet

$$\hat{\mathbf{a}}(m) = \psi(\mathbf{W}\mathbf{x}(m))$$

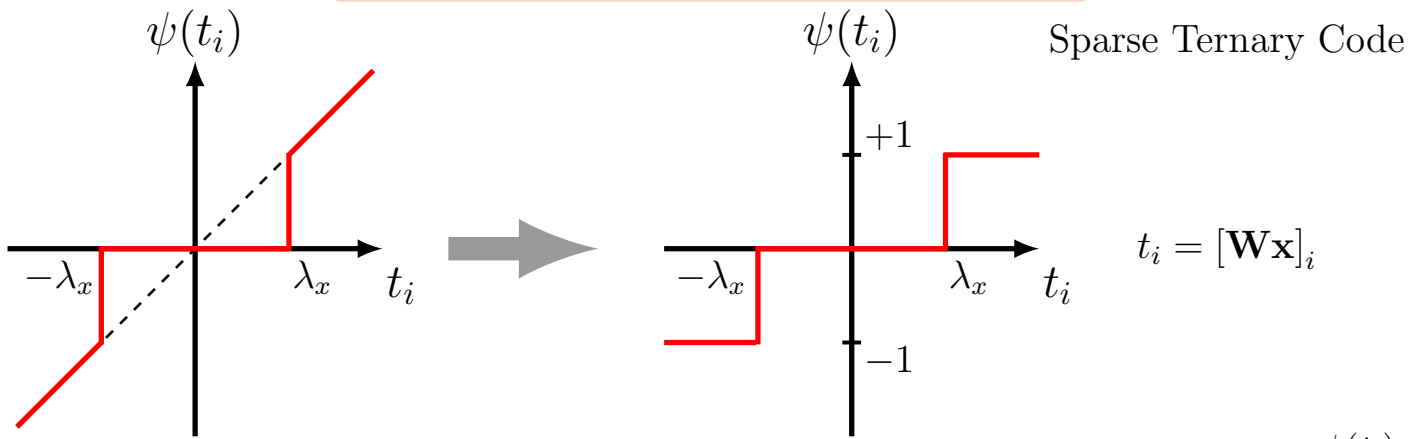
$$\text{s.t.} \qquad \mathbf{a}(m) \in \{-1, 0, +1\}$$



Encoder: Extra constraint on the alphabet

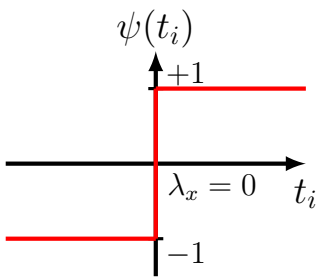
$$\hat{\mathbf{a}}(m) = \psi(\mathbf{W}\mathbf{x}(m))$$

$$\text{s.t.} \qquad \mathbf{a}(m) \in \{-1, 0, +1\}$$



Remark:

Binary hashing (like LSH) is the special case of our $\psi(.)$ for $\lambda_x = 0$.

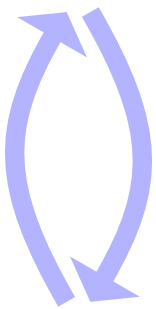


Learning Sparsifying Transform

General Formulation: joint learning

$$\left(\hat{\mathbf{W}}, \hat{\mathbf{A}}\right) = \arg \min_{(\mathbf{W},\mathbf{A})} \|\mathbf{WX} - \mathbf{A}\|_F^2 + \beta_W \Omega_W(\mathbf{W}) + \beta_A \Omega_A(\mathbf{A})$$

- **Sparse Coding Step** (Fixed $\mathbf{W}$):



$$\hat{\mathbf{A}} = \arg\min_{\mathbf{A}} \|\mathbf{WX} - \mathbf{A}\|_F^2 + \beta_A \Omega_A(\mathbf{A})$$

$$\hat{\mathbf{a}}(m) = \psi(\mathbf{W}\mathbf{x}(m))$$

- **Transform Update Step** (Fixed $\mathbf{A}$):

$$\hat{\mathbf{W}} = \arg\min_{\mathbf{W}} \|\mathbf{WX} - \mathbf{A}\|_F^2 + \beta_W \Omega_W(\mathbf{W})$$

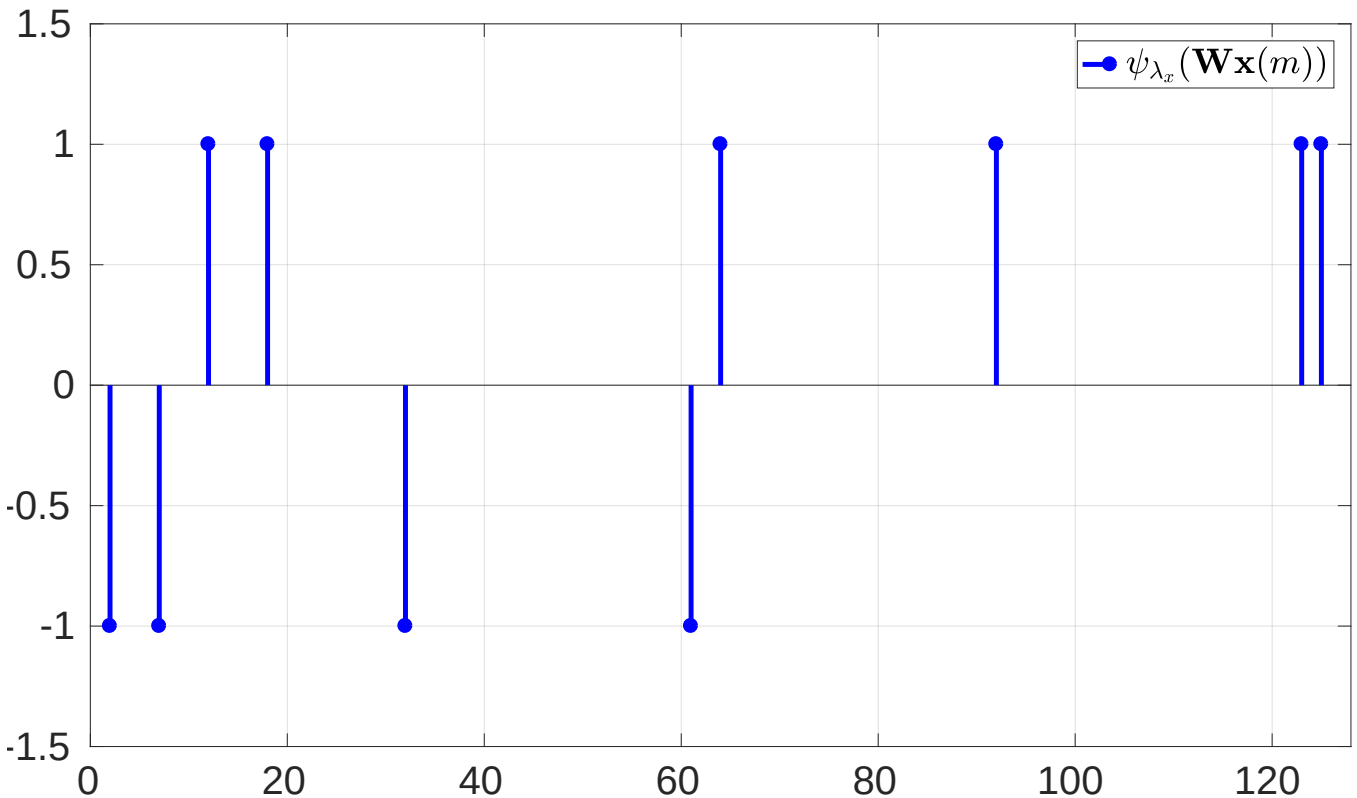
Linear Regression :
(with quadratic regularizer)

$$\hat{\mathbf{W}} = \mathbf{A}\mathbf{X}^T\left(\mathbf{X}\mathbf{X}^T + \beta_W \mathbf{I}_N\right)^{-1}$$

Ambiguization Scheme

Main Idea

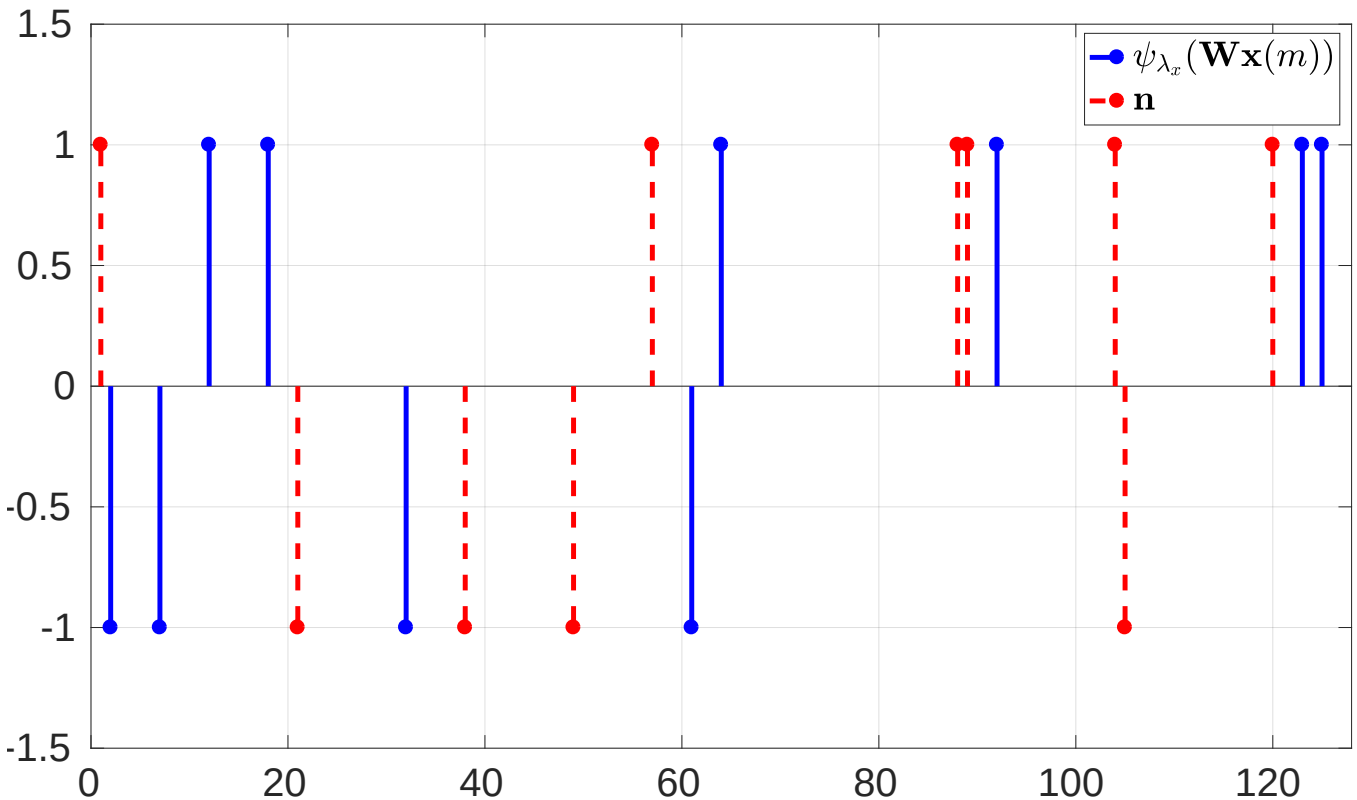
Add noise to **non-zero** components of sparse representation



Ambiguization Scheme

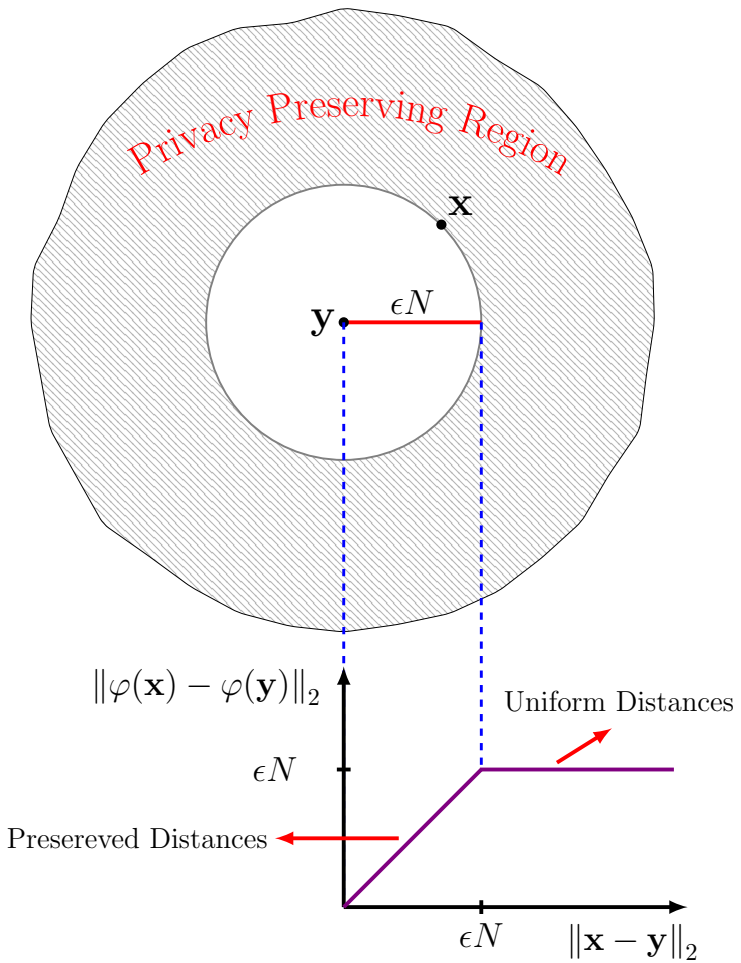
Main Idea

Add noise to **non-zero** components of sparse representation



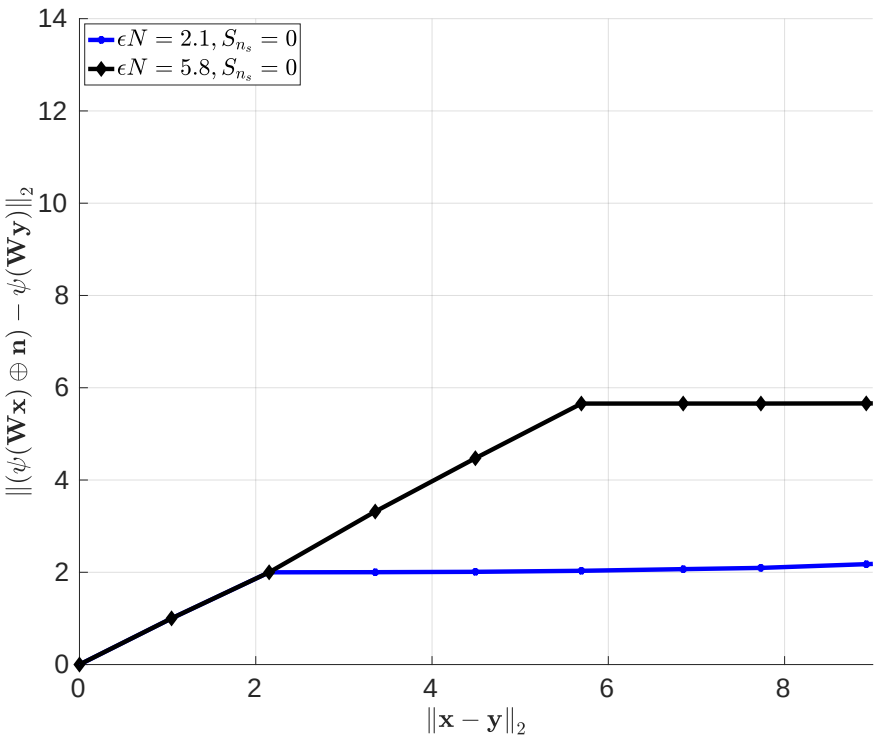
Desired property of mapping scheme

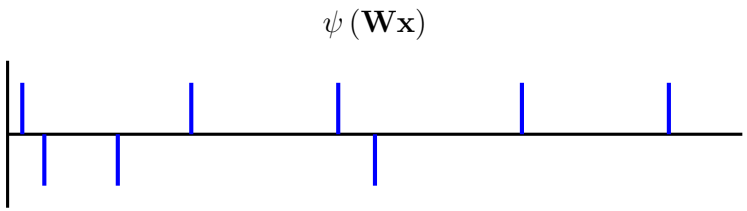
Distance preservation in the desired radius



Impact of Ambiguization at Server Side

Goal: The server should not distinguish distances $\| (\psi (\mathbf{Wx}) \oplus \mathbf{n}) - \psi (\mathbf{Wy}) \|_2$

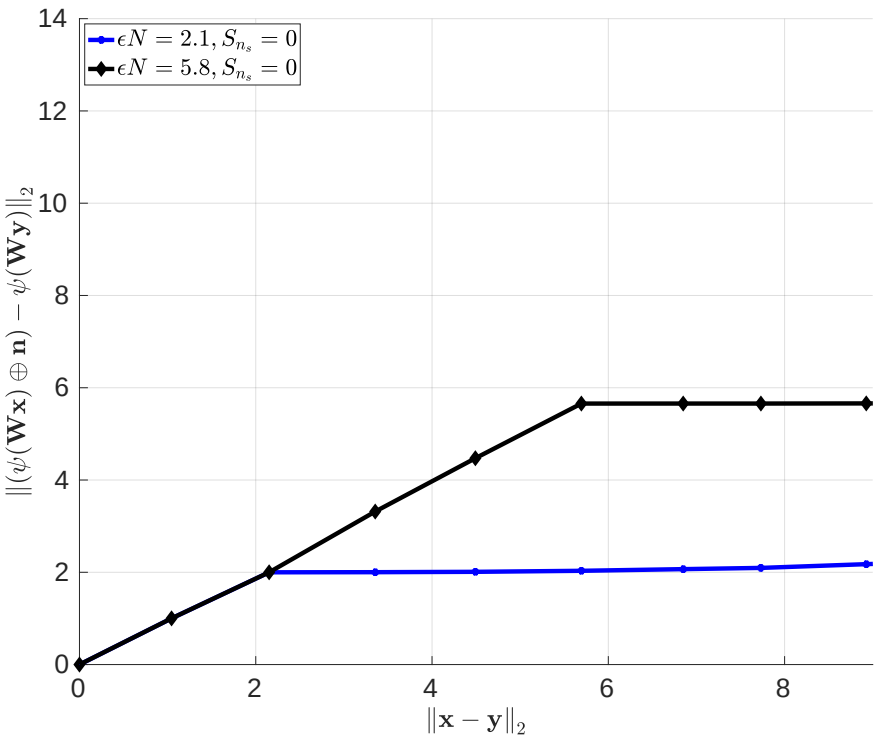


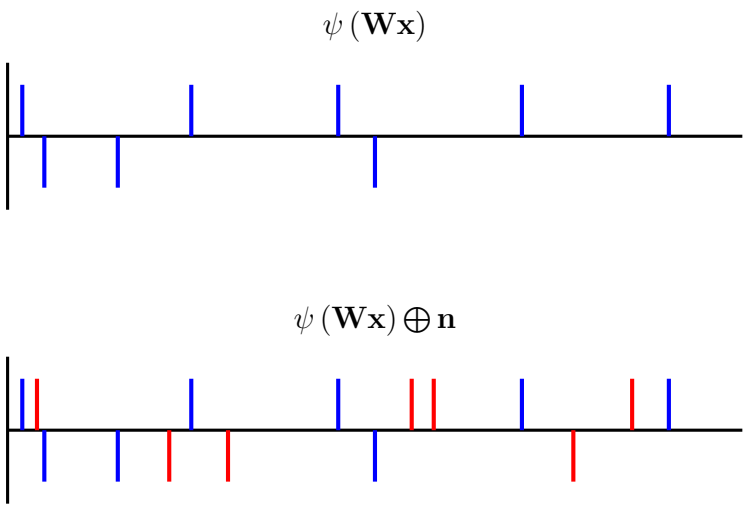


Distances are computed in the full length.

Impact of Ambiguization at Server Side

Goal: The server should not distinguish distances $\| (\psi (\mathbf{Wx}) \oplus \mathbf{n}) - \psi (\mathbf{Wy}) \|_2$

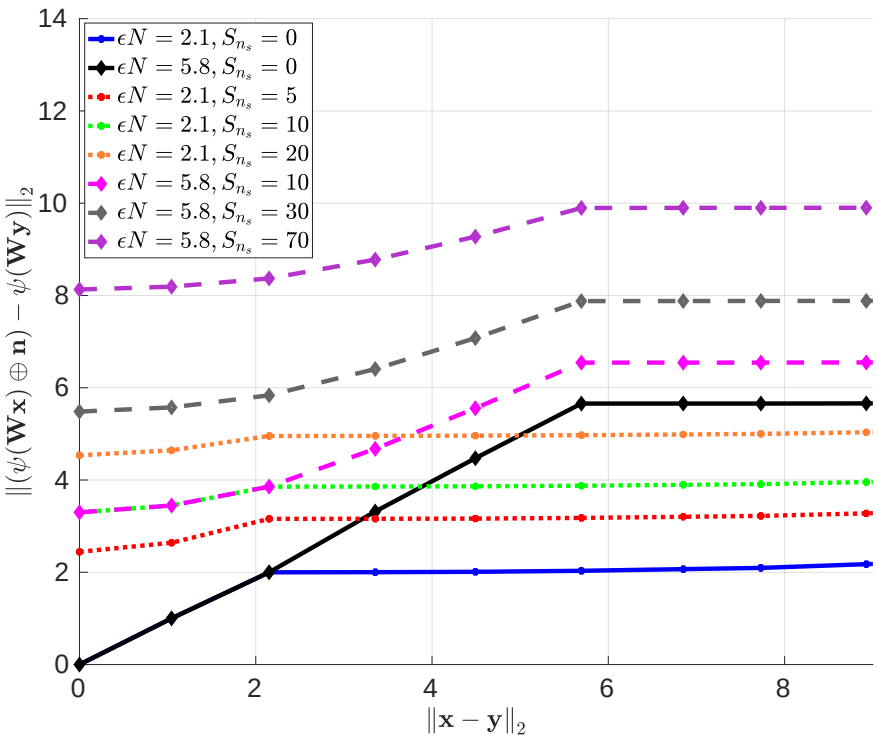


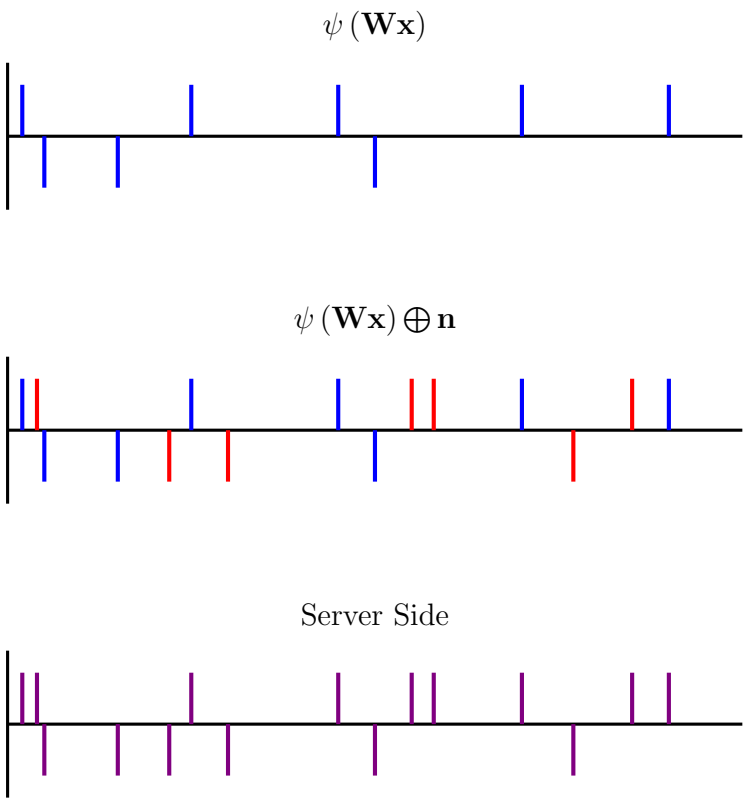


Distances are computed in the full length.

Impact of Ambiguization at Server Side

Goal: The server should not distinguish distances $\| (\psi (\mathbf{Wx}) \oplus \mathbf{n}) - \psi (\mathbf{Wy}) \|_2$

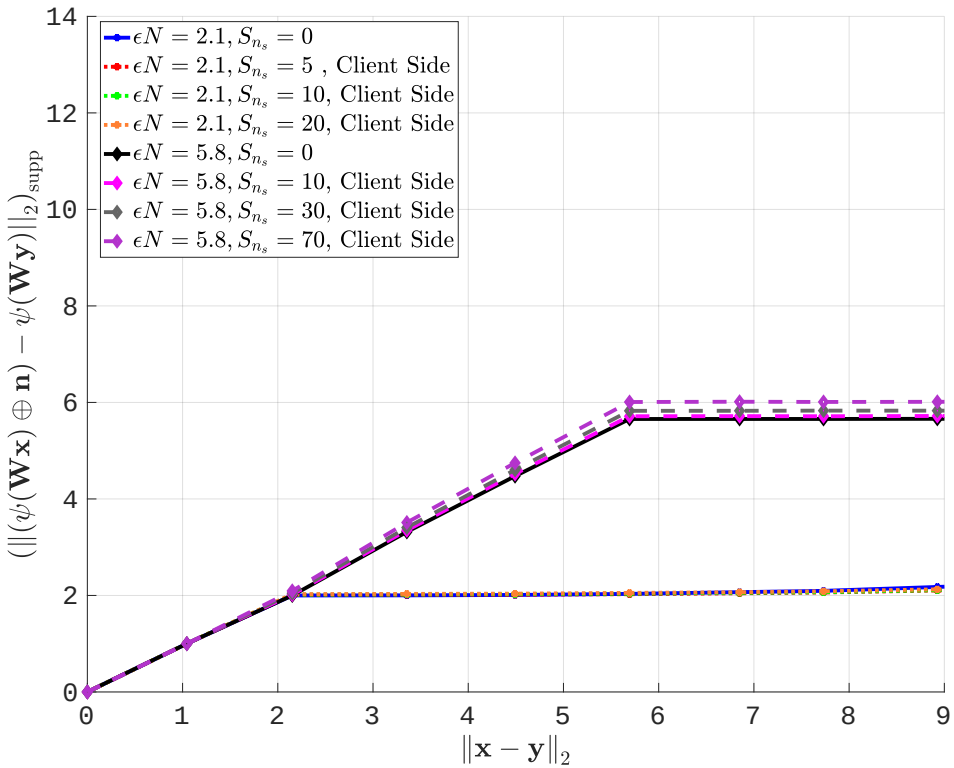


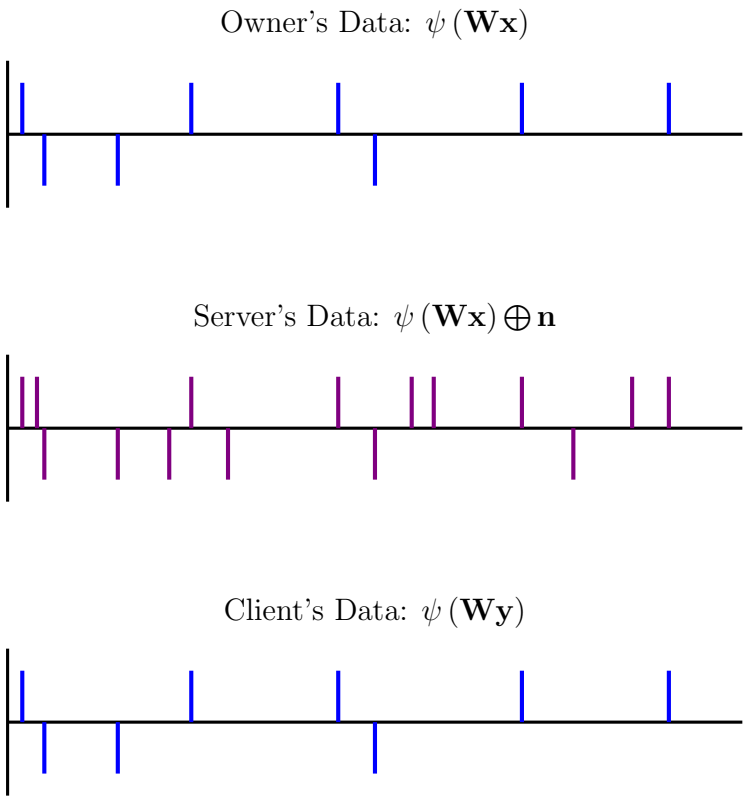


Distances are computed in the full length.

Impact of Ambiguization at Client Side

Goal: The client should distinguish distances $\left(\| \left(\psi\left(\mathbf{Wx}\right) \oplus \mathbf{n}\right) - \psi\left(\mathbf{Wy}\right) \|_2\right)_{\text{supp}}$



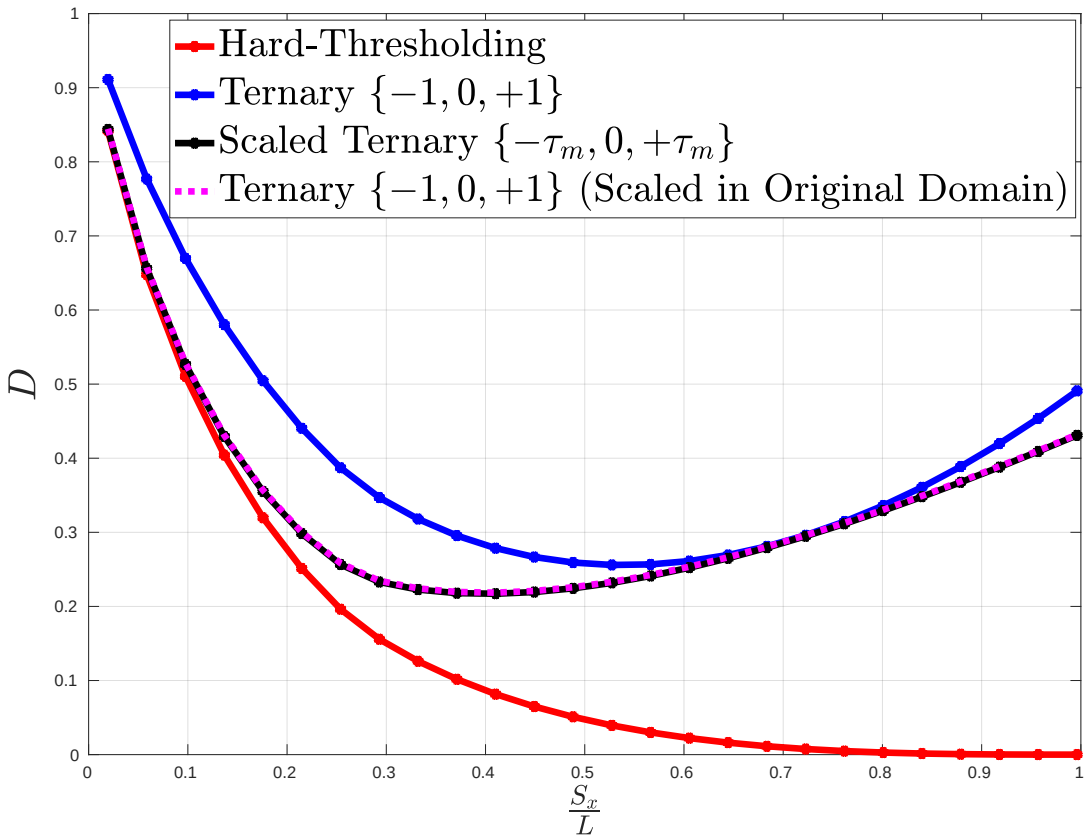


Distances are computed in the non-zero components of probe.

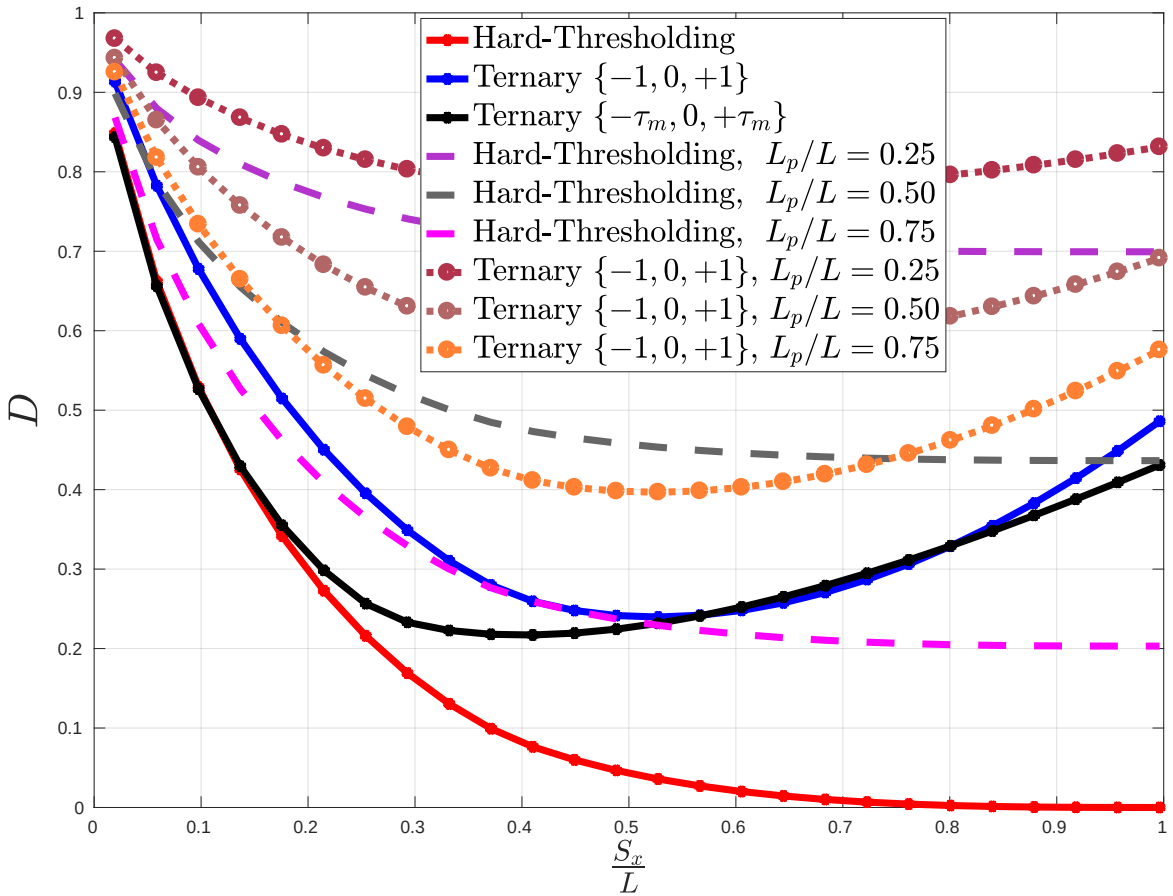
Reconstruction: Authorized User ▶ $\hat{\mathbf{x}} = \mathbf{W}^{\dagger}\mathbf{a}$

$\mathbf{x}$: i.i.d. Gaussian, with each sample $X_n \sim \mathcal{N}(0,1)$, $\frac{N}{L} = 1$

S_x : Sparsity Level



Reconstruction: Unauthorized User ▶ $\hat{\mathbf{x}} = \mathbf{W}^{\dagger}(\mathbf{a} \bigoplus \mathbf{n})$



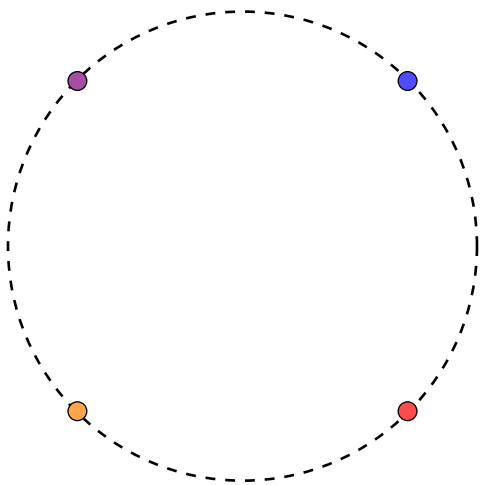
L: Length of Total Sparse Code

L_p: Length of Public Sparse Code

Clustering

Generate Structured Data

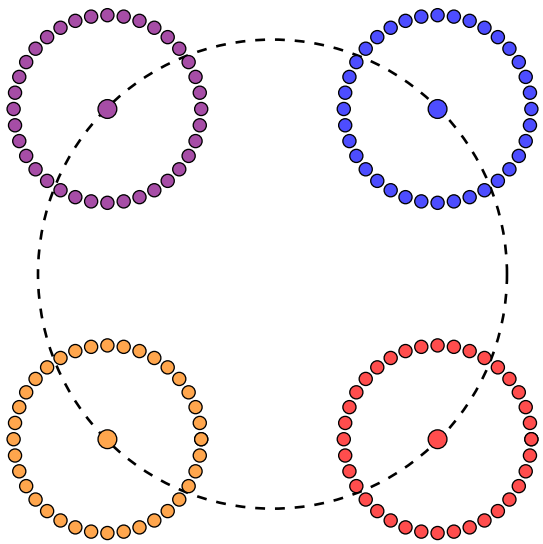
- Generate:
  - Four 512-dimensional i.i.d. vectors with distribution $\mathcal{N}(\mathbf{0}, \mathbf{1})$
  - 1000 512-dimensional i.i.d. vectors with distribution $\mathcal{N}(\mathbf{0}, \mathbf{0.1})$
- Add each 250 (out of 1000) low variance vectors to the four high variance ones



Clustering

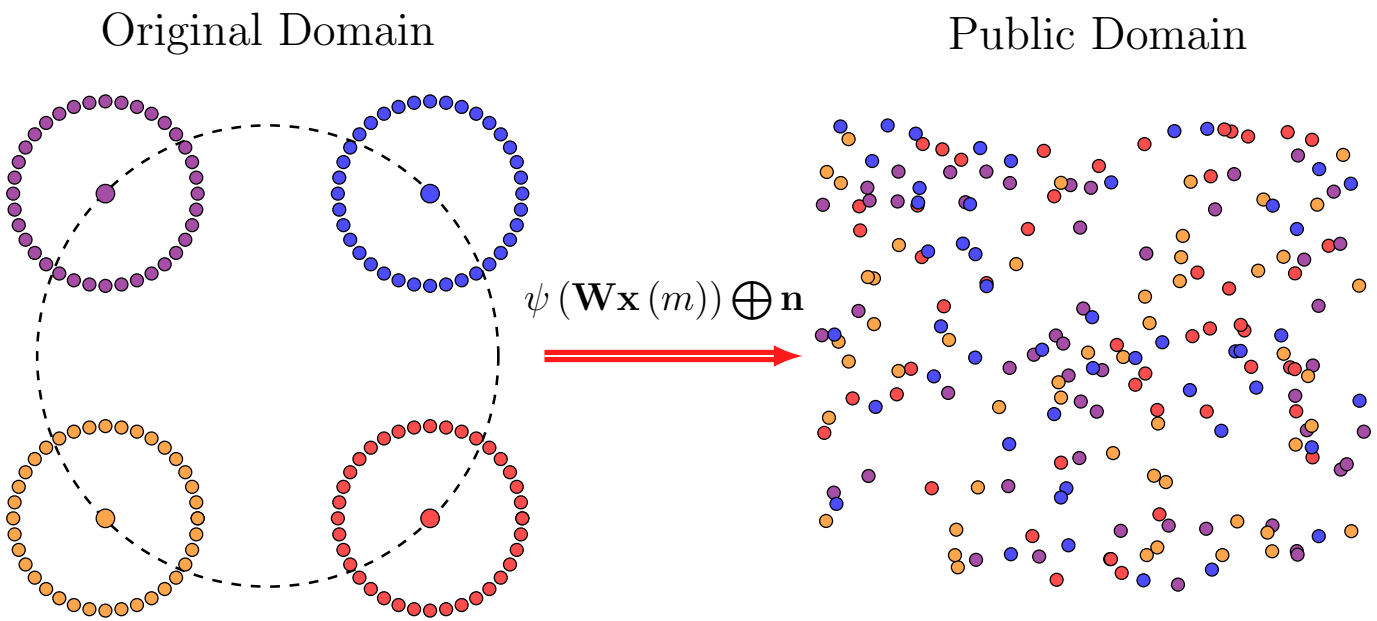
Generate Structured Data

- Generate:
  - Four 512-dimensional i.i.d. vectors with distribution $\mathcal{N}(\mathbf{0}, \mathbf{1})$
  - 1000 512-dimensional i.i.d. vectors with distribution $\mathcal{N}(\mathbf{0}, \mathbf{0.1})$
- Add each 250 (out of 1000) low variance vectors to the four high variance ones



Clustering

Goal: Hide structure of database



Clustering

Introduce Measure for Evaluation

Define:

- $\alpha_x = \frac{S_x}{L}$, S_x : Sparsity level

Denote:

- P_{intra} : PDF of 'intra-cluster' distances
- P_{inter} : PDF of 'inter-cluster' distances

Define:

- $P_1 = \alpha_x \, P_{\text{intra}} + (1 - \alpha_x) \, P_{\text{inter}}, \;\; 0 \leq \alpha_x \leq 1$

Denote:

- $P_2 \sim \mathcal{N}\left(\mu_2, \sigma_2^2\right)$, fit to P_1

Define:

- Privacy Leak Measure:

$$\begin{aligned} D\left(P_1 \| P_2\right) &= \alpha_x \, D\left(P_{\text{intra}} \| P_2\right) + (1 - \alpha_x) \, D\left(P_{\text{inter}} \| P_2\right) \\ &= \mathbb{E}_{P_1}\left[\log \frac{P_1}{P_2}\right] \end{aligned}$$

Clustering

Introduce Measure for Evaluation

Define:

- $\alpha_x = \frac{S_x}{L}$, S_x : Sparsity level

Denote:

- P_{intra} : PDF of 'intra-cluster' distances
- P_{inter} : PDF of 'inter-cluster' distances

Define:

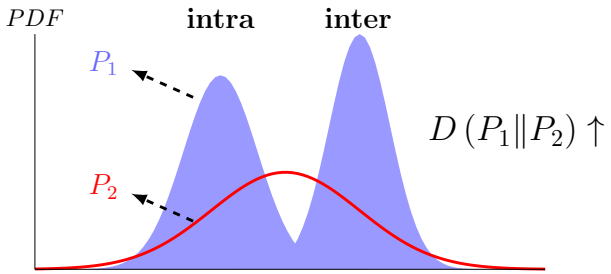
- $P_1 = \alpha_x \, P_{\text{intra}} + (1 - \alpha_x) \, P_{\text{inter}}, \quad 0 \leq \alpha_x \leq 1$

Denote:

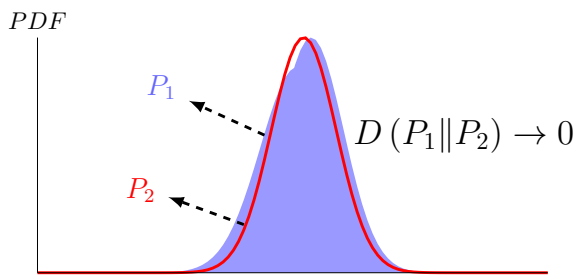
- $P_2 \sim \mathcal{N}\left(\mu_2, \sigma_2^2\right)$, fit to P_1

Define:

- Privacy Leak Measure:



Clear distinguishability based on inter&intra-distances

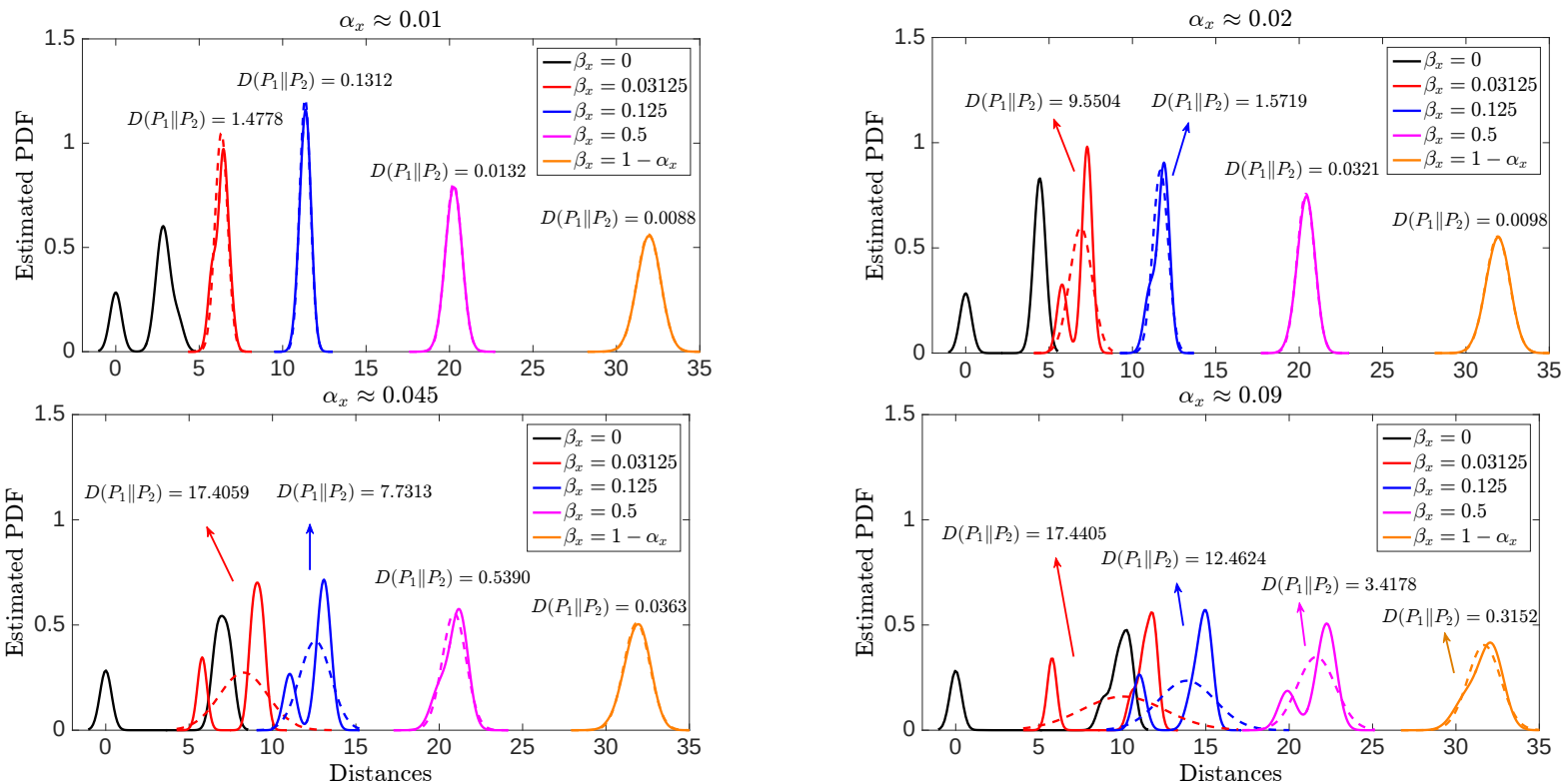


Not distinguishable

$$
\begin{aligned}
D\left(P_1 \| P_2\right) &= \alpha_x \, D\left(P_{\text{intra}} \| P_2\right) + (1 - \alpha_x) \, D\left(P_{\text{inter}} \| P_2\right) \\
&= \mathbb{E}_{P_1}\left[\log \frac{P_1}{P_2}\right]
\end{aligned}
$$

Clustering: How much ambiguization should be added to have indistinguishability for the server?

Evaluation of Our Scheme: $\alpha_x = \frac{S_x}{L}$, $\beta_x = \frac{S_{n_s}}{L}$, S_{n_s} : # of noise components for the server



Conclusions:

- Preserve distances up to the desired radius
- Ensure the reconstruction of data for authorized users
- Preclude the curious server to cluster or reconstruct the samples in the database
- Public decoding scheme


Thank You!