Privacy-Preserving Identification via Layered Sparse Code Design: Distributed Servers and Multiple Access Authorization

Behrooz Razeghi, **Slava Voloshynovskiy**, Sohrab Ferdowsi and Dimche Kostadinov

Stochastic Information Processing Group
University of Geneva
Switzerland

September 2018

UNIVERSITÉ DE GENÈVE

SIP stochastic information processing

Outline

Introduction

Privacy-preserving content identification

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

Introduction

Privacy-preserving content identification

- 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

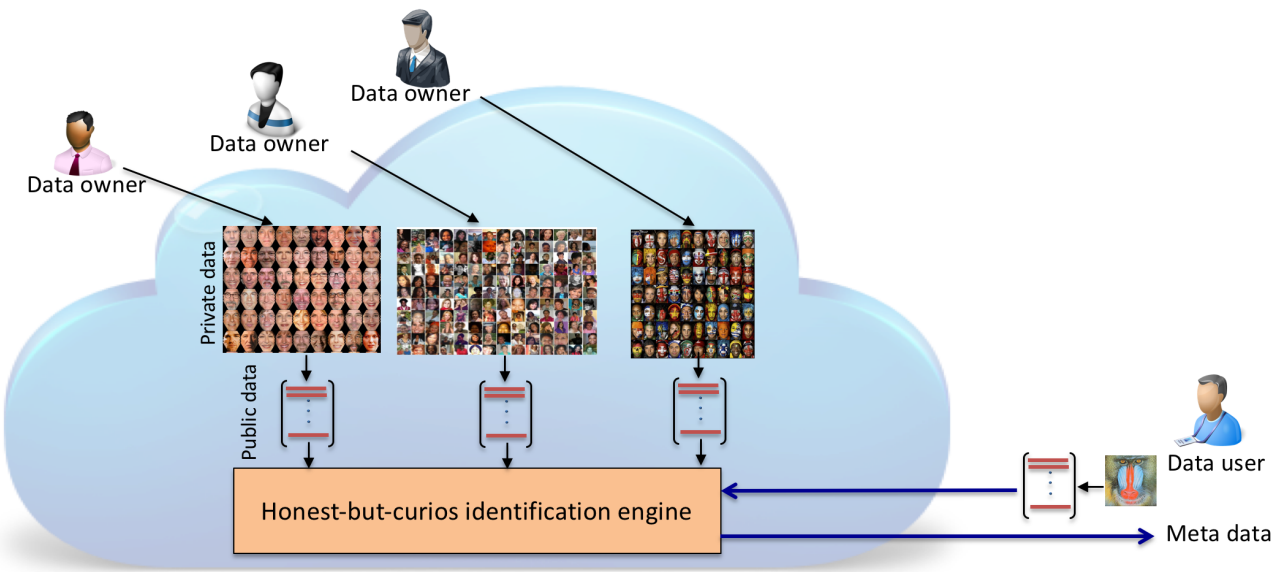
Privacy-preserving content identification

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

Recent Trends

Big Data & Distributed Applications

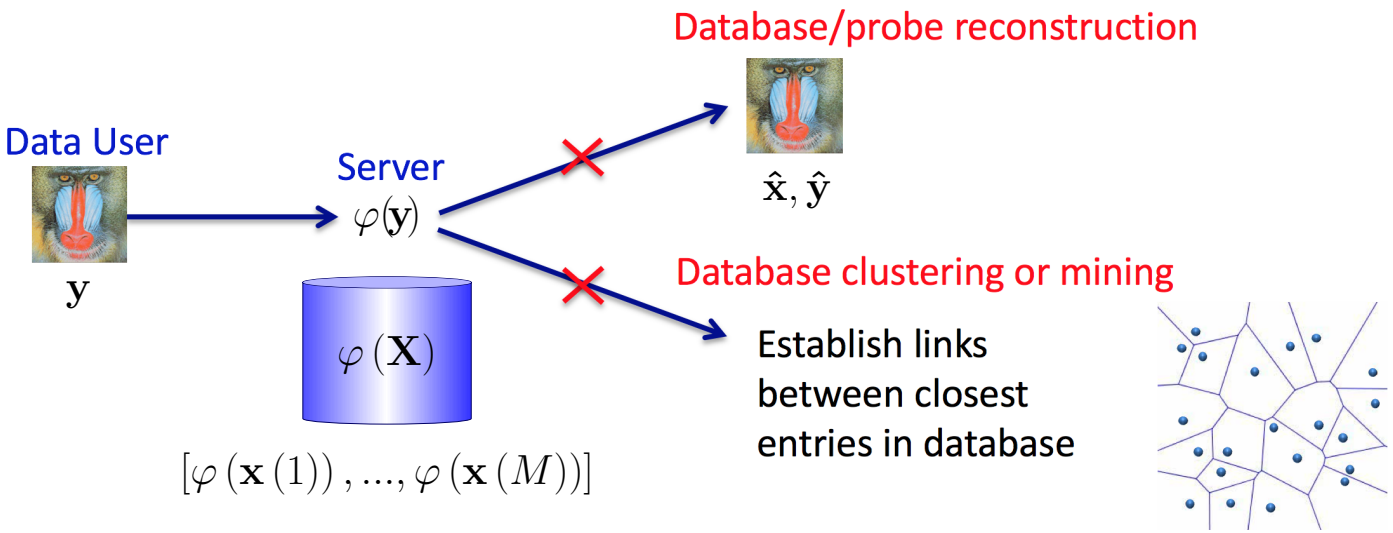
Services on outsourced cloud-based systems



Introduction

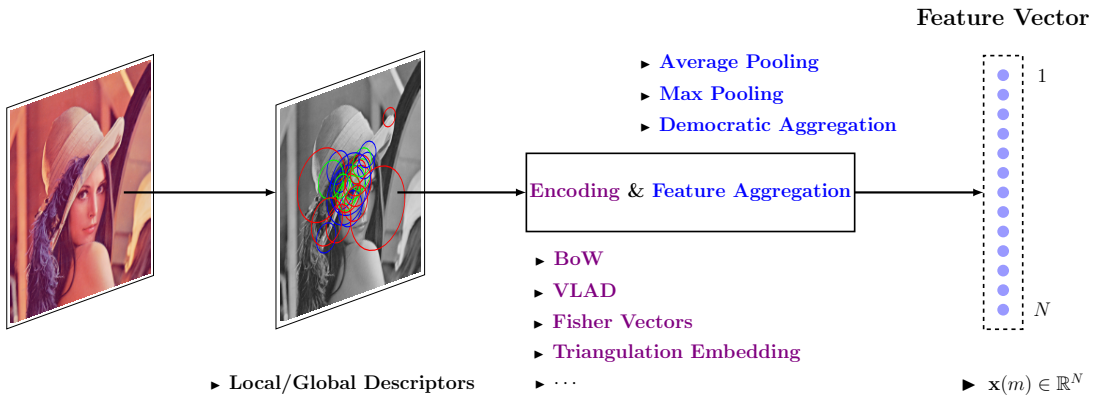
Problem Formulation

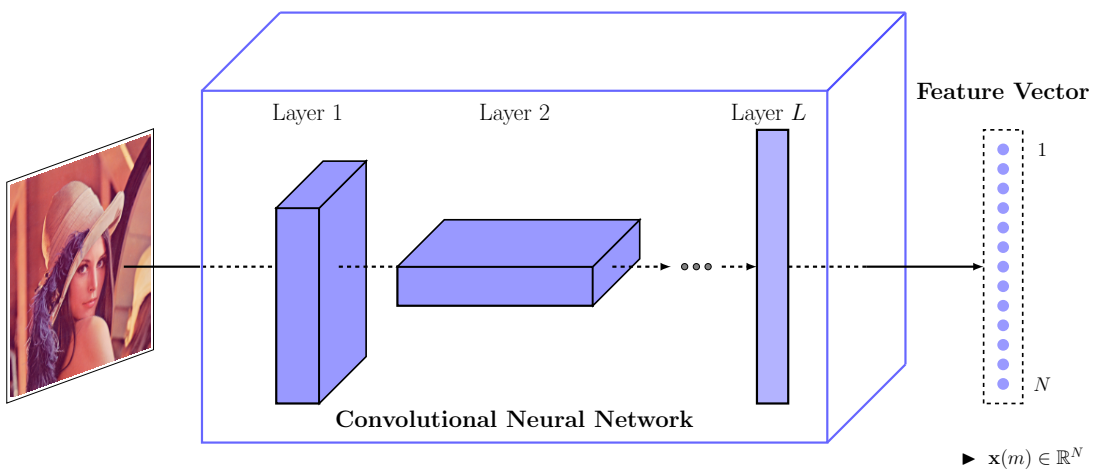
Goal of privacy protection in outsourced services



Introduction

How do we receive a feature vector?





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

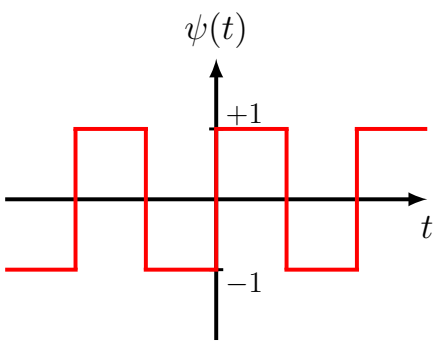
- **Cryptographic Methods - Homomorphic Encryption**
  - **Main Idea:** Similarity search in the encrypted domain
    - Brute force identification $\Longrightarrow$ huge complexity
- **Robust Hashing - a single hash from the whole content / local descriptors / last layer of CNN**
  - **Main Idea:** $\mathbf{x} \longrightarrow (011011100110)$ 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

Universal Quantization

- **Main Idea:** projection with the dimension reduction and periodic quantization
  - Binary quantization: in the region of low projected magnitudes - high P_b
  - Ambiguization due to periodization of quantizer - no possibility to recover data even for the authorized users
  - Server still can cluster data - privacy leakages
  - Information preservation in general - no link to $R(d)$ and recovery is demonstrated so far



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

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

Introduction

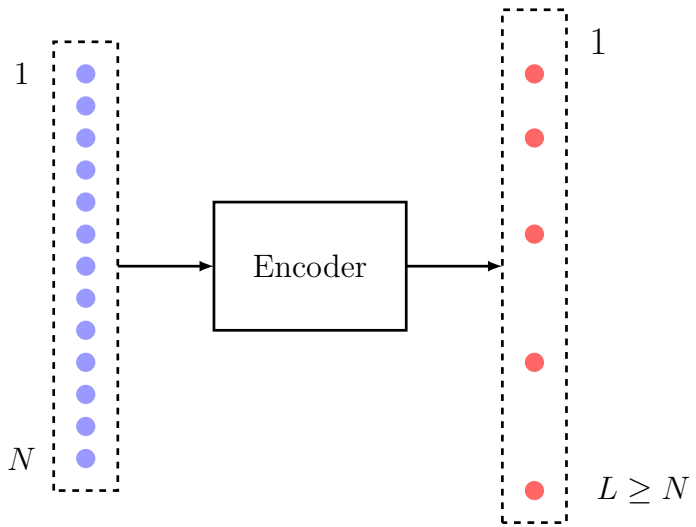
state-of-the-art

- **Sparse Approximation with Ambiguization**
- **Main Idea:** obtain an information-preserving sparse ternary representation of the data, while ensuring privacy
  - Fast search / memory efficient
  - Difficult to accurately reconstruct from probe
  - Server cannot reveal a structure of the database

Part 1:
Sparse Data Representation

Sparsification

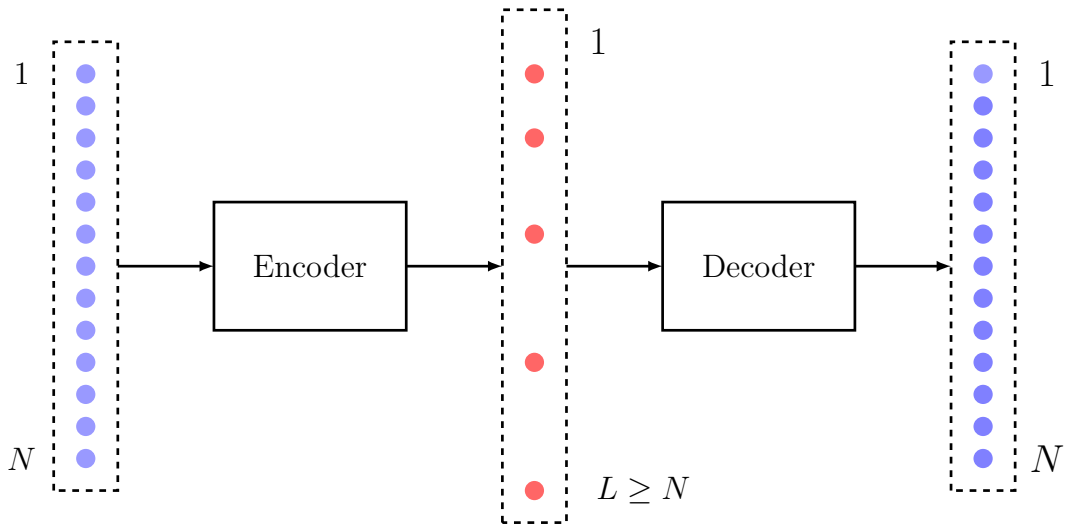
Main Idea



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

Sparsification

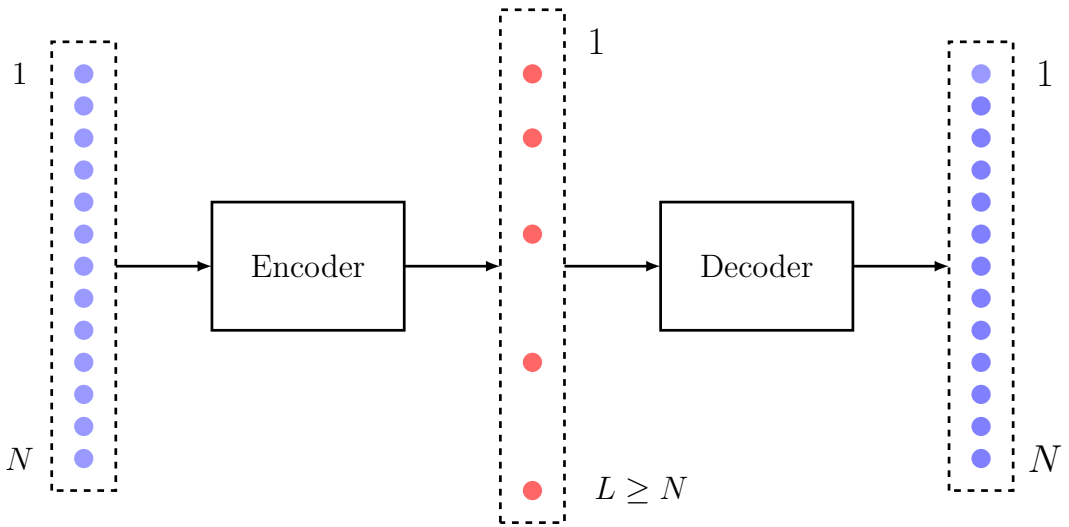
Main Idea

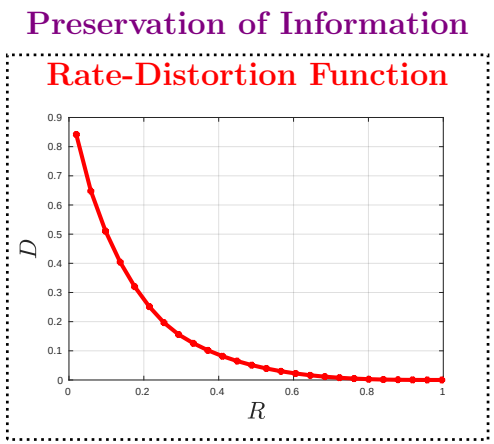


- $\mathbf{x}(m) \in \mathbb{R}^N$
- $\mathbf{x}(m) \sim p(\mathbf{x})$
- $\mathbf{u}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{u}(m)\|_0 \leq S_x$
- Rate: $R = \frac{1}{L} \log_2 \left(\binom{L}{S_x} 2^{S_x} \right)$
- $\hat{\mathbf{x}}(m) \in \mathbb{R}^N$
- Distortion : $\frac{1}{N} \|\mathbf{x}(m) - \hat{\mathbf{x}}(m)\|_2^2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

Sparsification

Main Idea



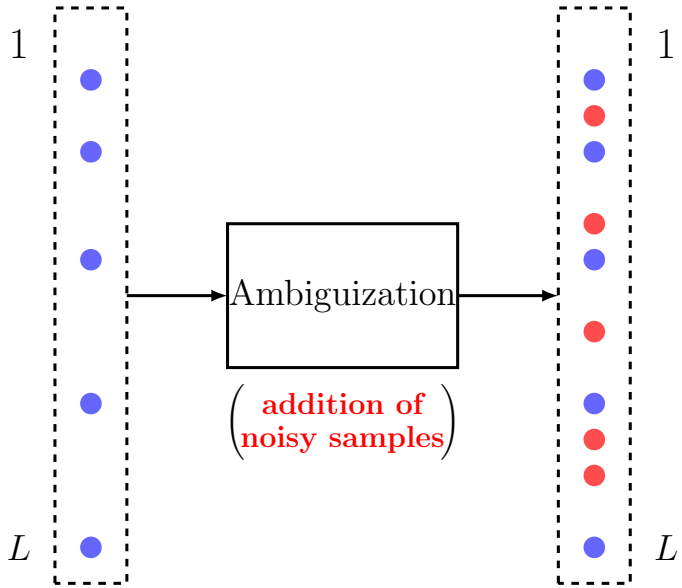


- $\mathbf{x}(m) \in \mathbb{R}^N$
- $\mathbf{x}(m) \sim p(\mathbf{x})$
- $\mathbf{u}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{u}(m)\|_0 \leq S_x$
- Rate: $R = \frac{1}{L} \log_2 \left(\binom{L}{S_x} 2^{S_x} \right)$
- $\hat{\mathbf{x}}(m) \in \mathbb{R}^N$
- Distortion : $\frac{1}{N} \|\mathbf{x}(m) - \hat{\mathbf{x}}(m)\|_2^2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

Part 2:
Ambiguization

Ambiguization

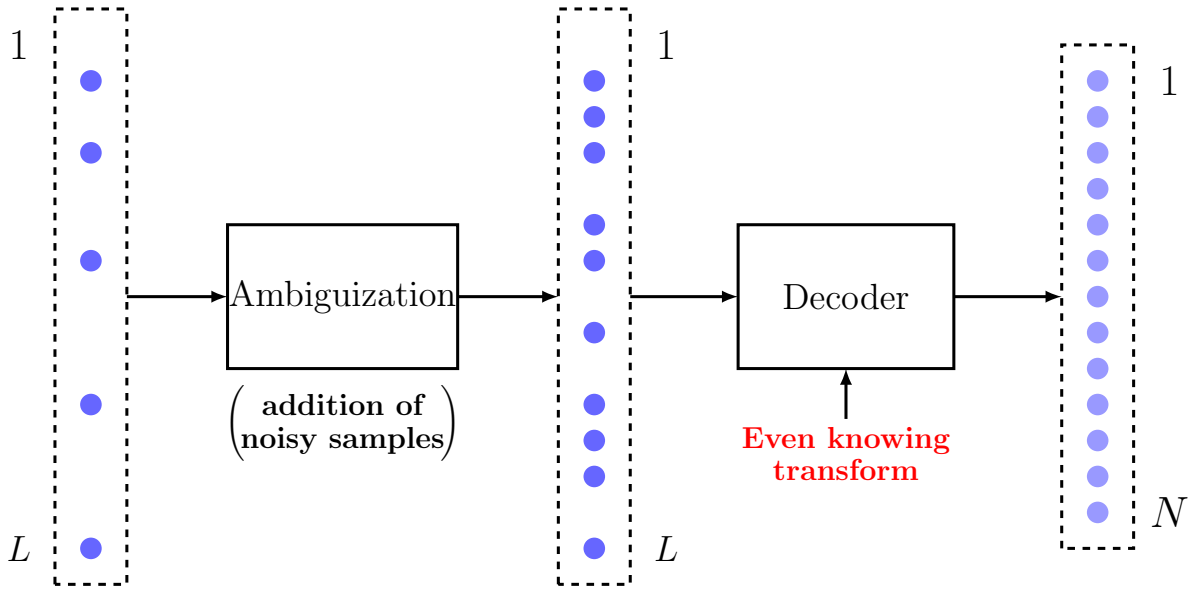
Main Idea



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

Ambiguization

Main Idea



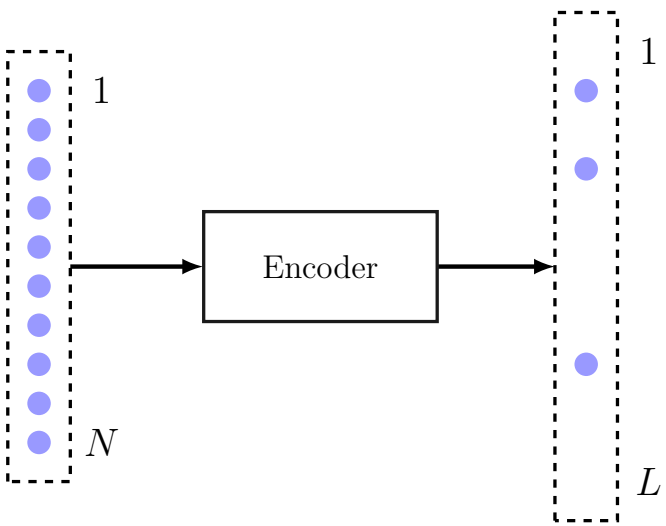
- $\mathbf{u}(m) \in \{-1, 0, +1\}^L$
- $\|\mathbf{u}(m)\|_0 \leq S_x$
- **Public Domain**
- $\mathbf{u}(m) \bigoplus \mathbf{n}$
- $\hat{\mathbf{x}}(m) \in \mathbb{R}^N$
- $\|\mathbf{x}(m) - \hat{\mathbf{x}}(m)\|_2^2 \to \simeq 2N\sigma_{\mathbf{x}}^2$

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

Part 3:
Privacy-Preserving Identification

Privacy-Preserving Identification: Search Scheme I

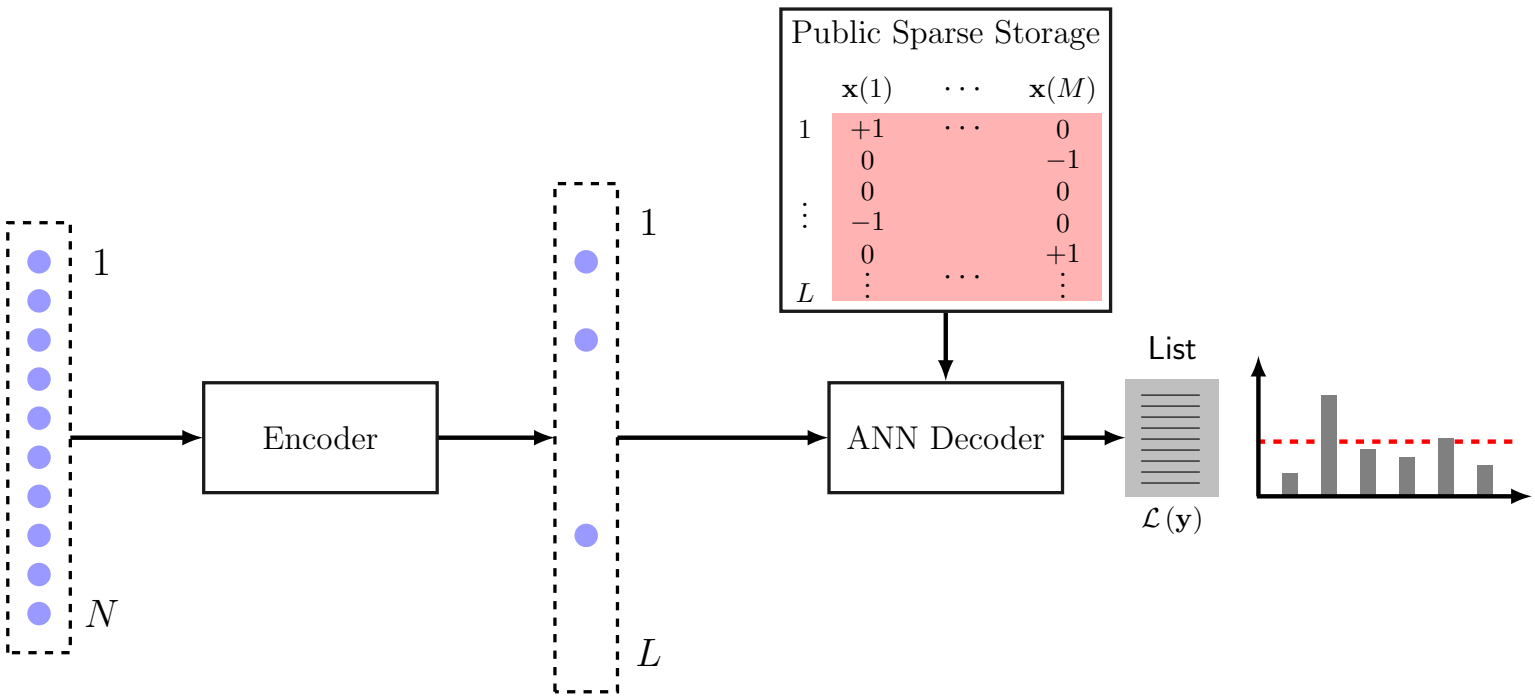
Main Idea: User discloses his probe completely



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

Privacy-Preserving Identification: Search Scheme I

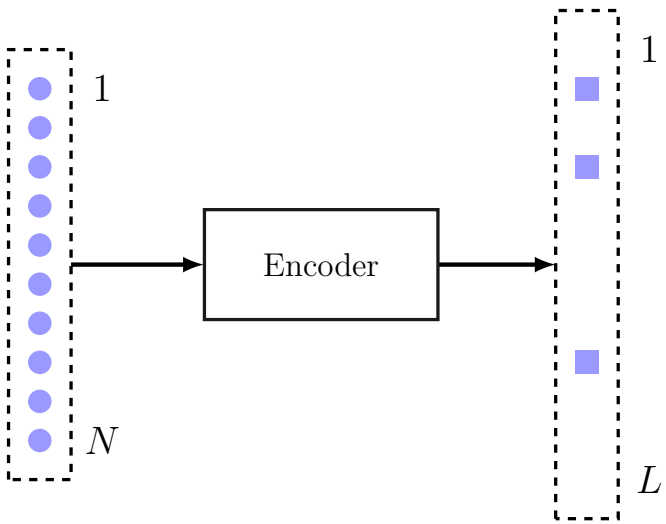
Main Idea: User discloses his probe completely



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

Privacy-Preserving Identification: Search Scheme II

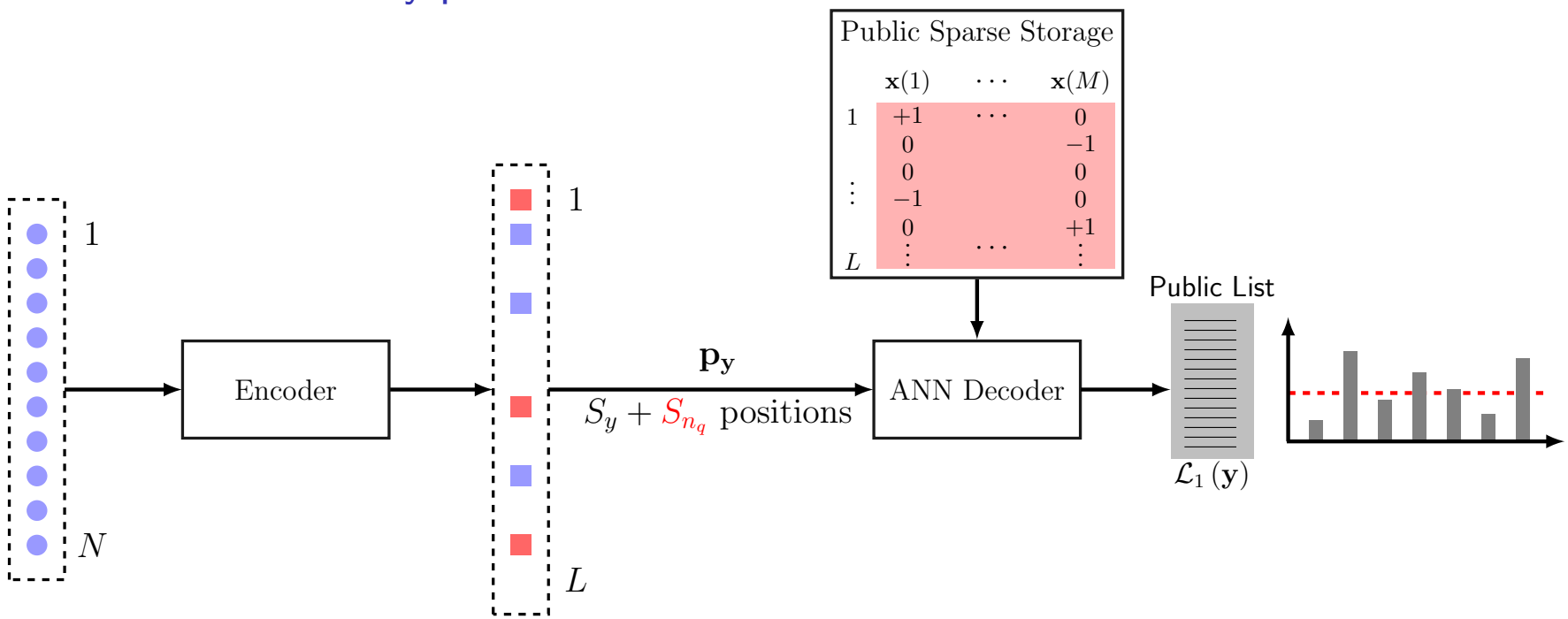
Main Idea: User sends only positions of interest



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

Privacy-Preserving Identification: Search Scheme II

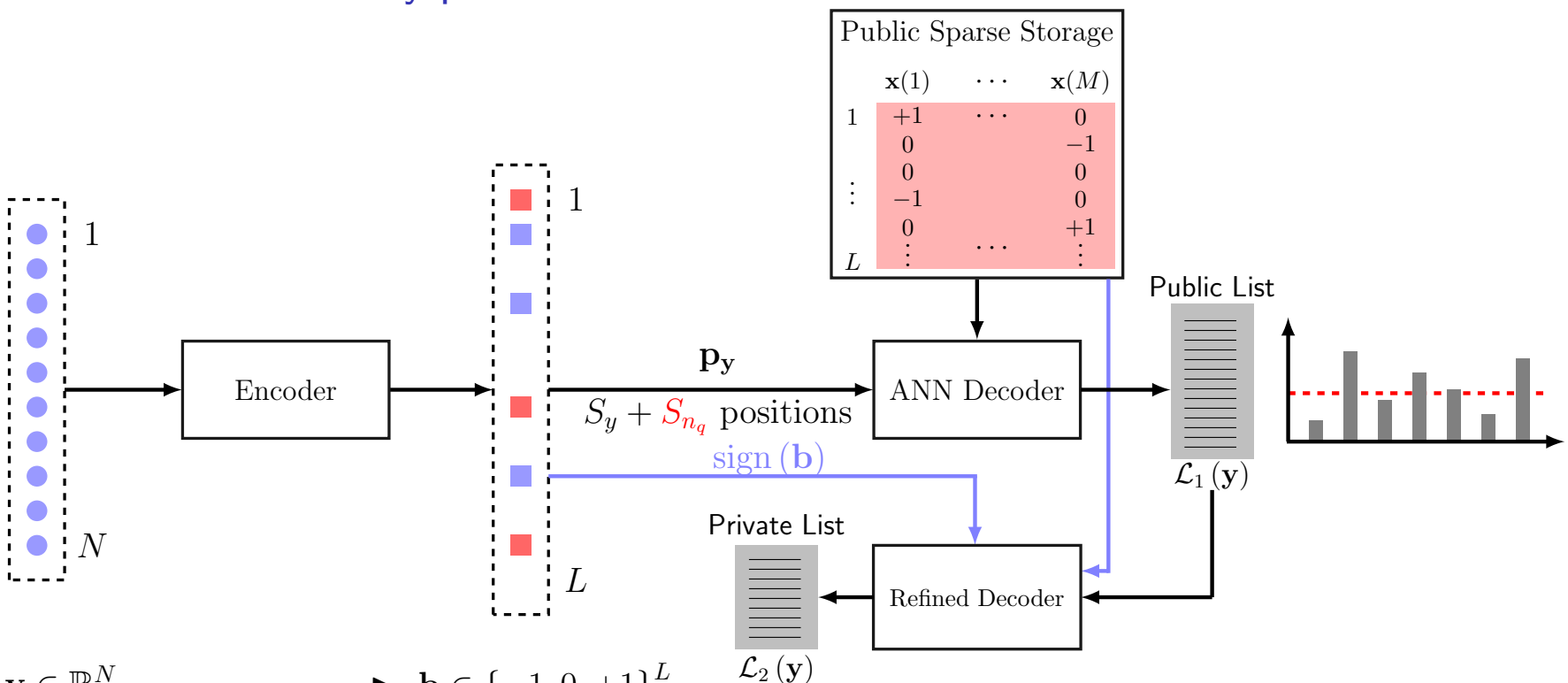
Main Idea: User sends only positions of interest



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

Privacy-Preserving Identification: Search Scheme II

Main Idea: User sends only positions of interest



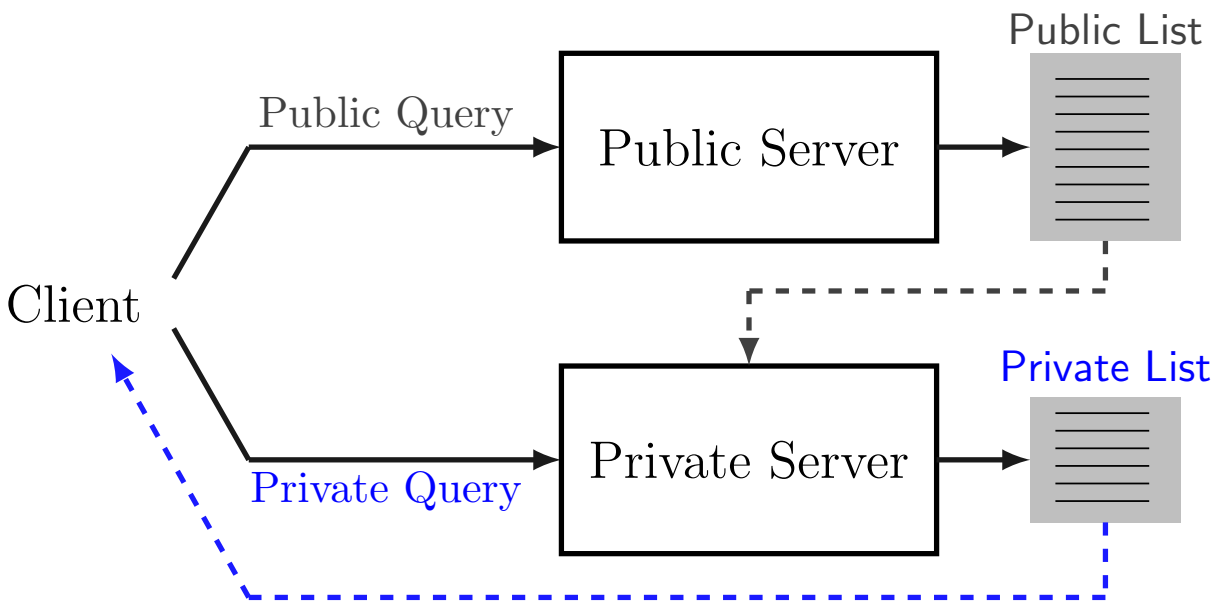
- $\mathbf{y} \in \mathbb{R}^N$
- $\mathbf{b} \in \{-1, 0, +1\}^L$
- $\|\mathbf{b}\|_0 \leq S_y$
- Add S_{n_q} random positions

Proposed Framework Overview

Types of Decoders

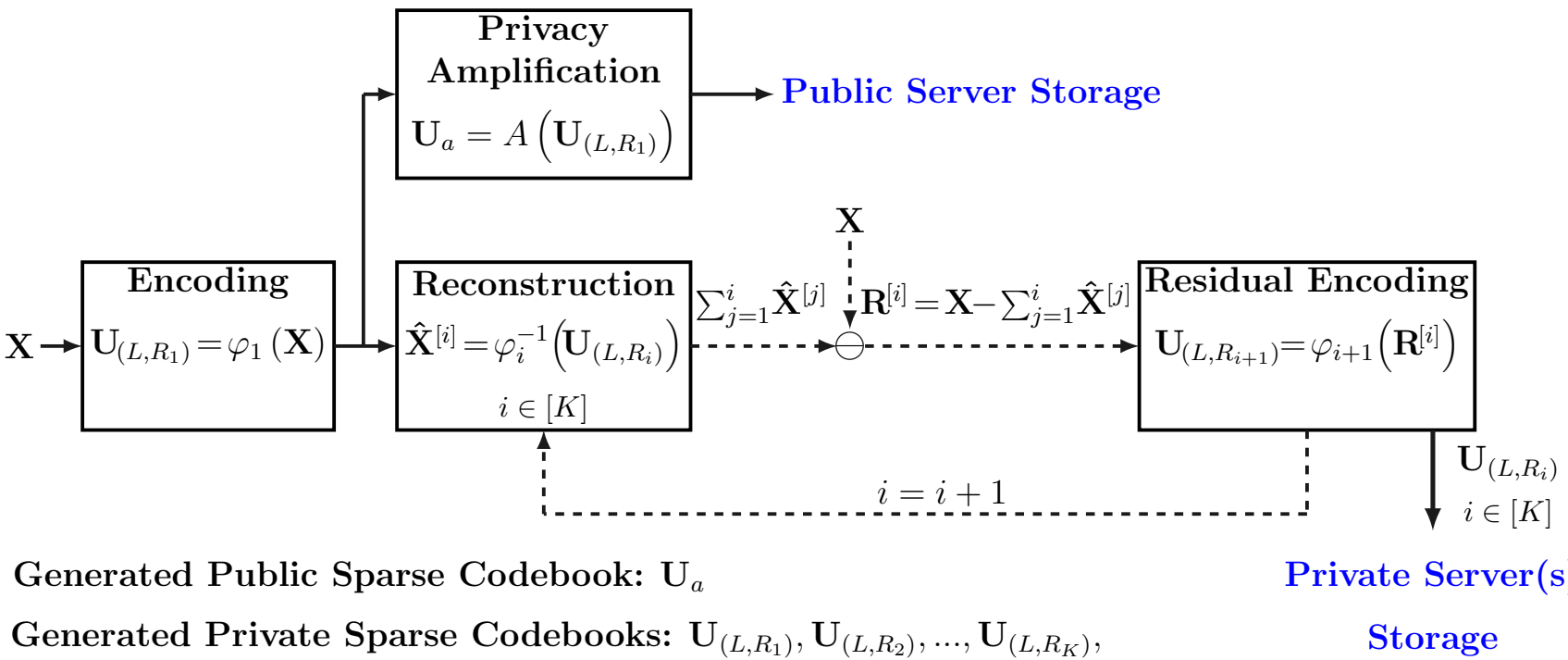
- **Type I:** search in the quantized $\mathbf{x}$ and quantized $\mathbf{y}$
- **Type II:** search is based on real $\mathbf{y}$ and reconstructed $\mathbf{x}$ (just from one stage using simple pseudo-inverse of quantized $\mathbf{x}$)
- **Type III:** search is based on real $\mathbf{y}$ and successively reconstructed $\mathbf{x}$ (from multiple stages as $\hat{\mathbf{x}}^{[1]} + \cdots + \hat{\mathbf{x}}^{[K]}$) - *that what we propose here*.

General block diagram of the proposed framework



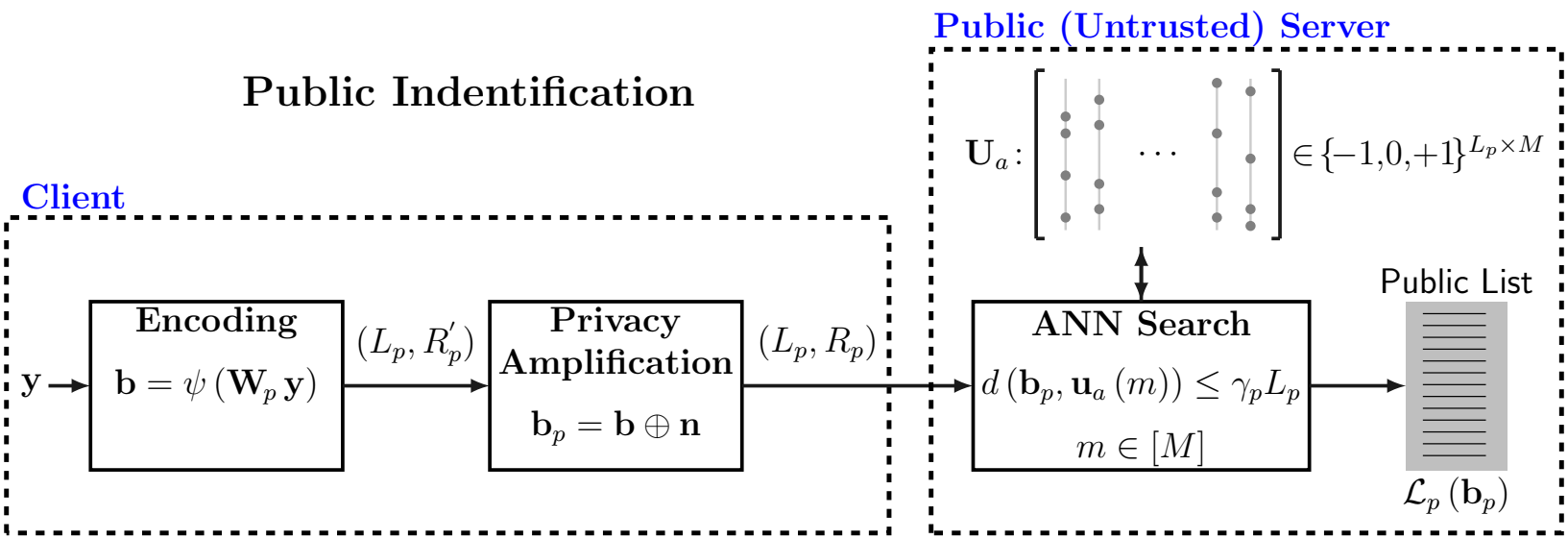
Successive Sparse Codebooks Generation Scheme

Proposed solution



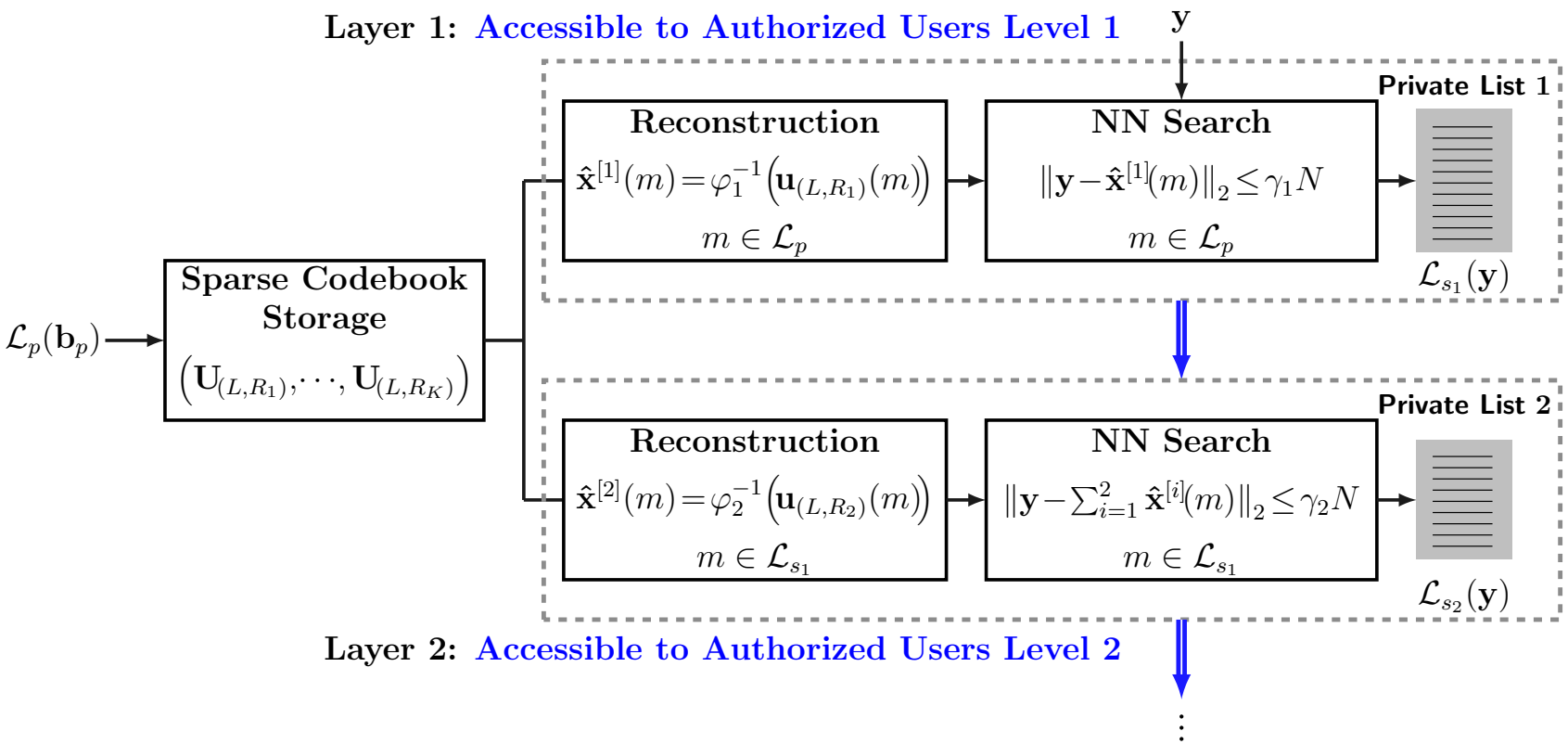
Public Identification Scheme

Proposed solution



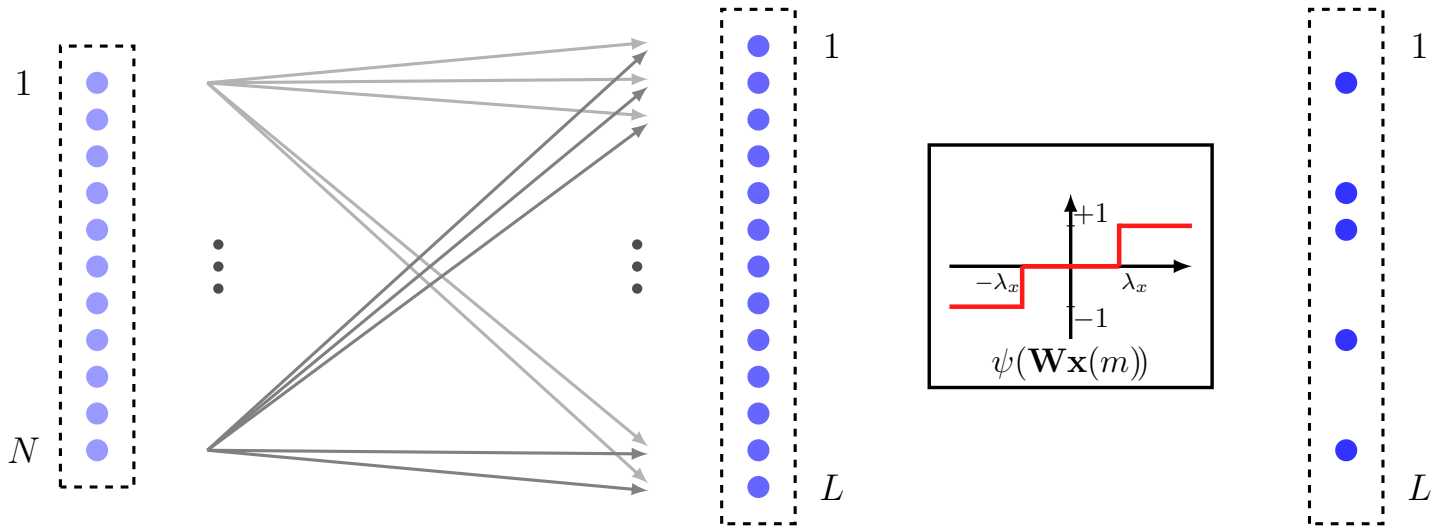
Private Multiple-access Identification Scheme

Proposed solution



Sparsifying Transform

A Schematic Idea



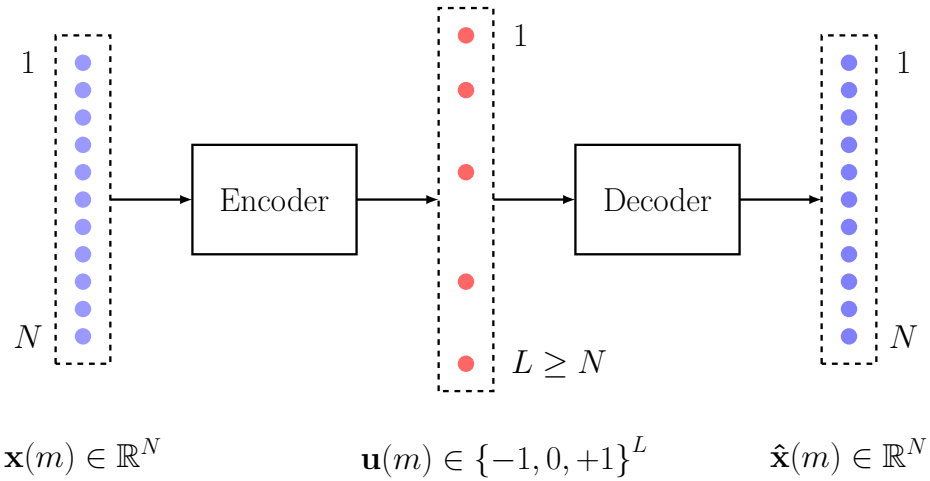
Linear Mapping Element-wise Non-linearity

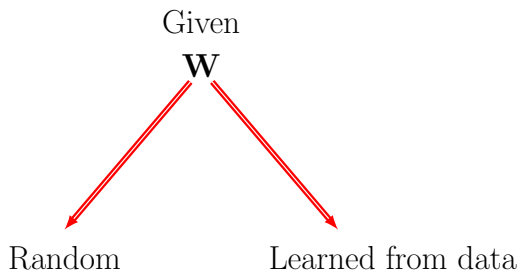
$$\mathbf{x}(m) \in \mathbb{R}^N \xrightarrow{\mathbf{W}} \mathbf{W}\mathbf{x}(m) \in \mathbb{R}^L \xrightarrow{\psi(.)} \mathbf{u}(m) \in \{-1, 0, +1\}^L$$

$$\varphi(.)$$

Sparsifying Transform

General Problem Formulation





- **Encoder:**

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

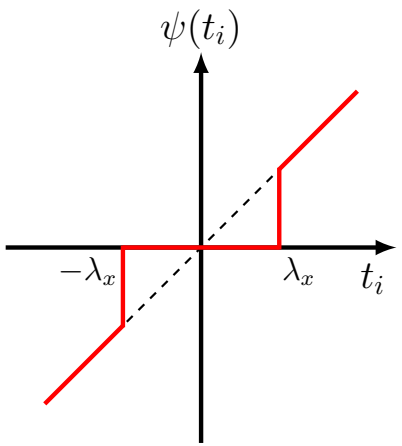
- **Decoder:**

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

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

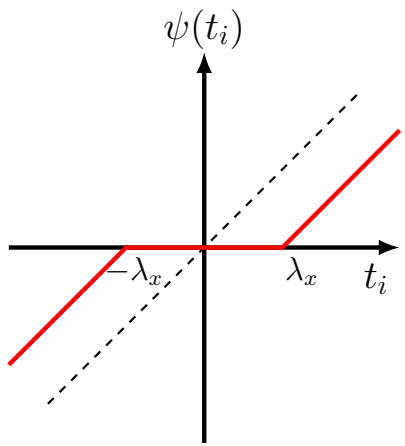
$$\widehat{\mathbf{a}}(m) = \underset{\mathbf{a}(m)\in\mathcal{A}^L}{\arg\min} \|\mathbf{W}\mathbf{x}(m) - \mathbf{a}(m)\|_2^2 + \beta\Omega\left(\mathbf{a}(m)\right), \forall m \in [M]$$

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



Hard-thresholding operator

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



Soft-thresholding operator

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

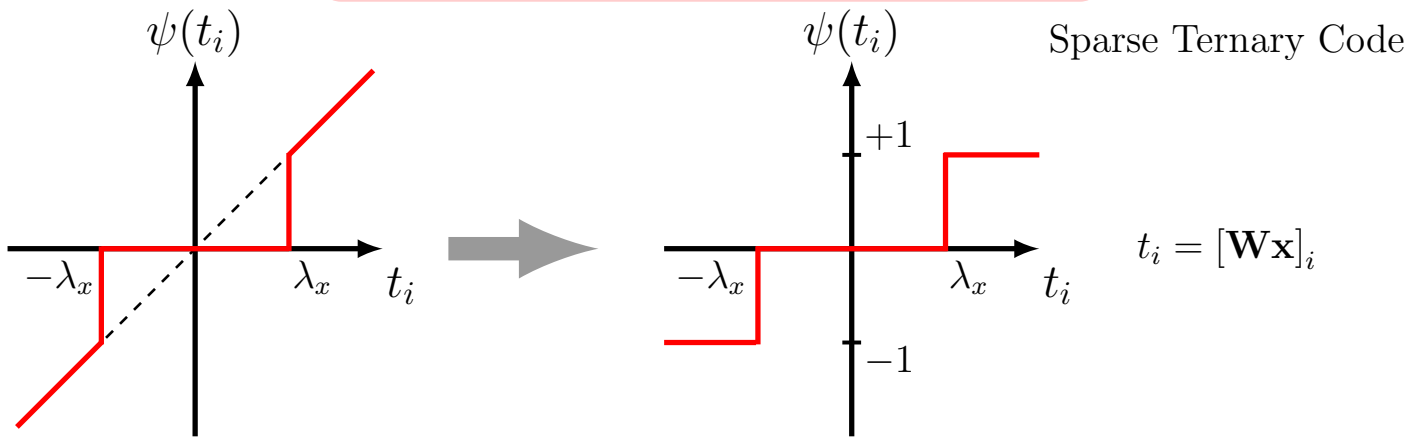
$$t_i = [\mathbf{W}\mathbf{x}]_i$$

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

Encoder: Extra constraint on the alphabet

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

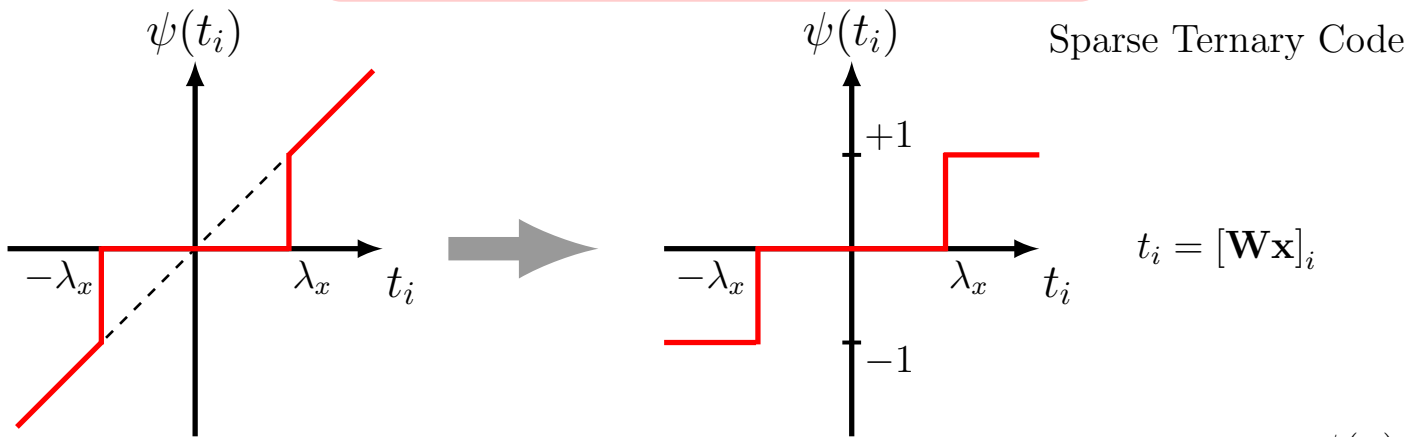
$$\text{s.t.} \qquad \mathbf{u}(m) \in \{-1, 0, +1\}$$



Encoder: Extra constraint on the alphabet

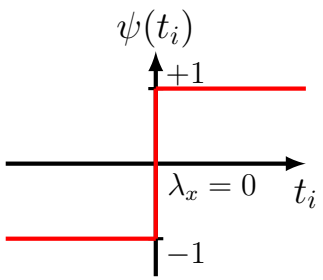
$$\hat{\mathbf{u}}(m) = \psi(\mathbf{W}\mathbf{x}(m))$$

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



Remark:

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

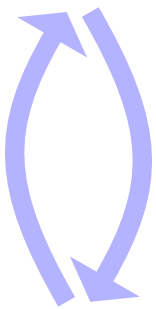


Learning Sparsifying Transform

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 $\mathbf{A}$):

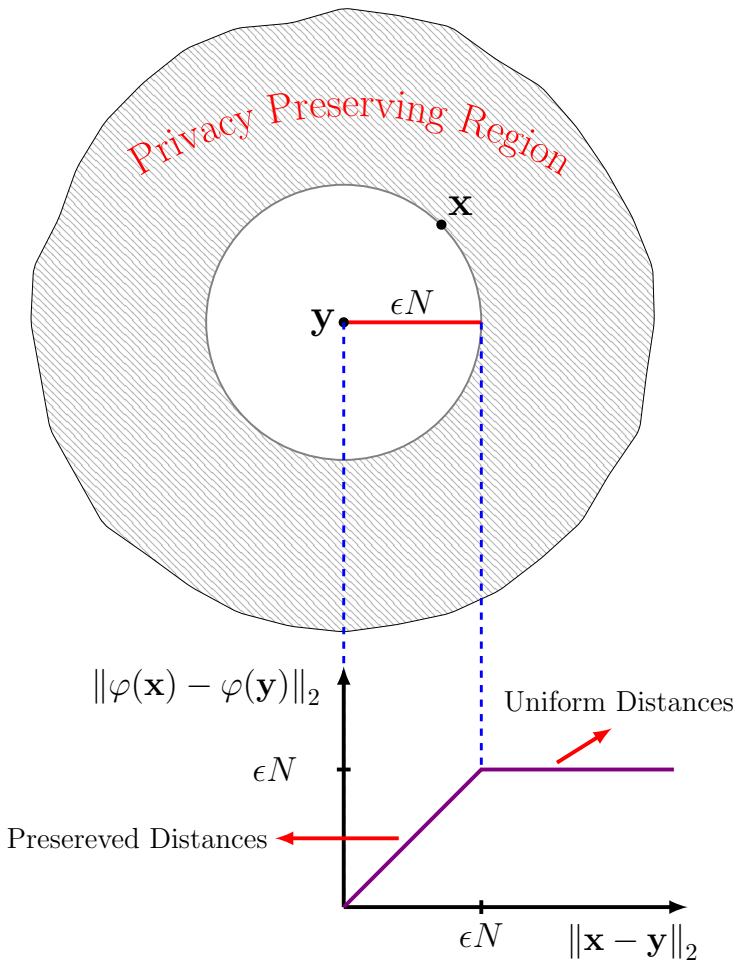
$$\hat{\mathbf{W}} = \arg\min_{\mathbf{W}} \|\mathbf{WX} - \mathbf{A}\|_F^2 + \beta_W \Omega_W(\mathbf{W})$$

Linear Regression :
(with quadratic regularizer)

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

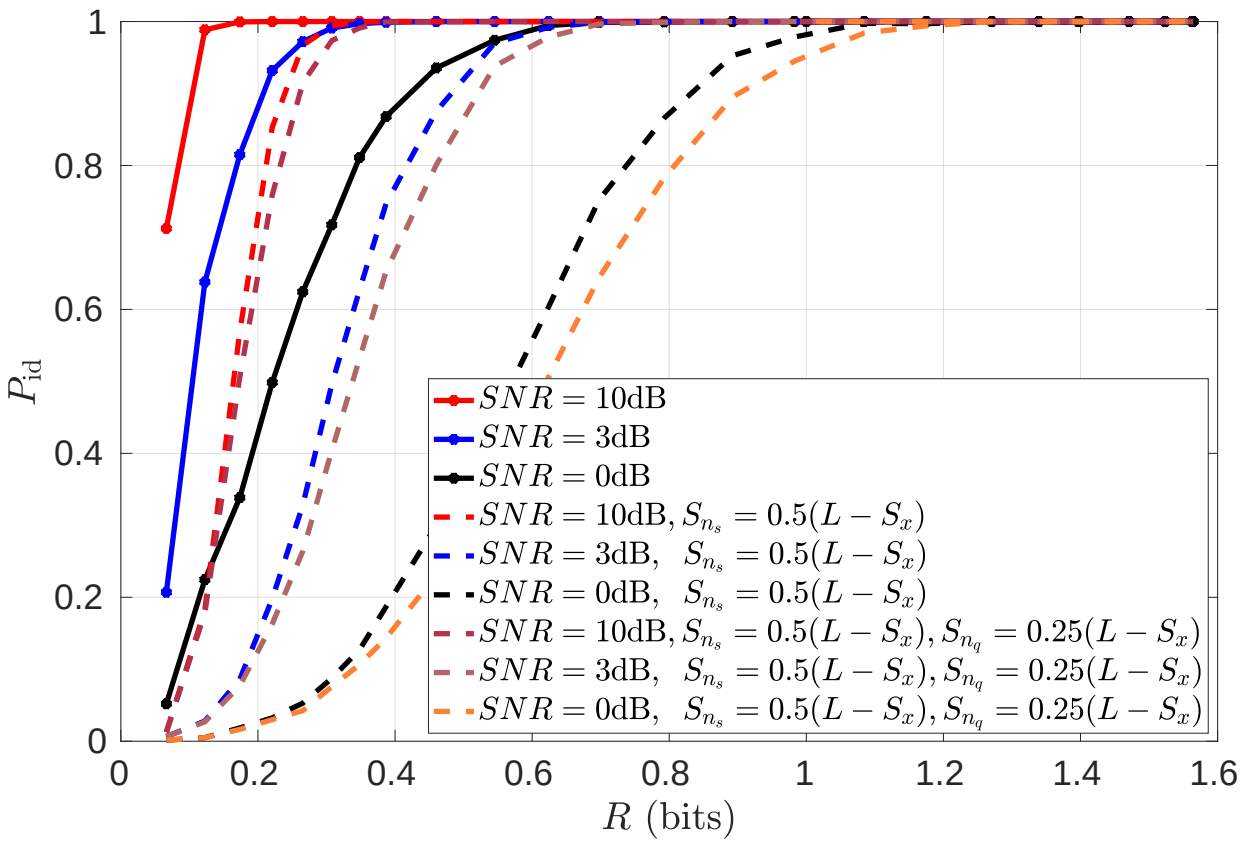
Desired property of mapping scheme

Distance preservation in the desired radius



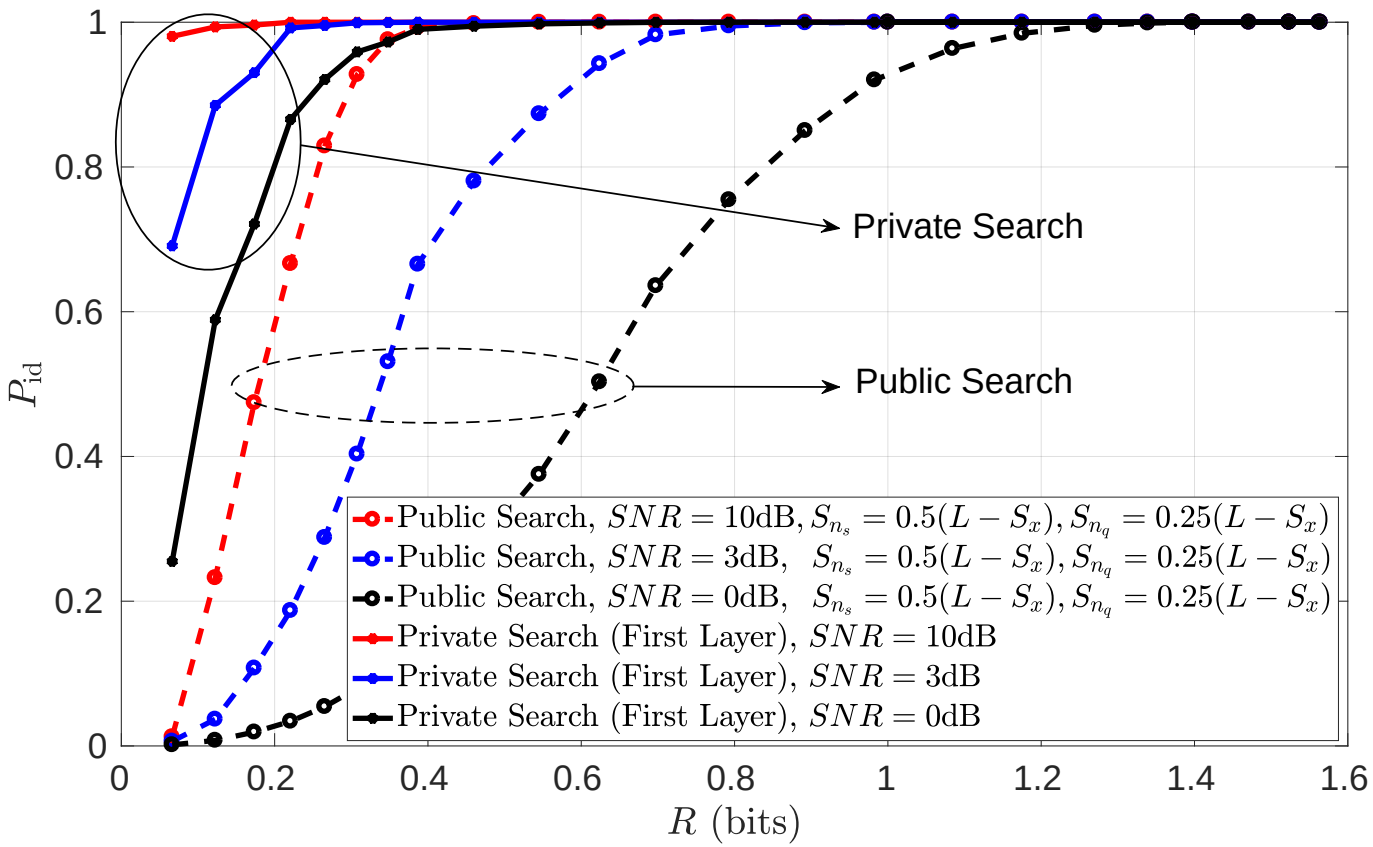
Probability of Correct Identification

Relation between probability of correct identification and encoding rate:



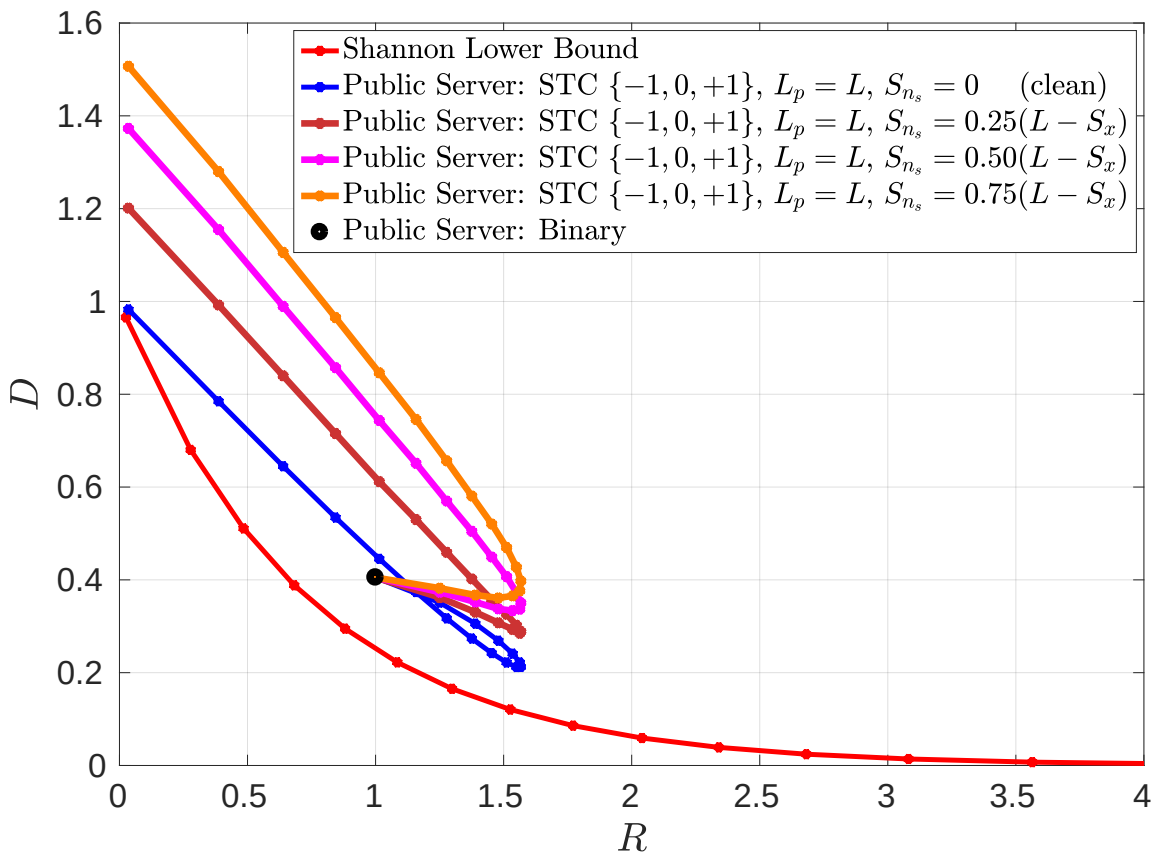
Probability of Correct Identification

Comparison between the probability of correct identification at the public server and private server:



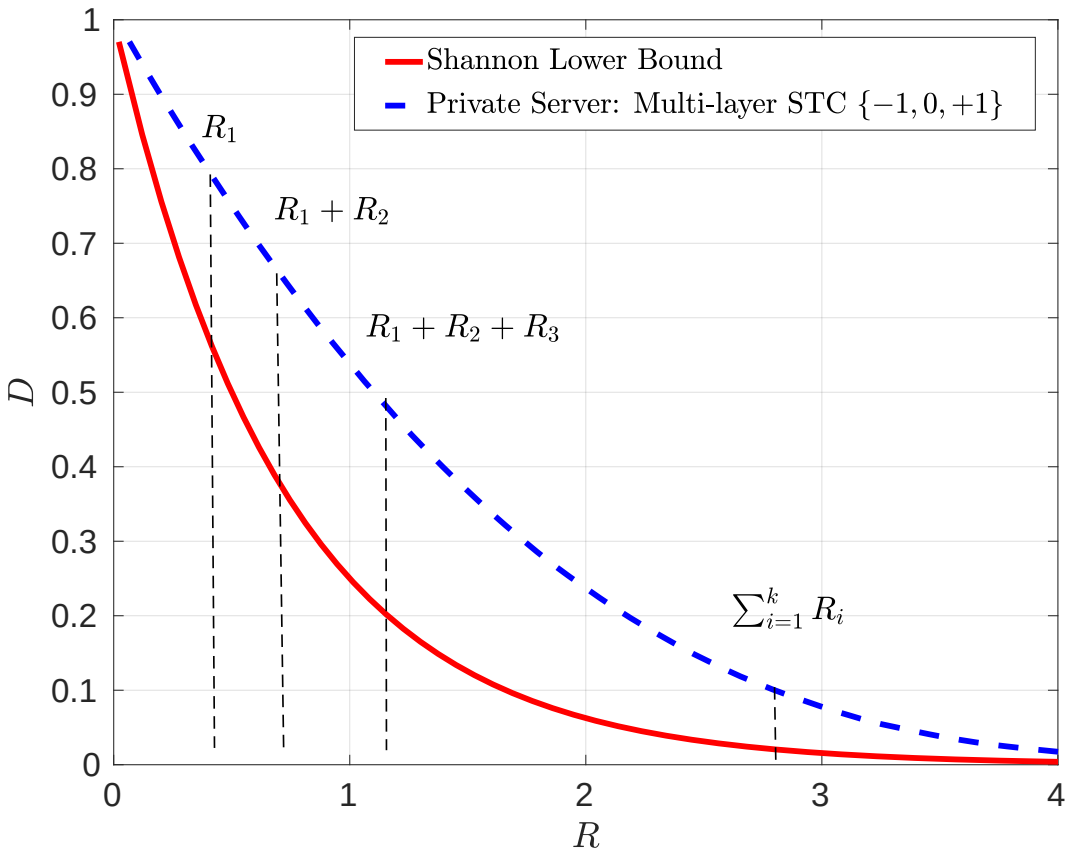
Information Loss

Distortion-rate behavior at the **public server**:



Information Loss

Distortion-rate behavior at the **private server**:



Conclusions:

- Fast search is performed on the public server
- Refined searches are performed on the distributed private server(s)
- Distributed security
- Accuracy of the private search is based on the authorization level of the clients


Thank You!