Numerical Estimation of Spatial Distributions under Differential Privacy

Leilei Du [1], Peng Cheng [1], Libin Zheng [2], Xiang Lian [3], Lei Chen [4,5], Wei Xi [6], Wangze Ni [7*]
[1]*East China Normal University, China;* [2]*Sun Yat-sen University, China;* [3]*Kent State University, USA;*
[4]*HKUST (GZ), China;* [5]*HKUST, China;* [6]*Xi'an Jiaotong University, China;* [7]*Zhejiang University, China*
leileidu@stu.ecnu.edu.cn; pcheng@sei.ecnu.edu.cn; zhenglb6@mail.sysu.edu.cn; xlian@kent.edu; leichen@cse.ust.hk;
xiwei@xjtu.edu.cn; niwangze@zju.edu.cn

***Abstract*—Estimating spatial distributions is important in data analysis, such as traffic flow forecasting and epidemic prevention. To achieve accurate spatial distribution estimation, the analysis needs to collect sufficient user data. However, collecting data directly from individuals could compromise their privacy. Most previous works focused on private distribution estimation for one-dimensional data, which does not consider spatial data relation and leads to poor accuracy for spatial distribution estimation. In this paper, we address the problem of private spatial distribution estimation, where we collect spatial data from individuals and aim to minimize the distance between the actual distribution and estimated one under Local Differential Privacy (LDP). To leverage the numerical nature of the domain, we project spatial data and its relationships onto a one-dimensional distribution. We then use this projection to estimate the overall spatial distribution. Specifically, we propose a reporting mechanism called Disk Area Mechanism (DAM), which projects the spatial domain onto a line and optimizes the estimation using the sliced Wasserstein distance. Through extensive experiments, we show the effectiveness of our DAM approach on both real and synthetic data sets, compared with the state-of-the-art methods, such as Multi-dimensional Square Wave Mechanism (MDSW) and Subset Exponential Mechanism with Geo-I (SEM-Geo-I). Our results show that our DAM always performs better than MDSW and is better than SEM-Geo-I when the data granularity is fine enough.**

I. Introduction

With the popularity of smart devices and the high quality of wireless networks, people can easily access the Internet and communicate with online services. Convenient online service platforms, such as ride-hailing apps, collect user data, analyze it, and provide better services in return. For example, collecting vehicle locations and analyzing traffic flow can help ride-hailing drivers avoid traffic jams. However, directly collecting data could compromise individuals' privacy, leading to users refusing to share their information. In traffic flow forecasting, if a driver submits his/her locations to the platform over a period (e.g., a month), a malicious platform attacker could predict the driver's activity range and surveil him/her.

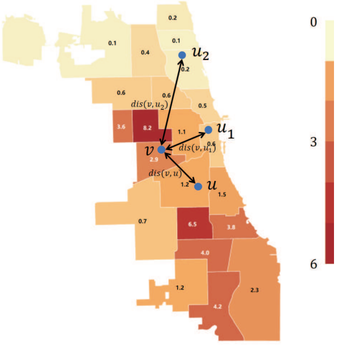


Fig. 1: shooting victims per 1,000 residents of Chicago in 2021

Differential Privacy (DP) [1] is a privacy standard that resolves conflicts between data privacy and data analysis with the aid of a trusted server. To further avoid information leakage on the trust server, a method for DP in a local setting, called Local Differential Privacy (LDP), has been proposed recently [2]. In LDP, there are multiple *users* and one *analyst*. First, all users randomize their actual information (to protect their privacy) themselves and send it to the analyst. Then, the analyst estimates the users' distribution based on the randomized information. These two steps by the users and analyst are encapsulated as Frequency Oracle [3] (FO) for count queries under LDP. As an efficient tool, FO has been widely used to resolve distribution estimation under LDP [3], [4], [5], [6], [7] and various private query issues, such as private range queries [8], [9], [10], [8], [11].

Traditional FO performs well for estimating categorical data distribution (i.e., data without order) [6]. Similar to existing studies [3], [7], [12], we can directly dividing the spatial area into unrelated grids and apply traditional FO to estimate the spatial distribution. However, in the spatial (2-Dim) context, there is a strong ordinal relationship between any pair of data points. For example, a heavily congested traffic junction is more likely to cause blockages at nearby junctions than those farther away. Similarly, a COVID-19 affected area is more likely to lead to outbreaks in surrounding areas than in distant ones. Therefore, if we use traditional FO, the ordinal relationship in the domain may be ignored, which may lead to poor estimation accuracy [6].

In this paper, we study the problem of private spatial distribution estimation, in which each user publishes their data under LDP, and the analyst estimates the distribution of these users to minimize the difference between the actual and recovered density distributions. To illustrate the motivation for this problem, we consider the following example:

Example 1. *As shown in Figure 1, an analyst wants to*

[*] Wangze Ni is also with The State Key Laboratory of Blockchain and Data Security; Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security.

estimate the shooting distribution in Chicago. To do this, the analyst needs to collect shooting points in this area and count the number of points at each location. In order to protect the actual shooting locations and maintain social stability, the police use an LDP mechanism to randomize the locations and send these randomized locations to the analyst. After collecting all randomized locations, the analyst can estimate the shooting distribution of Chicago.

Take point v as a shooting instance. Given another shooting instance point u, we denote the distance between v and u as $dis(v, u)$. If we regard locations as categorical points, according to traditional FO (i.e., Categorical Frequency Oracle (CFO) [6]), v will be published as u_1 or u_2 with the same low probability. This method neglects the location ordinal relationship among the nodes (i.e., $dis(v, u_1) < dis(v, u_2)$). In this way, it is both dangerous for the citizens of Chicago (the shooter can easily move to u_1 rather than u_2) and leads to poor estimation accuracy for shooting distribution. Considering the location ordinal relationship, u_1 is closer to v than u_2. Thus, for v's randomized points, the probability of choosing u_1 should be higher than that of u_2.

Many studies use mean absolute error, variances or Kullback-Leibler (KL) Divergence [13] as metrics for distribution estimation [6]. However, none of these metrics effectively capture the ordinal relationship. In this paper, we use the common-used 2-Dim Wasserstein distance [14] to measure the difference between two distributions while capturing the spatial ordinal relationship. Based on 2-Dim Wasserstein distance, we propose a general spatial distribution estimation mechanism called *Spatial Area Mechanism* (SAM), which achieves ϵ-LDP. Additionally, we introduce a simple implementation mechanism of Spatial Area Mechanism called *Hybrid Uniform-Exponential Mechanism* (HUEM). To optimize SAM, we need the close forms of 2-Dim Wasserstein Distance. However, except for the 2-Dim normal (Gaussian) distribution, there are no closed forms for 2-Dim Wasserstein distance when the data dimension is greater than 1 [14], making it difficult to optimize the estimation utility. A direct method is to optimize each dimension estimation according to the 1-Dim Wasserstein distance and then combine them (MSW [10]). However, this approach loses the spatial ordinal relationship. To address this problem, we use the Radon Transform [15] to project spatial data onto one-dimensional (1-Dim) data and transform the 2-Dim Wasserstein distance into the Sliced Wasserstein distance [16]. Based on the sliced Wasserstein distance metric, we propose *Disk Area Mechanism* (DAM) and prove that it is optimal among all types of SAM. To implement our DAM on real data (discretized domain), we design a *grid partition and shrinkage* method to effectively bucketize the data. Our DAM achieves a lower 2-Dim Wasserstein distance (between the recovered and actual density distributions) than the state-of-the-art Multi-dimensional Square Wave Mechanism (MDSW) [10] and the categorical Subset Exponential Mechanism with Geo-I (SEM-Geo-I) [12]. The contributions of this paper are as follows:

TABLE I: The summary of related studies.

classified name	**mechanism name**	**catch numeric**	**meet SDP**	**locally**
central privacy	PSD+Geocast [18]	×	√	×
local privacy	ID-LDP [19]	×	√	√
	Geo-I [20]	2-Dim	√	√
categoric	Bucket+CFO [3], [7]	×	√	√
numeric	SEM-Geo-I [12]	2-Dim	√	√
	SR [4]	1-Dim	×	√
	PM [5]	1-Dim	×	√
one-dimensional	SW-EMS [6]	1-Dim	×	√
multi-dimensional	PSD [21]	×	√	×
	AG [22]	×	√	×
	HIO [9]	×	√	√
	AHEAD [8]	×	√	√
	MSW, HDG [10]	1-Dim	√	√
\	**Our mechanism**	2-Dim	√	√

- We formally define our Private Spatial Distribution Estimation Problem (PSDEP) in Section III and propose a mechanism structure called Spatial Area Mechanism (SAM) and a direct baseline method called Hybrid Uniform-Exponential Mechanism (HUEM) in Section IV.
- We propose Disk Area Mechanism (DAM) and analyze how to choose the best norm distance b in Section V.
- We introduce the implementation of our DAM including grid partitioning, shrinkage and post-process in Section VI.
- We unify local differential privacy mechanisms (e.g., DAM) and Geo-I mechanisms (e.g., SEM-Geo-I [12]) by the *local privacy mechanism* [17] and conduct experimental evaluations of our proposed method on both real and synthetic datasets to demonstrate its efficiency and effectiveness in Section VII.

II. Related Work

The privacy protection is an important issue in spatial data statistics. It requires obtaining accurate statistical results while protecting individuals' information from being released. Differential privacy [1] is a key tool for privacy protection and privacy-preserving data release. We classify related work based on differential privacy into three dimensions and summarize it in Table I.

Central / Local Differential Privacy. Conventional differential privacy requires a trusted third party to collect individuals' data and randomize it under differential private mechanisms [18]. However, the third party may be attacked by malicious entities, hindering individuals from sharing their information. To address this issue, local differential privacy (LDP) [23], [24] is proposed, where individuals randomize their own information and then report the randomized messages to the estimator. Gu et al. [19] propose input-discriminative LDP, which can satisfy different privacy levels required by different individuals simultaneously. Andrés and Bordenabe [20] propose Geo-Indistinguishability (Geo-I), which provides high privacy within short distances and low privacy with long distances. However, both of these designs detriment the privacy of LDP.

Categorical / Numerical Frequency Oracle. To handle the issue of releasing numeric data under Local Differential Privacy (LDP), a popular method is to apply Categorical Frequency Oracle (CFO, FO) [3], [7]. The basic process is to first divide the numeric data into several buckets and then use CFO to estimate the result. However, simply dividing the data leads to information loss during comparison. Duchi et al. [4] propose Stochastic Rounding (SR) to handle numerical settings. In SR, a value v in the interval $[-1, 1]$ returns -1 with probability $\frac{1}{2} - \frac{e^{\epsilon}-1}{2(e^{\epsilon}+1)}v$ and 1 with probability $\frac{1}{2} + \frac{e^{\epsilon}-1}{2(e^{\epsilon}+1)}v$. Wang et al. [5] propose the Piecewise mechanism (PM), where the input domain is $[-1, 1]$ and the output domain is $[-s, s]$, with $s = \frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1}$. Given an input point v, it returns a point in the subinterval $[\frac{e^{\epsilon/2}v-1}{e^{\epsilon/2}-1}, \frac{e^{\epsilon/2}v+1}{e^{\epsilon/2}-1}]$ with probability $\frac{e^{\epsilon/2}(e^{\epsilon/2}-1)}{2(e^{\epsilon/2}+1)}$, and the complement subinterval with probability $\frac{e^{\epsilon/2}-1}{2e^{\epsilon/2}(e^{\epsilon/2}+1)}$. Note that both SR and PM focus on the specific task of mean estimation. Li et al. [6] propose the Square Wave mechanism with Expectation Maximization Smoothing (SW-EMS) to handle numerical distribution under local differential privacy (LDP). SW-EMS is a new numeric frequency oracle that makes full use of ordinal relations to obtain much more accurate estimations without breaching privacy. However, SW-EMS only focuses on one-dimensional data, and is therefore not suitable for estimating spatial distributions (SDP). Wang et al. [12] propose the Subset Exponential Mechanism under ϵ-Geo-I constraints (SEM-Geo-I). SEM-Geo-I can achieve accurate estimation, however, it only provides strictly weaker privacy based on Geo-I.

One / Multiple Dimensional Data Estimation. Several works have been proposed for handling spatial data with traditional differential privacy. Cormode et al. [21] design a new structure called PSD, which utilizes indexing methods such as quadtrees and kd-trees to generate spatial decompositions for describing the data distribution. Similarly, Qardaji et al. [22] present an Adaptive Grid (AG) approach to release a synopsis for 2-Dim geospatial data. However, both PSD and AG require the aid of a trusted third party. Yang et al. [10] propose the Multiplied Square Wave (MSW) mechanism, which extends the SW-EMS [6] mechanism. MSW provides an accurate estimation for multi-dimensional data under Local Differential Privacy (LDP). However, it can only capture the correlation in one dimension, which leads to high error. In order to capture the correlation among different dimensions, they propose the Hybrid-Dimensional Grids (HDG) method. HDG divides the n-Dim dimensional data into 1-Dim and 2-Dim grids and use these grids to capture the correlation among different dimensions in range query. However 1-Dim grids in HDG may still destroy the correlation among different dimension data. Du et al. [8] propose the Adaptive Hierarchical Decomposition (AHEAD) method based on HIO [9] to further improve the private range query by adaptively choosing the granularity of domain composition. However HDG and AHEAD do not catch the numeric (the distance) in spatial relationship from different randomized points to the real points.

Our mechanism can not only catch the numeric relationship and accurately estimate spatial distribution estimation under LDP, but also combine with the methods of HIO, HDG and AHEAD to further improve the accuracy in private range query.

TABLE II: Notations.

Notations	Description
k-Dim	k-dimension
$\mathcal{D}$, $\mathcal{I}$	the input domain
$\tilde{\mathcal{D}}$, $\mathcal{T}$	the output domain
$\hat{\mathcal{I}}$	the inferred (estimated) domain of $\mathcal{I}$ domain
D	an input instance
$\tilde{D}, O$	an output instance instance
$\boldsymbol{v}$	a spatial data point
$\tilde{\boldsymbol{v}}$	a disturbed point of $\boldsymbol{v}$
$M_{\boldsymbol{v}}(\tilde{\boldsymbol{v}})$	the probability of randomizing $\boldsymbol{v}$ as $\tilde{\boldsymbol{v}}$
$W(\cdot)$	the wave function
W_k^p	a k dimensional Wasserstein distance with p norm cost function
$W_k(\cdot)$	the p-th root of W_k^p (i.e., $W_k(\cdot) = \sqrt[p]{W_k^p}$)
SW_k^p	a k dimensional sliced Wasserstein distance with p norm cost function
b	a high dimensional radius
L	the side length of an input instance
g	the side length of a grid cell
d	the number of cells along a side of grid length
n	the number of cells in the grid

III. Problem definition

In this section, we provide basic notations and preliminaries, distance metrics, and formal definition of our *Private Spatial Distribution Estimation Problem* (PSDEP). Table II summarizes the key notations used throughout this paper.

A. Basic Notations and Preliminaries

We use the notation $[a_1 : a_2]$ to denote an integer series from a_1 to a_2 and abbreviate $[a_1 : a_2]$ to $[a_2]$ when $a_1 = 1$. We use $x \overset{\$}{\leftarrow} X$ to indicate uniformly sampling an element x from set X. We use v to indicate a point with index (x_v, y_v) in the Plan-Rectangular coordinate system [25] and (r_v, θ_v) in the Polar coordinate system [25]. The input domain is denoted as $\mathcal{D}$, and the output domain is denoted as $\tilde{\mathcal{D}}$. We use $\|M\|_p$ to denote the p-norm of any matrix M, where $p \in \mathbb{N} \cup \{\infty\}$. We denote the inner product of matrices A_1 and A_2 as $A_1 \cdot A_2$, the element-wise product (also called Hadamard product) as $A_1 \bigodot A_2$. For example, let $A_1 = (c_{i,j})_{n\times n}$ and $A_2 = (d_{i,j})_{n\times n}$ for $1 \le i, j \le n$. Then we have $A_1 \bigodot A_2 = (c_{i,j}d_{i,j})_{n\times n}$ for $1 \le i, j \le n$. We abbreviate k-dimension as k-Dim. When $k = 2$, we also call the data as *spatial* data.

We utilize Local Differential Privacy (LDP) [2] to protect the privacy of original data locations.

Definition 1. (ϵ-Local differential privacy, ϵ-LDP [2]). An algorithm $M(\cdot) : D \to \tilde{D}$ satisfies ϵ-local differential privacy (ϵ-LDP), where $\epsilon \ge 0$ if and only if for any input values $v_1, v_2 \in D$, we have

$$\forall S \subset \tilde{D} : \Pr[M(v_1) \in S] \le e^{\epsilon} \Pr[M(v_2) \in S],$$

where $\tilde{D}$ denotes the set of all possible output of M.

Based on the Local Differential Privacy model, a standard protocol called Frequency Oracle (FO) [26] for frequency estimation has been proposed. FO is composed of two functions, namely, the *randomized reporting function $FO.T$* and the *estimation function $FO.E$*. $FO.T$ is used to randomize the raw data into a kind of randomized data, while $FO.E$ is used to estimate the raw data based on the randomized data.

B. Distance Metrics

Definition 2. (Wasserstein Distance [14]). Let $\mathcal{P}_p(\mathbb{R}^k)$ be the space of Borel probability measures on $\mathbb{R}^k$ with finite p-th moments, i.e. for all $\mu \in \mathcal{P}_p(\mathbb{R}^k)$, $\int_{\mathbb{R}^k} |x|^p < \infty$. Let $\mu_A, \mu_B \in \mathcal{P}_p(\mathbb{R}^k)$ then we define the L_k^p-Wasserstein distance as:

$$W_k^p(\mu_A, \mu_B) = \inf \left\{ \int_{\mathbb{R}^k \times \mathbb{R}^k} |x-y|^p d\pi(x,y) : \pi \in \Pi(\mu_A, \mu_B) \right\},$$

where inf is the infimum (greatest lower bound) function and $\Pi(\mu_A, \mu_B)$ is the complete set of joint distributions of μ_A and μ_B.

Wasserstein distance [14] (also called Earth Mover's distance) is a metric on probability distributions used to measure the minimal effort of probability mass from one distribution to another. It can be used to measure the similarity between two distributions.

C. PSDEP Definition

We give our problem definition in Definition 3 as follows.

Definition 3. (Private Spatial Distribution Estimation Problem, PSDEP). Given a set of ordinal spatial values $V \subseteq \mathbb{R}^2$ with χ distinct values, a privacy budget ϵ, a PSDEP is to design a frequency oracle mechanism $FO =< T, E >$ satisfying that for the actual distribution $D \in \mathbb{R}^\chi$ of V, FO outputs $\tilde{D} \in \mathbb{R}^\chi$, where $FO.T$ satisfies ϵ-LDP and the L_2^2-Wasserstein distance $W_2^2(D, \tilde{D})$ is minimized.

IV. The Hybrid Uniform-Exponential Mechanism

In this section, we first declare the definition of the input/output domain and the randomized function. Then we propose a general Spatial Area Mechanism (SAM) and prove that it satisfies ϵ-LDP. After that we introduce a direct implementation mechanism of SAM called Hybrid Uniform-Exponential Mechanism (HUEM), and analyze its accuracy.

Input/Output Domain. Without loss of generality, we define the input domain $\mathcal{D} = \{\boldsymbol{v} | x_{\boldsymbol{v}} \in [0,1], y_{\boldsymbol{v}} \in [0,1]\}$ as a square with side length 1. For any input point $\boldsymbol{v}$, we define its b *distance set* as $DS_b(\boldsymbol{v}) = \{\boldsymbol{u} | \|\boldsymbol{u} - \boldsymbol{v}\|_2 \le b\}$. We define the output domain as the union set of all points' DS_b in $\mathcal{D}$, namely, $\tilde{\mathcal{D}} = \bigcup_{\boldsymbol{v} \in \mathcal{D}} \{DS_b\}$. We call b as the *high probability radius*. Figure 2 shows the input and output domains. The input domain $\mathcal{D}$ is the black square with side length 1. The output domain $\tilde{\mathcal{D}}$ is the red rounded square. For a point $v \in \mathcal{D}$, its DS_b is the point located within the green circle.

Randomized Reporting Function. For any input point $v \in \mathcal{D}$, let $M_{\boldsymbol{v}} : \tilde{\mathcal{D}} \to [0,1]$ be the probability density functions (PDF) over the output domain $\tilde{\mathcal{D}}$. Spatially, $M_{\boldsymbol{v}}(\tilde{\boldsymbol{v}})$ means the probability of randomizing $\boldsymbol{v}$ as $\tilde{\boldsymbol{v}}$. We define the randomized reporting functions as a family of PDF over the output domain (i.e., $\{M_{\boldsymbol{v}}(\cdot)\}_{\boldsymbol{v} \in \mathcal{D}}$).

Spatial Area Mechanism (SAM). Based on the input/output domain and randomized reporting function, we propose our Spatial Area Mechanism in Definition 4.

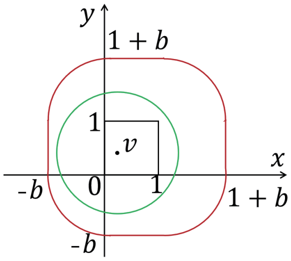


Fig. 2: Radon Transform and I/O domain with any real point.

Definition 4. (Spatial Area Mechanism (SAM)). A randomized mechanism $\Psi : \mathcal{D} \to \tilde{\mathcal{D}}$ is an instance of Spatial Area Mechanism if for all $\boldsymbol{v} \in \mathcal{D}$, there is a 2-dimension wave function $W : \mathbb{R}^2 \to [q, e^\epsilon q]$ with constant $q > 0$ and $\epsilon > 0$ such that the output probability density function $M_{\boldsymbol{v}}(\tilde{\boldsymbol{v}}) = W(\tilde{\boldsymbol{v}} - \boldsymbol{v})$ satisfies:

(1) $W(\boldsymbol{z}) = q$ for $\| \boldsymbol{z} \|_2 > b$

(2) $\iint_D W(\boldsymbol{z}) d\boldsymbol{z} = 1 - (4b+1)q$ for $D = \{\boldsymbol{z} | \| \boldsymbol{z} \|_2 \le b\}$

SAM is a general mechanism structure. It declares a wave function W with range between q and $e^\epsilon q$. Based on the function W, it claims two conditions for the areas within and out of b distance. Noted that, in condition (2) (distance within b), the distribution function of $W(\boldsymbol{z})$ is not defined. The only constrain is the integral in this area keeps $1 - (4b+1)q$.

Theorem IV.1. *SAM satisfies ϵ-LDP.*

Proof. For any two possible input values $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{D}$ and any set of possible outputs $O \subseteq \tilde{\mathcal{D}}$ of SAM, we have

$$\begin{aligned} \frac{\Pr[SAM(\boldsymbol{v}_1) \in O]}{\Pr[SAM(\boldsymbol{v}_2) \in O]} &= \frac{\iint_{\tilde{\boldsymbol{v}} \in O} M_{v_1}(\tilde{\boldsymbol{v}}) d\tilde{\boldsymbol{v}}}{\iint_{\tilde{\boldsymbol{v}} \in O} M_{v_2}(\tilde{\boldsymbol{v}}) d\tilde{\boldsymbol{v}}} \\ &\le \frac{\iint_{\tilde{\boldsymbol{v}} \in O} e^\epsilon q d\tilde{\boldsymbol{v}}}{\iint_{\tilde{\boldsymbol{v}} \in O} q d\tilde{\boldsymbol{v}}} = e^\epsilon \end{aligned} \tag{1}$$

□

For any $\boldsymbol{v} \in \mathcal{D}$ and $\tilde{\boldsymbol{v}} \in \tilde{\mathcal{D}}$, it is reasonable to assume that the reporting probability $M_{\boldsymbol{v}}(\tilde{\boldsymbol{v}})$ decreases as the $dis(\boldsymbol{v}, \tilde{\boldsymbol{v}})$ increases (similar to Reference [20]). To model this relationship, we propose our Hybrid Uniform-Exponential Mechanism in Definition 5.

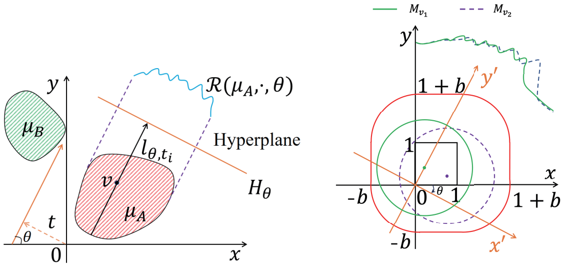
Definition 5. (Hybrid Uniform-Exponential Mechanism, HUEM). A SAM is called a Hybrid Uniform-Exponential Mechanism if the W function satisfies:

$$W(\boldsymbol{z}) = \begin{cases} q e^{(1 - \frac{\|\boldsymbol{z}\|_2}{b})\epsilon}, & \text{if } \|\boldsymbol{z}\|_2 \le b \\ q, & otherwise \end{cases} \tag{2}$$

where $q = \frac{\epsilon^2}{2\pi(e^\epsilon - 1 - \epsilon)b^2 + 4\epsilon^2 b + \epsilon^2}$.

HUEM is a type of SAM by adding constrain that W's value increases exponentially with distance $\|\boldsymbol{z}\|_2$ decreases. From Equation (2), we can see when $\boldsymbol{z} = \boldsymbol{0}$, $W(\boldsymbol{z}) = qe^\epsilon$. This means W achieves its maximum value (i.e., qe^ϵ) when the output point is exactly the same as the input one.

Let $\mathcal{C} = \{\boldsymbol{z} | \|\boldsymbol{z}\|_2 \le b\}$ and $r = \|\boldsymbol{z}\|_2$. According to $\iint_{\mathcal{C}} q e^{(1 - \frac{r}{b})\epsilon} r dr d\theta = 1 - (4b+1)q$, we can obtain $q = \frac{\epsilon^2}{2\pi(e^\epsilon - 1 - \epsilon)b^2 + 4\epsilon^2 b + \epsilon^2}$. As $\epsilon \to 0$, $q \to \frac{1}{\pi b^2 + 4b + 1}$. In this case, HUEM degenerates into uniform random mechanism. It reports any value uniformly and randomly, without any utility



(a) Radon transform (b) Wasserstein distance transform

Fig. 3: Radon transform and sliced Wasserstein distance transform.

guarantee. As $\epsilon \to +\infty$, $q \to 0$, which means HUEM reports the truthful value without any privacy protection.

We take HUEM as one of our basic mechanisms and compare it with others in the experiment.

V. The Disk Area Mechanism

Although HUEM achieves ϵ-LDP, it requires a strong assumption that the probability within radius b decreases with distance (similar to Geo-I [20]). In this section, we remove this assumption and study the best probability distribution mechanism of SAM to maximize the accuracy of distribution estimation, called Disk Area Mechanism (DAM). Then, we give the method for choosing the high probability radius b to further improve the estimation accuracy.

A. Sliced Wasserstein Distance

In order to get the best SAM, we need to use the closed form of $\mathcal{L}_2^2$-Wasserstein distance $W_2^2(D,\tilde{D})$ to deduce the relationship between the wave function W and $W_2^2(D,\tilde{D})$. However, except for the 2-Dim normal distribution, there is no closed form for Wasserstein distance of 2-Dim data distribution when the data dimension $k > 1$ [14], making the distribution analysis challenging.

To solve the above issue, we use sliced Wasserstein distance [16] instead of Wasserstein distance. Sliced Wasserstein distance is a variant of Wasserstein distance. It achieves the measurement effect of Wasserstein distance in high-dimension while simplifying the calculation process. The definition of sliced Wasserstein is based on Radon Transforms [15]. We first introduce Radon transform in Definition 6 and then give the definition of sliced Wasserstein distance in Definition 7.

Definition 6. (Radon Transform [15]). Let $\mathcal{L}^1(\mathbb{R}^k) = \{F : \mathbb{R}^k \to \mathbb{R} / \int_{\mathbb{R}^k} |F(x)|dx < \infty\}$ and $\mathbb{S}^{k-1} \subset \mathbb{R}^k$ the k-dimensional unit sphere. Let $\delta(\cdot)$ be the one-dimensional Dirac delta function. The standard Radon transform, defined as $\mathcal{R}$, maps a function $F \in \mathcal{L}^1(\mathbb{R}^k)$ to the infinite set of its integrals over the hyperplane of $\mathbb{R}^k$ and is defined as

$$\mathcal{R}(F,t,\theta) = \int_{\mathbb{R}^k} F(x)\delta(t - x \cdot \theta)dx,$$

where $(t,\theta) \in \mathbb{R} \times \mathbb{S}^{k-1}$.

Definition 7. (Sliced Wasserstein Distance [16]). Let $\mathcal{P}_p(\mathbb{R}^k)$ be the space of Borel probability measures on $\mathbb{R}^k$ with finite p-th moments. Given $\mu_A, \mu_B \in \mathcal{P}_p(\mathbb{R}^k)$, we define the $\mathcal{L}_k^p$-sliced Wasserstein distance as

$$SW_k^p(\mu_A,\mu_B) = \int_{\mathbb{S}^{k-1}} W_1^p(\mathcal{R}(\mu_A,\cdot,\theta), \mathcal{R}(\mu_B,\cdot,\theta))d\theta$$

The Radon transform maps a function $F(\mathbb{R}^k)$ to the infinite set of its integrals over hyperplanes in $\mathbb{R}^k$. The sliced Wasserstein distance in the domain $\mathbb{R}^k$ is defined as the integrals of the Wasserstein distance (between two distributions transformed by the Radon transform) over the unit sphere, denoted by $\mathbb{S}^{k-1}$, in $\mathbb{R}^k$. We give an example for Radon transforms and the sliced Wasserstein distance as follows.

Suppose the functions μ_A and μ_B are shown in Figure 3(a) and the dimension $k = 2$. As for Radon transform, if we fix θ and set $t = t_i$, we can get the position and direction of integration (described as line l_{θ,t_i}). When we want to get the Radon transform of μ_A, we can integrate all points in $\mu_A \cap l_{\theta,t_i}$ over l_{θ,t_i}. When we fix θ and alter t from $-\infty$ to $+\infty$, we obtain the Radon transforms $\mathcal{R}(\mu_A,\cdot,\theta)$ for μ_A, shown as the blue curve in Figure 3(a). By altering θ from 0 to 2π and t from $-\infty$ to $+\infty$, we can compute the $\mathcal{L}_2^1$-sliced Wasserstein distance between μ_A and μ_B as $SW_2^1(\mu_A,\mu_B) = \int_0^{2\pi} W_1^1(\mathcal{R}(\mu_A,\cdot,\theta), \mathcal{R}(\mu_B,\cdot,\theta))d\theta$.

B. Overview of DAM

According to Reference [6], we can get the optimal mechanism by maximizing the $\mathcal{L}_2^2$ Wasserstein distance between $M_{\boldsymbol{v}_1}$ and $M_{\boldsymbol{v}_2}$ for any point pair $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$. However, in the 2-Dim case, except for 2-Dim normal distributions, obtaining the closed-form solution of the $\mathcal{L}_2^2$ Wasserstein distance is difficult, which make the optimization objective hard. To solve this problem, we substitute the $\mathcal{L}_2^1$-sliced Wasserstein distance for the $\mathcal{L}_2^2$-Wasserstein distance. Thus, our optimization objective is transformed as *Maximizing the $\mathcal{L}_2^1$ sliced Wasserstein between $M_{\boldsymbol{v}_1}$ and $M_{\boldsymbol{v}_2}$ for any different two points $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{D}$.* Figure 3(b) shows an example of this transform with a fix θ.

Next, we describe Disk Area Mechanism in Definition 8, and then prove that it is the best estimation among all kinds of SAM.

Definition 8. (Disk Area Mechanism, DAM). A SAM is called a Disk Area Mechanism if the W function satisfies:

$$W(\boldsymbol{z}) = \begin{cases} p, & \text{if } \|\boldsymbol{z}\|_2 \le b \\ q, & otherwise \end{cases} \tag{3}$$

where $p = \frac{e^\epsilon}{\pi b^2 e^\epsilon + 4b + 1}$ and $q = \frac{1}{\pi b^2 e^\epsilon + 4b + 1}$.

DAM is also a type of SAM with W's value being constant in condition (2). In order to prove DAM is optimal, we need to get the partial derivative of the sliced Wasserstein in our optimization objective. We give the partial derivative in Theorem V.1 as follows.

Theorem V.1. *Given an angle $\theta \in [-\frac{\pi}{4}, 0]$ as the direction angle of projection line $l_{x'}$, $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{D}$ as inputs to SAM, where $\Delta = (\boldsymbol{v}_2 - \boldsymbol{v}_1) \cdot [\cos\theta, \sin\theta]^T > 0$, the partial derivative of sliced Wasserstein distance between the output distributions of SAM with respect to θ is $\Delta(1 - (\pi b^2 + 4b + 1)q)$.*

Proof. Let $\boldsymbol{u} = (\cos\theta, \sin\theta)$. Given two different inputs $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{D}$, where $(\boldsymbol{v}_2 - \boldsymbol{v}_1) \cdot \boldsymbol{u}^T = \Delta > 0$. Let $M_{\boldsymbol{v}_1}$ and $M_{\boldsymbol{v}_2}$ are corresponding output distributions. We define a difference function as $DIFF(\boldsymbol{z})$ in Equation (4):

$$DIFF(\boldsymbol{z}) = \begin{cases} 0, & \text{if } \boldsymbol{z} \cdot \boldsymbol{u}^T \leq -b\cos(\theta) \\ 1 - (\pi b^2 + 4b + 1)q, & \text{if } \boldsymbol{z} \cdot \boldsymbol{u}^T \geq b\cos(\theta) \\ \iint_{\mathcal{D}'}((W(\boldsymbol{z}) - q))d\boldsymbol{z}, & otherwise \end{cases} \tag{4}$$

Let the output domain be $\tilde{\mathcal{D}}$, $\tilde{Y}'$ be the projection domain of $\tilde{\mathcal{D}}$ on axis y'. Then we can write the cumulative function on the $l_{x'}$ as

$$P(M_{\boldsymbol{v}}, \tilde{\boldsymbol{v}}) = h(\theta, \tilde{\boldsymbol{v}}) + DIFF(\tilde{\boldsymbol{v}} - \boldsymbol{v}) \tag{5}$$

where $h(\theta, \tilde{\boldsymbol{v}}) = \int_{\sin\theta - b\cos\theta}^{\tilde{\boldsymbol{v}} \cdot \boldsymbol{u}^T} \left(\int_{\tilde{Y}'} q dy'\right) dx'$. Therefore, we have

$$\begin{aligned} \int_{\sin\theta - b\cos\theta}^{(1+b)\cos\theta} P(M_{\boldsymbol{v}}, \tilde{\boldsymbol{v}}) d\tilde{\boldsymbol{v}} &= \int_{\sin\theta - b\cos\theta}^{(1+b)\cos\theta} h(\theta, \tilde{\boldsymbol{v}}) d\tilde{\boldsymbol{v}} \\ &+ \int_{\sin\theta - b\cos\theta}^{(1+b)\cos\theta} DIFF(\tilde{\boldsymbol{v}} - \boldsymbol{v}) d\tilde{\boldsymbol{v}} \\ &= H(\theta) + \int_{-b\cos\theta}^{b\cos\theta} DIFF(\boldsymbol{z}) d\boldsymbol{z} \\ &+ (1 - (\pi b^2 + 4b + 1)q)(\cos\theta - \boldsymbol{v} \cdot \boldsymbol{u}^T) \end{aligned} \tag{6}$$

where $H(\theta) = \int_{\sin\theta - b\cos\theta}^{(1+b)\cos\theta} h(\theta, \tilde{\boldsymbol{v}}) d\tilde{\boldsymbol{v}}$. According to the definition of sliced Wasserstein distance, we have

$$\begin{aligned} \frac{\partial SW_2^1(M_{\boldsymbol{v}_1}, M_{\boldsymbol{v}_2})}{\partial\theta} &= \int_{\sin\theta - b\cos\theta}^{(1+b)\cos\theta} |P(M_{\boldsymbol{v}_1}, \tilde{\boldsymbol{v}}) - P(M_{\boldsymbol{v}_2}, \tilde{\boldsymbol{v}})| d\tilde{\boldsymbol{v}} \\ &= (1 - (\pi b^2 + 4b + 1)q) \cdot \Delta \end{aligned} \tag{7}$$

□

According to Equation (7), to maximize $SW_2^1(M_{\boldsymbol{v}_1}, M_{\boldsymbol{v}_2})$, we need to minimize q. Thus, we have Theorem V.2 as follows.

Theorem V.2. *For any fixed value b and ϵ, the minimum q for 2-norm mechanism is $q = \frac{1}{\pi b^2 e^\epsilon + 4b + 1}$. This minimum can be achieved if and only if the mechanism is DAM.*

Proof. For any point $\boldsymbol{v} \in \mathcal{D}$, let $\tilde{\mathcal{D}}_{\boldsymbol{v}} = \{\tilde{\boldsymbol{v}} | \parallel \tilde{\boldsymbol{v}} - \boldsymbol{v} \parallel_1 \leq b\}$. Then the area of $\tilde{\mathcal{D}}_{\boldsymbol{v}}$ is πb^2. Therefore, we have $\iint_{\tilde{\mathcal{D}}_{\boldsymbol{v}}} W(\tilde{\boldsymbol{v}} - \boldsymbol{v}) \leq \pi b^2 \cdot e^\epsilon q$. And we have

$$\begin{aligned} 1 &= (4b + 1)q + \iint_{\tilde{\mathcal{D}}_{\boldsymbol{v}}} W(\tilde{\boldsymbol{v}} - \boldsymbol{v}) \\ &\leq (4b + 1)q + \pi b^2 e^\epsilon q \\ &= (\pi b^2 e^\epsilon + 4b + 1)q. \end{aligned} \tag{8}$$

Thus, we have $q \geq \frac{1}{\pi b^2 e^\epsilon + 4b + 1}$. □

C. Choosing Radius b

In our DAM, a value within a distance of b from the true value is reported with a probability that is e^ϵ times as large as the one outside of b. The optimal choice of b depends on the privacy parameter ϵ.

Intuitively, as ϵ approaches infinity, b needs to approach 0 to fully recover the input distribution. Additionally, when the probability density of the private distribution is concentrated at one point, a smaller b is suitable, whereas when the probability has a more evenly distributed density, a larger b is appropriate. However, we do not know the distribution of the private points. There is a silver lining that we can choose a b value independent of the distribution while still performing reasonably well over different distributions. Similar to the case of one dimension [6], we choose b by maximizing the upper bound of mutual information between the input and output of our DAM in the 2-Dim case.

Unit Side Length Input. We consider the case where the input domain is a unit square. Let $\boldsymbol{V}$ and $\tilde{\boldsymbol{V}}$ be the random variables representing the input and output in our DAM. We can express the mutual information as the difference between the differential entropy of $\tilde{\boldsymbol{V}}$ and the conditional differential entropy of $\boldsymbol{V}$ and $\tilde{\boldsymbol{V}}$:

$$I(\boldsymbol{V}, \tilde{\boldsymbol{V}}) = h(\tilde{\boldsymbol{V}}) - h(\tilde{\boldsymbol{V}}|\boldsymbol{V}).$$

$h(\tilde{\boldsymbol{V}})$ is maximized when $\tilde{\boldsymbol{V}}$ is uniformly distributed on $\tilde{\boldsymbol{D}}$. For DAM, we have

$$\begin{aligned} I(\boldsymbol{V}, \tilde{\boldsymbol{V}}) &\leq h(\tilde{\boldsymbol{U}}) - h(\tilde{\boldsymbol{V}}|\boldsymbol{V}) \\ &= \log(\pi b^2 + 4b + 1) + (\pi b^2 p \log p + (4b + 1)q \log q) \\ &= \log\left(\frac{\pi b^2 + 4b + 1}{\pi b^2 e^\epsilon + 4b + 1}\right) + \epsilon \log e - \frac{(4b + 1)\epsilon \log e}{\pi b^2 e^\epsilon + 4b + 1}. \end{aligned} \tag{9}$$

We denote the expression on the right side in Equation (9) as $g(b)$. Then we have:

$$\frac{dg(b)}{db} = \frac{2\pi b(2b + 1)(-\pi e^\epsilon m_1 b^2 + 4m_2 b + m_2)}{(\pi b^2 + 4b + 1)(\pi b^2 e^\epsilon + 4b + 1)^2 \ln 2} \tag{10}$$

where $m_1 = e^\epsilon - 1 - \epsilon$ and $m_2 = 1 - e^\epsilon + \epsilon e^\epsilon$. Because ϵ and b are both positive, when $b = \frac{2m_2 + \sqrt{4m_2^2 + \pi e^\epsilon m_1 m_2}}{\pi e^\epsilon m_1}$, it achieves maximum. We can see that when $\epsilon \to 0$, $b \to \frac{2 + \sqrt{4 + \pi}}{\pi}$, and when $\epsilon \to +\infty$, $b \to 0$.

General Side Length Input. When the input domain is a square with length L, the mutual information of $\tilde{\boldsymbol{V}}$ and $\boldsymbol{V}$ can be express as follow:

$$\begin{aligned} I(\boldsymbol{V}, \tilde{\boldsymbol{V}}) &\leq \log(\pi b^2 + 4Lb + L^2) + (\pi b^2 p \log p + (4Lb + L^2)q \log q) \\ &= \log\left(\frac{\pi b^2 + 4Lb + L^2}{\pi b^2 e^\epsilon + 4Lb + L^2}\right) + \frac{\pi b^2 e^\epsilon \epsilon \log e}{\pi b^2 e^\epsilon + 4Lb + L^2}. \end{aligned} \tag{11}$$

And we have

$$\frac{dg(b)}{db} = \frac{2\pi Lb(2b + L)(-\pi e^\epsilon m_1 b^2 + 4dm_2 b + L^2 m_2)}{(\pi b^2 + 4Lb + L^2)(\pi b^2 e^\epsilon + 4Lb + L^2)^2 \ln 2}. \tag{12}$$

Let $m_1 = e^\epsilon - 1 - \epsilon$ and $m_2 = 1 - e^\epsilon + \epsilon e^\epsilon$. Let $\frac{dg(b)}{db} = 0$, we can get the best $b = \frac{2m_2 + \sqrt{4m_2^2 + \pi e^\epsilon m_1 m_2}}{\pi e^\epsilon m_1} \cdot L$.

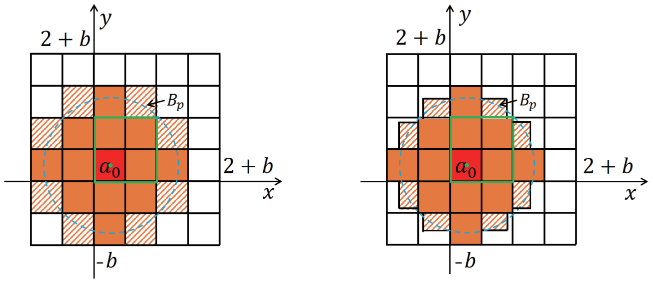
VI. Bucketizing and Post-processing

When we use any SAM (e.g., HUEM or DAM) in real-world scenarios, it is impossible to count the frequency of all types of points because there is infinite number of points in any continuity ranges (e.g., $\mathcal{D}$ and $\tilde{\mathcal{D}}$). Thus we need to bucketize the input/output domain into grids and execute SAM under grid domain. Additionally, we provide the method of post-processing under the grid condition. Finally, we give the total algorithms of solving PSDEP.

A. Bucketizing

To facilitate the reconstruction of the distribution, we need to divide the plane into grids and use our DAM on this grid plane. In other words, the problem is converted into estimating the histogram distribution on a 2-Dim plane using DAM.

Let g be the length of a grid cell. Let G be the grid input domain and $\tilde{G}$ be the grid output domain. We denote the side



(a) Non-shrunken areas (b) Shrunken areas

Fig. 4: Non-shrunken/Shrunken areas in grid division.

length of the grid as $d = \lfloor \frac{L}{g} \rfloor$ and the high probability radius in the grid as $\hat{b} = \lfloor \frac{b}{g} \rfloor$. Then, the coordinate unit is reset to the side length of a grid cell, and we use the central point of a cell to represent its position. For example, in Figure 4(a), the index of the cell a_0 is $(0, 0)$, and the index of the cell to the right of a_0 is $(1, 0)$.

Our DAM for grids is defined in Equation (13).

$$\forall v \in G, \tilde{v} \in \tilde{G}, M_{\boldsymbol{v}}(\tilde{\boldsymbol{v}}) = \begin{cases} \hat{p}, & \text{if } \|\tilde{\boldsymbol{v}} - \boldsymbol{v}\|_2 \le \hat{b}, \\ \hat{q}, & otherwise. \end{cases} \qquad (13)$$

Next, we decide how to calculate $\hat{p}$ and $\hat{q}$ to approximate the true values.

As is shown in Figure 4, given an input cell a_0 (the red rectangle), the blue dotted line (denoted as B_p) represents the border of high probability reporting. Based on the positional ordinal relationship between B_p and the output cells, the output domain can be divided into three areas:

(1) *the pure high probability area* A_p where the center of each cell is in or on B_p;

(2) *the pure low probability area* A_q where each cell neither intersects with B_p nor locates in B_p;

(3) *the mixed probability area* A_m where each cell intersects with B_p, however, the center point is out of B_p.

All these areas are shown as the orange cells, the white cells and shaded cells, respectively. Each cell $a^{(i)}$ in A_m can be further divided into high probability part $a_p^{(i)}$ and low probability part $a_p^{(i)}$, respectively. We combine all high probability areas ($A_{m,p} = \sum_i a_p^{(i)}$) in A_m with A_p to form the total high probability area A_H. Similarly, we combine all low probability areas ($A_{m,q} = \sum_i a_q^{(i)}$) in A_m with A_q to form the total low probability area A_L.

We consider the area size of each cell to be 1 (i.e., $S_a = 1$). To determine $\hat{p}$ and $\hat{q}$, we need to solve two problems:

(1) How can we determine the area size of $a_p^{(i)}$ for each cell in A_m to satisfy ϵ-LDP ?

(2) What is the area size of A_H and A_L ?

To solve Problem (1), we first determine the center of $a_p^{(i)}$ (denoted as C_N) by intersecting B_p and the line between $a^{(i)}$'s center and B_p's center. Then, we construct $a_p^{(i)}$ as a rectangle centered at C_N satisfying $a_p^{(i)}$'s left and bottom borders overlap $a_p^{(i)}$'s left and bottom borders respectively. To solve Problem (2), we first partition A_H and A_L into several parts and reconstruct them as different types of cells. Then, we count these cell areas by category. We introduce these methods in detail below.

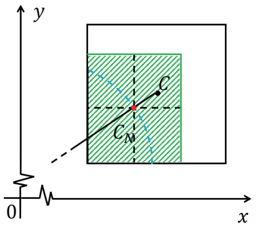


Fig. 5: The process of border shrinkage in discrete DAM.

As for the Problem (1), we determine whether the center $o^{(i)}$ of each cell $a^{(i)} \in A_m$ is inside B_p. If $o^{(i)}$ is outside of B_p, we create a new shrunken rectangle for $a^{(i)}$ and set it as $a_p^{(i)}$ while the remain part $a^{(i)} \setminus a_p^{(i)}$ is set as $a_q^{(i)}$. The method for constructing the new shrunken rectangle is as follows.

Suppose B_p crosses a grid cell a (with its central point noted as C) as shown in Figure 5, with the blue dot arc ARC indicating the intersection. We connect the center of B_p and the point C to obtain the intersection point C_N on ARC. We define C_N as the center of the shrunken rectangle $a_p^{(i)}$, and construct $a_p^{(i)}$ as shown in the green shaded part.

Next we give Theorem VI.1 to calculate the area size of the shrunken rectangle $a_p^{(i)}$.

Theorem VI.1. *Given a circle B_p with central cell index $(0, 0)$, a radius $\hat{b}$ and any cell a, the area size of a's shrunken cell a_p is $S_{a_p} = 4(\delta \cdot x + \frac{1}{2})(\delta \cdot y + \frac{1}{2})$, where $\delta = \frac{\hat{b}}{\sqrt{x^2+y^2}} - 1$, and a is any cell that intersects with B_p, whose central point (x, y) is outside the range of B_p.*

Proof. As shown in Figure 5, suppose the index of cell a is (x, y), then the index of a_p is $(\hat{b} \cdot \frac{x}{\sqrt{x^2+y^2}}, \hat{b} \cdot \frac{y}{\sqrt{x^2+y^2}})$. The line of a's left boundary is $X = x - \frac{1}{2}$ and the line of a's bottom boundary is $Y = y - \frac{1}{2}$. Thus, $S_{a_p} = 4(\hat{b} \cdot \frac{x}{\sqrt{x^2+y^2}} - (x - \frac{1}{2}))(\hat{b} \cdot \frac{y}{\sqrt{x^2+y^2}} - (y - \frac{1}{2}))$. Let $\delta = \frac{\hat{b}}{\sqrt{x^2+y^2}} - 1$. Then we have $S_{a_p} = 4(\delta \cdot x + \frac{1}{2})(\delta \cdot y + \frac{1}{2})$. □

As for the problem (2), we decompose $A_H = A_p + A_{m,p}$ and $A_L = A_q + A_{m,q}$. We need to calculate the area size of A_q, A_p and A_m (i.e., $A_{m,p} + A_{m,q}$). Next, we give Theorem VI.2, VI.3 and VI.4 to calculate the sizes of these three areas.

Theorem VI.2. *For any square input domain $\mathcal{D}$ with integer side length d and any integer high probability radius $\hat{b}$, the area size of pure low probability area A_q is $d^2 + 4\hat{b}d - 4\hat{b} - 1$.*

Proof. Please refer to details of Theorem VI.2 in Appendix B1 in our technical report [27]. □

Theorem VI.2 gives the method to calculate the area size of A_q. As for A_p and A_m, according to the centripetal symmetry and axial symmetry of a circle, we only need to analyze the part within angle $[0, \frac{\pi}{4}]$. Figure 6 shows the conditions that $\hat{b}$ is $1, 2, ..., 7$. The cells in directions of 0 and $\frac{\pi}{4}$ are in yellow while others are in green.

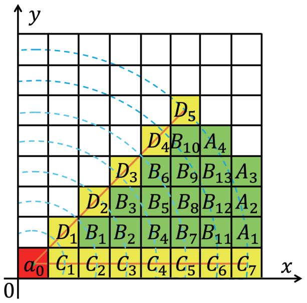


Fig. 6: Quarter of the total area.

We define $E_{\hat{b},\theta}$ as the cells in direction θ within the radial range of $\hat{b}$. We define $E_{\hat{b},(\theta_1,\theta_2)}$ as the cells within the radial range of $\hat{b}$ and the direction range of (θ_1,θ_2). We define *strict quarter* A_m (denoted as $E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}$) as the cells belonging to A_m in $E_{\hat{b},(0,\frac{\pi}{4})}$, and *strict quarter* A_p (denoted as $E^{(p)}_{\hat{b},(0,\frac{\pi}{4})}$) as the cells belonging to A_p in $E_{\hat{b},(0,\frac{\pi}{4})}$. Similar to A_m, the strict quarter A_m can be divided into the high probability part and low probability part. We call these two parts as *strict quarter* $A_{m,p}$ and and *strict quarter* $A_{m,q}$ respectively. For example, in Figure 6, $E_{\hat{7},\frac{\pi}{4}} = \{a_0\} \cup \{D_i | i \in [5]\}$, $E^{(m)}_{7,(0,\frac{\pi}{4})} = \{A_1, A_2, A_3, A_4\}$, the quantity of $E^{(p)}_{7,(0,\frac{\pi}{4})}$ is $|E^{(p)}_{7,(0,\frac{\pi}{4})}| = |\{B_i | i \in [13]\}| = 13$.

In order to get the area size of strict quarter A_m (i.e., strict quarter $A_{m,p}$ and strict quarter $A_{m,q}$), we need to know each cell's index in $E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}$. Based on these cell indexes and Theorem VI.1, we can calculate each cell's shrunken area size and remaining area size in $E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}$ (i.e., strict quarter $A_{m,p}$ and strict quarter $A_{m,q}$). We present Theorems VI.3 to get the cell indexes in $E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}$ as follows.

Theorem VI.3. *Given a positive integer $\hat{b}$, the quantity of $E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}$ is $\lceil \frac{\hat{b}}{\sqrt{2}} - \frac{1}{2} \rceil - \lfloor \frac{r}{\hat{b}} \rfloor$, where $r = \sqrt{r_1^2 + 1 + \sqrt{2} r_1}$ and $r_1 = \lfloor \frac{\hat{b}}{\sqrt{2}} - \frac{1}{2} \rfloor \cdot \sqrt{2} + \frac{1}{\sqrt{2}}$. The index of each cell in $E^{m}_{\hat{b},(0,\frac{\pi}{4})}$ is $(\lceil \sqrt{\hat{b}^2 - (i - \frac{1}{2})^2} - \frac{1}{2} \rceil, i)$ for $i \in [|E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}|]$.*

Proof. Please refer to details of Theorem VI.3 in Appendix B2 in our technical report [27]. □

In order to get the area size of strict quarter A_p, we need to count the cell number in this area. Theorem VI.4 gives the method to calculate this count.

Theorem VI.4. *Given a positive integer $\hat{b}$, the quantity of $E^{(p)}_{\hat{b},(0,\frac{\pi}{4})}$ is $\frac{1}{2}\lceil \frac{\hat{b}}{\sqrt{2}} - \frac{1}{2} \rceil (\lceil \frac{\hat{b}}{\sqrt{2}} - \frac{1}{2} \rceil - 2|E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}| - 1) + \sum_{i=1}^{|E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}|} \lceil \sqrt{\hat{b}^2 - (i - \frac{1}{2})^2} - \frac{1}{2} \rceil$.*

Proof. Please refer to details of Theorem VI.4 in Appendix B3 in our technical report [27]. □

According to Theorems VI.1, VI.3, and VI.4, we can calculate $\hat{p}_2$ and $\hat{q}_2$ as follows.

```
Algorithm 1: DAM Processing Framework
    Input: original data point set $X$, square range $L \times L$,
           cell side length $g$, privacy budget $\epsilon$
    Output: distribution map $R$
 1  Split square range into $\lceil \frac{L}{g} \times \frac{L}{g} \rceil$ grids with index set
    $\mathcal{I} = [0 : \lceil \frac{L}{g} \rceil - 1] \times [0 : \lceil \frac{L}{g} \rceil - 1]$;
 2  Calculate the noisy domain index set $\hat{\mathcal{I}}$;
 3  Initialize noisy map $NR$ by setting items as $(\hat{i}, 0)$ for
    each $\hat{i} \in \hat{\mathcal{I}}$;
 4  for each point $x$ in $X$ do
 5      Get the grid index $\mathcal{I}(x)$;
 6      $\hat{\mathcal{I}}_x \leftarrow GridAreaResponse(\mathcal{I}(x))$;
 7      $NM(\mathcal{I}(x)) \leftarrow NM(\mathcal{I}(x)) + 1$;
 8  $R \leftarrow PostProcess(NR, I)$;
 9  return $R$;
```

Let $S^{(m,p)}_a$ be the shrunken area size of $a \in E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}$, which can be calculated by Theorem VI.1. Similarly, let $S^{(m,p)}_{\frac{\pi}{4}}$ denote the shrunken area size of cell $a \in E^{\frac{\pi}{4}}_{\hat{b}} \cap A_m$. According to Theorem VI.1, we have

$$S^{(m,p)}_{\frac{\pi}{4}} = \begin{cases} 4(b'_{\frac{\pi}{4}} - \hat{b}_{\frac{\pi}{4}})^2, & \text{if } b'_{\frac{\pi}{4}} - \hat{b}_{\frac{\pi}{4}} < \frac{1}{2}, \\ 1, & otherwise \end{cases} \tag{14}$$

where $b'_{\frac{\pi}{4}} = \frac{\hat{b}}{\sqrt{2}} - \frac{1}{2}$ and $\hat{b}_{\frac{\pi}{4}} = \lfloor b'_{\frac{\pi}{4}} \rfloor$.

Finally, we can calculate the probabilities $\hat{p}$ and $\hat{q}$ as:

$$\hat{p} = \frac{e^\epsilon}{S_H \cdot e^\epsilon + S_L}, \quad \hat{q}_2 = \frac{1}{S_H \cdot e^\epsilon + S_L},$$

where $S_H = 1 + 4(\hat{b} + \hat{b}_{\frac{\pi}{4}} + S^{(m,p)}_{\frac{\pi}{4}}) + 8(|E^{(p)}_{\hat{b},(0,\frac{\pi}{4})}| + \sum_{a \in E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}} S^{(m,p)}_a)$ and $A_L = A_q + 4(1 - S^{(m,p)}_{\frac{\pi}{4}}) + 8 \sum_{a \in E^{(m)}_{\hat{b},(0,\frac{\pi}{4})}} (1 - S^{(m,p)}_a)$.

Regarding the discretization of HUEM, the high probability areas can be divided into $\hat{b}$ fan rings $\{FR_j\}_{j=1}^{\hat{b}}$. For any unit cell in FR_j, the reported probability is $p^{(I)}_j = qe^{1 - \frac{j-1}{\hat{b}}}$. For a unit cell a on the border of FR_{j-1} and FR_j, the reported probability is $p^{(B)}_j = S^{(p)}_a \cdot p^{(I)}_{j-1} + (1 - S^{(p)}_a) \cdot p^{(I)}_j$, where $S^{(p)}_a$ is the shrunken area size of a. For more details on discretization of HUEM, please refer to Appendix A in our technical report [27].

B. The PSDEP Processing Algorithm

We give the processing framework for our DAM shown in Algorithm 1. The input square range with an area size of $L \times L$ will be divided into grids. For each point in this area, we first project it onto a grid cell (Line 5), and then randomize the cell into a random noisy cell (Line 6) using *GridAreaResponse*. All the points in each noisy cell will be counted and stored in the noisy map NM. Finally, we obtain the distribution estimation using *PostProcess*.

In Algorithm 1, the *GridAreaResponse* process is to pick a randomized cell index satisfying ϵ-LDP. The *PostProcess* process is to handle the values to obtain an accurate estimation distribution, which is the Expectation-Maximization (EM) [6]

```
Algorithm 2: GridAreaResponse
    Input: original grid index $i$
    Output: noisy grid index $\hat{i}$
1   Find the pure high probability cell index set $\hat{\mathcal{I}}_p(i)$ and calculate its total area size $S_p$;
2   Find the pure low probability cell index set $\hat{\mathcal{I}}_q(i)$ and calculate its area size $S_q$;
3   Find the high probability border cell set $\hat{\mathcal{I}}_m(i)$ and calculate the sum shrunken area $S_{m,p} = \sum_{\hat{i} \in \hat{\mathcal{I}}_m} S_{m,p}(\hat{i})$ and the complement area $\overline{S}_{m,p} = \sum_{\hat{i} \in \hat{\mathcal{I}}_m} \overline{S}_{m,p}(\hat{i})$;
4   Set value list $vl =< A_{PL}, \overline{S}_{m,p}, S_{m,p}, A_{PH} >$;
5   Set weighted list $wl =< 1, 1, e^{\epsilon}, e^{\epsilon} >$;
6   Sample $ind$ as $i$ with probability as $p_i = \frac{vl_i \cdot wl_i}{\sum_{j=1}^{4} vl_j \cdot wl_j}$;
7   if $ind = 1$ then
8       $\hat{i} \xleftarrow{\$} \hat{\mathcal{I}}_q(i)$;
9   else if $ind = 4$ then
10      $\hat{i} \xleftarrow{\$} \hat{\mathcal{I}}_p(i)$;
11  else
12      Set $vl =< ws_1, ..., ws_n >$ for each $ws_j = \overline{sa}_j + sa_j \cdot e^{\epsilon}$;
13      Set $wl =< 1, ..., 1 >$ with $n$ elements;
14      Sample $ind$ as $i$ with probability as $p_i = \frac{vl_i \cdot wl_i}{\sum_{j=1}^{4} vl_j \cdot wl_j}$;
15      $\hat{i} \leftarrow$ cell with $ind$ in $vl$;
16  return $\hat{i}$;
```

Algorithm. Next, we give the processes of *GridAreaResponse* in Algorithm 2.

In *GridAreaResponse*, a cell point in range b will have a higher probability of being responded to while those outside of it will have a lower probability. Specifically, the areas are divided into three parts: the pure low probability area, the mixed probability area, and the pure high probability area. Given an original grid index i, the algorithm calculates the area size of high probability part $\hat{\mathcal{I}}_p(i)$, the low probability part $\hat{\mathcal{I}}_q(i)$ and the mixed probability area $\hat{\mathcal{I}}_m(i)$. The cells that are crossed by the circle centered at cell $(0, 0)$ with radius b make up $\hat{\mathcal{I}}_m(i)$. All the cells in the mixed probability area need to be further divided into two parts: the shrunken part and the remain part. Therefore, there are four parts of the area that can be chosen as a candidate sample domain. The algorithm uses a weighted sample (Line 6) to determine which part to choose. The value $ind = 1$ refers to the choice of the low probability part, and $ind = 4$ refers to the choice of the high probability part. Both of these two cases use the uniform sample to choose $\hat{i}$ (Line 8 and Line 10). When it comes to the case of border area containing n cells, rather than using the uniform sample, the sampling probability needs to be proportional to the weighted area size ws_j for each cell in the mixed probability area (Line 12). After that, the weighted sampling algorithm is used with identical weight for each cell to sample the result response cell (Line 14).

TABLE III: The range and data points of Data sets.

	Chicago Crimes		NYC Green Taxies	
	Range	Point size	Range	Point size
Part A	[41.72°,41,81°] ×[-87.68°,-87.59°]	216,595	[40.65°, 40.75°] ×[-73.84°, -73.74°]	10,561
Part B	[41.82°,41.91°] ×[-87.73°,-87.64°]	173,552	[40.65°,40.74°] ×[-73.95°,-73.86°]	42,195
Part C	[41.92°,41.99°] ×[-87.77°,-87.70°]	69,068	[40.82°,40.89°] ×[-73.90°,-73.83°]	9,186

TABLE IV: Experimental Settings.

Parameters	**Values**
the norm distance, b	$\lfloor 0.33\check{b} \rfloor$, $\lfloor 0.67\check{b} \rfloor$, $\check{\mathbf{b}}$, $\lfloor 1.33\check{b} \rfloor$, $\lfloor 1.67\check{b} \rfloor$
the discrete side length, d	1, 2, 3, 4, **5**, 10, $\underline{15}$, 20
the privacy budget, ϵ	0.7, 1.4, 2.1, 2.8, **3.5**, $\underline{5}$, 6, 7, 8, 9

Time and Memory Complexity Analysis. Let n be the number of users. Let g be the grid number of the input domain. The time complexity of GridAreaResponse algorithms is $O(g)$. Let m be the repeat times before converging in PostProcess algorithm. The time complexity of PostProcess is $O(nk)$. Therefore, the time complexity of DAM Processing Framework is $O(ng + nk)$. The memory complexity of GridAreaResponse and PostProcess algorithms are $O(g)$. Therefore, the memory complexity of DAM Processing Framework is $O(g)$.

VII. Experimental Evaluation

In this section, we compare the accuracy of our mechanisms with state-of-the-art methods across various parameters. Our experiments aim to determine which method achieves the smallest Wasserstein distances between the real and recovered obfuscated density distributions under equivalent privacy levels or grid sizes.

A. Experimental Setup

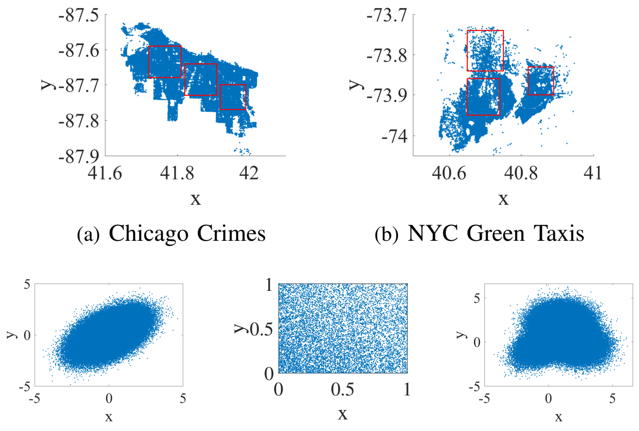
Data sets. We demonstrate all above mechanisms on the following 5 data sets. The first two data sets are real, and the other three ones are synthetic.

Chicago Crime [28] (Crime): It is collected to monitor crime events in Chicago from January 1st to June 30th, 2022. It contains 105,453 data items, each representing a crime event. We extract events with a latitude range $[40°, 42°]$ and a longitude range $[-87.9°, -87.54°]$. Finally, we get $101,146$ items.

NYC Green Taxis [29] (NYC): It records green taxi order information in New York City in 2016. It contains $448,181$ order items. We only extract orders with a pickup location latitude and longitude within the ranges of $[40.55°, 40.88°]$ and $[-74.05°, -73.73°]$, respectively. Finally, we get $446,110$ items.

The latitude and longitude of Chicago crime event locations and NYC green taxi pick-up locations are shown in Figure 7(a) and 7(b). We project the latitude and longitude onto a plane, which does not affect our experimental results.

To address the irregularity of these positions, we further extract three parts (marked as squares in Figure 7(a) and 7(b)) of the two real data sets and estimate the distributions within each part. Table III shows the number of data points in each area for Chicago Crimes and NYC Green Taxis. For the



(a) Chicago Crimes

(b) NYC Green Taxis

(c) Normal

(d) SZipf

(e) MNormal

Fig. 7: Data sets.

experiment on the full domain of the real data sets, please refer to Appendix C in our technical report [27].

Normal(0, 0, 1, 1, 0.5) (Normal): We generate $300,000$ 2-Dim data points in the plane, where each point follows a 2-Dim Gaussian distribution with $\mu_x = \mu_y = 0$, $\sigma_x^2 = \sigma_y^2 = 1$, and $\rho = 0.5$. The correlation between x and y is described by $\rho \in (-1, 1)$, where $-1 < \rho < 0$ indicates negative correlation, $0 < \rho < 1$ indicates positive correlation, and $\rho = 0$ indicates independence between x and y. The points are all within the range $(-5, 5) \times (-5, 5)$. The range of these points is $[-4.44, 4.65] \times [-4.87, 4.58]$.

Skew Zipf($\frac{1}{\ln 2}$, 1,1) (SZipf): We generate 100,000 2-Dim data points in the plane. Each dimension of each point follows a skew Zipf distribution with a CDF of $\frac{1/\ln 2}{X+1}$. The points are limited to the range $[0, 1) \times [0, 1)$. We show one-tenth of the point distribution in Figure 7(d).

Multi-center Normal (MNormal): We generate $300,000$ 2-Dim data points in the plane. These points can be divided into three parts, each containing $100,000$ points. The parts follow a normal distribution with parameters *Normal(0, 0, 1, 1, 0.5)*, *Normal(0, 0, 1, 1, 0)*, and *Normal(0, 0, 1, 1, -0.2)*, respectively. The range of these points is $[-4.25, 6.18] \times [-4.32, 6.44]$.

Parameter Settings. We vary the norm distance b from $0.33\check{b}$ to $1.67\check{b}$, where $\check{b}$ is the best choice of b. We define the discrete side length d as L/g, where L is the side length of the input data set area, g is the side length of a grid cell. We change d from 1 to 20 and ϵ from 0.7 to 9. The parameter settings are shown in Table IV with default values marked as bold or underlined.

We conduct our experiment in Java on an Intel(R) Xeon(R) Silver 4210R CPU @ 2.4GHz with 128 GB RAM. We run our experiment 10 times and use the average result as our final result.

B. Mechanisms and Measures

We compare our mechanisms HUEM and DAM with Multi-dimensional Square Wave Mechanism (MDSW) [10] and Subset Exponential Mechanism with Geo-I (SEM-Geo-I) [12]. We also compare our DAM with its version without shrinkage (i.e., Disk Area Mechanism with Non-Shrink, DAM-NS). Furthermore, we evaluate our mechanism against recent research on private trajectory estimation: Locally Differentially Private Trajectory Synthesis (LDPTrace) [30] and Trajecotry Data Collectin with Local Differential Privacy (PivotTrace) [31]. For detailed comparisons with the trajectory mechanisms, please refer to Appendix D in our technical report [27].

Actually, it is hard to make DAM and SEM-Geo-I comparable because DAM and SEM-Geo-I are based on different privacy definition (DAM is based on LDP while SEM-Geo-I is based on Geo-I). However, the definitions of both LDP and Geo-I are based on *privacy loss* [1] which is a more fundamental privacy definition. Thus, given the same input domain, we can set the same privacy loss in DAM and SEM-Geo-I and compare the utilities between these two mechanisms.

Givena a fixed privacy budget ϵ, DAM achieves ϵ-LDP which means for any $\boldsymbol{v} \in \mathcal{D}$, the privacy loss of randomizing $\boldsymbol{v}$ to $\tilde{\boldsymbol{v}} \in \tilde{\mathcal{D}}$ is ϵ. However, SEM-Geo-I achieves ϵ-Geo-I which means for any $\boldsymbol{v} \in \mathcal{D}$, the privacy loss of randomizing $\boldsymbol{v}$ to $\tilde{\boldsymbol{v}} \in \tilde{\mathcal{D}}$ is $\epsilon \cdot dis(\boldsymbol{v}, \tilde{\boldsymbol{v}})$ where $dis(\boldsymbol{v}, \tilde{\boldsymbol{v}})$ is the Euclidean distance between $\boldsymbol{v}$ and $\tilde{\boldsymbol{v}}$ (i.e., $dis(\boldsymbol{v}, \tilde{\boldsymbol{v}}) = \|\boldsymbol{v} - \tilde{\boldsymbol{v}}\|_2$). We find if $dis(\boldsymbol{v}, \tilde{\boldsymbol{v}}) < 1$, SEM-Geo-I provides higher level privacy protection than DAM, if $dis(\boldsymbol{v}, \tilde{\boldsymbol{v}}) > 1$, DAM provides higher level privacy protection than SEM-Geo-I.

Next, we introduce the definition of an enhanced loss privacy called Local Privacy (LP) [17] to make DAM and SEM-Geo-I comparable on both utility and privacy. Let $\mathcal{I}$ be the input domain, and $\mathcal{T}$ be the output domain. Let $\hat{\mathcal{I}}$ be the inferred domain of $\mathcal{I}$. Based on the unbiased results of DAM and SEM-Geo-I, we have $\hat{\mathcal{I}} = \mathcal{I}$. Thus, the local privacy is defined as:

$$\begin{aligned} LP &= \sum_{i' \in \mathcal{T}} LP_{\mathcal{I}}(i') = \sum_{i, \hat{i} \in \mathcal{I}} LP_{\mathcal{T}}(i, \hat{i}) \\ &= \sum_{i, \hat{i} \in \mathcal{I}, i' \in \mathcal{T}} \Pr(i) \Pr(i'|i) \Pr(\hat{i}|i') d_p(\hat{i}, i) \end{aligned} \tag{15}$$

In Equation (15), $\Pr(i)$ is the probability of being at location i when accessing the location-based service. $\Pr(i'|i)$ is the location obfuscation function implemented by privacy mechanisms, which is defined as the probability of replacing i with i'. $\Pr(\hat{i}|i')$ is the adversary attack function, which is defined as the probability of estimating $\hat{i}$ as the user's actual location if i' is observed. $d_p(\hat{i}, i)$ is the privacy of the user at location i, given that the adversary's estimation is $\hat{i}$. This is defined as the distance between $\hat{i}$ and i, using 2-norm distance.

Suppose the truthful points obey a uniform distribution. Then, we have $\Pr(i) = \frac{1}{n}$, where n is the number of truthful locations. According to the unbiased estimation for LDP, we have $\Pr(\hat{i}) = \Pr(i) = \frac{1}{n}$ and $\Pr(i'|i) = \Pr(i'|\hat{i})$ when $i = \hat{i}$. Therefore, for DAM and SEM-Geo-I, we have:

$$\begin{aligned} LP_{\mathcal{I}}(i') &= \frac{1}{n} \sum_{i, \hat{i} \in \mathcal{I}} \Pr(i'|i) \Pr(\hat{i}|i') d_p(\hat{i}, i) \\ &= \frac{1}{n} \sum_{i, \hat{i} \in \mathcal{I}} \frac{\Pr(i'|i) \cdot \Pr(i'|\hat{i}) \Pr(\hat{i}) \cdot d_p(\hat{i}, i)}{\sum_{\hat{i}_j \in \mathcal{I}} \Pr(i'|\hat{i}_j) \Pr(\hat{i}_j)} \\ &= \frac{1}{n} \sum_{i, \hat{i} \in \mathcal{I}} \frac{\Pr(i'|i) \Pr(i'|\hat{i}) d_p(\hat{i}, i)}{\sum_{\hat{i}_j \in \mathcal{I}} \Pr(i'|\hat{i}_j)} \\ &= \frac{1}{n \sum_{\hat{i}_j \in \mathcal{I}} \Pr(i'|\hat{i}_j)} \sum_{i, \hat{i} \in \mathcal{I}} \Pr(i'|i) \Pr(i'|\hat{i}) d_p(\hat{i}, i) \end{aligned} \tag{16}$$

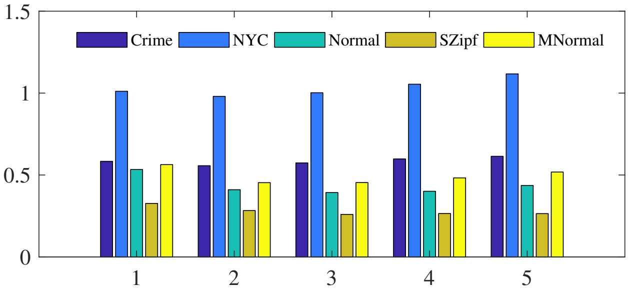


Fig. 8: Wasserstein distances with b varied.

To calculate the value of LP for DAM, traverse all $i' \in \mathcal{I}'$, where $\mathcal{I}'$ is the output domain of DAM. For SEM-Geo-I, calculate the value of LP by traversing all $i' \in \mathcal{S}_k$, where $\mathcal{S}_k$ is the k-subset domain of $\mathcal{I}$. In our experiment, we set ϵ in DAM as the values in Table IV and calculate the corresponding ϵ' in SEM-Geo-I with their local privacy equal. We compare the accuracy of the mechanisms above, described by the 2-Dim Wasserstein distance. Since there is no closed-form solution for high-dimensional Wasserstein distance [14], we calculate the 2-Dim Wasserstein distance using Linear Programming.

Note that in our models, all distributions are finite and the input and output domains are divided into grids. Therefore, in our models, the Wasserstein distance involves multidimensional optimization in finite spaces. We can formalize this as follows:

Suppose $\mathcal{D} = \{X_1, ..., X_m\}$ and $\tilde{\mathcal{D}} = \{Y_1, ..., Y_n\}$. Let $M = \{\|X_i - Y_j\|_p^p\}_{i \in [m], j \in [n]}$ be the matrix where each element is the p norm to the p for the pair of X and Y. Let $R = \{\Pr[X_i, Y_j]\}_{i \in [m], j \in [n]}$ be the matrix where each element is the joint probability of X_i and Y_j. Then,

$$\begin{aligned} W_2^p(\mathcal{D}, \tilde{\mathcal{D}}) = \min \quad & \|M \bigodot R\|_F \\ s.t. \quad & \text{sum}_r(R) = \Pr[\mathcal{D}] \\ & \text{sum}_c(R) = \Pr[\tilde{\mathcal{D}}] \\ & R_{i,j} \geq 0; \forall i \in [m] \text{ and } j \in [n] \end{aligned} \tag{17}$$

where $\bigodot$ is Hadmard production, $\|\cdot\|_F$ is Frobenius norm.

C. Experimental Results

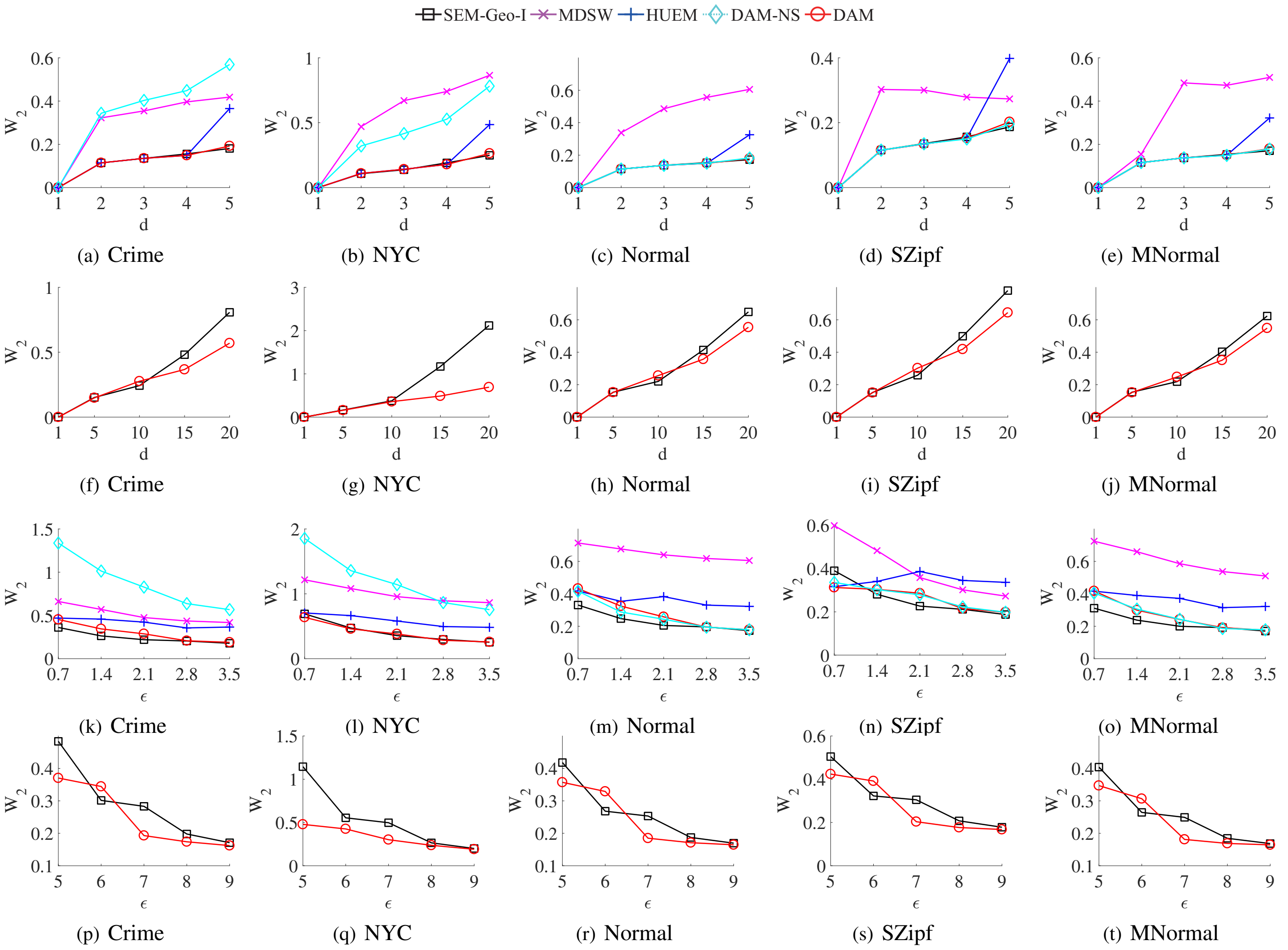
We compared the estimation results of methods for distribution estimation. We used the 2-norm Wasserstein distance $W_2 = \sqrt{W_2^2}$ between the recovered and actual density distributions in a discrete situation. We compared the results on different data sets with varying values for the norm distance b, discrete side length d, and privacy budget ϵ. For the divided data sets (Chicago Crime and NYC Green Taxis), we used the mean value of each part's W_2 as the estimation results.

1) Norm Distance b: Figure 8 shows the impact of the norm distance b on W_2. The value of b varies from $0.33\check{b}$ to $1.66\check{b}$, where $\check{b}$ is the optimal value of b in a discrete situation. We set the default discrete side length $d = 15$ and the default privacy budget $\epsilon = 3.5$. In this case, the optimal norm distance $\check{b}$ is approximately equal to 3. We can see that, in both the real and synthetic data sets, W_2 first decreases and then increases. When b is approximately equal to $\check{b}$, W_2 achieves its minimum value, which is consistent with our analysis in section V-C. However, W_2 is not minimal when $b = \check{b}$ in some data sets due to the error from grid division.

2) Discrete side length d: As the grid cells' side length g decreases, d increases with fixed L. Here we vary d from 1 to 5. As shown in Figure 9(a) to 9(e), W_2 increases with the increase of d in most mechanisms except for MDSW on data set SZipf. This is because, as d increases, the number of grid cells becomes larger, and the gap between the recovered and actual density distributions widens. HUEM is better than MDSW in most cases and DAM is always better than MDSW. It is because HUEM and DAM retain the ordinal relationship of x-coordinate, y-coordinate and (x, y)-union among all points, however, MDSW only retains ordinal relationship of x-coordinate and y-coordinate. On the other hand, it indicates that considering the relationship between each dimension is useful. Additionally, our DAM is superior to HUEM, which demonstrates its effectiveness in 2-Dim area mechanisms. Moreover, DAM outperforms DAM-NS in real data sets. This is because both data sets are road network data sets where the shrunken method has more advantages over the non-shrunken method.

The difference between SEM-Geo-I and our DAM is small. That is because when d is small, the side length of a grid cell is large, and the shape of discrete DAM is very different from that of continue DAM. This makes the discrete DAM performs worse than SEM-Geo-I. We further compare these two mechanism under larger d. However, as d becomes larger, it becomes more difficult to calculate the Wasserstein distance within an acceptable time. Therefore, we use Sinkhorn's algorithm [32] to approximately calculate the Wasserstein distance. We vary d from 1 to 20 and set ϵ as 5 to further compare SEM-Geo-I and our DAM from Figure 9(f) to Figure 9(j). We can see, as d increases, the Wasserstein distances of both SEM-Geo-I and DAM also increase. Our DAM is better than SEM-Geo-I when d is larger. This occurs because as d increases, the discrete DAM gradually approaches to the continuous DAM in shape, and its error from grid diminishes. Consequently, the advantages of DAM become increasingly apparent.

3) Privacy Budget ϵ: The privacy budget ϵ not only affects the reported probability, but also influences the norm distance b. Figures 9(k) to 9(o) show how the value of W_2 changes with the change in ϵ. As ϵ increases, W_2 decreases slightly. This is because a large ϵ leads to a high probability report of the real data set, which makes the recovered density closed to the actual one. Our solution, DAM, is always better than MDSW. As ϵ increases, DAM achieves better estimation than HUEM. In addition, SEM-Geo-I slightly outperforms our DAM when ϵ is small. That occurs because a small ϵ causes the high probability domain to cover the input domain, making the differences between input cells less distinguishable. This will diminishes DAM's advantage. For SEM-Geo-I, as ϵ decreases, its output domain space complexity grows by $n^k = O(n^{n/e^{\epsilon}})$ $(n = d^2)$, exceeding our experiments' tolerance range for large d. To keep SEM-Geo-I feasible, we must set d to a small value when ϵ is small. However, a small d further distorts the shape of discrete DAM (see the *Discrete side length d* analysis



(a) Crime (b) NYC (c) Normal (d) SZipf (e) MNormal

(f) Crime (g) NYC (h) Normal (i) SZipf (j) MNormal

(k) Crime (l) NYC (m) Normal (n) SZipf (o) MNormal

(p) Crime (q) NYC (r) Normal (s) SZipf (t) MNormal

Fig. 9: Wasserstein distances with d or ϵ varied.

in Subsection VII-C2), leading to its poor performance. We further compare our DAM to SEM-Geo-I under larger ϵ by Sinkhorn's algorithm [32] in Figure 9(p) to 9(t). We set the d as 15 and vary ϵ from 5 to 9. In both DAM and SEM-Geo-I, W_2 decreases as ϵ increases. As ϵ becomes larger, W_2 of the two mechanisms approach 0, because a larger ϵ leads to higher accuracy for private distribution estimation. DAM outperforms SEM-Geo-I when ϵ is large.

VIII. Conclusion

In this paper, we study Private Spatial Distribution Estimation Problem. We propose a general framework called Spatial Area Mechanism (SAM) and a simple mechanism called Hybrid Uniform-Exponential Mechanism (HUEM). We further propose the optimal solution DAM among all SAM, leveraging the ordinal relationship between each data point to improve the accuracy of private distribution estimation. Besides, we propose a shrinkage method to improve the estimation accuracy in the grid circumstance. What's more, we compare our DAM with the state-of-the-art mechanisms to demonstrate that DAM can achieve the minimum Wasserstein distance among all mechanisms.

Acknowledgment

Peng Cheng's work is supported by the National Natural Science Foundation of China under Grant No. 62102149. Libin Zheng's work is supported by National Natural Science Foundation of China No. 62472455 and U22B2060. Xiang Lian's work is supported by Natural Science Foundation (NSF CCF-2217104). Lei Chen's work is partially supported by National Key Research and Development Program of China Grant No. 2023YFF0725100, National Science Foundation of China (NSFC) under Grant No. U22B2060, the Hong Kong RGC GRF Project 16213620, RIF Project R6020-19, AOE Project AoE/E-603/18, Theme-based project TRS T41-603/20R, CRF Project C2004-21G, Guangdong Province Science and Technology Plan Project 2023A0505030011, Hong Kong ITC ITF grants MHX/078/21 and PRP/004/22FX, Zhujiang scholar program 2021JC02X170, Microsoft Research Asia Collaborative Research Grant, HKUST-Webank joint research lab and HKUST(GZ)-Chuanglin Graph Data Joint Lab. Xuemin Lin's work is supported by NSFC U2241211 and U20B2046. Corresponding Author: Peng Cheng.

References

[1] C. Dwork, "Differential privacy," in *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II*, ser. Lecture Notes in Computer Science, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds., vol. 4052. Springer, 2006, pp. 1–12.

[2] R. Bassily and A. D. Smith, "Local, private, efficient protocols for succinct histograms," in *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, R. A. Servedio and R. Rubinfeld, Eds. ACM, 2015, pp. 127–135.

[3] T. Wang, J. Blocki, N. Li, and S. Jha, "Locally differentially private protocols for frequency estimation," in *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*, E. Kirda and T. Ristenpart, Eds. USENIX Association, 2017, pp. 729–745.

[4] J. C. Duchi, M. J. Wainwright, and M. I. Jordan, "Minimax optimal procedures for locally private estimation," *CoRR*, vol. abs/1604.02390, 2016.

[5] N. Wang, X. Xiao, Y. Yang, T. D. Hoang, H. Shin, J. Shin, and G. Yu, "Privtrie: Effective frequent term discovery under local differential privacy," in *34th IEEE International Conference on Data Engineering, ICDE 2018, Paris, France, April 16-19, 2018*. IEEE Computer Society, 2018, pp. 821–832.

[6] Z. Li, T. Wang, M. Lopuhaä-Zwakenberg, N. Li, and B. Skoric, "Estimating numerical distributions under local differential privacy," in *Proceedings of the 2020 International Conference on Management of Data, SIGMOD Conference 2020, online conference [Portland, OR, USA], June 14-19, 2020*, D. Maier, R. Pottinger, A. Doan, W. Tan, A. Alawini, and H. Q. Ngo, Eds. ACM, 2020, pp. 621–635.

[7] G. Cormode, S. Maddock, and C. Maple, "Frequency estimation under local differential privacy," *Proc. VLDB Endow.*, vol. 14, no. 11, pp. 2046–2058, 2021.

[8] L. Du, Z. Zhang, S. Bai, C. Liu, S. Ji, P. Cheng, and J. Chen, "AHEAD: adaptive hierarchical decomposition for range query under local differential privacy," in *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*, Y. Kim, J. Kim, G. Vigna, and E. Shi, Eds. ACM, 2021, pp. 1266–1288.

[9] T. Wang, B. Ding, J. Zhou, C. Hong, Z. Huang, N. Li, and S. Jha, "Answering multi-dimensional analytical queries under local differential privacy," in *Proceedings of the 2019 International Conference on Management of Data, SIGMOD Conference 2019, Amsterdam, The Netherlands, June 30 - July 5, 2019*, P. A. Boncz, S. Manegold, A. Ailamaki, A. Deshpande, and T. Kraska, Eds. ACM, 2019, pp. 159–176.

[10] J. Yang, T. Wang, N. Li, X. Cheng, and S. Su, "Answering multi-dimensional range queries under local differential privacy," *Proc. VLDB Endow.*, vol. 14, no. 3, pp. 378–390, 2020.

[11] N. Wang, Y. Wang, Z. Wang, J. Nie, Z. Wei, P. Tang, Y. Gu, and G. Yu, "Privnud: Effective range query processing under local differential privacy," in *39th IEEE International Conference on Data Engineering, ICDE 2023, Anaheim, CA, USA, April 3-7, 2023*. IEEE, 2023, pp. 2660–2672.

[12] S. Wang, Y. Nie, P. Wang, H. Xu, W. Yang, and L. Huang, "Local private ordinal data distribution estimation," in *2017 IEEE Conference on Computer Communications, INFOCOM 2017, Atlanta, GA, USA, May 1-4, 2017*. IEEE, 2017, pp. 1–9.

[13] R. B. Ash, *Information theory*. Courier Corporation, 2012.

[14] V. M. Panaretos and Y. Zemel, "Statistical aspects of wasserstein distances," *Annual review of statistics and its application*, vol. 6, pp. 405–431, 2019.

[15] S. Helgason and S. Helgason, *The radon transform*. Springer, 1980, vol. 2.

[16] S. Kolouri, K. Nadjahi, U. Simsekli, R. Badeau, and G. K. Rohde, "Generalized sliced wasserstein distances," in *Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, NeurIPS 2019, December 8-14, 2019, Vancouver, BC, Canada*, H. M. Wallach, H. Larochelle, A. Beygelzimer, F. d'Alché-Buc, E. B. Fox, and R. Garnett, Eds., 2019, pp. 261–272.

[17] R. Shokri, G. Theodorakopoulos, C. Troncoso, J. Hubaux, and J. L. Boudec, "Protecting location privacy: optimal strategy against localization attacks," in *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, T. Yu, G. Danezis, and V. D. Gligor, Eds. ACM, 2012, pp. 617–627.

[18] H. To, G. Ghinita, L. Fan, and C. Shahabi, "Differentially private location protection for worker datasets in spatial crowdsourcing," *IEEE Trans. Mob. Comput.*, vol. 16, no. 4, pp. 934–949, 2017.

[19] X. Gu, M. Li, L. Xiong, and Y. Cao, "Providing input-discriminative protection for local differential privacy," in *36th IEEE International Conference on Data Engineering, ICDE 2020, Dallas, TX, USA, April 20-24, 2020*. IEEE, 2020, pp. 505–516.

[20] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: differential privacy for location-based systems," in *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, A. Sadeghi, V. D. Gligor, and M. Yung, Eds. ACM, 2013, pp. 901–914.

[21] G. Cormode, C. M. Procopiuc, D. Srivastava, E. Shen, and T. Yu, "Differentially private spatial decompositions," in *IEEE 28th International Conference on Data Engineering (ICDE 2012), Washington, DC, USA (Arlington, Virginia), 1-5 April, 2012*, A. Kementsietsidis and M. A. V. Salles, Eds. IEEE Computer Society, 2012, pp. 20–31.

[22] W. H. Qardaji, W. Yang, and N. Li, "Priview: practical differentially private release of marginal contingency tables," in *International Conference on Management of Data, SIGMOD 2014, Snowbird, UT, USA, June 22-27, 2014*, C. E. Dyreson, F. Li, and M. T. Özsu, Eds. ACM, 2014, pp. 1435–1446.

[23] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. D. Smith, "What can we learn privately?" in *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*. IEEE Computer Society, 2008, pp. 531–540.

[24] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*. IEEE Computer Society, 2013, pp. 429–438.

[25] J. D. Bossler, J. Campbell, R. Mcmaster, and C. Rizos, "Coordinates and coordinate systems," *Manual of Geospatial Science and Technology*, pp. 9–16, 2010.

[26] T. Wang, M. Lopuhaä-Zwakenberg, Z. Li, B. Skoric, and N. Li, "Locally differentially private frequency estimation with consistency," in *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society, 2020.

[27] L. Du, P. Cheng, L. Zheng, X. Lian, L. Chen, W. Xi, and W. Ni, "Numerical estimation of spatial distributions under differential privacy," *arXiv preprint arXiv:2412.06541*, 2024.

[28] "[online] Chicago Crimes 2022," https://data.cityofchicago.org/Public-Safety/Crimes-2022/9hwr-2zxp, 2024.

[29] "[online] NYC Green Taxi Trip 2016," https://data.cityofnewyork.us/Transportation/2016-Green-Taxi-Trip-Data/hvrh-b6nb, 2024.

[30] Y. Du, Y. Hu, Z. Zhang, Z. Fang, L. Chen, B. Zheng, and Y. Gao, "Ldptrace: Locally differentially private trajectory synthesis," *Proc. VLDB Endow.*, vol. 16, no. 8, pp. 1897–1909, 2023.

[31] Y. Zhang, Q. Ye, R. Chen, H. Hu, and Q. Han, "Trajectory data collection with local differential privacy," *Proc. VLDB Endow.*, vol. 16, no. 10, pp. 2591–2604, 2023.

[32] M. Cuturi, "Sinkhorn distances: Lightspeed computation of optimal transport," in *Advances in Neural Information Processing Systems 26: 27th Annual Conference on Neural Information Processing Systems 2013. Proceedings of a meeting held December 5-8, 2013, Lake Tahoe, Nevada, United States*, C. J. C. Burges, L. Bottou, Z. Ghahramani, and K. Q. Weinberger, Eds., 2013, pp. 2292–2300.