

USING KD-LAPLACE TO TRAIN PRIVACY-PRESERVING CLUSTER ALGORITHMS ON DISTRIBUTED K-DIMENSIONAL DATA

by

Tjibbe van der Ende

in partial fulfillment of the requirements for the degree of

Master of Science
in Software Engineering

at the Open University, faculty of Management, Science and Technology
Master Software Engineering
to be defended publicly on Day Month DD, YYYY at HH:00 PM.

Student number: 852372917
Course code: IMA0002
Thesis committee: Dr. Ir. Mina Sheikhalishahi (chairman), Open University
Dr. Ir. Clara Maathuis (supervisor), Open University

CONTENTS

1	Introduction	1
2	Literature review	4
2.1	Differential privacy	5
2.2	Clustering	10
2.3	Literature review	16
3	nD-Laplace	26
3.1	2D-Laplace	26
3.2	3D-Laplace	31
3.3	kD-Laplace	35
4	Attacks on privacy	47
4.1	Membership inference attacks	47
4.2	Reconstruction attack	49
4.3	Attack evaluation	50
5	Methodology	52
5.1	Research design	52
5.2	Data collection	56
5.3	Data analysis	61
6	Results	62
6.1	Cluster utility	62
6.2	Mechanism utility	75
6.3	Privacy	81
7	Discussion	92
8	Conclusion	93
Bibliography		i
Hyperparameters		xi
.1	K-Means	xi
.2	Agglomerative clustering	xiii
Theory		xx
.3	Big O Notation	xx
Results		xxi
.4	Mechanism utility	xxi
.5	Privacy	xxvi

1

INTRODUCTION

Data has become an increasingly important part of our daily lives, and its applications are continuously growing. Personal and sensitive information, such as scrolling through Facebook or Instagram, is often sourced from various structured and unstructured data origins. As many businesses see the potential of data [noa, b], the urgency of protecting sensitive information also increases. This development is why there have been several regulations regarding data and privacy. Therefore, the European Union created the GDPR [noa, a], and the United States created the privacy act [Division, 2007]. For instance, the GDPR describes in Article 34 that data should always be stored in an "incomprehensible way for unauthorized people". Due to these regulations, it is challenging for companies to store and analyze data to gain insights.

A method for gaining insights into data is using unsupervised machine learning. It can be used to find a structure or pattern in uncategorized data [Dridi, 2021]. Clustering is a type of unsupervised learning commonly applied to group similar data points and reveal patterns and structures [Dridi, 2021]. Cluster algorithms need to be trained on an adequate amount of historical data, so the data needs to be stored and processed in an accessible location.

A common solution for hiding data from unauthorized access is encryption. Although this method is widely used for databases, it is unsuitable for data analysis. The data is unreadable for examination, and it adds communication overhead [Liu et al., 2022]. For this reason, researchers have explored methods for anonymizing data to protect the privacy of individuals [Sweeney, 2002]. But, this can still reveal much information about a person, as the range of possible values is limited. A more effective way to preserve privacy is by using differential privacy. This mechanism adds noise to the original data to hide the actual value, controlled by a privacy budget [Dwork, 2006]. Due to the configurability of this mechanism, it is possible to trade off privacy and utility in such a way it is possible to preserve data patterns. In recent years, the method was extended to add noise locally before sending it to a central server and called **Local Differential Privacy (LDP)** [Kasiviswanathan et al., 2010]. Although this method reduces privacy leakage risks because no plain data is stored on the server, the amount of data is limited in the local view. This makes the noise more significant, impacting the data utility [Yang et al., 2020].

RELATED WORK

The difficulty in preserving utility for clustering while preserving privacy is a well-known problem in the literature. A study that focuses on preserving the cluster shapes sends the feature's distance information to the server instead of the feature value [Sun et al., 2019]. Their method works on multiple cluster algorithms, compared to other studies focusing on a single cluster algorithm. However, their method leaks distance information. Another study aimed to improve this using a distance-aware randomization algorithm Xia et al. [2020]. This study was extended by Huang et al. to reduce the difference between actual and perturbed values [Huang et al., 2021]. Both studies focus on K-means and LDP but do not have direct support for other algorithms.

Existing literature focuses primarily on K-Means, without considering different cluster algorithms. Also, most of the work uses 2-dimensional synthetic, which is not representative of real-world data. Due to this inflexibility and lack of practical testing in the current literature, developing a solution closer to practical applicability becomes essential. Our research incorporates realistic attacks and datasets to test privacy and utility to bridge this gap and move towards a practically deployable LDP mechanism. Therefore, the overarching goal of this thesis is to develop a privacy framework that facilitates secure training of cluster algorithms on distributed n-dimensional data.

RESEARCH OBJECTIVE

Another take on Differential Privacy (DP) is called Geo-indistinguishability (GI) and is specifically used for geographical data [Andrés et al., 2012]. The 2D-Laplace mechanism adds noise to two data points (latitude/longitude) by generating random locations based on the amount of distance. The mechanism is configurable by a privacy budget and holds within a radius of the original location. An extension of this mechanism, called 3D-Laplace, added support for including the altitude to support indoor navigation [Min et al., 2022]. The mechanism has also been extended to nD-Laplace to support n-dimensional data; however, its application focuses entirely on text vectors [Fernandes et al., 2019].

Because the proposed method relies on distance-based considerations, it is plausible that the shape and structure of the data will be preserved during the clustering process. Consequently, we expect this algorithm to perform well for data clustering tasks. To our knowledge, GI has never been previously applied for data clustering. Therefore, the primary research objective of this study is to extend the use of GI to optimize specifically the clustering of data.

This thesis aims at developing a new privacy framework for training cluster algorithms on distributed n-dimensional data. It does so by extending and optimizing the three variants of nD-Laplace to support cluster algorithms. Our contribution to the current literature is as follows:

1. We aim to create a new privacy framework named kd-Laplace using the three variants of Laplace to train privacy-preserving cluster algorithms on distributed n-dimensional data.
2. In addition to K-means, we also demonstrate the working of our method on multiple other cluster algorithms.

3. We introduce different optimization techniques to improve the utility of kd-Laplace using kd-tree.
4. We demonstrate the privacy of kd-Laplace using real-world datasets and attacks.

RESEARCH QUESTION AND METHODS

To reach our goals and objectives, we have formulated the following main question:

"How can the kD-Laplace algorithm be applied in training privacy-preserving clustering algorithms on distributed k-dimensional data?"

Much literature is consulted to answer this research question, and we experiment extensively to gather enough qualitative data. Both external and internal validation methods are employed to assess the utility and privacy of the privacy mechanism. The qualitative data from these experiments are analyzed to compare the different privacy mechanisms and their performance concerning clustering tasks.

ROADMAP

The first chapter is devoted to literature study and review. We explain the various concepts related to clustering and differential privacy. This chapter concludes with a literature review. The second chapter explicitly focuses on the kd-Laplace part, explaining the relevant algorithms and concepts. We then delve deeper into privacy attacks and how they can be evaluated.

The following chapter is dedicated to describing the research itself and the methodology. Subsequently, we present the results, and finally, we conclude with the discussion and conclusions.

2

LITERATURE REVIEW

The current chapter explains the theoretical aspects of the research and evaluates similar and previous studies. First, the concept of Differential Privacy and its various types is explained. Next, we examine cluster algorithms and the methods for evaluating their performance. Regarding the related literature, we first look at studies that have used differential privacy and then the studies that have combined it with cluster methods.

2.1. DIFFERENTIAL PRIVACY

In practice, data is often sent to a central storage point. This requires trust, and because all data is collected in one place, the risk of private data leakage becomes very high. By applying DP, noise can be added to the data to protect it. This principle is illustrated in figure 2.1 with the following actors:

1. Trusted curator: The system that receives data from users. It is assumed in this setting that the system is trustworthy and that the data is securely stored.
2. Adversary: An adversary is someone who uses the data. This could be, for example, a data scientist who wants accurate results or an attacker who wants to obtain as much data as possible.
3. The users are clients (for example, websites or mobile apps) who entrust their data to a central server.

To a certain extent, a user's privacy would be ensured with differential privacy.

Although differential privacy solves privacy problems, it remains challenging to calibrate the mechanism. There is an important trade-off between utility and privacy for the adversary. For example, a data scientist wants accurate data. At the same time, the noise must be sufficient to prevent an attacker from obtaining too much information. For this reason, a few sections will be devoted to outlining the mathematical background of differential privacy. We will examine which factors influence this calibration and whether other methods contribute. Afterward, we will further explain other types of differential privacy (local and geo-indistinguishable) similarly.

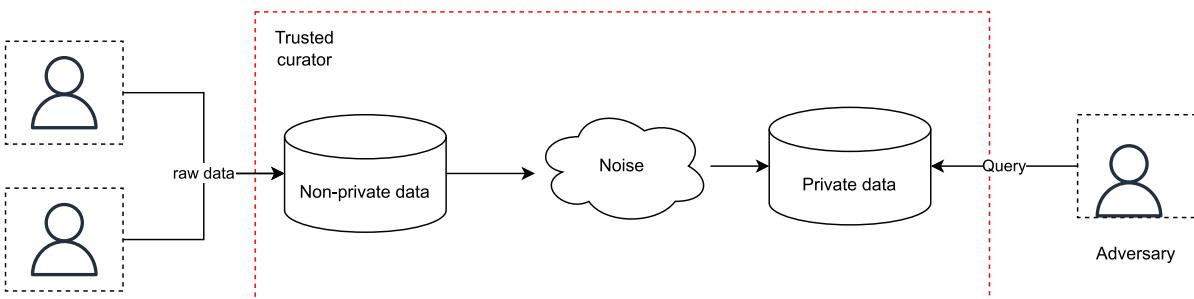


Figure 2.1: General approach for setting up (central) differential privacy.

On the left side are the users, who send their data to the trusted curator. The trusted curator collects all the data (e.g., a database) and adds noise to the data. The adversary (right) can access the private data but should not be able to access the non-private data.

2.1.1. DEFINITIONS

We examine the different notations and types of differential privacy we consider in this research.

ϵ -DIFFERENTIAL PRIVACY

Dwork et al. formulated the notion of privacy: Participating in a database should not significantly increase the risk of an individual's privacy being compromised [Dwork \[2006\]](#). This is mathematically formulated in the same research named [DP](#). Using the definition of privacy, it is formulated as the maximal possible change when adding or removing a single record [\[Dwork, 2006; Friedman and Schuster, 2010\]](#). This is reflected using the formal mathematical formulation as formulated by Dwork et al:

$$\Pr[K(D_1) \in S] \leq \exp(\epsilon) \times \Pr[K(D_2) \in S] \quad (2.1)$$

So, given a randomization function K , it gives ϵ -differential privacy if dataset D_1 and D_2 are differing at most one element [\[Dwork, 2006\]](#). The ϵ determines the amount of noise (privacy budget) [\[Friedman and Schuster, 2010\]](#). The lower the value of ϵ , the higher the privacy guarantee. In this regard, it is essential for a method that ensures differential privacy to consider this. For this reason, a common way to calibrate the ϵ is to calculate the sensitivity. This value is calculated based on the impact of a function or query on the data. For example, if there is a method called *sum* for the summation of data points, the method's sensitivity is 1. This is because removing one data point would significantly affect the outcome, and ϵ -differential privacy could no longer be guaranteed. It is also mathematically defined by Dwork et al.:

$$\Delta f = \max_{D_1, D_2} \|f(D_1) - f(D_2)\|_1 \quad (2.2)$$

(ϵ, δ) -DIFFERENTIAL PRIVACY

The formal notion of differential privacy has only the privacy budget ϵ as a parameter. This formulation is strict, but most methods relax this a little, with (ϵ, δ) :

$$\Pr[K(D_1) \in S] \leq \exp(\epsilon) \times \Pr[K(D_2) \in S] + \delta \quad (2.3)$$

This equation means the sensitivity (δ) loosens the formal definition of differential privacy. The δ is added to the upper bound of the exponential, so the desired noise can be higher. To some extent, the delta represents the probability of the algorithm leaking information [\[Aitsam, 2021\]](#). With ϵ -differential privacy, there would be no difference in the case of information leakage ($\delta = 0$). However, with (ϵ, δ) -differential privacy, the information can leak up to the probability of delta.

ϵ -LOCAL DIFFERENTIAL PRIVACY

As the name suggests, LDP is executed on the client side instead of on the server (See Figure 2.1). Local differential privacy removes the "trusted" curator (See Figure 2.2), preventing sensitive data leakage even if an attacker gains access to the dataset [Xiong et al., 2020a]. The definition for LDP is the same as for equation 2.3 with $\delta = 0$ being equal to equation 2.1.

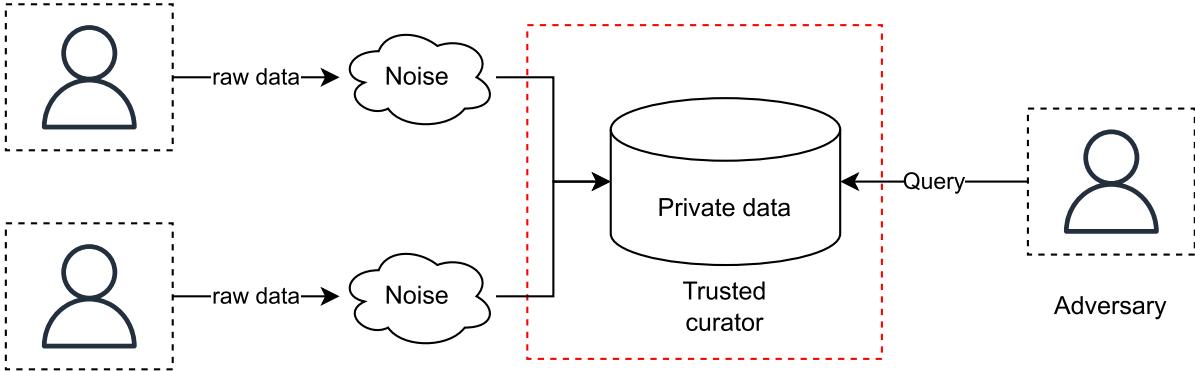


Figure 2.2: Local differential privacy, which moves the noise-adding step to the client-side.

Local differential privacy has two different frameworks. It can be set up as interactive or non-interactive [Xiong et al., 2020a]. Where interactive can be distinguished as either sequentially interactive or fully interactive¹:

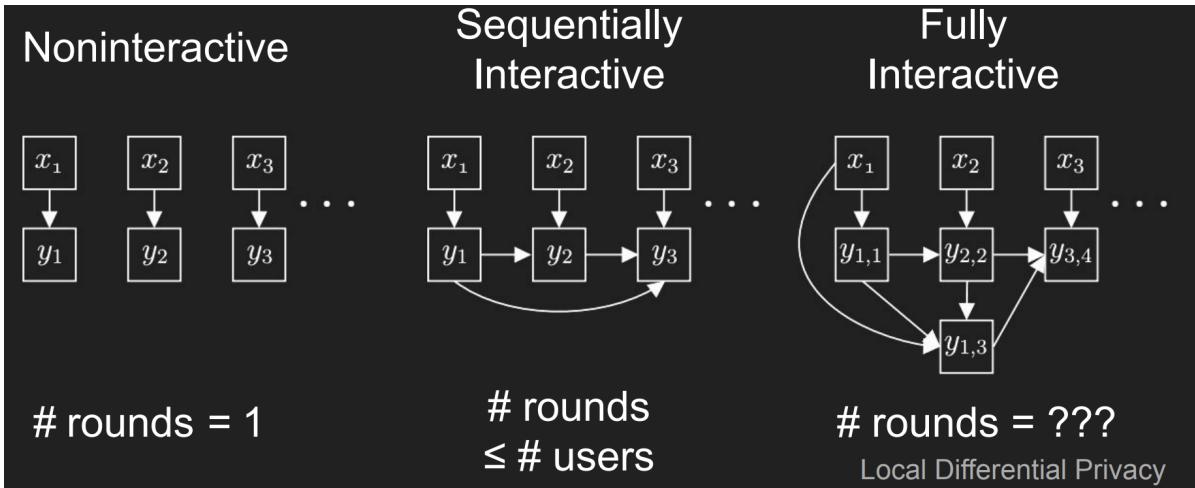


Figure 2.3: Non-interactive versus sequentially interactive versus fully interactive local differential privacy [Joseph et al., 2019]

In the non-interactive framework, the privacy mechanism operates on a single data instance (e.g., users' smartphones) without requiring interaction with other clients or between data points. This interaction means that each data point is perturbed independently, and the privacy guarantees are achieved without communication or coordination between the data points. In the interactive framework, the privacy mechanism involves a process of iterative interactions between users and clients. Each data point considers other data points' responses to determine its own perturbation or privacy level. The interactions can

¹Image source: https://www.majos.net/focs_19_talk.pdf

occur through a communication channel, where data points exchange information with each other or a trusted mediator. The iterative nature of the interactive framework allows for refining and improving the privacy guarantees based on the global knowledge of the data set.

In figure 2.3, the different interactive types are visualized, where the most notable difference is the around of rounds [Xiong et al., 2020b]. A sequentially interactive framework passes at most one message between data points. A fully interactive framework could provide an unknown and unlimited amount of messages between data points. The interactive framework has unlimited access to other data points, which is most suitable for practical appliances [Xiong et al., 2020b]. The practical applications are better because the data points' mutual correlation also contributes to utility [Wang et al., 2020].

ϵ -GEO-INDISTINGUISHABILITY

The last and most important type of differential privacy for this study is GI. GI can be applied to preserve privacy using a differential privacy method specific to spatial data [Andrés et al., 2012]. Consider a local-based system (LBS) that provides a map service to its users (e.g., Google Maps). The users can query the LBS for a route from their current location to a destination. Instead of the exact (private) location, the LBS should only receive an approximate location enough to provide the service at an adequate level. This approximation happens entirely locally, so no central server exists.

Users can define a privacy radius r around their location x . A fake location z is generated within this radius based on the Euclidean distance d .

The amount of noise within r depends on the privacy budget ϵ . The privacy budget is based on the privacy level l , combined with r to obtain ϵ using the formula $\epsilon = \frac{l}{r}$.

Calculating the privacy budget is illustrated in the figure below:

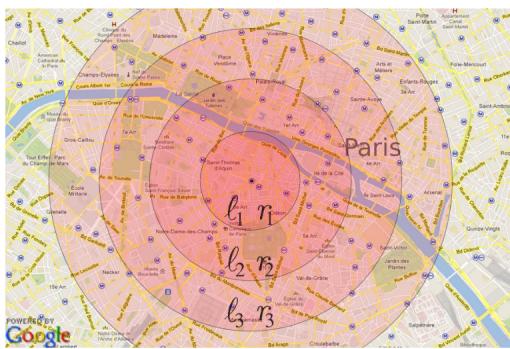


Figure 2.4: Visualisation of radius r with l to provide Geo-indistinguishability mechanism [Andrés et al., 2012]

The formula for GI to measure if an algorithm preserves ϵ -geo-indistinguishability can be expressed as:

$$K(x)(y) \leq e^{\epsilon * d(x, x')} K(x')(y) \quad (2.4)$$

K is a probability method reporting $x, x' \in X$ as $z \in Z$. The intuition for this definition is that it displays the distinguishability level between two secret locations/points x and x' [Chatzikokolakis et al., 2015]. An extension of this is called d_x -privacy, a more general notation of distance-aware differential privacy. Therefore, their definition for GI is d_2 -privacy, but is essentially the same as the proof provided for GI.

2.1.2. MECHANISMS

This section explains the various mechanisms used to achieve differential privacy. The different mechanisms are not limited to the type of DP; some can be applied to multiple types.

RANDOMIZED RESPONSE MECHANISM

The random response method is relatively simple and was first applied in 1965 by Warner et al. It was originally used to mask individuals' answers by randomly switching them with predictable randomness [Warner, 1965]. Therefore, the method is mainly used for categorical data. This method satisfies its own set of requirements for LDP [Xiong et al., 2020a], which differs from the formal definition that was mentioned earlier

Since then, it is still one of the better-known methods, and larger organizations such as Google have used it [Erlingsson et al., 2014]. They have named their extension RAPPOR and expanded it with bloom filters to be able to collect numerical data as well. It is possible to ensure ϵ -differential privacy, and it is also possible to preserve LDP [Xiong et al., 2020a].

LAPLACE MECHANISM

The method that was initially proposed in the differential privacy paper by Dwork et al. is the Laplace algorithm [Dwork, 2006]. Therefore, the method configures the ϵ and δ . A shorthand definition is provided by Rey et al. [Xiong et al., 2020a]:

$$M(f(x), \epsilon) = f(x) + (Z_1, \dots, Z_d) \quad (2.5)$$

The mechanism is based on the Laplace distribution with scale $\lambda f / \epsilon$, where λf is the same as in equation 2.2. Therefore, the Laplace mechanism is tightly linked to the definition of DP [Dwork, 2006]. In addition to this, it is also suitable for preserving LDP [Xiong et al., 2020a]. One disadvantage is that sensitivity is always required, and this parameter can sometimes be difficult to configure. Especially when there is no clear function and the entire dataset is perturbed. This can make finding the right balance between ensuring privacy and utility challenging.

To this end, the sensitivity can be calculated in two forms: global and local. Global sensitivity is independently calculated over two different datasets and is part of the original definition of DP [Dwork, 2006]. Usually, this is not the desired situation since local sensitivity always has more context of the dataset in question [Nissim et al., 2007]. As a result, the trade-off for noise is much more precise, and the balance between utility and privacy is much better. The definition of local sensitivity is the following [Nissim et al., 2007].

$$LS(f, x) = \max_{x' : d(x, x') \leq 1} |f(x) - f(x')| \quad (2.6)$$

A methodology to calculate the local sensitivity is using the smooth sensitivity method, proposed by the same authors [Nissim et al., 2007]. This method aims at smoothing out the local sensitivity by focusing on reducing the noise without the risk of revealing more information. Because it calculates many different configurations, a disadvantage of this method is that it can be computationally expensive. Also, the introduction of this method makes Laplace preserve (ϵ, δ) -DP instead of pure ϵ -DP.

2.2. CLUSTERING

This section explains the various cluster algorithms used in the research. Subsequently, we will explain and indicate how the hyperparameters are handled in the research for each algorithm.

2.2.1. TYPES OF CLUSTER ALGORITHMS

Multiple cluster types can be utilized for clustering data [Xu and Tian, 2015]. For this study, we selected the types that use some form of distance for clustering. We explain each cluster type with corresponding cluster algorithms.

PARTITION BASED CLUSTERING

With this type, the data is partitioned and allocated into a fixed amount of clusters. A well-known and popular cluster algorithm is K-means. Based on Loyd et al.'s original method, this algorithm randomly selects k points as cluster centroids [Lloyd, 1982]. Iteratively each data point is assigned to its nearest centroid. It keeps proceeding until the distance between the cluster centroids is optimal. Although K-means serves its purpose well, it requires pre-defining the number of clusters and is sensitive to outliers [Keller et al., 2021]. Therefore, a parameterless alternative to K-means is **Affinity Propagation (AP)** [Frey and Dueck, 2007].

AP is an algorithm that clusters data points by iteratively passing messages between them. Each point sends and receives messages about the attractiveness of other points as cluster centers (exemplars) and the suitability of itself as a center [Keller et al., 2021].

DENSITY BASED CLUSTERING

The data points are partitioned for this clustering type based on nearest neighbors [Fahad et al., 2014]. A region with a high data density is considered a cluster [Xu and Tian, 2015]. A popular density-based cluster algorithm is **Density-based spatial clustering of applications with noise (DBSCAN)**. The method was introduced by Ester et al. and worked by drawing a radius ($radius(\epsilon)$, not to be confused with the privacy budget ϵ) around data points [Ester et al.]. It then groups all points within this radius as clusters. The main advantage is its ability to find arbitrarily shaped clusters and detect outliers [Liu et al., 2012].

Another density-based algorithm is **Ordering Points to Identify Clustering Structure (OPTICS)**, an extension of DBSCAN. This algorithm attempts different $radius(\epsilon)$ values to achieve the best result [Ankerst et al.]. Instead of directly assigning data points to clusters, specific distance calculations are stored in a list. For each data point, it tracks two values: core distance and reachability distance. These values represent the shortest distance to make a data point, p , a core point, and the shortest distance from p to another core point, p' , respectively. A specific ordering is maintained to ensure that clusters with higher density values are processed first. Based on this ordering, the DBSCAN algorithm is constructed hierarchically [Schubert et al., 2017].

HIERARCHICAL CLUSTERING

A hierarchy of clusters is generated and merged according to the closeness of data points [Meng et al., 2021]. Hierarchical clustering can be divided into agglomerative and divisive [Meng et al., 2021]. This approach means the clustering occurs from the bottom-up or top-down, respectively. Of the two approaches, agglomerative is the most common one [Meng et al., 2021]. For the implementation, there are four popular methods: Single link, Average

link, Complete link, and Ward's method [Roux, 2015]. These methods are used to calculate (dis)similarities between objects.

Another Hierarchical cluster algorithm is **Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH)**. This algorithm works by constructing a tree with nodes (so-called clustering feature) [Zhang et al., 1996]. The algorithm does this iteratively until a cluster becomes too large or diverse. The algorithm will split again into similar clusters until all data is processed [Zhang et al., 1996].

RESEARCH DIRECTION

There are three different types of cluster algorithms that we have considered for this research. Therefore, we will choose one algorithm for each type to ensure a representative selection.

Based on the different types of clustering algorithms, we have chosen to use K-Means for this research. K-Mean clustering is widely used in the literature and, therefore, easily compared with other studies.

For density-based clustering, we will solely focus on **OPTICS** in this study. The parameter *radius*(ϵ) in **DBSCAN** is influenced by the data shape, which is further affected by our privacy mechanism. However, as **OPTICS** automatically determines the *radius*(ϵ), the impact of this parameter is less significant, enabling us to emphasize the evaluation of the privacy mechanism itself.

As for hierarchical clustering, we have decided to go for agglomerative clustering. This approach is the most common and straightforward compared to **BIRCH**.

2.2.2. PARAMETER SELECTION

A list of important hyperparameters that can influence the results is provided for each clustering algorithm. Subsequently, we briefly discuss the methods for determining these hyperparameters for the algorithms.

We use the same distance function for all algorithms to have all the algorithms in the same setting. This function will be Euclidean distance, as used for **GI**.

K-MEANS

The most crucial parameter of the K-Means algorithm is the value of k . This value determines the number of clusters to consider and influences the results by a lot [Ahmed et al., 2020]. The first method is called an "elbow" plot [Kodinariya and Makwana, 2013]. This method finds the best k by applying the K-Means algorithm multiple times and estimating the best k . In this situation, a Silhouette plot can be used to determine the k . This method uses the Silhouette coefficient for each cluster [SAPUTRA et al., 2020]. Because this metric measures the separation and cohesion of the cluster, it can be used to choose an optimal amount of clusters [SAPUTRA et al., 2020]. By visualizing the silhouette scores, the k with the highest coefficient has the best-separated clusters.

Another method is the Gap statistic method [Yuan and Yang, 2019]. It compares the total within-cluster variation for different values of k with their expected values under a null reference distribution of the data [Tibshirani et al., 2001]. A practical appliance of this method uses a line plot for comparing the k -value and gap value [Yuan and Yang, 2019]. Based on the line's visual change, someone can select the best k (see Figure 2.5).

In summary, no fixed method exists to choose a good k for K-Means. The elbow method is standard in the existing literature and is very popular due to its simplicity. However,

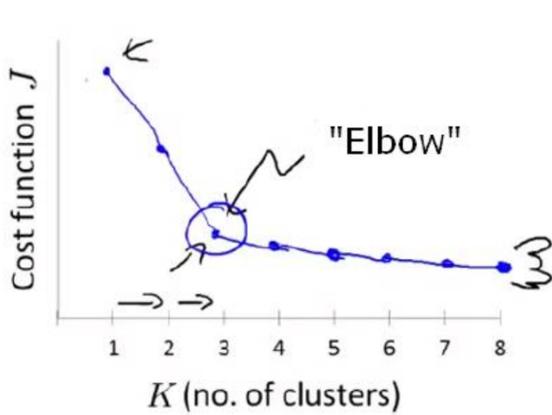


Figure 2.5: Illustration of determining k using the "elbow" method [Kodinariya and Makwana, 2013]

one disadvantage is that it can be challenging to determine the "elbow" point, as it is not always present [Kodinariya and Makwana, 2013]. In that case, the silhouette or gap statistic method is a good alternative, where the silhouette score is the simpler method.

AGGLOMERATIVE CLUSTERING

The agglomerative clustering algorithm has two essential hyperparameters: the linkage method and the number of clusters.

Choosing linkage: This decision is crucial for the algorithm as it determines the similarity measurement. Choosing a linkage method that uses Euclidean distance is important for our research. From the four different types of linkage methods, we have chosen the Ward method because this method uses Euclidean distance [Roux, 2015; Seetharaman et al., 2019].

Choosing number of clusters: There are not many methods for determining the initial number of clusters. Therefore, the approach is similar to K-Means. The amount of clusters is selected based on the "elbow" with the highest silhouette score.

OPTICS

With the introduction of OPTICS, we no longer need to worry about the $\text{radius}(\epsilon)$ value. Therefore, only minPts remains an important parameter to consider.

The minPts is the minimum amount of points that have to be within the $\text{radius}(\epsilon)$ to mark it a cluster. This hyperparameter is analyzed in a paper by Sander et al. The work describes calculating this parameter by applying two times the feature amount [Sander et al., 1998]. So, using this approach, a dataset with two features will have an minPts of four [Schubert et al., 2017].

DBSCAN is a little more complicated due to the variety of datasets and noise-altering mechanisms we experiment with. This complexity is why we use OPTICS to determine the best value for $\text{radius}(\epsilon)$ and choose minPts based on the number of features times two.

2.2.3. EVALUATION METHODS

Clustering comparison measures are important in cluster analysis for external validation by comparing clustering solutions to a "ground truth" clustering [Vinh et al.]. These external validity indices are a common way to assess the quality of unsupervised machine learning methods like clustering [Warrens and van der Hoef, 2022]. A method that could be used for

this is the Rand Index [Rand, 1971]. It is a commonly applied method for comparing two cluster algorithms [Wagner and Wagner]. An improvement of this method is adjusted for chance by considering the similarity of pairwise cluster comparisons [Vinh et al.]. Both the Rand Index (RI) and Adjusted Rand Index (ARI) [Hubert and Arabie, 1985] report a value between 0 and 1. Where 0 is for no-similarity and 1 for identical clusters. Alternatives for RI are the Fowlkes-Mallows Index and Mirkin Metric. However, these two methods have their disadvantages. They are, respectively, sensitive to a few clusters and cluster sizes [Wagner and Wagner]. The ARI metric suffers from cluster size imbalance as well, so it only provides not a lot of information on smaller clusters [Warrens and van der Hoef, 2022]. Instead, they recommend using the cluster index metric proposed by Fränti et al. [Fränti et al., 2014].

Another popular group of methods is the information theoretic-based measures [Vinh et al.]. This metric measures the information between centroids; the higher the value, the better [Vinh et al.]. Mutual Information (MI) is a metric that calculates the probability of an element belonging to cluster C or C' . But, it is not easy to interpret as it does not have a maximum value [Wagner and Wagner]. To this end, Normalized Mutual Information (NMI) can be used to report a value between 0 and 1 using the geometric mean [Strehl and Ghosh, 2002]. The metric also exists in an adjusted version as Adjusted Mutual Information (AMI). This metric works in the same way as for the Adjusted Rank Index (ARI) and is mainly needed if the number of data items is small in comparison to the number of clusters [Vinh et al.].

Besides the external validity measurements for clustering, it is also possible to use internal validation methods. These metrics focus entirely on the intrinsic dataset properties instead of relying on an external baseline cluster algorithm [Craenendonck and Blockeel]. They are assessing two essential concepts of clustering: compactness and separation [Hassani and Seidl, 2017]. Both studies consider three different metrics and measure both concepts at the same time [Hassani and Seidl, 2017]:

1. Calinski-Harabasz Index (CHI) [Caliński and Harabasz, 1974] is used to measure the cluster variance (well-separated clusters) and low variance within the clusters (tightly coupled data). A high score indicates better clustering.
2. Silhouette Coefficient (SC) [Rousseeuw, 1987] This metric is similar in measuring cohesion within and separating clusters. However, this metric uses the pairwise distance Hassani and Seidl [2017]. A score of -1 indicates incorrect clustering and +1 for dense clusters Rousseeuw [1987].
3. Davies-Bouldin (DB) [Davies and Bouldin, 1979] uses the average distance between centroids. A lower score indicates good clustering.

K-Means scores relatively high for CHI [Craenendonck and Blockeel; Hassani and Seidl, 2017] and SC [Craenendonck and Blockeel]. The same applies to OPTICS/DBSCAN, which scores relatively high on SC and DB due to noise sensitivity [Craenendonck and Blockeel].

EXISTING LITERATURE

Comparable studies with differential privacy use external validation [Sun et al., 2022; Xia et al., 2020]. Their experiment setup uses a so-called non-private cluster algorithm as external validation. This cluster algorithm is trained without the perturbed data and compared

with the same clustering algorithm trained with perturbed data. Thus, the non-private variant provides the ground truth as an external validation.

They compare the mutual information between a baseline cluster algorithm using **AMI** [Huang et al., 2021] or **NMI** [Sun et al., 2022; Xia et al., 2020]. Another study for evaluating **DP** with **AP** uses both **ARI** and **AMI**. In addition to mutual information and rand index scores, it is also not uncommon to calculate the error between the two cluster algorithm's centroids [Huang et al., 2021; Xia et al., 2020]. These two studies used Relative Error (RE) for this.

RESEARCH DIRECTION

This chapter outlines the evaluation methods used and provides a definition and brief explanation for each method.

In the literature, both internal and external evaluation methods are commonly used. While some studies choose one over the other, this thesis will perform both validations. This approach is crucial to measure how well the data shape is preserved (internal validation) and how the algorithm performs in real-world scenarios (external validation). Our research will focus on **AMI** for external validation. Because it holds the same value as **ARI**, but it is better explainable. The second metric we use is for external validation. We use **SC** because this metric returns a bounded value between -1 and 1.

Based on existing studies and the literature, we have selected metrics adjusted to compensate for the data distribution characteristics. Hence, we will focus on these metrics' "adjusted" variants:

1. Internal validation:

- (a) **Silhouette coefficient:** This metric is defined as follows [Liu et al., 2010; Rousseeuw, 1987]:

$$s(i) = \frac{b(i) - a(i)}{\max(b(i) - a(i))} \quad (2.7)$$

- i. $s(i)$ is the silhouette coefficient for a single datapoint i .
- ii. $a(i)$ is the mean distance of i and all the other points in the same cluster.
- iii. $b(i)$ is the mean distance of i and all the other points in the next nearest cluster.

Finally, the final silhouette score is the mean of all datapoint coefficients $s(i)$.

2. External validation:

- (a) **Adjusted Mutual Information:** As was the case for the **ARI**, the **AMI** is also defined in two steps. The first step is to calculate the actual **MI**, and the second is to adjust it for chance. The **MI** is defined as follows [Vinh et al.]:

$$H = - \sum_{i=1}^U p(i) \cdot \log p(i) \quad (2.8)$$

H is the uncertainty for one variable given another variable. So it can be used to measure the (dis)similarity between two variables.

- i. U is a label to calculate the uncertainty for.

ii. $p(i)$ is the probability of a random point i falling into class/labe U .

This same calculation is executed for the second label V and divided by each other.

$$MI = \frac{MI - \text{Expected}(MI)}{\text{mean}(H(U), H(V)) - \text{Expected}(MI)} \quad (2.9)$$

2.3. LITERATURE REVIEW

In the search for related literature, we focused mainly on (L)DP mechanisms that can be used for general purposes (e.g. not only mean estimation), which is the most comparable to our mechanism. The related literature is divided into three parts:

1. Differential privacy and clustering: We explain how differential privacy is used for clustering.
2. Differential privacy methods: We explain the different methods for differential privacy.
3. Cluster methods with (L)DP: We explain the different methods for clustering with (L)DP.

Afterward, we provide a summary for both in a table. This table includes components such as the type (LDP or DP) and whether a public code is available.

2.3.1. DIFFERENTIAL PRIVACY AND CLUSTERING

There are different ways how to combine differential privacy with clustering [Baraheem and Yao, 2022]:

1. Input perturbation: This method adds noise to the input data, so the cluster algorithms are trained on perturbed data.
2. Gradient perturbation: The term gradient is used in machine learning algorithms that solve an optimization problem like deep learning [Hassan et al., 2019]. Perturbing the gradients ensures the optimization algorithm is private [Ji et al., 2014].
3. Output/label perturbation: This method adds noise to the output of the clustering algorithm. The noise is added to the cluster labels, so the results are perturbed.
4. Objective perturbation: This method slightly differs from output/label perturbation but also adds noise to the output. The difference is it is added to the output of a loss function instead of the labels (for example, logistic regression) [Baraheem and Yao, 2022].

Many approaches targeting local differential privacy mechanisms must adapt the clustering algorithm (for example, k-Cluster) [Sun et al., 2019], which we explain later in this chapter. For this reason, we concentrate on input perturbation in this study, as it allows the dataset to be used multiple times to train various clustering algorithms.

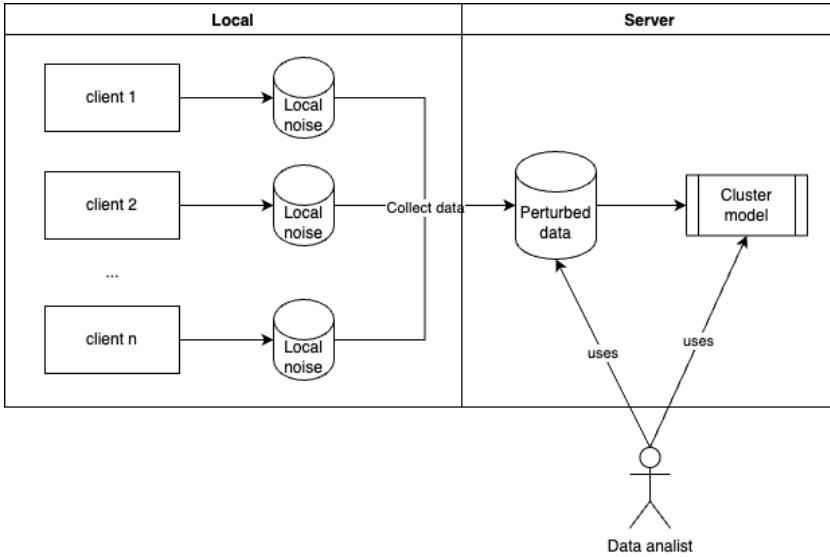


Figure 2.6: Example on how our approach of private training works for clustering and DP

1. Left, each local dataset is perturbed using our method (locally).
2. All data is collected and used to train a clustering algorithm (on the server).
3. A cluster model is privately trained because we train the algorithm on private data.
4. Because we use input perturbation, a third party like a "data analyst" can also directly access the data privately.

The following section focuses on the differential privacy algorithms that are of interest to this type of input perturbation.

2.3.2. DIFFERENTIAL PRIVACY METHODS

As discussed earlier, the Laplace method was the first to establish DP [Dwork, 2006]. The first paper we discuss is provided by Soria-Comas et al. and considers the distribution of the dataset for generating noise [Soria-Comas and Domingo-Ferrer, 2013]. Their work claims the Laplace mechanism is not optimal for a univariate function and aims at improving it by extending the Laplace mechanism. The proposed method performs slightly better than Laplace on multivariate/multiple queries.

Quan et al. also proposed a new method to extend Dwork et al.'s Laplace algorithm [Geng et al., 2015]. They introduced the Staircase mechanism for 1-dimensional noise, which was later extended to support multidimensional data [Geng et al., 2015]. The mechanism aims to improve utility by adding the same level of privacy while adding less noise. It represents a staircase-shaped **Probability Density Function (PDF)**, hence the name Staircase Mechanism (SM). This mechanism accepts three configurable parameters comparable to those of the Laplace mechanism. The authors' work can handle multidimensional numerical data and preserve the (ϵ) -differential privacy. In the previous two paragraphs, we have mainly focused on the interesting literature regarding differential privacy. Next, the succeeding paragraphs will mainly center on related literature concerning local differential privacy.

Nguyen et al. introduced a new **LDP** mechanism for working with numerical data [Nguyễn et al., 2016]. Their primary focus is estimating means and frequencies on data and applying machine learning techniques such as Support Vector Machines (SVM) and linear regression using Empirical Risk Minimization. Initially, the authors analyze Duchi et al.'s method [Duchi et al., 2013] and highlight several shortcomings. To address these issues, they introduce Harmony as a mechanism for **LDP** perturbation. This mechanism can perturb categorical and numerical data, providing high accuracy for classification and regression tasks. To compare Harmony to other methods, they create the Hybrid Mechanism (HM), a combination of two existing methods for categorical and numerical data. For this purpose, they extend other work [Bassily and Smith, 2015] for perturbing multidimensional categorical attributes and use Duchi et al.'s method for numerical data [Duchi et al., 2013]. This combination of mechanisms allows them to compare their Harmony mechanism to the hybrid mechanism and measure the utility/accuracy differences.

Duchi et al. improved their method by formalizing the trade-off between statistical utility and (local) privacy, analyzing multiple estimation problems [Duchi et al., 2017]. Examples include mean, median, and density estimation. To achieve this, they use minimax, a technique for finding the worst-case probability distribution. Additionally, they focus on existing work and propose several optimization strategies.

Duchi et al.'s method was extended a couple of years later by adding support for bounded and multidimensional data [Wang et al., 2019]. The authors introduce the **Piecewise Mechanism (PM)** to handle numeric and categorical data and the Hybrid Mechanism (HM), which combines **PM** and Duchi et al.'s method for 1-dimensional data. Their method's effectiveness is demonstrated using **Support Vector Machine (SVM)**, linear regression, and mean estimation. **PM** and HM are compared to Laplace and Duchi et al.'s solutions. Optimized Unary Encoding (OUE) [Wang et al.] is also used for comparison, but for categorical data only, as the other methods do not support this.

2.3.3. CLUSTER METHODS WITH (L)DP

This chapter examines the various studies conducted on clustering in combination with differential privacy. Initially, we looked at the most fundamental papers in this field. Subsequently, the focus shifted toward researching well-known papers published since 2020.

The first work we highlight was proposed by Nissim et al. and aimed at improving differential privacy methods, such as Laplace, which uses sensitivity to compensate the noise for a function [Nissim et al., 2007]. In addition to compensating the function, they also consider the dataset itself. The algorithm is called "smooth sensitivity" and is used for instance-specific noise. To apply it, the authors introduce a method/framework to calculate it effectively. They use K-means, among other cluster algorithms, to demonstrate the method's effectiveness. Their method requires the calculation of cluster distances using Wasserstein distance instead of Euclidean distance.

Another study focuses on interactive and non-interactive approaches for differential privacy in K-Means [Su et al., 2015]. The study builds upon the work done for DPLlloyd, an interactive privacy extension of K-Means described by Blum et al. [Blum et al., 2005]. The DPLlloyd mechanism partitions an n -dimensional dataset into a grid and releases the count for each grid by adding Laplacian noise to each count. Another part of their research focuses on determining the width of the data cells. The grid estimation method used in their research is called the extended uniform grid approach (EUG), and the complete K-Means method is called EUGkM. The experiment evaluates it against the DPLlloyd mechanism, which performs better in an interactive setting. Therefore, they combine their algorithm for combining both aspects into a hybrid approach (EUGkM + DPLlloyd approach) and show a better final performance.

The study of Nissim et al. researches finding the smallest possible radius in the Euclidean space R^d for a set of n points [Nissim and Stemmer, 2018]. They propose a new solution that uses locality-sensitive hashing (LSH) for differential privacy to find 1-cluster in the d -dimensional Euclidean space. This method works for differential privacy (LSH-GoodCenter), but they also extend this to the local model (LDP-GoodCenter). The algorithm to find this radius is used to count the points enclosed by the radius, and Laplace noise is added to the count to preserve differential privacy. The mechanism is combined and applied to work with the K-Means algorithm (LDP-K-Mean). This mechanism was extended in a paper proposed by Kaplan et al. and introduced a similar LDP method [Kaplan and Stemmer, 2018]. They aim to reduce the number of interactions needed between the server and users to one, instead of the $O(k \log n)$ required for Nissam et al.'s solution [Nissim and Stemmer, 2018]. To increase the success probability, they use the same idea but extend it to have multiple centers instead of a single large one. They call it the LSH-Procedure, and the algorithm Private-Centers is applied to generate centers to use with K-Means. Then, they apply the same method to the LDP method initially proposed by Nissam et al. (LDP-GoodCenter). The most recent work by Stemmer et al. focuses on improving the work done by Kaplan et al. [Kaplan and Stemmer, 2018; Stemmer, 2021]. Because the original mechanism has a higher additive error, the noise added introduces a lot of error. To solve this, the authors aim to reduce this error by improving the original GoodCenter algorithm [Nissim and Stemmer, 2018]. Their extended method is called WeightedCenters and also adds weights to candidate centers. In the final iteration, the weights are used to create the K-Means or K-Median clusters.

Sun et al. proposed a mechanism for distributed clustering using local differential pri-

vacy (LDP) to preserve distance-based information. They claim to have the first non-interactive LDP algorithm for clustering [Su et al., 2015]. This means they can perturb the data locally at once and send it to the server to cluster with both K-Means and DBSCAN without interaction between data points. They encode the client-side data into an anonymous hamming space using Bit Vector (BV) and modify the encoding to preserve Euclidean distance. Their mechanism only shares distance information, so they could not use K-Means directly. To overcome this, they modified the algorithm and called it K-Cluster. Finally, the method is evaluated using Normalized Mutual Information (NMI) and Average Estimated Error (AEE).

Xia et al. noticed the shortcoming of Sun et al.'s work which is the need to share privacy-sensitive distance information [Xia et al., 2020]. Therefore, they create an interactive method for distributed K-means clustering using LDP. The method converts features to binary strings and uses the Random Response mechanism (RR) to perturb each feature into a feature vector. The privacy cost depends on the length of the bits of each feature transformation, meaning that a longer length yields more information at the expense of the privacy budget. In each iteration, the serverside calculates and sends K-means centroids to each user, who recalculates distances until the centroids become stable. The approach has the disadvantage of a high correlation between user data and the clusters. To solve this problem, the algorithm is improved by having the client side send the user data and a set of random zero strings. The server side then performs similar calculations to determine the actual cluster. Huang et al. propose a private distributed K-means clustering algorithm for interval data that addresses a shortcoming in Xia et al.'s work by using Condensed Local Differential Privacy (CLDP) for small-scale values and LDP for large-scale values [Huang et al., 2021]. They preserve distance using a Square Wave (SW) mechanism and apply a classical K-Means algorithm on the server side to the perturbed data.

A recent mechanism that also builds around K-Means to preserve LDP is called the LDPK mechanism [Yuan et al., 2021]. As K-Means works only with numerical data, they use K-prototypes for supporting mixed data types. The LDPK mechanism perturbs the user data first locally and interactively exchanges information with the server to complete the clustering process. The mechanism they use for perturbation is the Harmony algorithm, proposed earlier by [Nguyen et al., 2016]. The S-Hist method is used to support categorical data, which was also introduced by Nguyen et al. The server could still infer the correct information because of the correlation between the cluster centroids and the actual data. Therefore, the author replaces S-Hist with OUE [Wang et al.] to improve accuracy. To improve their mechanism further, the authors disturb the user's cluster information with an extra extension to the LDPK method, called ELDPK. For this purpose, they perturb the clusters with the GRR (Generalized Random Response) algorithm. They show that the clustering quality increases if the data points increase.

Most existing work focuses on (L)DP in combination with K-Means. Finally, two interesting studies focus on differential privacy for AP or DBSCAN. A study conducted by Cai et al. focuses on AP [Cai et al., 2020]. Their method involves adding Laplace noise to the responsibility matrix. For each sample data, a neighborhood is specified using a radius around the data point. This area is called the neighborhood density, and each sample point's preference value is adjusted according to its density value. Higher density yields a higher chance of belonging to a cluster center and being ranked based on size. The perturbed responsibility matrix and densities are combined and used to run AP. They evaluated

their method using the ARI, Fowlkes-Mallows Index (FMI), and AMI.

Another study focuses on differential privacy for DBSCAN [Bozdemir et al.]. The proposed solution involves clustering data between two or more parties using two servers. Secure two-party computation (S2PC) is used to achieve this. Using S2PC, both servers receive a random-looking secret share. To recover the original data, both servers must combine their shares using S2PC, which combines the data without the servers having access to the full value. The proposed protocol is privacy-preserving DBSCAN (ppDBSCAN). The calculations in this study are based on squared Euclidean distance (SED) and are evaluated using different methods. To evaluate the performance of ppDBSCAN, the study compares its Adjusted Rand Index (ARI) to that of K-means.

Paper	Data type	Dataset	Code	Preserving	Type	Interactive	Methods
[Sun et al., 2022]	-	Synthetic dataset	-	(ϵ, δ) -LDP	K-Means	Non interactive	-
[Huang et al., 2021]	-	-	-	LDP	K-Means	Interactive	-
[Stemmer, 2021]	numerical	-	-	LDP	K-Means	Interactive	-
[Yuan et al., 2021]	numerical	Adult dataset, US Census dataset Deer dataset, Lsun dataset, S1	-	LDP	K-Prototypes	Interactive	LDPK and ELDPK
[Bozdemir et al.]	-	Iris dataset, Seeds dataset	-	DP	DBSCAN	-	ppDBSCAN
[Cai et al., 2020]	-	3D Road Network, CarGPS	-	DP	AP	-	DP-AP
[Xia et al., 2020]	n-dimensional numerical data	Aggregation dataset , Digit dataset, Pathbased d...	-	LDP	K-Means	Interactive	LDPKmeans
[Sun et al., 2019]	n-dimensional numerical data	-	-	DBSCAN, K-Means	-	Non interactive	Distance Aware Bit Vector (DPBV)
[Nissim and Stemmer, 2018]	n-dimensional numerical data	-	-	(ϵ, δ) -LDP	K-Means	Interactive	LDP-GOODCenter
[Nissim and Stemmer, 2018]	-	-	-	-	K-Means	Interactive	LSH-Procedure & Private-Centers
[Su et al., 2015]	n-dimensional numerical data	Adult dataset, Gowalla dataset, Image dataset	2	DP	K-Means	Both	EUGkM and hybrid EUGkM + DPLloyd
[Nissim et al., 2007]	n-dimensional numerical data	-	-	(ϵ, δ) -LDP	K-Means	Non interactive	Smooth sensitivity

Table 2.1: Summary table of the literature review for (L)DP clustering algorithms.

Paper	Data type	Dataset	Code	Preserving	Interactive	Methods
[Wang et al., 2019]	n-dimensional and 1-dimensional	BR, MR	³	LDP	-	- Piecewise Mechanism (PM) - Hybrid Mechanism (HM)
[Duchi et al., 2017]	1-dimensional numerical, binary and categorical data.	-	⁴	LDP	-	-
[Nguyễn et al., 2016]	n-dimensional	BR	-	ϵ -LDP		Harmony
[Geng et al., 2015]	n-dimensional	-	⁵	DP	-	Staircase mechanism (SM)
[Geng and Viswanath, 2013]	n-dimensional	-	-	ϵ -DP	Non interactive	-

Table 2.2: Summary table of the literature review for (L)DP algorithms.

number	name	samples	features	target	Source	Realworld data?
23	1 Adult	48,842	14 numerical /categorical /boolean	income (>50k, <= 50k)	UCI	Yes
	2 Seeds	210	7 numerical	type	UCI	Yes
	3 Iris	150	4 numerical	class (type of iris)	UCI	Yes
	4 CarGPS	17,785,500	3 geographical data	-	-	Yes
	5 3D Road Network	434,874	3 geographical data	-	-	Yes
	6 Pathbased	300	2 numerical	ground truth clusters	PapersWithCode	No
	7 Aggregation	788	2 numerical	-	-	Unknown
	8 Digit	1797	8x8 numerical	number	Scikit-learn	Yes
	9 Lsun	400	2 numerical	ground truth clusters	-	No
	10 S1	1500	2 numerical	ground truth clusters	-	No
	11 Deer	20,033	2 numerical	-	-	Yes
	13 Gowalla	6,442,890	5 (geographical, data, ids and time)	-	⁶	Yes

Table 2.3: The different datasets used in the related literature.

2.3.4. EVALUATION

It is important to compare our kD-Laplace method with other studies for this research. Studies that are similar to ours mainly utilize LDP for clustering and add noise to cluster centroids [Huang et al., 2021; Xia et al., 2020; Yuan et al., 2021]. Or, require modifications of the K-Means algorithm [Sun et al., 2019].

As explained earlier, we aim to create a general-purpose LDP mechanism that can be used with multiple cluster algorithms 2.3.1. Based on the literature study, two LDP mechanisms fall into this category: Harmony and Piecewise [Nguyễn et al., 2016; Wang et al., 2019]. Published open-source code is available for Piecewise but, unfortunately, not for Harmony. Therefore, we will only focus on the Piecewise mechanism as means of comparison material. The following sections focus on investigating the Piecewise mechanism.

DUCHI ET AL.'S MECHANISM

The Piecewise mechanism is based on Duchi et al.'s mechanism for one-dimensional data. Therefore, we start by explaining this mechanism first. Duchi et al.'s mechanism is a relatively simple method based on the Bernoulli distribution [Duchi et al., 2017]. This distribution yields either a 0 (negative) or a 1 (false) based on specified probabilities ⁷. The mechanism works on a domain tuple [-1, 1] and returns -1 or 1. Hence, the PDF of this function is as follows ⁸:

$$P(n) = \begin{cases} 1-p & \text{if } n=0 \\ p & \text{if } n=1 \end{cases} \quad (2.10)$$

The probabilities are calculated based on the input value and can then be used to estimate a mean value. Compared to Laplace, Duchi et al. solution performs better in variance for epsilons smaller than 2 [Wang et al., 2019]. However, it performs worse when the epsilon value is higher because the algorithm does not consider the privacy budget for values that are 0. The multidimensional variant looks like the one-dimensional version but samples each data point's noise independently.

PIECEWISE MECHANISM

The authors aim to create a method that combines the advantages of the Laplace mechanism and Duchi et al.'s methods [Wang et al., 2019]. The goal is to reduce the variance for a broader range of privacy budgets. Like the mechanism above, the Piecewise mechanism only accepts data from -1 to 1. We first explain the one-dimensional variant and then the multidimensional variant.

The mechanism for one-dimensional has an output of $c \in [-C, C]$. Which is defined based on the privacy budget:

$$C = \frac{\exp(\epsilon/2) + 1}{\exp(\epsilon/2) - 1} \quad (2.11)$$

The noise is sampled from this distribution by conditionally executing one of two algorithms (see for reference Wang et al.'s paper) [Wang et al., 2019]. Due to the symmetric nature of their mechanism's PDF, the authors can handle the value of 0. Imagine it as a histogram with the distribution centered around 0. The histogram consists of three "parts" on the left, right, and center (0). This approach allows for determining the probability of 0 based on a certain likelihood, unlike Duchi et al.'s solution.

⁷<https://mathworld.wolfram.com/BernoulliDistribution.html>

⁸<https://mathworld.wolfram.com/BernoulliDistribution.html>

The authors generate a randomly sampled set of values k for the multidimensional approach. Next, for each value from k , the value is sampled using the one-dimensional Piecewise mechanism. A critical factor in the overall calculation is the scale factor C_d , which, in addition to C (referring to Equation 2.11), also considers the number of dimensions d . Finally, the authors also provide an extension to support categorical data.

3

ND-LAPLACE

In this chapter, we delve deeper into geo-indistinguishability and the various mechanisms that work with it. We also explain the theory behind the nD-Laplace mechanism and how we modify it and apply it for clustering. This explanation is build-up out of several sections, each dedicated 2, 3, and n-dimensional data:

1. 2D-Laplace
2. 3D-Laplace
3. nD-Laplace

For each mechanism, we explain the equation for GI, the mechanism, and the data truncation.

3.1. 2D-LAPLACE

The idea of GI was introduced to solve the issue of privacy and location data [Andrés et al., 2012]. To recall what was explained earlier (Equation 2.4). It offers an alternative approach for achieving (local) differential privacy for geographical data (latitude/longitude). The mechanism achieves this by locally adding noise to the location before sending it to a location-based system (LBS). This section starts with an introduction to mathematics, and for each of the different subsections, we visualize and explain open challenges and theoretic for applying them for clustering.

3.1.1. PLANAR AND POLAR LAPLACE

In section 2.1.1, an explanation of the concept of GI has been given. As indicated, the method works on 2-dimensional data, and when visualized, this can be done with a so-called plane [Andrés et al., 2012]. From there, the term "Planar" Laplace originated and was used thoughtfully by Andres et al.

The idea of Planar Laplace is to generate an area around $x_0 \in X$ according to the multivariate Laplace distribution. The mechanism of planar Laplace is a modification of the Laplace algorithm to support distance [Andrés et al., 2012]. This distance method $dist(x, x')$ is a method to calculate the Euclidean distance between two points x and x' . Recalling the

definition of Laplace, this method $|x - x'|$ is replaced by the distance metric. Hence, the definition of the PDF by Andrés et al. is:

$$\frac{\epsilon^2}{2 * \pi} e(-\epsilon d(x_0, x)) \quad (3.1)$$

Which is the likelihood a generated point $z \in Z$ is close to x_0 . The method works for Cartesian coordinates but was modified to support polar coordinates by including θ . So each point is reflected as (r, θ) . A point $z \in Z$ where $z = (r, \theta)$ is randomly generated using two separate methods for calculating r and θ . This idea is visualized in the following figure:

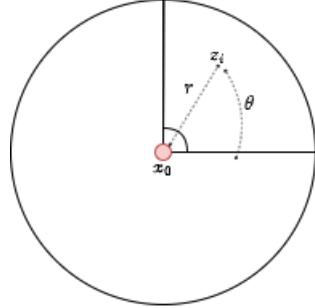


Figure 3.1: Representation of the generated $z = r\theta$ and original point x_0 .

Calculating r : This variable is defined as $dist(x_0, z)$ and can be randomly drawn by inverting the Cumulative Distribution Function (CDF) for the Laplace distribution:

$$C_\epsilon^{-1}(p) = -\frac{1}{\epsilon}(W_{-1}(\frac{p-1}{e}) + 1) \quad (3.2)$$

For this equation, W_{-1} is a Lambert W function with a -1 branch. The Lambert w function (also called the product logarithm) is defined as $W(x)e^{W(x)} = x$ [Lehtonen, 2016]. The purpose of the Lambert w function is to invert the CDF of the Laplace distribution to generate random noise for one of the coordinates (r) using the random value of p .

Calculating θ : The other variable (θ) is defined as a random number $[0, 2\pi]$. To visualize the data, it is necessary to convert the polar coordinates for $z = (r, \theta)$ back to planar coordinates $z = (x, y)$. This conversion is described as step 4 of the planar Laplace algorithm [Andrés et al., 2012] and visualized using figure 3.2.

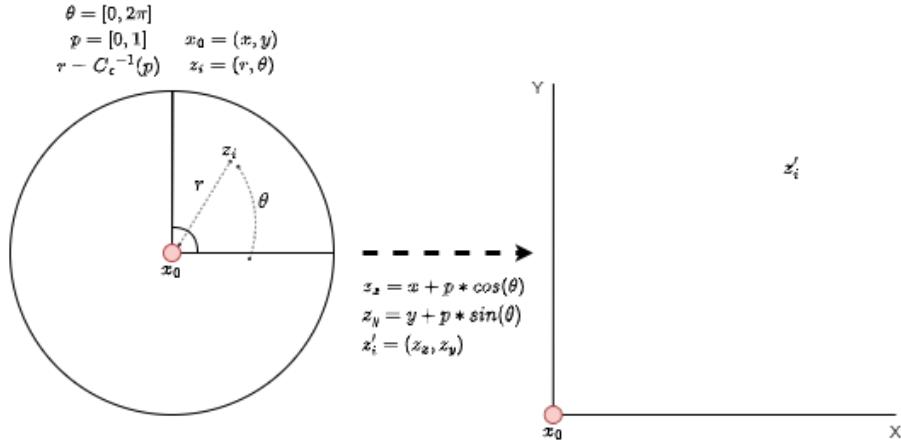


Figure 3.2: Representation of converting the perturbed point $z = (r, \theta)$ to a point z_x, z_y

3.1.2. TRUNCATION

After adding the noise to the data, it cannot be ensured the data is within the original domain (figure 3.3). If this is not the case, the data is easily distinguished by an unwanted adversary [Andrés et al., 2012; Min et al., 2022]. The truncation is an essential part of the mechanism to ensure the data is contained within the domain of the original data X . A vi-

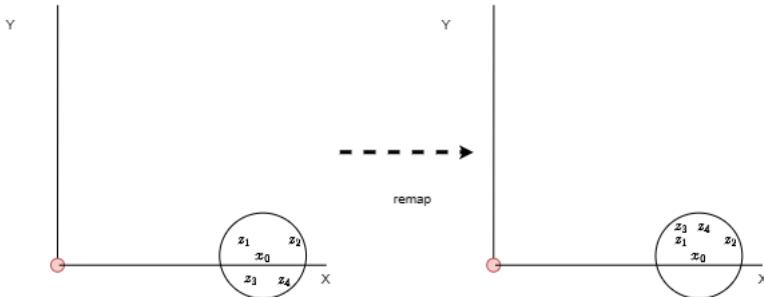


Figure 3.3: Representation of truncation of data points for 2-dimensional Laplace mechanism.

able solution is to create a grid around the diameter of the set of points $X = R^2$ that belong to the user [Andrés et al., 2012]. This grid is defined as $G = \{g_1, g_2, \dots, g_n\}$ where g_i is a grid point. So, a point generated outside the given domain is remapped to the closest in $X \subset G$.

This idea was later improved by Chatzikokolakis et al., introducing an optimized way of remapping [Chatzikokolakis et al., 2017]. The algorithm uses the Bayesian rule to minimize the loss of utility while remapping the data. Instead of remapping to the closest point, it remaps to a location where the loss is minimal. To decrease the performance impact of this algorithm, it is possible only to consider a specific region around the perturbed point z . The disadvantage of this method is the need for a prior set of data points to calculate the optimal remapping.

3.1.3. OPTIMIZING FOR CLUSTERING

The decision of the parameters for the algorithm is straightforward as it depends on the ϵ . This constant is calculated by defining the radius r , and the desired level of privacy l and ϵ is calculated using l/r . The l is a predefined constant $l \in R^+$ but usually will be below 10.

For geographical data, the r can be configured using meters as a unit of measure. So, for example, $r = 200$ corresponds to a radius of 200m around point x_0 . Without a unit, it is a challenge to define a reasonable radius.

In that regard, the radius can also be a flexible value defined based on the crowdedness of a region [Chatzikokolakis et al., 2015]. Suppose a user's location is within a crowded area. In that case, the radius can be smaller than if the user is located in a rural area (because the user's location is indistinguishable due to the overlap of other users' locations). Instead of providing GI, the authors introduce a more flexible privacy definition d_x -privacy. The r is calculated based on the mass of other regional locations r , which they call *privacy mass*. So, the total mass of a set A is defined as $M(A) = \sum_{x \in A} m(x) = a + q(x)b$. Where $m(x)$ is the mass of a location x and is of value $[0, 1]$. For this formula, a is the number of points assigned to each location. The authors define $q(x)$ as the "quality" of a point, which is essentially the number of other users that are also interested in the same point (e.g. a mall).

The a is defined as a Euclidean ball $B_r = x' | d_{euc}(x, x') \leq r$, which returns all locations within the radius r . To retrieve a value within $[0, 1]$, the authors use the following formula:

$$a = \frac{1}{|B_r|} \quad (3.3)$$

If the locations are only considered for space and not quality, $q(x)$ is defined as 0 [Chatzikokolakis et al., 2015].

Although the method is an interesting approach to increasing utility while not reducing privacy, it is hard to adopt for clustering. For applying it for LDP, it is required to supply each user with prior knowledge of the dataset. This approach would require interaction between data points, hence an interactive setup of the mechanism instead of a non-interactive one.

Nonetheless, the idea of using crowded locations is an exciting approach that is researched further in section 3.3.2

3.1.4. FINAL MECHANISM

Finally, we provide as means of a summary the final algorithm for the Laplace mechanism for 2D space

Algorithm 1 Full algorithm for perturbing training data for 2D-clustering using planar/2D-Laplace [Andrés et al., 2012]

```

Input:  $x \in X$                                      ▷ 2D array of points
Input:  $l \in R^+$ 
Input:  $r \in R^+$                                 ▷ sensitivity
Output:  $z \in Z$                                  ▷ 2D array of perturbed points
 $\epsilon = \frac{l}{r}$                                ▷ Calculating privacy budget [Andrés et al., 2012]
 $x_{min} \leftarrow min(X)$ 
 $x_{max} \leftarrow max(X)$ 
 $Z \leftarrow []$ 
for  $point_i \in X$  do
     $\theta \leftarrow [0, \pi/2]$                          ▷ Random noise for  $\theta$ 
     $p \leftarrow [0, 1]$ 
     $z_i \leftarrow C_\epsilon^{-1}(p)$                   ▷ formula 3.2
     $x_{perturbed} \leftarrow point_{i_x} + (z_{i_x} * \cos(\theta))$  ▷ add noise to x-coordinate
     $y_{perturbed} \leftarrow point_{i_y} + (z_{i_y} * \sin(\theta))$  ▷ add noise to y-coordinate
    append  $x_{perturbed}, y_{perturbed}$  to Z
end for
return Z

```

3.2. 3D-LAPLACE

The previous sub-section described the use of 2-dimensional noise on geographical data. This approach has recently been extended to support 3-dimensional data, which benefits indoor navigation [Min et al., 2022]. The method is similar to the 2D approach but includes the azimuth angle ψ besides the polar angle θ and radial distance r .

3.2.1. GEO-INDISTINGUISHABILITY

To establish the same privacy guarantees for 3-dimensional data as for 2-dimensional data, the original equation 2.4 is extended [Min et al., 2022].

$$K(x_1)(z) \leq e^{\epsilon * d_3(x_1, x_2)} K(x_2)(z) \quad (3.4)$$

Where x_1 and x_2 are two real data points in the same dataset X .

3.2.2. SPHERICAL LAPLACE

The implementation of Min et al. projects the dimensions onto a sphere instead of a circle [Min et al., 2022]. This sphere is a unit sphere calculated with a radius of 1. The polar angle θ and azimuth angle ψ are randomly calculated based on this sphere.

Calculating θ and ψ : The tuple $U = (\theta, \psi)$ is randomly drawn from the unit sphere using the following equations [Min et al., 2022]:

$$\theta = \frac{1}{\pi} \quad (3.5)$$

$$\psi = \frac{1}{2\pi} \quad (3.6)$$

Calculating r : The radial distance r is calculated using the following equation:

$$r = \frac{1}{2} \epsilon^3 * r^2 * e^{-\epsilon * r} \quad (3.7)$$

The gamma scale is the same as for 2D-Laplace but with a shape of 3 instead of 2. The noise is added to the original location x to obtain the perturbed location $z = x + U * r$. A clear example of the generated noise by this method is shown in figure 3.4. Finally, the spherical coordinates are converted to the Cartesian coordinate system to obtain the perturbed location z :

$$\begin{aligned} z_x &= r * \sin(\theta) * \sin(\psi) \\ z_y &= r * \sin(\theta) * \cos(\psi) \\ z_z &= r * \cos(\theta) \end{aligned}$$

The complete overview is visualized in figure 3.5.

Kernel density plot of a point x_0 (centre) with 50 random generated points according to the formula for 3D-Laplace in a projected sphere with epsilon 3

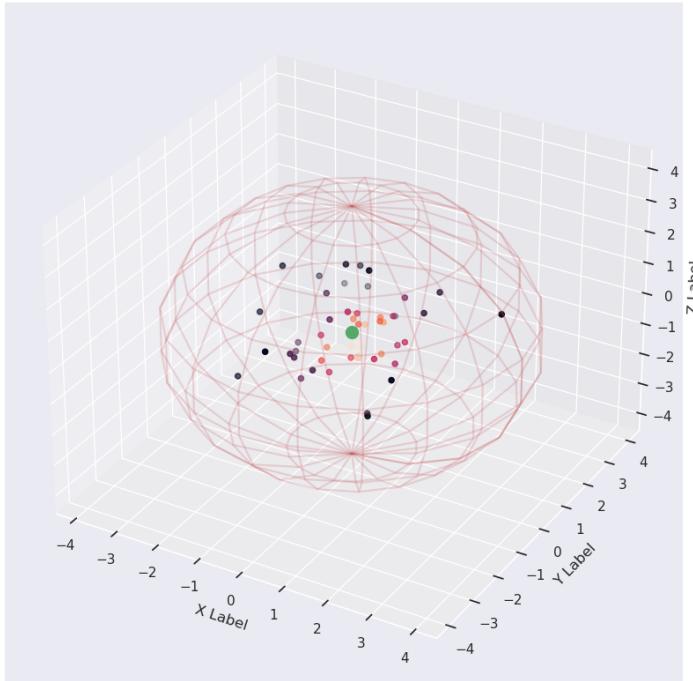


Figure 3.4: 50 random noise samples generated around point x_0 (green dot) using the 3D-Laplace noise method [Min et al., 2022] plotted on a sphere.

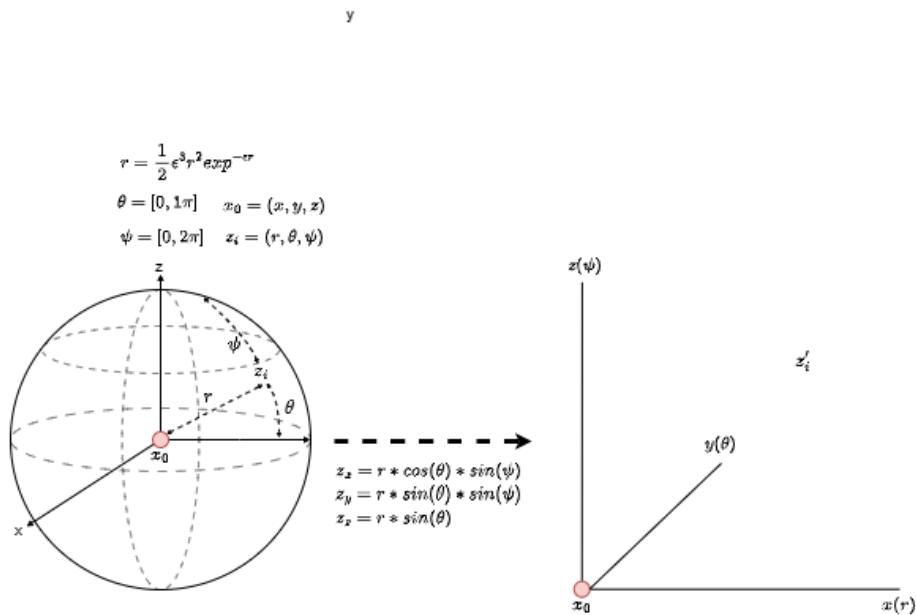


Figure 3.5: 3D-Laplace noise distribution according to the method proposed by Min et al. [Min et al., 2022]

3.2.3. TRUNCATION

As with the 2D-Laplace method, the 3D-Laplace method also needs a truncation method. This truncation method is also based on the same method as the 2D-Laplace method. Instead of a plane grid, a cuboid grid is used for 3-dimensional space. This cuboid remaps the noise to the closest grid cell $g \in G$ or existing point in X . We plotted example data points on a 3-dimensional grid in figure 3.6 to demonstrate this:

Example of generating noise for a dataset
and remapping it to $X \subset G$ when outside the domain

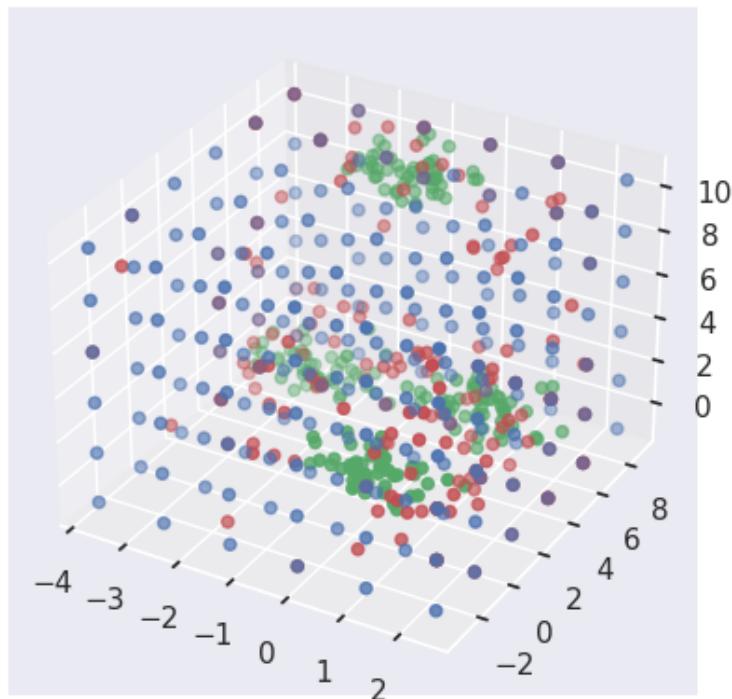


Figure 3.6: Applying 3-dimensional noise with $\epsilon = 1$ (red dots) to a dataset X (green dots). Demonstrating remapping to the closest grid point (blue) or X .

3.2.4. FINAL MECHANISM

Finally, we provide as means of a summary the final algorithm for the Laplace mechanism for 3D space

Algorithm 2 Full algorithm for perturbing training data for 3D-clustering using planar/2D-Laplace [Andrés et al., 2012]

```

Input:  $x \in X$                                      ▷ 3D array of points
Input:  $l \in R^+$ 
Input:  $r \in R^+$ 
Output:  $z \in Z$                                      ▷ 3D array of perturbed points
 $\epsilon \leftarrow \frac{l}{r}$                            ▷ Calculating privacy budget [Andrés et al., 2012]
 $Z \leftarrow []$ 
for  $point_i \in X$  do
     $\theta \leftarrow 1, \pi 2$                          ▷ Random noise according to equation 3.7
     $p \leftarrow \frac{1}{2\pi}$                         ▷ Random noise according to equation 3.8
     $r \leftarrow \frac{1}{2}\epsilon^3 * r^2 * e^{-\epsilon * r}$  ▷ Draw  $r$  based on equation 3.7
     $z_x \leftarrow r * \sin(\theta) * \sin(p)$ 
     $z_y \leftarrow r * \sin(\theta) * \cos(p)$ 
     $z_z \leftarrow r * \cos(\theta)$ 
     $Z ::= Add(z)$                                 ▷ Adds z to the list Z.
end for
return Z

```

3.3. KD-LAPLACE

As mentioned in the previous chapter, the paper introduced by Min et al. can handle 3-dimensional data. A small recap: a point (r, θ, ψ) gives us the spherical coordinates of a given 3-dimensional sphere. An important property is that these coordinates can be generated separately [Andrés et al., 2012; Min et al., 2022]. The r gives us the radius or distance from (θ, ψ) to the center of the sphere¹. So, instead of having just these two coordinates, we can extend this to n-dimensions by considering an n-hypersphere [Fernandes et al., 2019; Min et al., 2022]. To this end, in addition to points θ and ψ , we consider $\theta \in S^n$, where S is a unit hypersphere.

The first step to generate the noise is first to select the r . This method is almost identical to the one for 3-dimensional (3.7). But, instead of applying a scale of 3, the scale will be n for the number of dimensions in the data [Fernandes et al., 2019]:

$$\gamma(n, 1/\epsilon) \quad (3.8)$$

For the other dimensions, we consider a vector $U = (\theta_1, \theta_2, \theta_n)$ which is uniformly selected based on a unit n -hypersphere S^n [Fernandes et al., 2019]. We consider the work that was proposed by Marsaglia et al. for a 4d-sphere that can be used for selecting points from an n-hypersphere [Marsaglia, 1972]. This method resolves around selecting points from a hypersphere by using a uniform distribution for the domain $[0, 1]$. For this purpose, an approach to draw data points from a Gaussian distribution is adopted².

3.3.1. CARTESIAN COORDINATES

As with the 2/3D-Laplace, the spherical coordinates need to be converted to Cartesian to be able to cluster. It is comparable to the way it was done in the previous chapters; however, as there are an n -amount of angles, the equation is repeated and slightly different:

$$x_1 = r * \cos(\theta_1) \quad (3.9)$$

$$x_2 = r * \sin(\theta_1) * \cos(\theta_2) \quad (3.10)$$

$$x_n = r * \sin(\theta_1) \dots \sin(\theta_{n-2}) * \cos(\theta_{n-1}) \quad (3.11)$$

$$x_n = r * \sin(\theta_{n-1}) * \sin(\theta_{n-2}) * \sin(\theta_{n-1}) \quad (3.12)$$

The combination of sections 1 and 2 of this chapter provides a good overview of the solution using a similar image as the 2D and 3D variants (figure 3.7).

¹<https://mathworld.wolfram.com/SphericalCoordinates.html>

²<https://mathworld.wolfram.com/SpherePointPicking.html>

$$r = \gamma(4, 1/\epsilon)$$

$$U = \frac{1}{1\sqrt{2\pi}} \exp^{-\frac{1}{2}(\frac{x-0}{1})^2}$$

$$\theta_n \in U$$

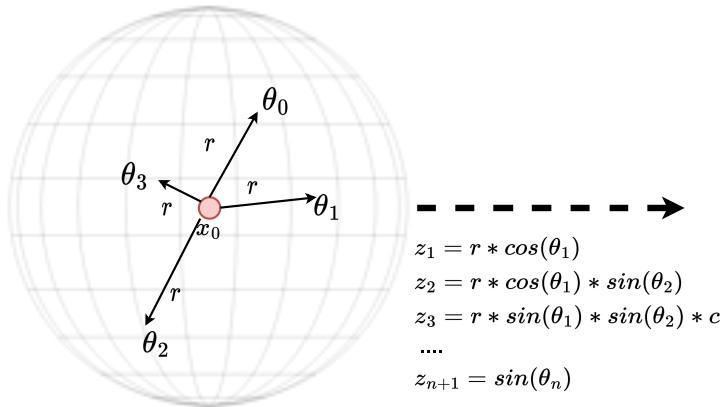


Figure 3.7: Overview of the nD-Laplace mechanism

3.3.2. PRIVACY VERSUS UTILITY

If we continue adding dimensions, we notice the noise is shrinking proportionally. We must first examine the formula for a hypersphere's volume to understand this behavior.

$$S_n = \frac{2\pi^{n/2}}{\Gamma(\frac{1}{2}n)} \quad (3.13)$$

γ is the Gamma distribution determined based on the number of dimensions n ³. As the amount of dimensions increases, the most volume is located on the hypersphere surface. When we convert the points to Cartesian coordinates, some will be located at the center (e.g., 0.5), while others will be close to the surface (e.g., 0.0). However, as the number of dimensions increases, most will be close to the surface (e.g., 0.99). The decreasing amount of volume is illustrated using this figure:

³<https://mathworld.wolfram.com/Hypersphere.html>

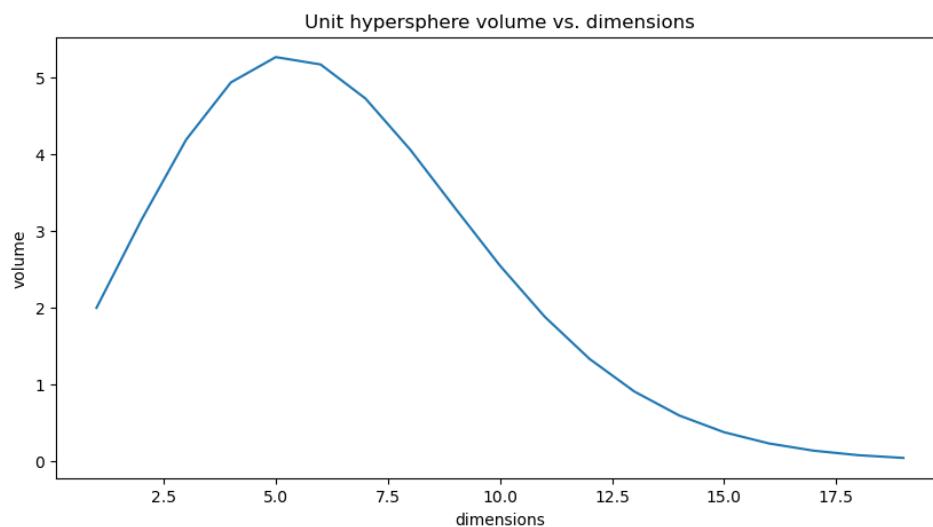


Figure 3.8: Illustration of the decreasing volume while increasing the number of dimensions

The noise decreases as the dimensions increase, increasing utility. Hence, observing the behavior of privacy relative to utility is intriguing. This behavior will be further emphasized in a later stage of this research.

3.3.3. TRUNCATION

In section 3.1.3, we introduced a method to optimize the 2D Laplace mechanism based on crowdedness (point density). This method is extended with the help of a more recent paper provided by Chatzikokolakis et al. [Chatzikokolakis et al., 2017]. We use this work to extend and optimize the grid-remapping method for 2D/3D Laplace (Sections 3.1.2 and 3.1.3) and introduce optimal grid-remapping to improve the utility further. We want to emphasize that this section focuses on improving utility with remapping. Any remap method preserves geo-indistinguishability Chatzikokolakis et al. [2017], so the required privacy is still preserved.

Recalling both mechanisms, the 2D version operates on a plane and approximates on a grid G , while the 3D version works in a 3D space using a cuboid grid. Given a set of input points $X \subset R^2$, we can truncate points that are outside the domain by remapping them to points within G ($Z = X \cap G$) [Andrés et al., 2012]. Here, X represents other data points reported locally by the same user. To extend this approach to n-dimensional data, we need an efficient way to search points in an n-dimensional hypersphere. To do this, we adopt the idea proposed by Chatzikokolakis et al. of using a kd-tree to search the grid efficiently [Chatzikokolakis et al., 2017]. In their research, they describe the utilization of a kd-tree for searching nearby points for a given point. For this reason, we also use a kd-tree for the following tasks:

1. Finding nearby points for $z \in G$ (section: [Grid with kd-tree remapping](#)).
2. Finding nearby points for $x \in X$ and $z \in Z$ (section [Optimal remapping](#)).

For visualization purposes, this section will primarily focus on 2D data. However, it is essential to emphasize that the same algorithm will also be applied to 3D and nD data. The underlying principles and steps of the algorithm remain the same.

We first introduce kd-trees on the next page and then explain how we apply them for the two tasks.

KD-TREES

A kd-tree algorithm can search a grid for nearby points [Bentley, 1975]. It can do so by recursively splitting the grid into a binary tree to search for grid coordinates [Washington, 2]. In addition, it preserves spatial information of the data so it can be utilized to find nearby points using Euclidean distance (nearest neighbor search). The following example provides an idea of how this works (Figure 3.9):

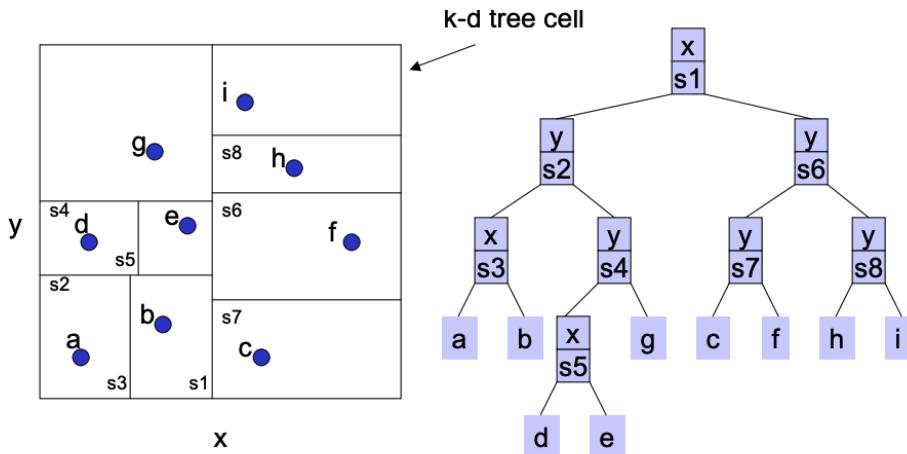


Figure 3.9: Representation of constructing a kd-tree with 2 dimensions [Washington, 2].

Take, for example, the 2D Laplace algorithm that utilizes a plane (left side). The data points can be divided based on their x and y coordinates. Each coordinate becomes a node in the binary tree, and the grid is divided based on these splits. The binary tree allows us to search the grid efficiently. An example of this is provided in the following image (Figure 3.10):

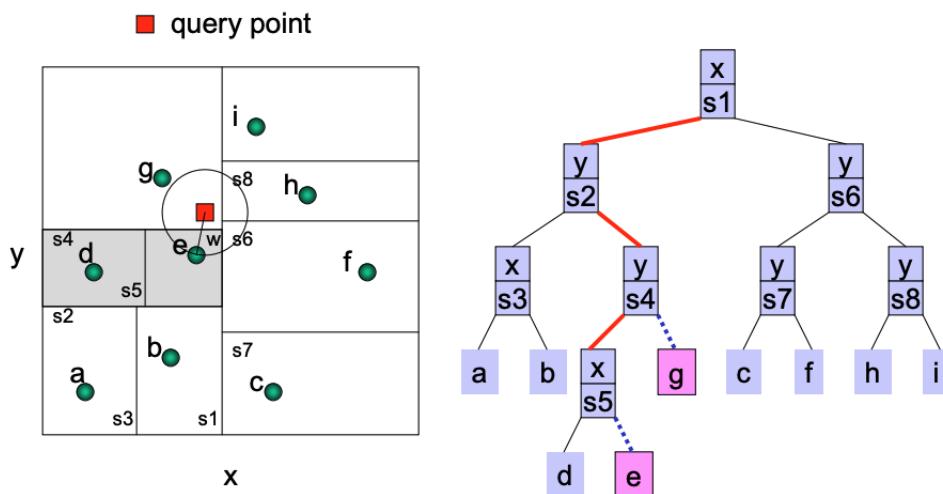


Figure 3.10: Representation of searching a kd-tree with 2 dimensions [Washington, 2].

In the example, we are searching for all points that fall within the radius of a random query point. Thanks to the grid being divided into a binary tree, a portion can be efficiently

searched, evaluated, and referenced. The most significant advantage is that this greatly reduces the complexity of searching. Constructing the kd-tree costs $O(kn)$, where k is the number of dimensions and n is the dataset size. Searching for the nearest neighbor is a little less efficient, with a time complexity of $O(\log n)$ [Washington, 2] (See Figure 17 for an overview of the Big-O notation). A reference to the Big O notation can be found in the appendix (See Figure 17).

GRID WITH KD-TREE REMAPPING

As explained in the previous paragraph, a kd-tree can be used to perform a nearest neighbor search. This search method is highly relevant to our research as it proves to be beneficial for the optimizations we are striving for. To this end, we adopt this approach for remapping the perturbed data points $z \in Z$ to a grid G .

We have illustrated the three steps required for this below:

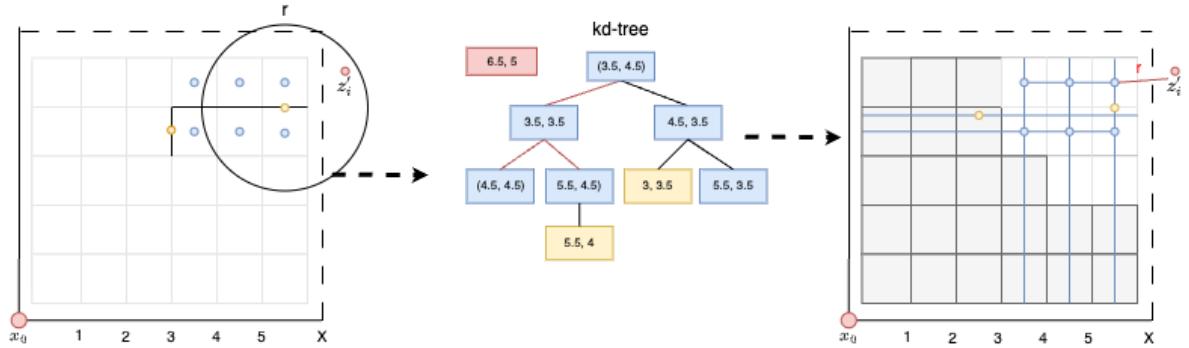


Figure 3.11: Representation of a kd-tree with 2 dimensions to remap based on a grid.

The above illustration presents the grid-remapping algorithm. Firstly, a grid is generated, where each (blue) point represents the center of a grid cell. Together, these centroids form the grid dataset, denoted as G . The yellow points and x_i are part of the original collection, denoted as X . Here, r represents the radius used to generate a private version of the data point x_i , named z_i , based on 2D-Laplace (in this case). In the illustration, you can observe that z_i falls outside the original domain of X , so it needs to be remapped. We accomplish this by utilizing the nearest-neighbor search from the kd-tree algorithm, allowing us to search in $X \cup G$. Using this algorithm, we can effectively remap point $z \in Z$ to either X or G based on the closest Euclidean distance (Algorithm 4 and Algorithm 3).

The utility of this method depends on the number of grid cells in G since a smaller distance will result in more frequent mapping to the surface of the grid. When ϵ is very low (and thus farther away), the data points are more likely to map to the grid surface (3.4, 3.6). Increasing the number of grid cells can improve the utility, but this comes at the cost of significantly increased space complexity for k dimensions. This is because a grid of $n * m$ dimensions has a $O(n^2)$ complexity. Therefore, we also explore the optimal remapping algorithm proposed by Chatzikokolakis et al. [Chatzikokolakis et al., 2017].

Algorithm 3 Algorithm for finding points outside the domain of X .

Input: $x \in X$ ▷ original dataset
Input: $z \in Z$ ▷ perturbed dataset

$X_{domain} \leftarrow \text{KDTREE::QUERY}(Z)$ ▷ find the closest points.
 $X_{features} \leftarrow \text{LIST::GETFEATURES}(X)$ ▷ retrieve dataset dimensions

$X_{outside-domain} \leftarrow []$

for $feature \in X_{features}$ **do** ▷ iterate over all features and check if any points are outside the domain.

if $feature \leq X::\text{MIN}(Z)$ **then**
 ROW::APPEND($X_{outside-domain}$)
 end if
 if $feature \geq X::\text{MAX}(Z)$ **then**
 ROW::APPEND($X_{outside-domain}$)
 end if
end for

return $X_{outside-domain}$ ▷ The index of points outside the domain of X .

Algorithm 4 Algorithm for generating and remapping to a grid.

Input: $x \in X$ ▷ original dataset
Input: $z \in Z$ ▷ perturbed dataset
Input: $grid$ ▷ grid structure ($n * m$)

$d_X = Z::\text{DIST}(X)$ ▷ euclidean distances between X and Z .
 $d_{grid} = Z::\text{DIST}(grid)$

$Z_{out-domain} \leftarrow X::\text{FINDPOINTSOUTSIDEDOMAIN}(Z)$ ▷ Algorithm 3

$grid_{tree} \leftarrow \text{KDTREE::BUILDTREE}(grid)$ ▷ create kd-tree

$grid_{mask} \leftarrow \text{KDTREE::QUERY}(Z)$ ▷ find indices of $z \in Z$ that are closeby grid cells.

$Z_{grid-mask} \leftarrow Z_{out-domain} \cup d_{grid} < d_X$ ▷ All points $z \in Z$ that are closeby grid cells and are outside domain.

$Z' \leftarrow Z[grid[grid_{mask}][Z_{grid-mask}]]$ ▷ combinate masks to set appropriate indexes to $g \in grid$.

return Z'

DENSITY REMAPPING

As discussed, the remapping will be performance intensive to provide good utility, so we adopt the optimal remapping [Chatzikokolakis et al., 2017]. Consider the grid proposed in 3.11.

After remapping point z_i , it is mapped to the center for the grid cell. The distance to the original point x_i and z_i could be considerable based on the cell width. We aim to remap the center of the grid cell (now z_i) to a point closer to x_i (if applicable).

This remapping is visualized by zooming into the last step of the grid-remapping (Figure 3.11).

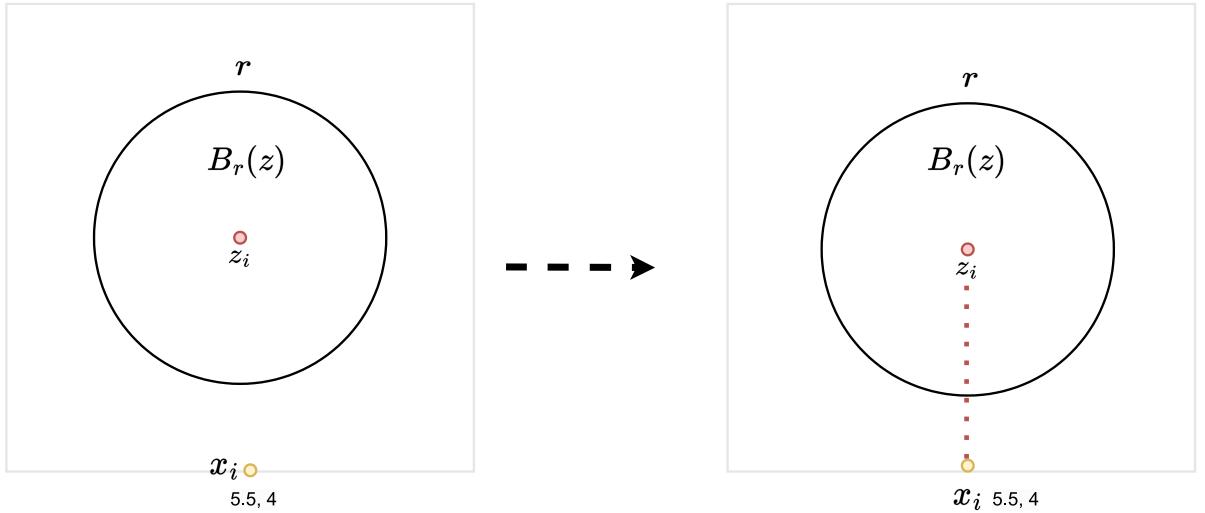


Figure 3.12: Representation of optimal remapping [Chatzikokolakis et al., 2017], where z_i is remapped to x_i using $\sigma(x)$ instead of the center of the grid cell.

In Figure 3.12, we can observe that z_i is remapped to the center of the grid cell as a consequence of the grid-remapping. For the reasons mentioned earlier, this is not optimal, and we can further optimize it by utilizing the other data points. The remapping algorithm works on the idea of crowded places 3.1.3, with the intuition that a crowded place leverages indistinguishability by crowdedness [Chatzikokolakis et al., 2017]. For the remainder of this thesis, we will use the term "density" instead of "crowdedness" because it better aligns with the clustering of data. In addition, we refer to the term "density remapping" instead of "optimal remapping" to be more descriptive from now on.

The first step is to calculate $B_r(z)$, which refers to all the data points within the original radius r around the data point z_i . The next step in the algorithm is to collect the data points around x_i to calculate how closely it can be remapped to z_i while preserving distinguishability. This variable is the collection (convex hull) of all original data points $x \in X$ close to x_i , determined based on the radius r around x_i . Finally, we combine both sets to obtain $Q_r = B_r \cap X$. Now that we have the sets of points around x_i and z_i , we can calculate the density for each point $q \in Q_r$ [Chatzikokolakis et al., 2017]:

$$\forall x \in Q_r \quad \sigma(x) = \frac{w(x)e^{-\epsilon d(x,z)}}{\sum_{q \in Q_r} w(q)e^{-\epsilon d(q,z)}} \quad (3.14)$$

Where $w(q)$ is the weight of a point q in Q_r and can be seen as points visited earlier by the user or other users (e.g., point of interest). We will revisit this topic in the next paragraph

when discussing the practical implementation of the kD-Laplace algorithm. The same applies to $w(x)$ but for an individual point $q \in Q_r$ instead of the summation. The outcome of the formula is a collection of values that indicate the degree of density, which we call $\sigma \in S$. With this data, we can calculate a new z' closer to x_i to minimize the expected loss of utility [Chatzikokolakis et al., 2017].

The collection S can be seen as the coefficient for each point $x \in X$, which can be used as a scale to apply for each point X [Chatzikokolakis et al., 2017]:

$$\bar{\sigma} = \sum_{\sigma \in S} \sigma(x) * x \quad (3.15)$$

Then next, the probabilities are calculated:

$$W = \forall \sigma \in S = \frac{\sigma(x)}{\bar{\sigma}} \quad (3.16)$$

Finally, the z' is calculated by calculating the average with the probabilities as weight:

$$z' = \frac{\sum_{weight \in W} x * weight}{\sum_{weight \in W} weight} \quad (3.17)$$

Algorithm 5 Algorithm to implement the density remapping of $z \in Z$ to be in the domain of $x \in X$

```

Input:  $x \in X$                                 ▷ n-dimensional array of original points
Input:  $z \in Z$                                 ▷ n-dimensional array of grid-remapped perturbed points
Input:  $epsilon$                                 ▷ privacy budget
Output:  $z' \in Z$                                 ▷ n-dimensional array of optimal-remapped perturbed points
 $Z' = FindRemappedPoints(Z)$ 
 $tree \leftarrow KDTree(X)$                       ▷ construct a KDTree from the original data.
for  $z' \in Z'$  do
     $r = FINDRADIUS((z'))$                       ▷ Get original radius  $r$ .
     $X_r \leftarrow KDTREE::QUERY(x)$                 ▷ find  $q \in X$  around  $x$  with radius  $r$ .
     $B_r \leftarrow KDTREE::QUERY(z')$ 
     $sigma(x) = []$ 
     $Q_r = X_r \cap B_r$ 
    for  $q \in Q_r$  do
         $q \leftarrow KDTREE::QUERY(q)$ 
         $w_x = LENGTH(X_r, B_r)$                   ▷ weight is simply adding density of  $X_r$  and  $B_r$ .
         $w_q = LENGTH(Q_r)$                       ▷  $w_q$  is the density of each point  $q$  within  $Q_r$ .
         $sigma(w_x) \leftarrow REMAP(w_x, epsilon)$     ▷ Use equation 3.14 to remap  $w_x$ .
         $sigma(x) \leftarrow APPEND(sigma(x), \frac{sigma(w_x)}{w_q})$  ▷ add to the list  $sigma(x)$ .
    end for
     $z' \leftarrow AVERAGE(sigma(x), P)$     ▷ Calculate  $z'$  using the equations: 3.15, 3.16 and 3.17.
end for

```

3.3.4. PUTTING IT TOGETHER: KD-LAPLACE

Now that we have defined everything, we can write the algorithm in a step-by-step manner:

Algorithm 6 Full algorithm for perturbing training data for nD-clustering using kd-Laplace

Input: $x \in X$ ▷ n-dimensional array of original points
Input: ϵ ▷ privacy budget
Output: $z \in Z$ ▷ n-dimensional array of optimal-remapped perturbed points
 $sphere = \text{GENERATEUNITS SPHERE}(x)$ ▷ construct a sphere around x .
for $row \in X$ **do**
 $d \leftarrow \text{LENGTH}(row)$ ▷ amount of dimensions
 $r \leftarrow \text{GENERATERADIUS}(d)$ ▷ generate radius r using Equation 3.8.
 $sphere \leftarrow \text{GENERATETHETA}(d)$ ▷ perturb the sphere Figure 3.7.
 $noise \leftarrow \text{CARTESIAN}(row, \epsilon)$ ▷ use Equation 3.12 to perturb row and convert
 to cartesian.
 $z = x + noise$
 $\text{APPEND}(Z, z)$
end for
return Z

It is important to note that with the introduction of this algorithm, it is no longer a non-interactive method, as the data points now interact with each other. Therefore, we expect the introduction of optimal grid remapping with kd-tree will bring more utility [Wang et al., 2020; Xiong et al., 2020b]. The introduction of the kd-tree is also why we present our method as *kd-Laplace*, where k is the number of dimensions.

3.3.5. MECHANISM FLOWCHART

All formulas and theories are established for 2D, 3D, and kD-Laplace, so the mechanism design applies to all three variants:

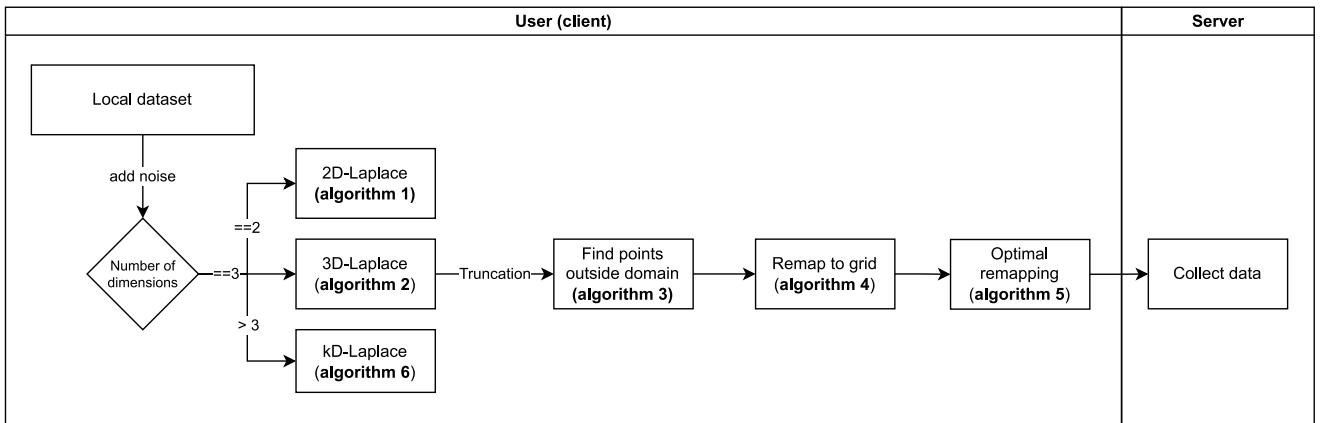


Figure 3.13: Non-interactive mechanism design for kD-Laplace.

For easy navigation, we provide a list of all algorithms:

1. 2D-Laplace: 1
2. 3D-Laplace: 2
3. kD-Laplace: 6
4. Find points outside domain: 3
5. Grid remapping: 4
6. Distance remapping: 5

PRACTICAL EXAMPLE

The shape of the dataset is necessary for the usefulness of clustering. With our algorithm, there are four different shapes/variants of the dataset. For example, this has been visualized using a 3D dataset based on the heart dataset (5.1.3). Our mechanism aims to provide privacy and preserve the dataset's shape to benefit the utility of clustering. Grid remapping and optimal remapping are used to achieve this goal.

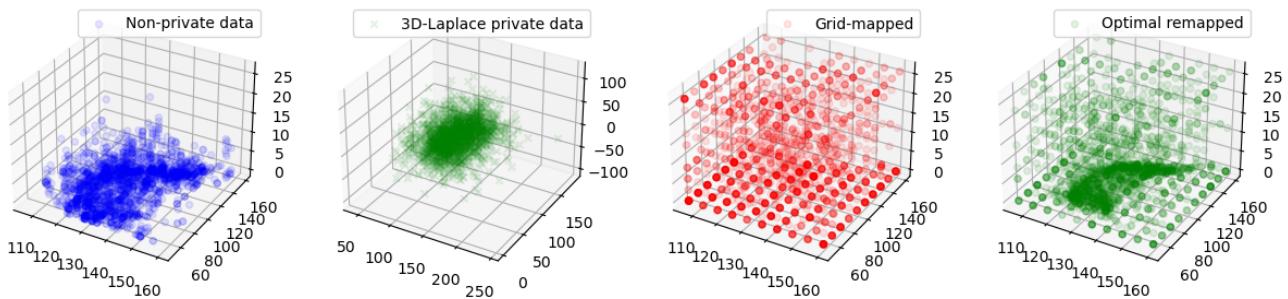


Figure 3.14: Example of optimal remapping for the 3D-dataset: Cardiotocography. The example shows the different steps of the mechanism in sequence for a dataset perturbed with a privacy budget of 0.1.

1. Dataset: the blue dots represent the original dataset without any modifications.
2. Adding noise: the green crosses represent the dataset after adding noise; for this particular example, this is 3D-Laplace (Algorithm 2): As can be observed, the data is generated from the center, causing many data points to fall outside the original domain of the dataset.
3. Grid-remapping: the red dots represent the dataset after grid-remapping (Algorithm 4) After performing the grid remapping algorithm, all points within the domain are plotted. However, the original shape of the data is mostly lost. This makes it challenging to cluster the data as was possible with the original data.
4. Optimal-remapping: the green dots represent the dataset after optimal-remapping (Algorithm 5). After completing the previous step, the data points are again remapped based on the (original) density. This results in restoring the original shape of the data and, consequently, the clusters.

4

ATTACKS ON PRIVACY

This chapter is devoted to investigating and evaluating attacks on machine learning models. Differential privacy protects the centrally stored dataset from leaking sensitive information. Therefore, assessing the mechanism's privacy is best measurable using common attacks [Jayaraman and Evans]. In this context, we evaluate attacks that explicitly uncover training data from a privately trained model. We consider two types of attacks:

1. **Membership inference attack:** An adversary attempts to infer whether a data point was used for training.
2. **Reconstruction attack:** An adversary attempts to reconstruct the training data using the model.

The knowledge of the attacker (adversarial knowledge) is an important factor to consider. This knowledge can be divided into white-box and black-box approaches [Hu et al., 2022].

1. **White-box:** The attacker has all the needed data. Including target model parameters, the training dataset and even the architecture [Hu et al., 2022].
2. **Black-box:** The attacker has limited information, like training data distribution and the trained model [Hu et al., 2022].

We will discuss both types of attacks and types in the next two sections.

4.1. MEMBERSHIP INFERENCE ATTACKS

An attack model that plays a significant role in machine learning is **Membership Inference Attack (MIA)**. With this attack, an adversary attempts to infer the training data $x \in X$ (member) from a given data point $z \in Z$ (non-member). The attack happens exclusively on supervised learning models, which predict labels or probabilities. Most attacks on models trained on a centralized dataset occur during the inference phase, where the trained model is used to make predictions. [Rigaki and Garcia, 2021]. This is also why we are primarily interested in this phase, as we are not using a distributed learning model.

The most well-known member inference attack is training shadow models [Rigaki and Garcia, 2021]. In this attack, an attacker trains multiple models. These models do not necessarily have to be the same as the original model, and the focus is mainly on the data

input/output. It is a black-box attack, but the attacker often needs knowledge of the data distribution to create a good shadow dataset [Rigaki and Garcia, 2021].

One of the earlier works that used this attack was Shokri et al. [Shokri et al., 2017]. An attacker trains multiple models (shadow model) to overfit the original modal. This idea is based on the model giving higher scores to the data on which it was trained (overfitting). Using this approach, attackers can retrieve the model's training data (member data) by injecting many fake data (non-membership data).

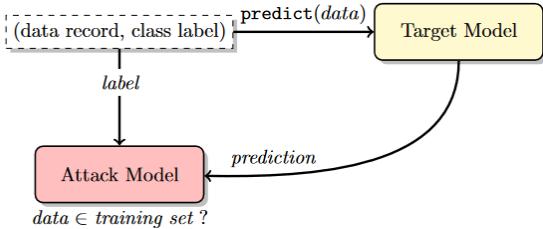


Figure 4.1: Black-box MIA attack on a machine learning model [Shokri et al., 2017]

Another approach to a black-box attack was introduced by Peng et al. and only considers that the attacker has access to the already trained model. They first rescale the probabilities using temperature scaling to compensate for overconfident models [Peng et al.]. So instead of having a probability between two classes with, for example, 99% against 1%, it will be more evenly distributed based on the training data. They then cluster the probabilities into two clusters using K-Means and label the higher confidence scores as members.

The above attacks do rely on the model to also provide the confidence or probabilities of the predictions. This information is often unavailable, so Choquette-Choo et al. introduced a label-only attack. While the existing models exploit MIA's probability output, they rely solely on labels [Choquette-Choo et al., 2021]. They use the "HopSkipJump" attack, a so-called decision-based attack [Chen et al., 2020]. Choquette-Choo et al. consider a more semi-black-box approach, for which the attacker still requires access to a subset of the original training data and the trained model. Another paper using "HopSkipJump" requires only the trained model and achieves higher accuracy using an approach with random data [Li and Zhang, 2021].

Access to only the output of the model is a typical characteristic of black-box attacks. If the attacker also knows architecture, for example, it is referred to as a white-box attack. Another take on this is prediction and confidence-based MIA, both proposed by [Yeom et al., 2018]. They assume that an attacker knows the standard error and has access to the perturbation dataset. The algorithm can then extract the truth label by minimizing the loss.

4.2. RECONSTRUCTION ATTACK

The concept of reconstruction attacks predates differential privacy, as this principle also gave rise to the idea of necessary database privatization [Dinur and Nissim, 2003]. An adversary could reconstruct training data from a given (classifier) model using a reconstruction attack. Their research evaluates the perturbation that needs to be added to a database to protect it versus a reconstruction attack.

A general reconstruction attack for our use-case is the attribute inference attack [Dwork et al., 2017] or model inference [Rigaki and Garcia, 2021]. Both terms are essentially the same, and we have chosen to name attribute inference attack, as it is the most common one in most literature [Jegorova et al., 2022]. Attribute inference focuses on a reconstruction attack with the adversary's goal of retrieving the secret from each user [Dwork et al., 2017]. For example, an attacker may attempt to reconstruct information about someone's heart disease using the individual's properties.

A practical implementation of the attack was provided by Fredrikson et al. as a way to infer sensitive features [Fredrikson et al., 2015]. To accomplish this, they used a decision tree attack, a white-box approach, as they also accessed the count of instances for each decision tree branch. They also considered a black-box approach with access only to the target model (ML-as-a-service in this example). The attack targets gradient descent, which is used to optimize the input data of an attack to mimic the original data. It has only been shown to work on a neural network for face identification images (named MIFace) [Fredrikson et al., 2015], but it could be extended to another machine learning classifier if it uses gradient descent (e.g. Support Vector Machines) [Nicolae et al., 2019]. A more general approach was undertaken by Yeom et al., building upon the same research discussed in the previous section (Member inference). In their work, Yeom et al. proposed a membership inference attack, which can also be utilized for attribute inference in a white-box setting. The attribute inference attack follows a similar methodology, wherein the target model is queried to assess the loss of synthetic data based on adversarial knowledge. Repeating the process, the attack identifies and selects the value with the highest prior probability, incorporating membership information [Jayaraman and Evans, 2022; Yeom et al., 2018]. Evaluating the effectiveness of such attacks is challenging, as it relies on the correlation between attributes, irrespective of whether the data belongs to the training or test dataset [Zhao et al., 2021]. Therefore, Yeom et al. focus on the similarity between membership/attribute-inference and combine them to evaluate the attribute inference attack [Yeom et al., 2018].

Differential privacy aims to introduce sufficient noise to mitigate the risk of various attacks [Dwork et al., 2017; Jayaraman and Evans]. Assessing the privacy leakage of our model can be effectively accomplished by employing attribute/membership inference techniques. Within this thesis, our focus is mainly on MIA. We aim to establish a quantifiable measure for our mechanism, and combining both attribute and membership attacks is not beneficial since they essentially capture the same information. Therefore, it is sufficient to concentrate on membership inference attacks.

4.3. ATTACK EVALUATION

In this section, we evaluate the membership inference attack and evaluate it as it is the most appropriate for this study (See previous chapter). We assess whether differential privacy provides protection against the attack and discuss how this can be measured.

4.3.1. MEMBER INFERENCE ATTACKS

Most current research for MIA is evaluated for neural networks [Rigaki and Garcia, 2021]. A tiny percentage evaluates this attack for supervised learning, with the majority using classification with decision trees. Most studies have used a black-box approach [Rigaki and Garcia, 2021] for these attacks. This approach is not surprising, as these attacks have a high success rate and pose a greater risk of exploitation.

Introducing differential privacy reduces the impact of a member inference attack [Hu et al., 2022; Rigaki and Garcia, 2021]. This is because the input to the model is perturbed. While it is still possible to retrieve the training data, the leaked privacy is significantly reduced. A simple but effective way to measure the privacy leakage is by calculating the accuracy of correctly predicting membership by the adversary [Choquette-Choo et al., 2021].

Yeom et al. created a metric specifically for membership inference attacks which can be measured using an "adversarial advantage." This metric describes the percentage of privacy compromised during a member inference attack [Yeom et al., 2018]. This metric is calculated by subtracting the False Positive Rate (FPR) from the True Positive Rate (TPR). The TPR represents the number of correctly predicted member data (training data), and the FPR represents the number of correctly predicted non-member data. Although these metrics are commonly applied in the literature for MIA, they do not provide enough information [Carlini et al., 2022]. Both metrics do not consider the imbalance between the TPR and FPR. The metric should emphasize the TPR, as this is the percentage of correctly predicted member data. Therefore, they propose to use a ROC curve to show the effectiveness of a membership inference attack [Carlini et al., 2022].

In conclusion, the attacks that use MIA are all (mis)using supervised machine learning. However, in this study, we use cluster algorithms. Therefore, a semi-supervised approach can be used, as illustrated in figure 4.2.

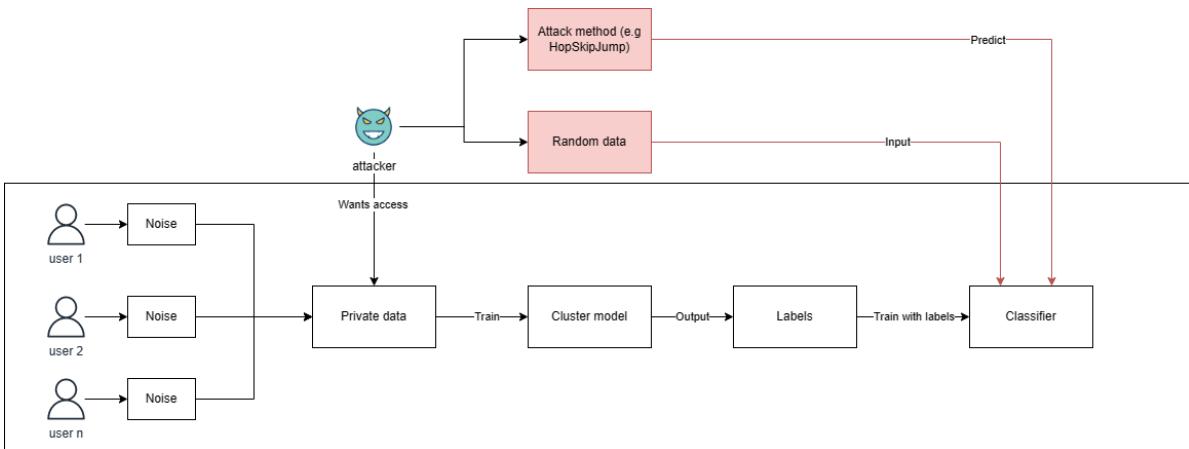


Figure 4.2: Semi-supervised black-box approach to execute a member inference attack.

1. On the left side of the figure, there are users providing data. Because this approach uses local noise, the noise added and sent to the server.
2. The private data is collected and saved on the server, where the clustering algorithm is trained.
3. From the output of the clustering algorithm, the cluster labels are extracted and used to train a classifier (semi-supervised setup).
4. The attacker (green user) uses an attack model (e.g., HopSkipJump) to exploit the classifier's confidence in predicting training or test data.
5. The attacker can then use the classifier to predict if the data is a member or not. However, this will be less accurate if the cluster/classifier models are trained on private data.

5

METHODOLOGY

We conducted experiments to gain insights into the proposed methods for researching the appliance of kD-Laplace for clustering algorithms. The experiment results are used to evaluate our method against other literature. In this chapter, we explain:

1. Research design: The background and research questions are explained. Furthermore, we explain the datasets and privacy mechanisms used in the experiments.
2. Data collection: The methods used to collect the data necessary to answer the research questions. These are methods for running experiments to collect data about utility and privacy.
3. Data analysis: We explain how we analyze the data collected in the previous step.

5.1. RESEARCH DESIGN

This section describes the overall setup of the research.

5.1.1. RESEARCH BACKGROUND

Clustering data is a crucial part of machine learning, aiming to discover patterns in the data that may not be immediately visible to the human eye. To achieve this, the data is trained on large datasets. However, storing such data is unsafe, as unauthorized access could lead to breaches.

LDP has been introduced to safeguard user privacy while preserving data patterns. Adding local noise means the plain data is never stored on a central server. But, the limited available data in the local view distorts the patterns excessively in each noise addition.

Current literature has attempted to address this challenge, but the solutions fall short. They either require modifications to the clustering algorithm or lack practical applicability due to the use of synthetic data. Existing literature focuses mainly on 2-dimensional data with K-Means as the clustering algorithm.

To address these limitations, we propose a new LDP method called kD-Laplace, utilizing distance to preserve data patterns using the concept of GI.

Our method enables secure training of cluster algorithms based on input-perturbation. Due to this approach, we can train multiple cluster algorithms without modifications and

extend them to n-dimensional data. We will test three variants of the kD-Laplace mechanism to assess their utility and privacy characteristics.

1. kD-Laplace: Plain mechanism without any additions for truncation.
2. grid-kD-Laplace: Mechanism with truncation using grid-remapping (See Equation: 4).
3. density-kD-Laplace: Mechanism with truncation using density-remapping (See Equation: 5).

We will compare the kD-Laplace mechanism to Piecewise, which is another LDP mechanism (See Section 2.3). And assess the effectiveness of the proposed kd-Laplace variants.

This research combines real-world and synthetic data to demonstrate practical applicability. Extensive external and internal validation experiments will be conducted to establish the method's practical relevance and effectiveness.

5.1.2. RESEARCH QUESTIONS

The main question of the research is as follows:

"How can the kD-Laplace algorithm be applied in training privacy-preserving clustering algorithms on distributed k-dimensional data?"

This question is divided into three smaller sub-questions:

1. *RQ1: How can 2D-Laplace be used to protect the privacy of 2-dimensional data employed for training clustering algorithms?*

This research question investigates the utility and privacy differences among the three kd-Laplace variants and compares the mechanism with the Piecewise Mechanism. We focus on the implementation of kd-Laplace on n-dimensional data.

2. *RQ2: How can 3D-Laplace be extended to protect the privacy of n-dimensional data employed for training clustering algorithms?*

The setup for this research question is the same as for research question 1, but instead of 2D data, we focus on 3D and n-dimensional data.

3. *RQ3: How do dataset characteristics impact the kD-Laplace mechanism for utility and privacy?*

In this research question, we evaluate the dataset characteristics and their influence on kD-Laplace. Also, we investigate if we can improve the utility and privacy of kd-Laplace by adopting grid-kD-Laplace and density-kD-Laplace (3.12). We use several hypotheses questions to answer research question 3.

In the last two hypotheses, we specifically focus on the K-Means clustering algorithm to test our hypotheses. The choice of K-Means is due to its simplicity, making it suitable for our hypothesis tests. Also, we assume that the K-Means results are representative of the other clustering algorithms.

- (a) *H1: Adding remapping based on density improves utility without sacrificing privacy:* Since the noise is updated based on the density of the data points, the clusters stay preserved (5). As a result, the utility increases while the data points

remain indistinguishable. Therefore, we have extended our mechanism with density remapping and named it density-kD-Laplace.

- (b) *H2: The privacy leakage (adversary advantage) and utility increases for more dimensions:* The hypothesis arose from our observation while investigating/implementing kD-laplace(3.3.2). Adding more dimensions ($5 >$) decreases the added noise gradually, increasing utility. On the other hand, privacy is expected to decrease because the noise is less.
- (c) *H3: The shape of the data negatively impacts the kd-Laplace mechanism in terms of privacy and utility:* Because the mechanism heavily relies on Euclidean distance, the shape (distance between the data points) can ultimately harm utility and privacy. We have already observed this difference when comparing the heart and seed datasets in research questions 1 and 2. But, to rule out the potential impact of the number of data points (the heart dataset has 2126 samples and the seed-dataset 210), we generate three synthetic datasets, each with 1000 samples (See section 5.1.3).

5.1.3. DATASETS

For this research, we selected two real-world datasets based on the related papers (2.3). The datasets are sourced from the UCI Machine Learning Repository [noa, c].

1. **Seeds dataset**¹: This dataset was used in several related works and contains 210 samples with 7 (numerical) attributes. The dataset contains information about seeds, like kernel width and density. We conducted experiments with 2, 3, and 7 dimensions and decided to use the following features (based on the correlation between the features):
 - (a) 2-dimensional data: area and perimeter.
 - (b) 3-dimensional data: the kernel's area, perimeter, and length.
 - (c) 7-dimensional data: All numerical features.
2. **Heart dataset**²: This dataset is selected because of the mixed data and amount of instances. It has 23 attributes, including ten numerical attributes and 2126 samples. The dataset contains information about measurements of fetal heart rate (FHR) and uterine contraction (UC). We conducted experiments with 2, 3, and 10 dimensions and decided to use the following features (based on the correlation between the features):
 - (a) 2-dimensional data: FHR baseline and histogram-min.
 - (b) 3-dimensional data: FHR baseline, histogram-min, and accelerations.
 - (c) 10-dimensional data: All numerical features.

The following datasets are for the H3 (shape) hypothesis investigated in research question 3. For this purpose, we generated a 2-dimensional and 3-dimensional dataset with 1000 samples.

¹<http://archive.ics.uci.edu/ml/datasets/seeds>

²<https://archive.ics.uci.edu/ml/datasets/cardiotocography>

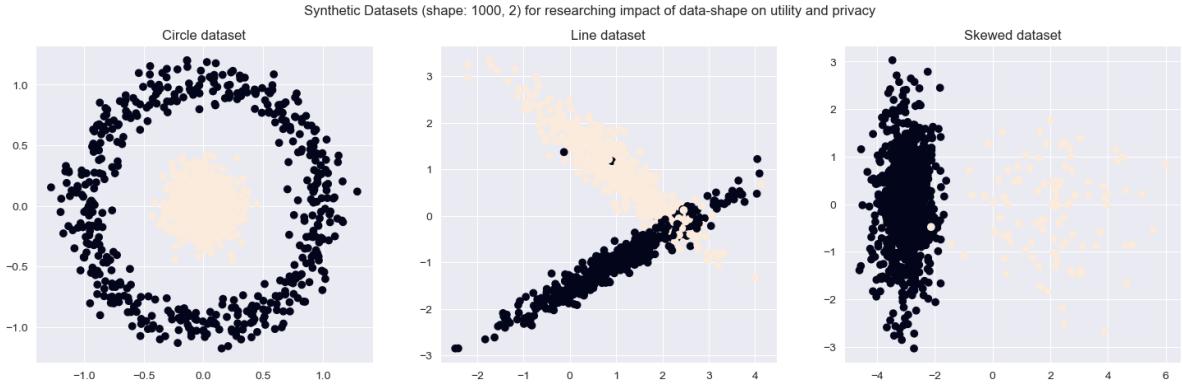


Figure 5.1: Synthetic datasets with 1000 samples and 2-dimensions

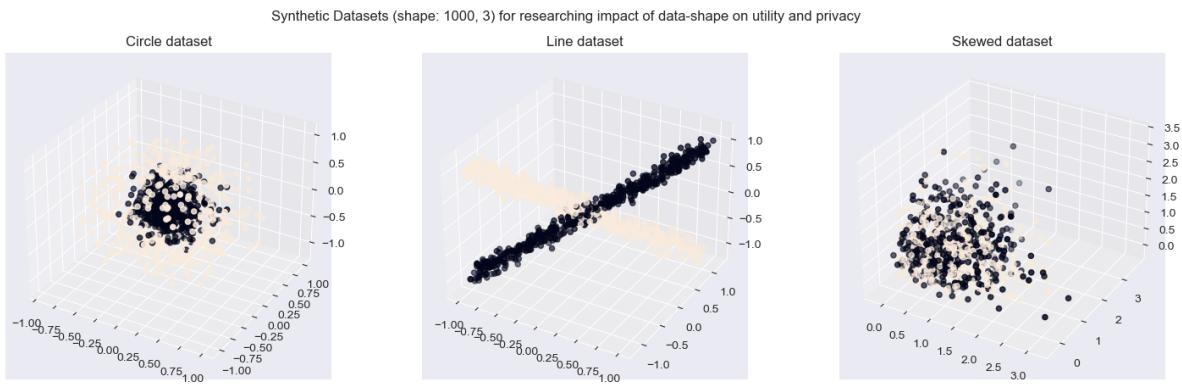


Figure 5.2: Synthetic datasets with 1000 samples and 3-dimensions

1. **Circle dataset:** Dataset with a circle shape.
2. **Line dataset:** Dataset is a line (shape is much like the seeds dataset).
3. **Skewed dataset:** Dataset samples are skewed/concentrated to one side (shape is much like the heart dataset).

5.1.4. EXPERIMENT SETUP

We evaluate all privacy mechanisms by comparing them in utility and privacy. To reduce the measurement bias of results, we executed them ten times for multiple privacy budgets and reported the average for each [Huang et al., 2021].

1. The experiments run ten times, and we report the mean.
2. All experiments run for multiple ϵ s: 0.5, 0.7, 1, 1.5, 2, 3.5, 5, 7, 9.

5.1.5. ENVIRONMENTAL SETUP

For running the experiments, we use 16GB RAM and an i7-10750H 2.6Ghz processor. The experiments are run using a Docker container which runs a pre-configured distribution of Linux Alpine. It includes a pre-installed Anaconda environment for Python ^{3,4}. We run the container using the dev-container feature for visual-studio code ⁵. This allows us to create a reproducible experiment environment.

LIBRARIES & CODE VERSIONS

We use Python version 3.9.13 with Jupyter Notebook for creating a reproducible experimental environment. The packages for Python are:

- Scikit-learn: 1.0.*
- Yellow-brick: 1.5
- Numpy: 1.24.*
- Pandas: 2.0.*
- Seaborn: 0.11.*
- Matplotlib: 3.5.*

5.2. DATA COLLECTION

This section explains what methods/ algorithms we use to collect the data necessary to answer the research questions.

5.2.1. HYPERPARAMETER SELECTION

For the three different algorithms: K-Means, AP, and OPTICS, we analyzed the most important decisions regarding hyperparameter selection (See section 3.1.3). This section gives a short list and explanation of the parameters we used throughout the experiments.

K-MEANS

Parameter	Description	Value	Dataset
K-value	Calculated based on an "elbow" plot.	k=4 (see Figure 1)	Seeds dataset
K-value	""	k=4	Heart dataset
K-value	""	k=5 (see Figure 2)	circle dataset
K-value	""	k=4 (see Figure 3)	line dataset
K-value	""	k=4 (see Figure 4)	skewed dataset

Table 5.1: K-Means hyperparameters for dataset 1 - 3

The above table shows the relevant hyperparameters for the K-Means clustering algorithm. The hyperparameter differs for each dataset, so we must display it for each. This

³<https://github.com/devcontainers/images/tree/main/src/anaconda>

⁴tag: mcr.microsoft.com/devcontainers/anaconda:0-3

⁵<https://code.visualstudio.com/docs/devcontainers/containers>

hyperparameter is the k-value used to determine the number of clusters. The "value" column shows the value we used for the experiments, with the corresponding "elbow" plot in the referenced figure.

AGGLOMERATIVE CLUSTERING

Parameter	Description	Value	Dataset(s)
Number of clusters	This is decided based on elbow plots with the SC metric 2.2.2	n_clusters=2	Heart-dataset (2 & 3 dimensions) Seeds-dataset (7 dimensions) Circle-dataset (3 dimensions) Line-dataset (2 dimensions)
Number of clusters	""	n_clusters=3	Heart-dataset (9 dimensions) Seeds-dataset (2 & 3 dimensions) Skewed dataset (2 dimensions)
Number of clusters	""	n_clusters=4	Skewed dataset (2 dimensions)
Number of clusters	""	n_clusters=5	Circle dataset (2 dimensions) Line-dataset (3 dimensions)

Table 5.2: Agglomerative clustering hyperparameters for the datasets

The above table shows the relevant hyperparameters for the [Agglomerative Clustering \(AG\)](#) clustering algorithm per dataset. Because the hyperparameters "n_clusters" rely heavily on the number of dimensions, each dataset's dimensions were provided. For the "n_clusters," we used the [SC](#) in corporation with the elbow method to determine the number of clusters. In addition, there is the "linkage," which is "ward" for all configurations (See Section [2.2.2](#)).

OPTICS

Parameter	Description	Value	Dataset
Minimum points	Decided using the formula $minPts = n * 2$, where n is the number of features (2.2.2)	$minPts = 4$	Seeds dataset Heart dataset Circle dataset Line dataset Skewed dataset (2-dimensions)
Minimum points	""	$minPts = 6$	Seeds dataset Heart dataset Circle dataset Line dataset Skewed dataset (3-dimensions)
Minimum points	""	$minPts = 14$	Seeds dataset (7-dimensions)
Minimum points	""	$minPts = 20$	Heart dataset (10-dimensions)

Table 5.3: DBSCAN hyperparameters for datasets 1 - 3

The above table shows the relevant hyperparameters for the **OPTICS** clustering algorithm for each dataset. Because the minimum points depend on the number of dimensions, we must display them for each dataset (See Section: 2.2.2). We omitted the synthetic datasets for the same reason specified for **AP**. The first two rows display the minimum points for the datasets that have 2 and 3-dimensional data. The last two rows display the minimum points for the datasets that have 7 and 10-dimensional data.

5.2.2. UTILITY AND PRIVACY EVALUATION

UTILITY

To measure cluster utility, both internal and external validation methods are used:

1. **External validation:** The external validation is measured by comparing the labels of non-private trained cluster algorithms with those trained using a privacy mechanism. The outcome is between 0 and 1, where 1 indicates the highest similarity (thus the best result). AMI (Adjusted Mutual Information) is used to assess the external validity of the cluster algorithms (See Section 2.2.3).
2. **Internal validation:** The internal validation measures the intrinsic properties of the clustering algorithms. The outcome is a value between -1 and 1 for the SC evaluation. Where -1 indicates incorrect and 1 dense clustering (See Section 2.2.3).

Because the cluster algorithms rely on Euclidean distance, we need to apply some data standardization. For this purpose, we use standard scaling provided by the Scikit-learn package⁶.

PRIVACY

Privacy is hard to quantify, but we can measure the privacy loss/gain by calculating the Euclidean distance between the non-perturbed and perturbed data. In addition, we evaluate privacy by simulating a membership inference attack and calculating the adversary advantage.

1. **Privacy distance:** The first measurement we evaluate is the distance between the dataset's non-private and private variants. This metric gives us a sense of how much extra distance (and privacy) the privacy mechanisms offer compared to the non-private variant. To this end, the average Euclidean distance is measured and reported per epsilon. A higher distance indicates more privacy.
2. **Adversarial advantage:** We used the Membership Inference Attack (MIA) that Shokri et al. proposed with the implementation that was provided by Adversarial Robustness Toolkit (ART) [Nicolae et al., 2019]. An earlier study also explored this attack to evaluate differential privacy. Similar to this attack, we train a classifier with perturbed data and evaluate it using non-perturbed data (test-data / shadow-data) [Zhao et al., 2020]. We consider a semi-supervised setup (Figure 4.2), where we train a classifier with the perturbed data and evaluate it using non-perturbed data (test-data / shadow-data). For the classifier, we use a RandomForestClassifier [Rigaki and Garcia, 2021]. Finally, we evaluate the adversary advantage (percentage) using $TPR - FPR$ [Yeom et al., 2018]. Figure: 5.3 provides a visual setup of the experiment.

Although the adversary advantage is a proven method for measuring MI attacks, we also include the TPR as an essential measurement. This metric is most interesting to us because this displays the percentage of the actual leaked labels (see Section 4.3).

⁶<https://scikit-learn.org/stable/modules/preprocessing.html>

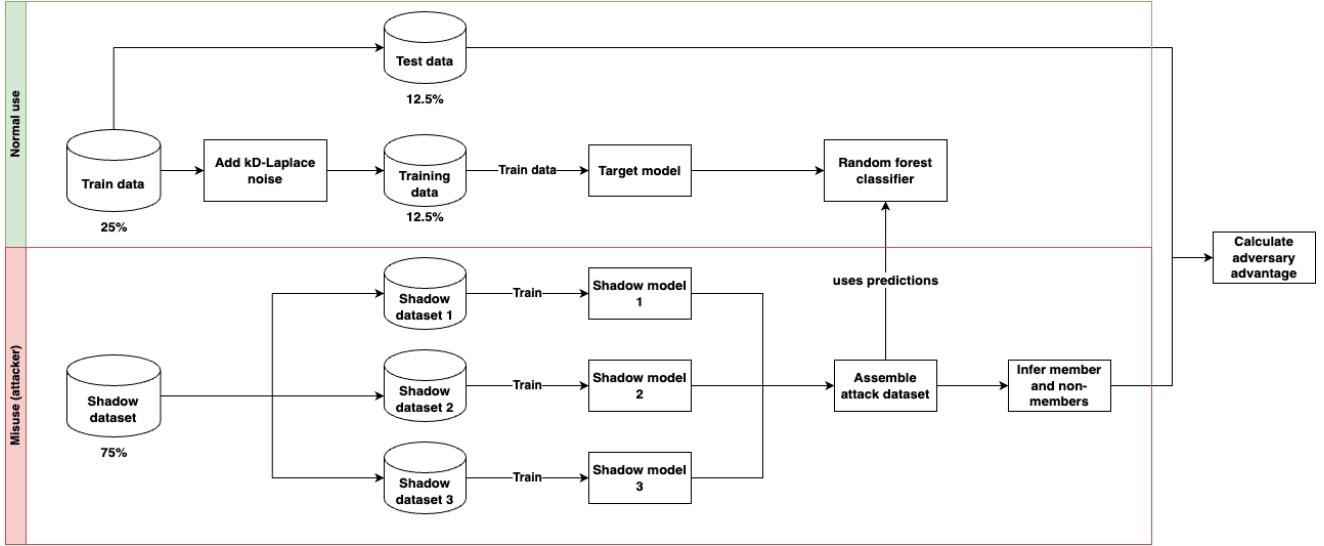


Figure 5.3: Member inference attack using shadow models. The green swim lane illustrates the normal setup, and the red swim lane projects the adversary steps.

The figure above visually represents the **MIA** attack we set up using semi-supervised learning. The green swim lane illustrates the setup of an honest person, and the red swim lane projects the attacker's steps. This green lane is a standard system usage where the actor (e.g., data analyst) trains a model with the perturbed data. Because the model in the green lane was trained using perturbed data, the labels are slightly different from the original labels.

The attacks use shadow models to train a classifier to predict the labels. So, because the original model was trained using perturbed data, the labels are slightly different, and the shadow models cannot infer the original labels.

The attacker could infer many original labels if the adversary advantage or **TPR** is high. In this case, a lower score is better than a higher score.

5.2.3. RESEARCH ROADMAP

This section explains the experiments' setup and the result reporting order.

1. Cluster utility: The mechanisms kD-Laplace and Piecewise are compared using the external and internal validation methods. We report the **AMI** and **SC** in the results for both mechanisms and each dataset. For this experiment, we only consider real-world datasets.
2. Mechanism utility: Both mechanisms are compared against each other by evaluating the **AMI** and **sc**. In this research, we also conduct experiments to assess the impact of the number of dimensions on the utility of each dataset.
3. Mechanism privacy: We do the same for utility, but now with privacy. For this purpose, we evaluate the adversary advantage and privacy distance.
4. Mechanism comparison: Now we established the performance of kD-Laplace and Piecewise, we compare the different variants of kD-Laplace.

5.3. DATA ANALYSIS

For the data analysis, we utilize visualization libraries in Python, primarily Matplotlib, in combination with Seaborn.

- Line/bar plot: These plots visualize comparisons between the different privacy mechanisms. The different epsilon values are displayed on the x-axis, and the utility/privacy metric is displayed on the y-axis.
- Heatmap plot: These plots visualize the interaction between dimensions and epsilons. This way, we can display two categorical values (dimension/epsilon) and one continuous value.

6

RESULTS

This chapter aims to present the results to the reader. As indicated in the methodology, we tested four mechanisms (three variants of kd-Laplace and Piecewise) for their utility and privacy.

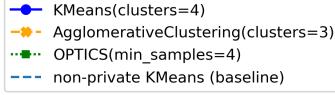
1. Cluster utility: Visualise the utility of kD-Laplace and Piecewise for 2/3/n-dimensional data. The results are displayed using a line diagram, using **AMI** and **SC**.
2. Mechanism utility: Visualise the utility of kD-Laplace and Piecewise using a heatmap plot. The results for each dimension and privacy budget are provided for only the **AMI** score.
3. Mechanism privacy: Visualise the privacy of kD-Laplace and Piecewise using a heatmap plot. The results for each dimension and privacy budget are provided for only the adversary advantage and privacy distance.
4. Mechanism comparison: Visualise the comparison between the variants of kD-Laplace and Piecewise. The results for each mechanism & variant are provided using a bar-plot for the **AMI** score (utility) and the adversary advantage (privacy).

All results are reported for each dataset (See methodology: [5.1.3](#)) separately.

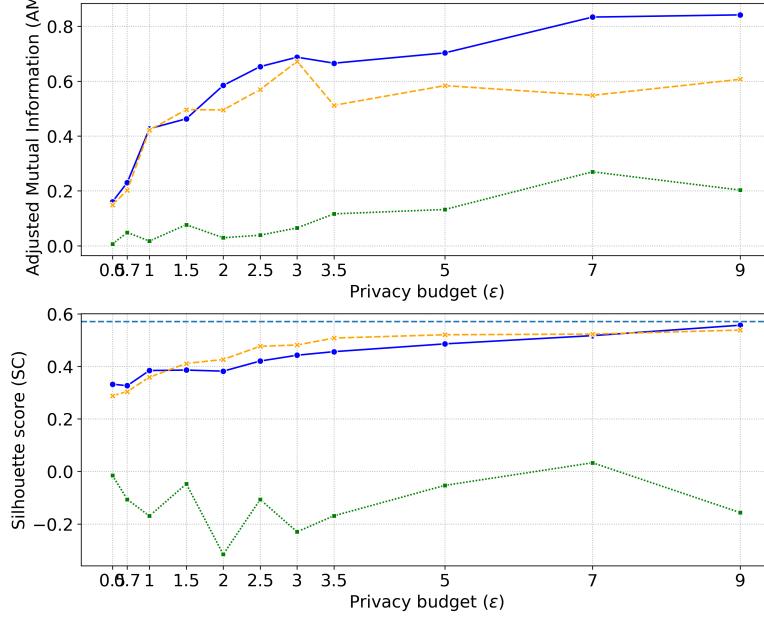
6.1. CLUSTER UTILITY

The results below display the difference in external and internal utility for the three cluster algorithms using the kd-Laplace and Piecewise mechanisms. The x-axis shows the privacy budget, and the y-axis shows the **AMI**. Please refer to the plots in the appendix for the same scores for kD-Laplace variants (See [.4](#)).

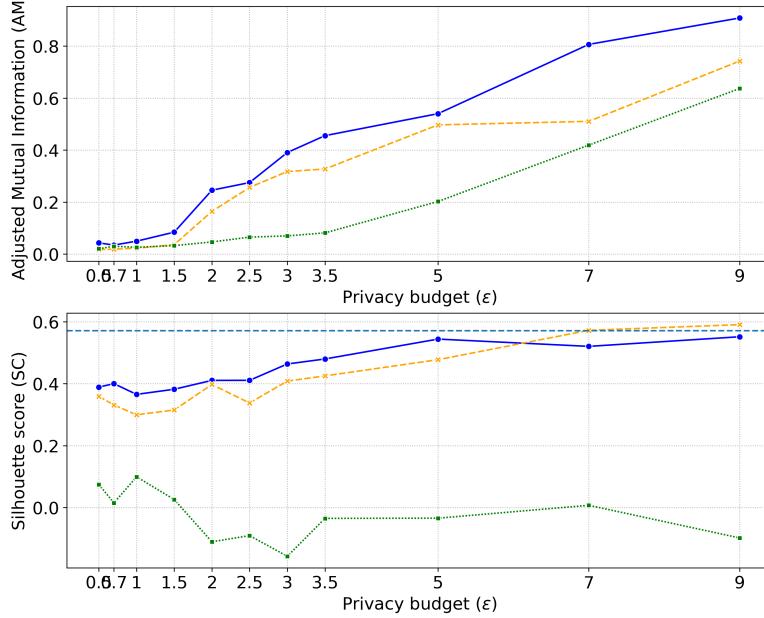
6.1.1. 2-DIMENSIONAL DATA



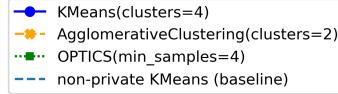
(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the 2-dimensional data seeds-dataset



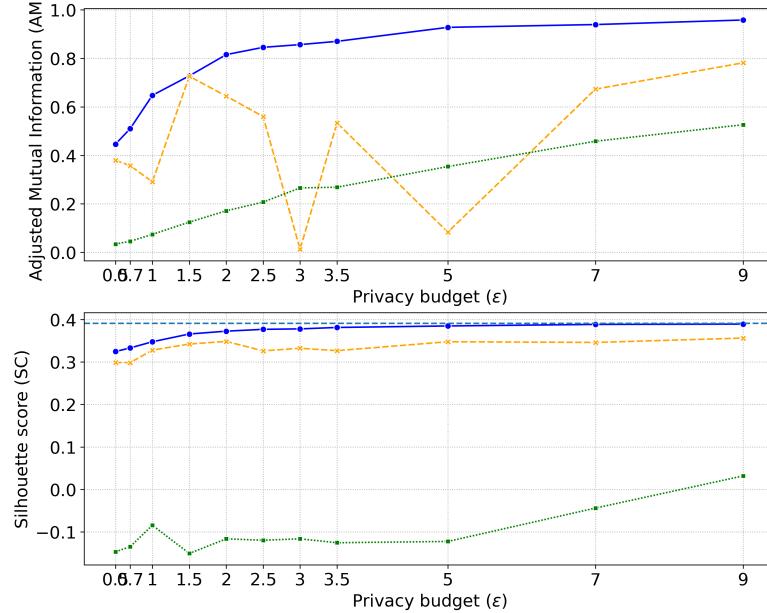
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 2-dimensional data seeds-dataset



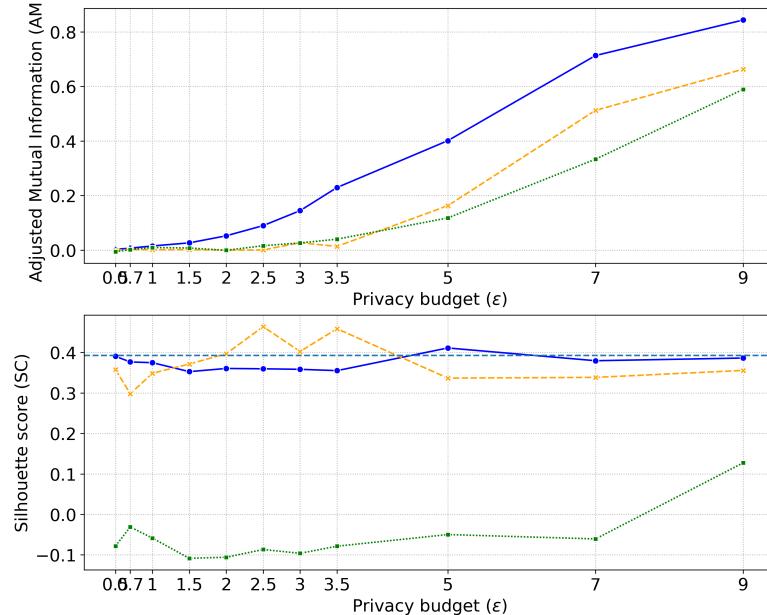
Piecewise shows a higher **AMI** for privacy budgets (epsilon) 7 and 9. In contrast, the kd-Laplace mechanism scores higher for all the other epsilons (0.1 onward 7). K-Means achieves the best score for both mechanisms with a slight margin compared to AG, but they score equal for **SC**. For both the mechanisms, OPTICS underperforms heavily but still scores the same as AP for Piecewise.



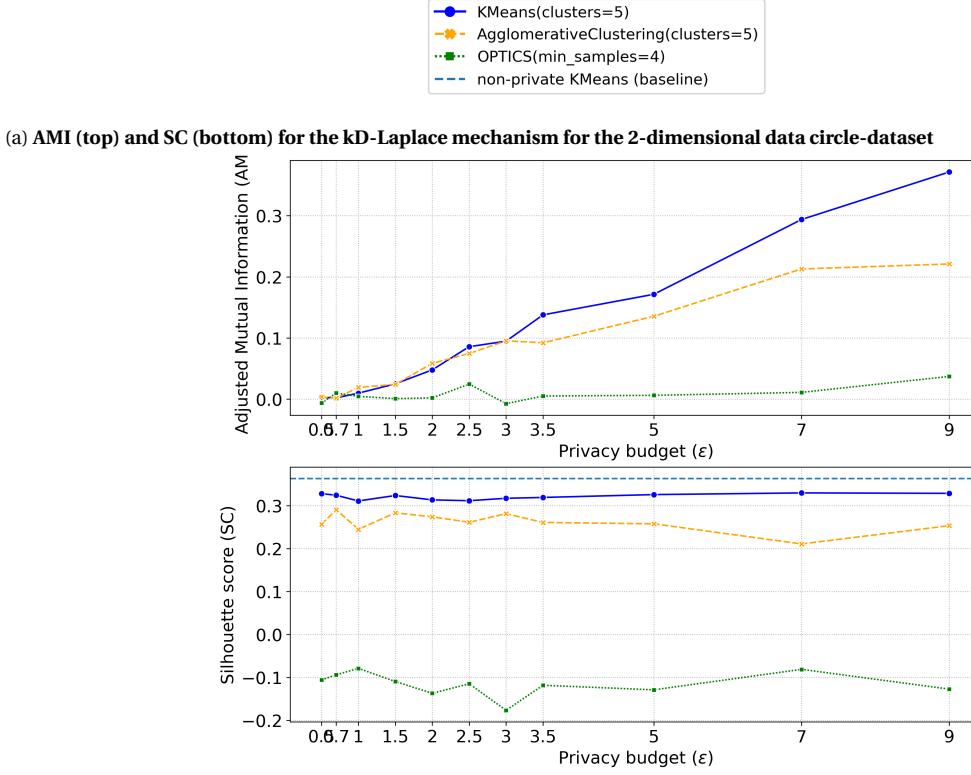
(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the 2-dimensional data heart-dataset



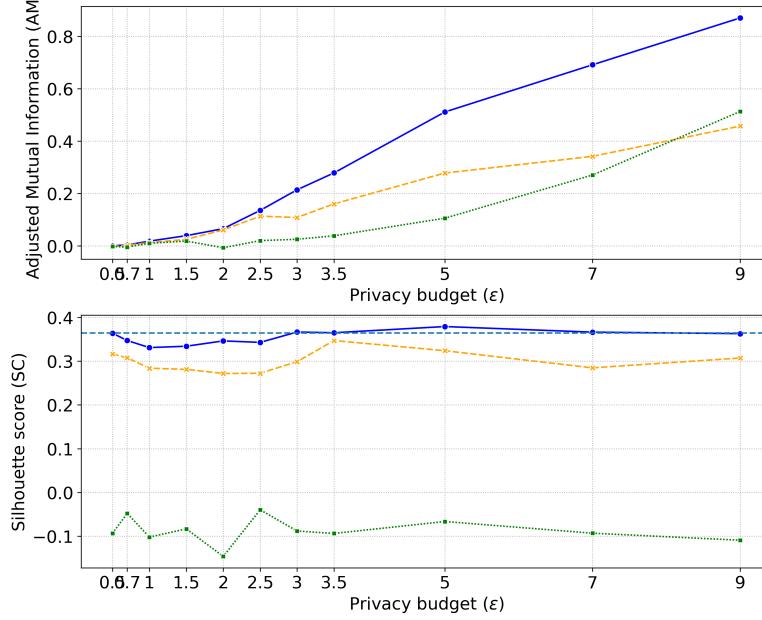
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 2-dimensional data heart-dataset



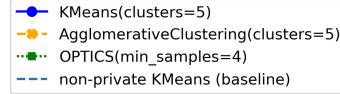
K-Means achieves a high **AMI** score of 0.95+ using kD-Laplace from privacy budgets 5 to 9, compared to Piecewise scoring between 0.4 to 0.8. Both mechanisms score high for **AG** and K-Means, reaching the baseline value, but **OPTICS** performs poorly. **AG** fluctuates more with kD-Laplace. For **SC**, both kD-Laplace and Piecewise reach the baseline for **AG** and K-Means, while **OPTICS** performs poorly.



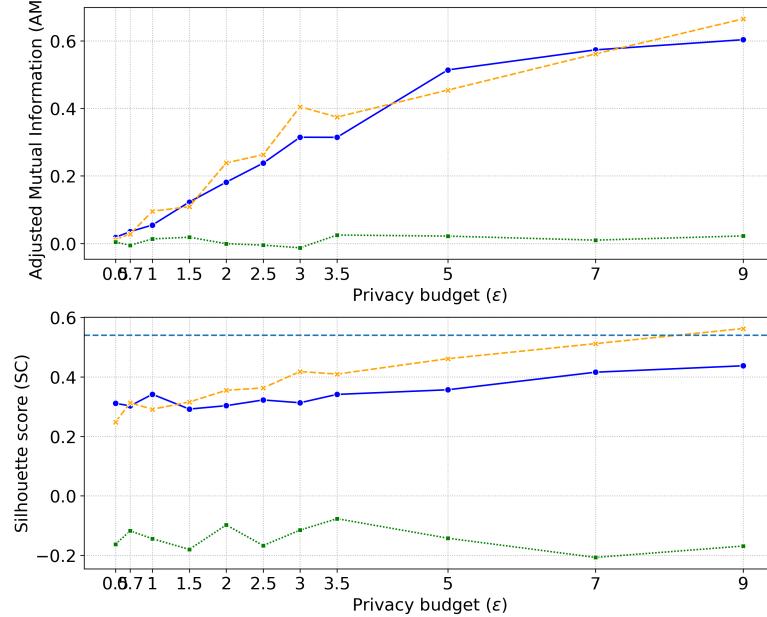
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 2-dimensional data circle-dataset



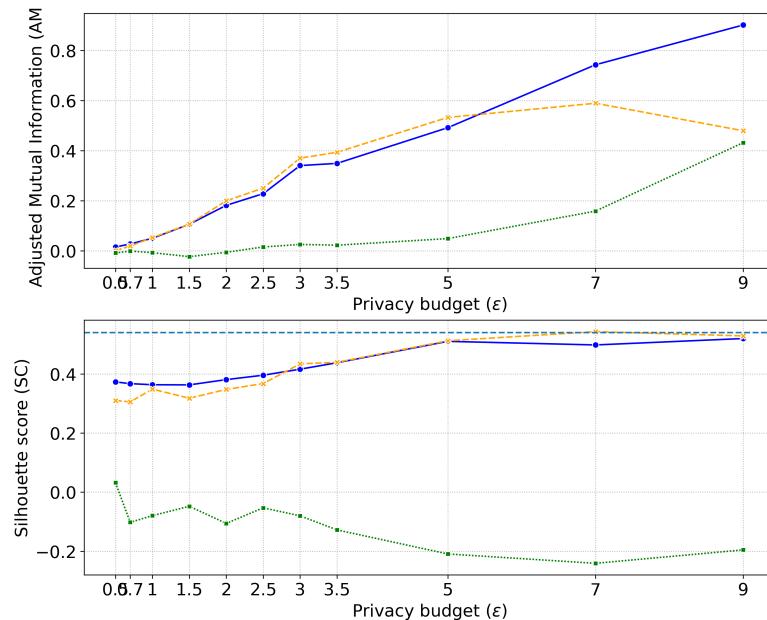
For both mechanisms, K-Means scores the privacy budgets from 2.5. Compared to Piecewise, the kD-Laplace mechanism scores the worst overall for almost all privacy budgets. The Piecewise algorithm scores 0.84 as the highest **AMI** for K-Means, while kd-Laplace scores 0.36. The difference is a little less for **SC**, but overall Piecewise is 0.10 higher. K-Means is for Piecewise on the baseline value for privacy budgets 3 to 9.



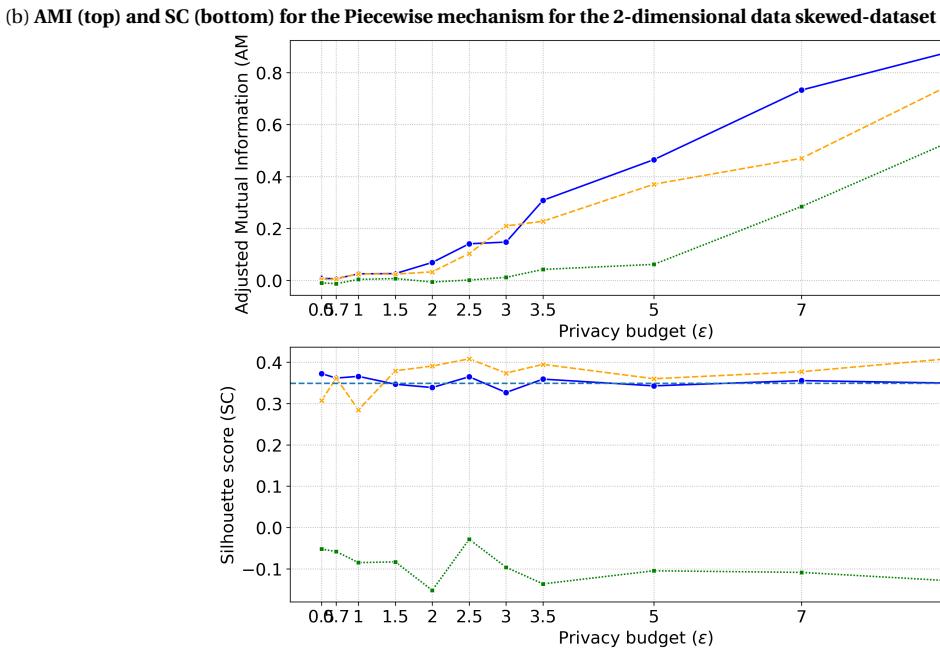
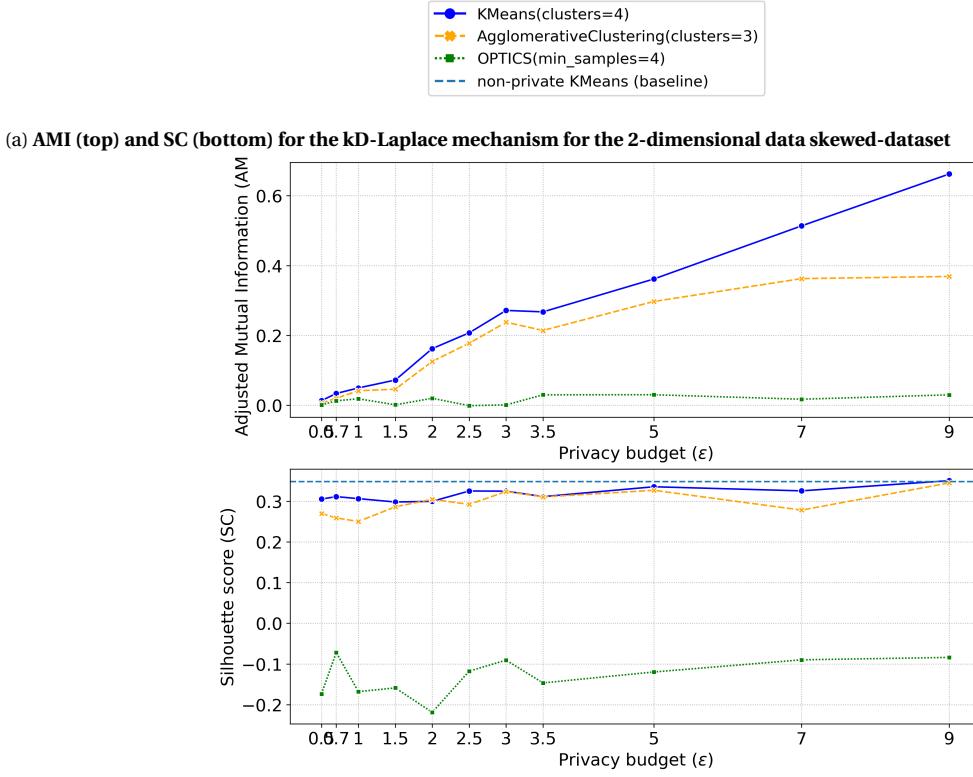
(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the 2-dimensional data line-dataset



(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 2-dimensional data line-dataset

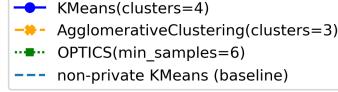


The kD-Laplace algorithm performs best with a privacy budget of 5 for K-Means (AMI 0.55 - 0.6). AG performs slightly better with a budget of 9 (AMI 0.63). Piecewise outperforms other methods, scoring 0.83 AMI for K-Means at budget 9 and better for different budgets, except for AG. For SC, the mechanisms have similar scores, with Piecewise at baseline from budget 5, kD-Laplace at 7, and AG beyond baseline from budget 9.

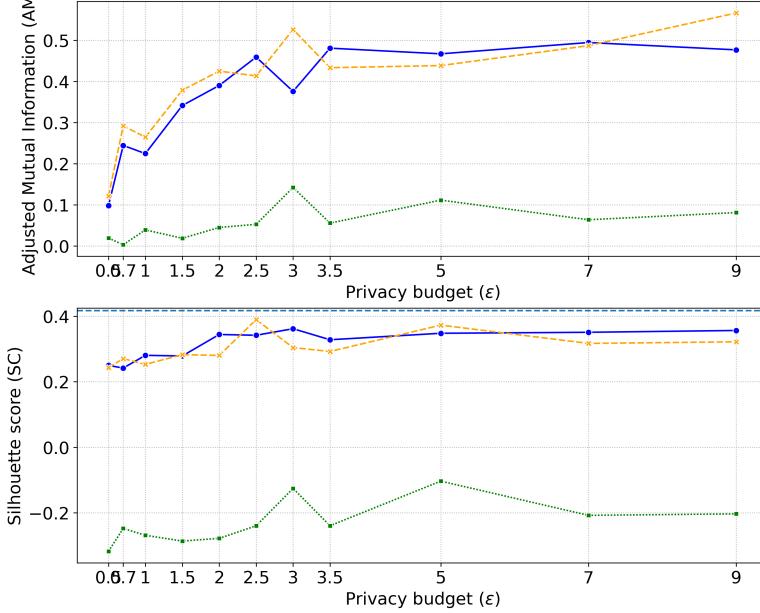


kD-Laplace performs best with K-Means, reaching 0.63 AMI at privacy budget 9. AG follows, scoring 0.38 AMI at budgets 7 and 9. Piecewise outperforms kD-Laplace for all clustering algorithms, scoring 0.82 AMI for K-Means at budget 9. In terms of SC, Piecewise also outperforms both K-Means and AG, scoring above the baseline (0.4), while kD-Laplace is slightly worse (around 0.3).

6.1.2. 3-DIMENSIONAL DATA



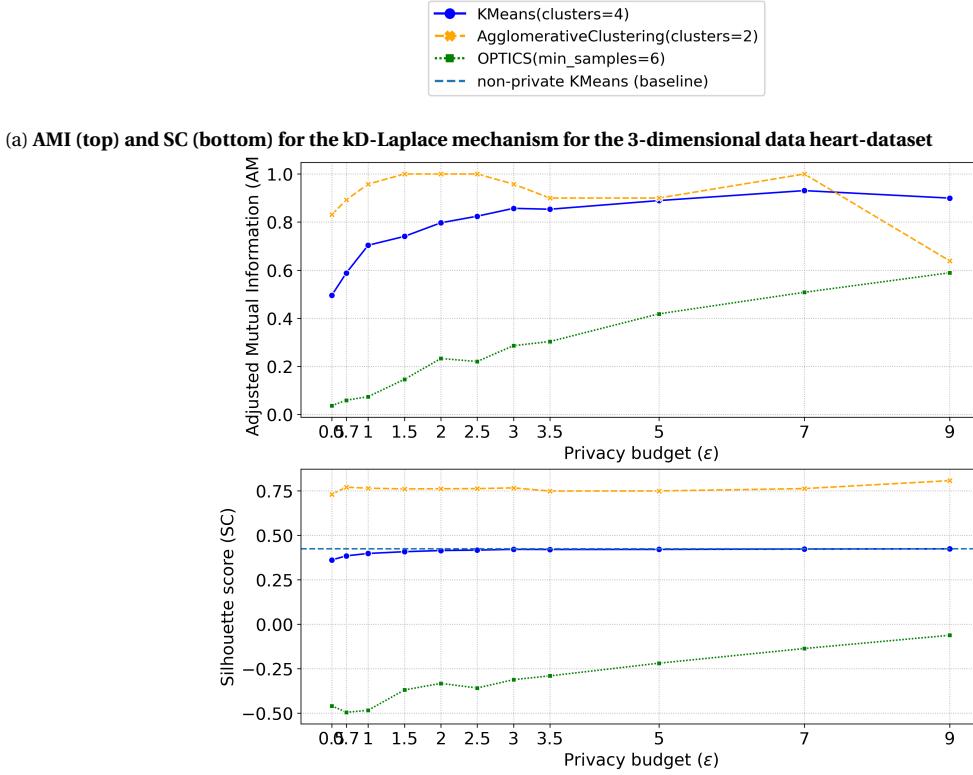
(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the 3-dimensional data seeds-dataset



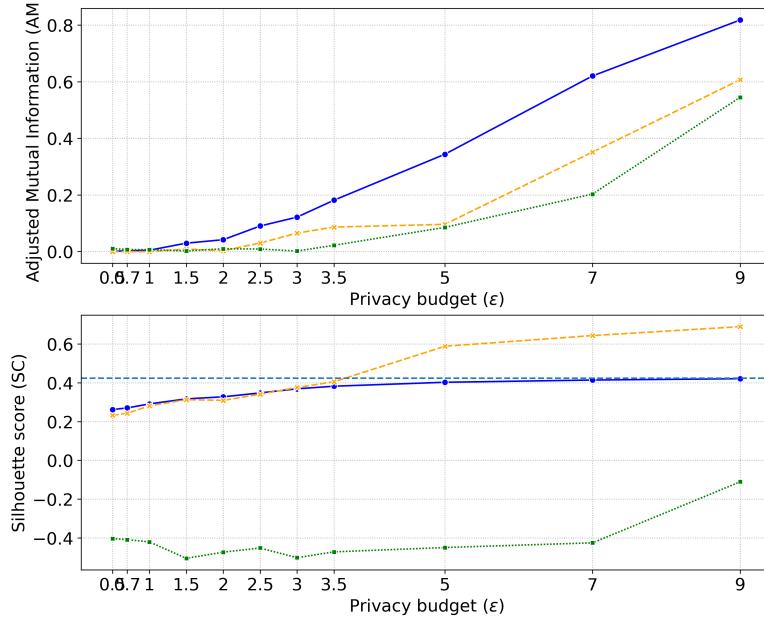
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 3-dimensional data seeds-dataset



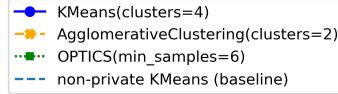
Piecewise performs better for the **AMI** for privacy budgets 3.5 to 9 but worse for the lower epsilons (0.1 - 3.5). K-Means scores 0.5 from epsilon 2 to 9 for kD-Laplace. For both mechanisms, **AG** scores the same as K-Means for both **AMI** and **SC**. **OPTICS** scores low (< 0.1) for kD-Laplace, but for Piecewise, it scores 0.4 and 0.6 for epsilon 7 and 9, respectively.



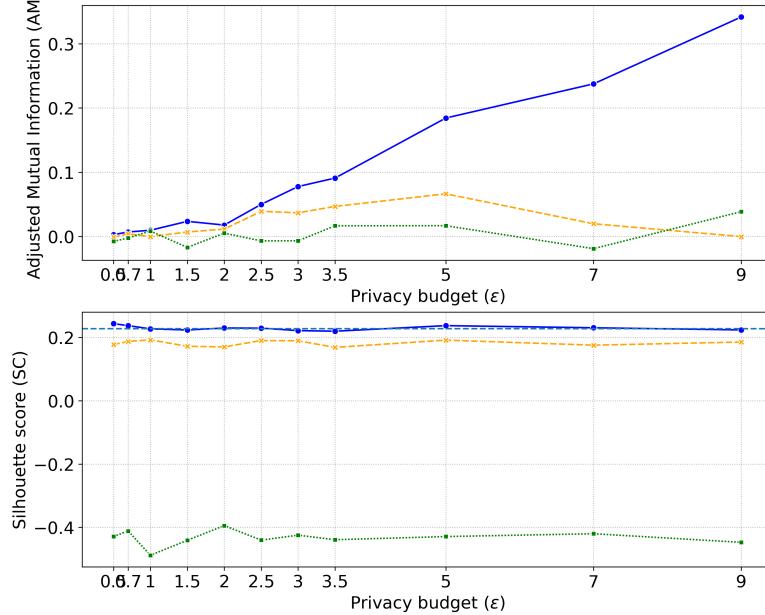
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 3-dimensional data heart-dataset



KD-Laplace performs well (+/- 0.90 AMI) for K-Means at budgets 7 and 9. AG scores around +/- 1.0 AMI for epsilon values of 1.5 to 2.5, staying above 0.8 for most budgets. OPTICS scores better (0.6 AMI at budget 9). Piecewise scores below 0.6 AMI for budgets < 7, reaching a maximum of 0.8 AMI for K-Means. For SC, both Piecewise and kD-Laplace reach the baseline for AG and K-Means. KD-Laplace surpasses the baseline by 0.25 for AG.



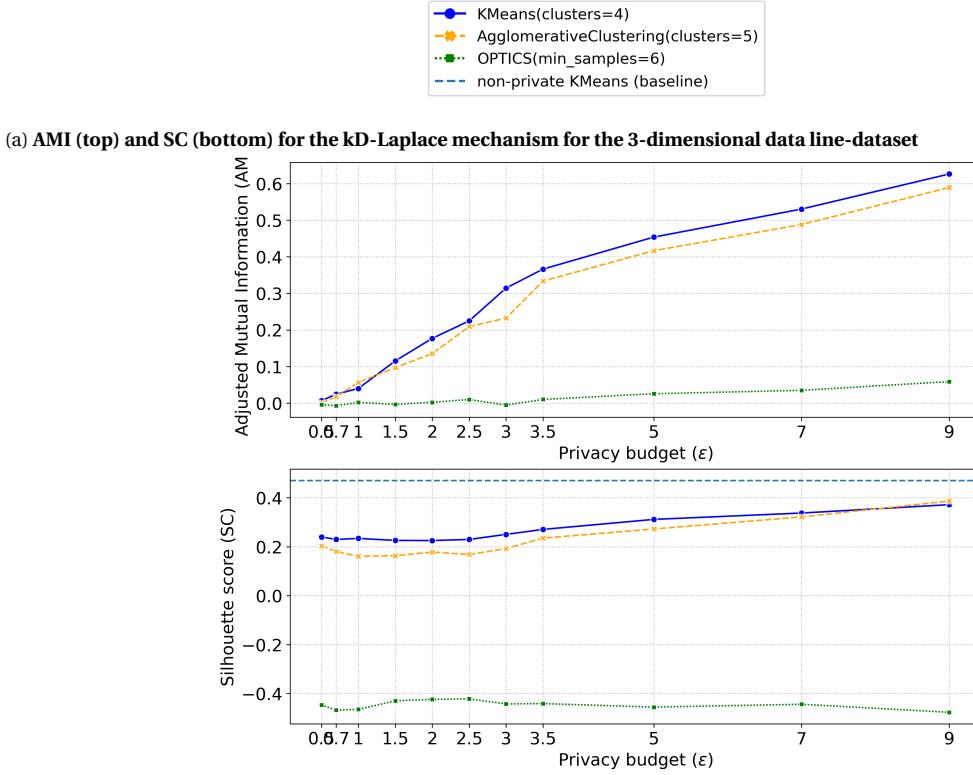
(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the 3-dimensional data circle-dataset



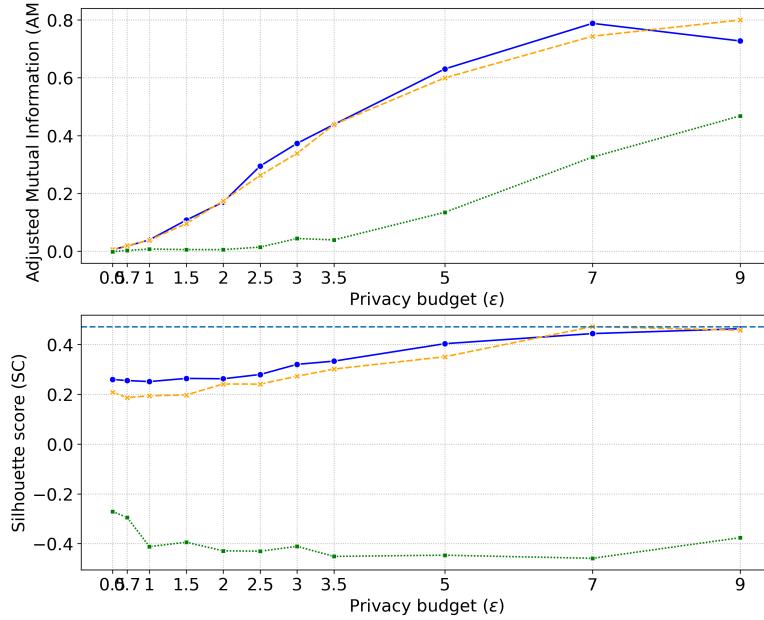
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 3-dimensional data circle-dataset



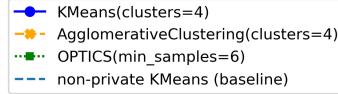
kD-Laplace performs best with K-Means, scoring a maximum of 0.33 AMI. The other algorithms perform poorly (< 0.1 AMI). Piecewise also shows the best results with K-Means, scoring 0.82 AMI, while the other algorithms perform weakly (< 0.2 AMI). OPTICS performs relatively well with 0.49 AMI at privacy budget 9. Both mechanisms have similar SC scores (around 0.2), which is at the baseline level. OPTICS performs below 0 SC for all privacy budgets.



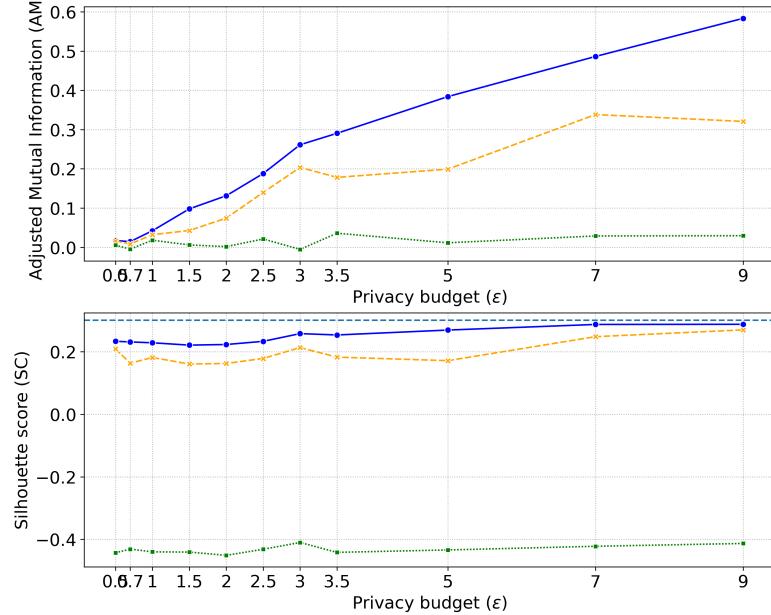
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 3-dimensional data line-dataset



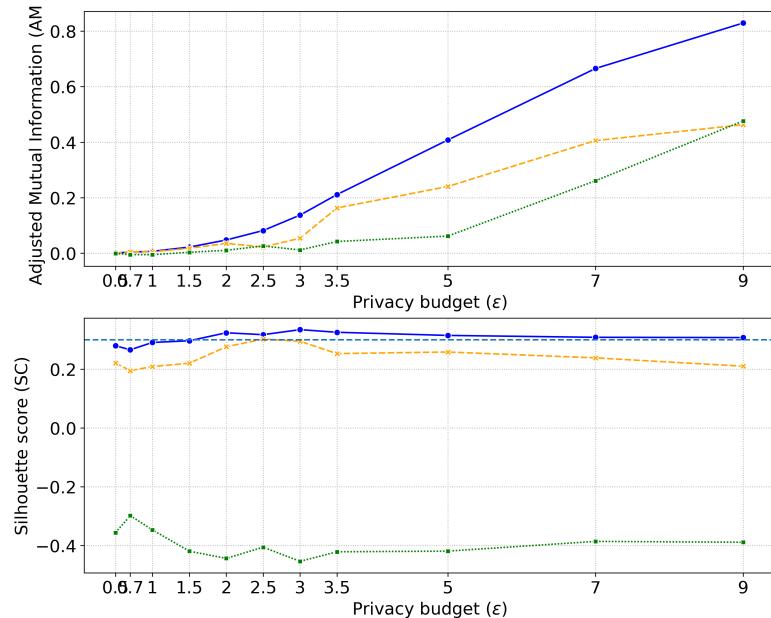
K-Means performs best with kD-Laplace, scoring 0.6 AMI from privacy budget 3.5 to 9. AG follows the same pattern but with around 0.2 AMI lower. OPTICS scores poorly (< 0.1 AMI). Piecewise shows a similar trend as kD-Laplace, with slightly higher scores. OPTICS improves to 0.43 AMI at privacy budget 9. Both mechanisms are similar for SC, with Piecewise slightly higher, while OPTICS remains relatively lower.



(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the 3-dimensional data skewed-dataset

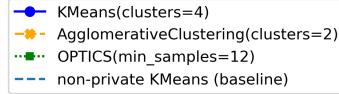


(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the 3-dimensional data skewed-dataset

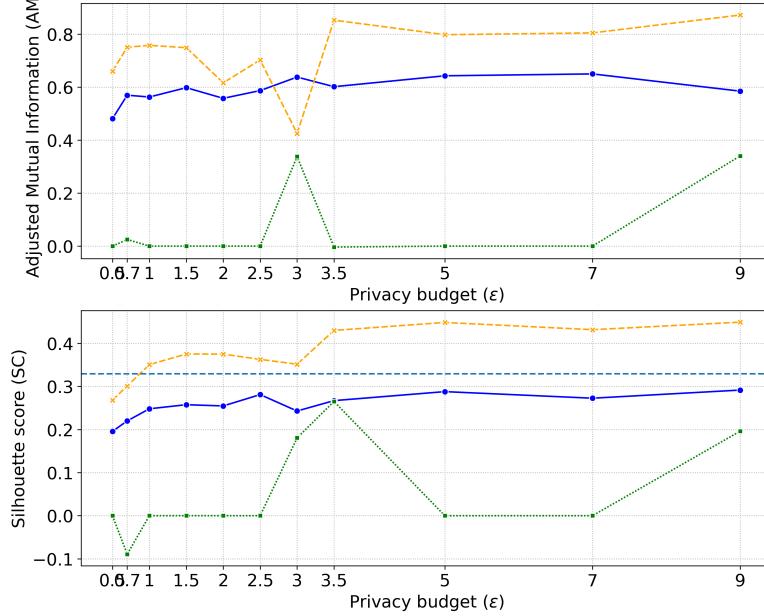


kD-Laplace scores best with the K-Means algorithm, 0.59 AMI for privacy budget 9. In contrast, AG is +/- 0.3 for privacy budgets 7 and 9. OPTICS scores worst with a maximum value of 0.02 AMI. The Piecewise mechanism scores much better with a AMI of 0.8 for K-Means. The same trend is observed for AG and OPTICS as with kD-Laplace. Both score worse, but OPTICS scores equal to AG for privacy budget 9. Both mechanisms score equal for the SC, but Piecewise is slightly higher and scores equal to the baseline.

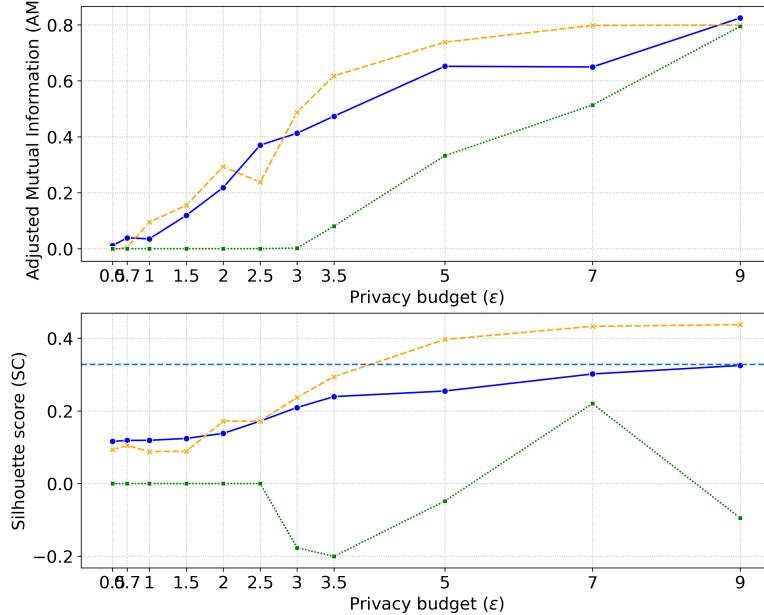
6.1.3. N-DIMENSIONAL DATA



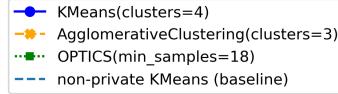
(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the n-dimensional data seeds-dataset



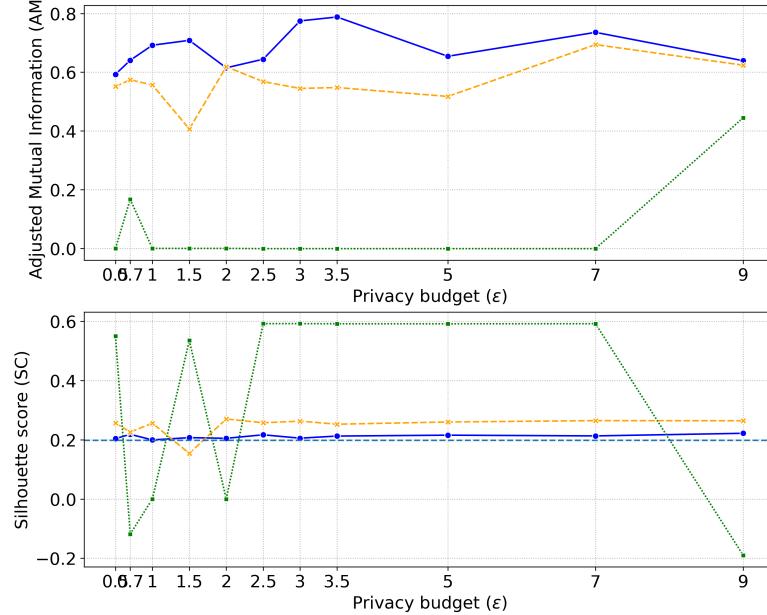
(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the n-dimensional data seeds-dataset



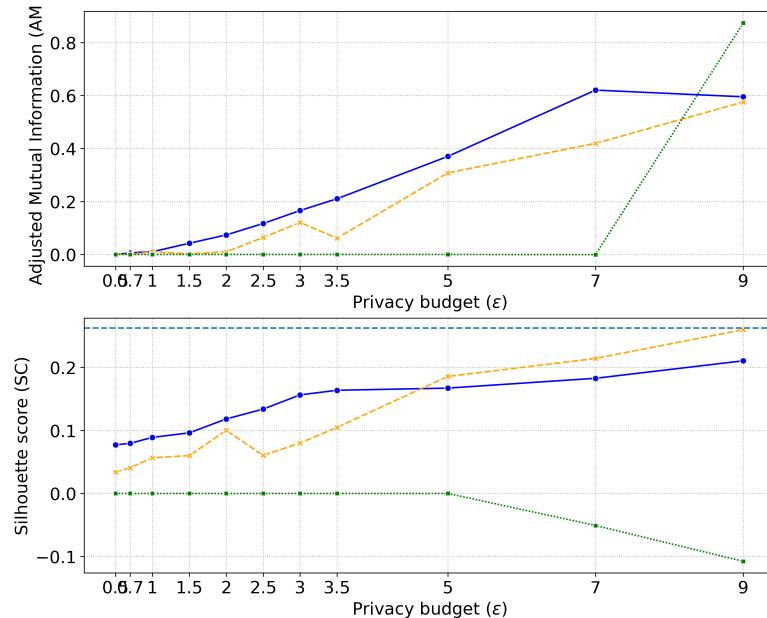
kD-Laplace scores 0.83 **AMI** for **AG** at privacy budget 9, while K-Means scores 0.5 to 0.6 **AMI** for all budgets. Piecewise shows a similar trend, with all algorithms scoring nearly equal at budget 9. **SC** follows a similar trend as **AMI**, with peaks at epsilon 3 and 3.5 for kD-Laplace with **OPTICS**. Overall, **OPTICS** scores lower for both mechanisms, with an upward trend for Piecewise but not for kD-Laplace.



(a) AMI (top) and SC (bottom) for the kD-Laplace mechanism for the n-dimensional data heart-dataset



(b) AMI (top) and SC (bottom) for the Piecewise mechanism for the n-dimensional data heart-dataset



kD-Laplace shows consistently high scores for K-Means and AG. Piecewise scores worse for K-Means (0.6) at budgets 7 and 9, while AG scores slightly lower. Remarkably, OPTICS achieves 0.85 AMI for privacy budgets 9 but zero for other budgets. For SC, kD-Laplace performs well for K-Means and AG, while OPTICS fluctuates from -0.1 to 0.6. Similarly, for Piecewise, OPTICS scores zero for most budgets but 0.1 for budgets 7 and 9.

6.2. MECHANISM UTILITY

The kd-Laplace and Piecewise mechanisms are compared using a heatmap in the sections below. We used a heatmap to show both the privacy budget (epsilon) and the number of dimensions. As explained earlier in the research design, only the K-Means algorithm was used to calculate the AMI. The x-axis displays the privacy budget, and the y-axis shows the number of dimensions.

Please refer to the plots in the appendix for:

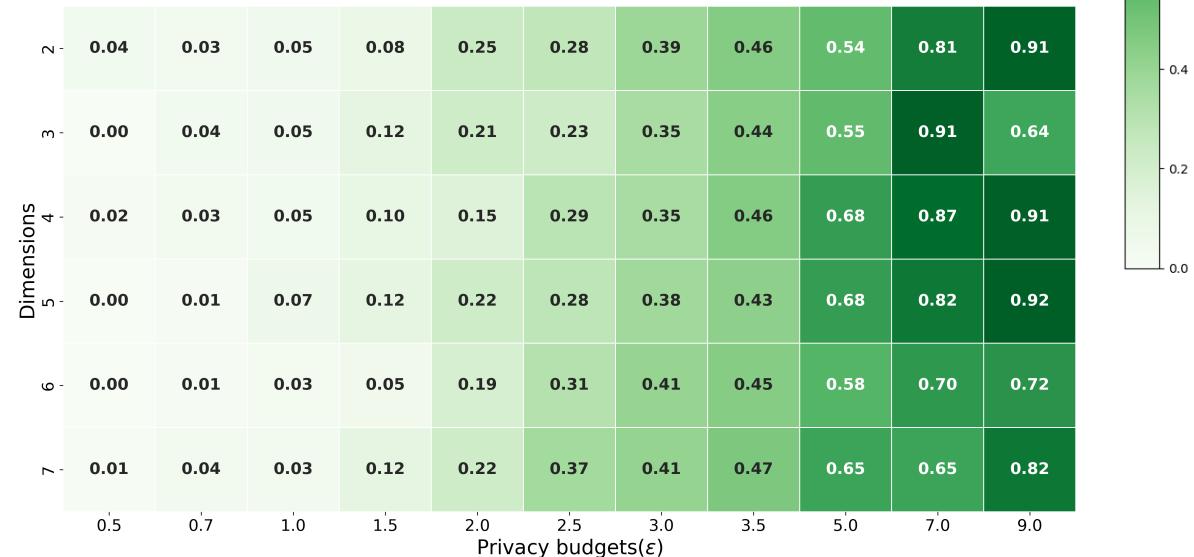
1. Privacy distance: .5.
2. True Positive Rate: .5.

6.2.1. SEEDS-DATASET

(a) Adjusted Mutual Information comparison for the kd-Laplace mechanism



(b) Adjusted Mutual Information comparison for the Piecewise mechanism



The two plots compare external validation (AMI) between the two privacy mechanisms. The kd-Laplace mechanism scores better for all privacy budgets (epsilon) for K-Means, except for privacy budgets 7 and 9. For epsilon 5, Piecewise is slightly better, but kD-Laplace scores better for 2 dimensions. KD-Laplace scores low for 2 - 5 dimensions and epsilon 0.5 and 0.7. However, Piecewise scores < 0.10 AMI for epsilons < 3 for all dimensions.

6.2.2. HEART-DATASET

(a) Adjusted Mutual Information comparison for the kd-Laplace mechanism

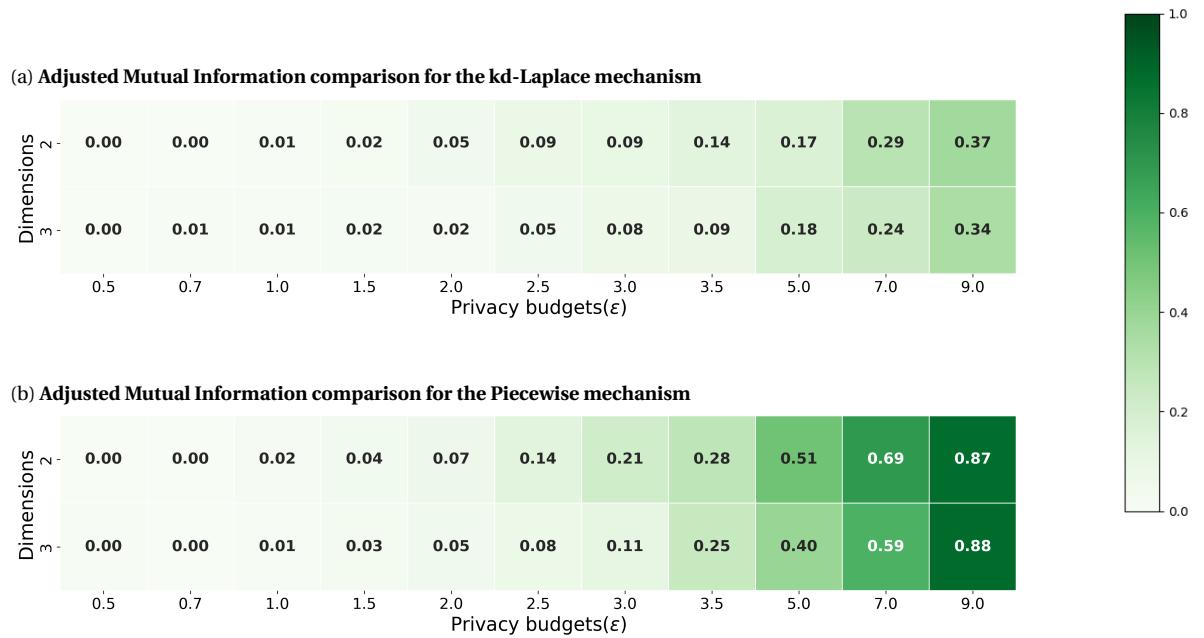


(b) Adjusted Mutual Information comparison for the Piecewise mechanism



For kd-Laplace, all scores are higher than 0.23 AMI. Dimensions from 4 to 10 with a privacy budget of 0.5 have the lowest scores, but then the AMI increases. Piecewise scores a maximum of 0.24 AMI for privacy budgets 0.5 to 3.5, with most values below 0.10. The number of dimensions does not seem to have an influence here. The values for privacy budgets 7 and 9 are approximately 0.70 and 0.80 AMI, respectively.

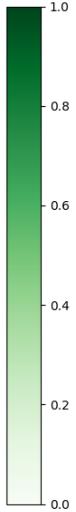
6.2.3. CIRCLE-DATASET



kD-Laplace achieves the highest value of 0.37 **AMI** for privacy budget 9. However, the score remains low for the other privacy budgets, regardless of the dimension. For Piecewise, the highest score is significantly higher, reaching a maximum of 0.88 **AMI** for privacy budget 9. The dimension does not seem to have much impact here, either.

6.2.4. LINE-DATASET

(a) Adjusted Mutual Information comparison for the kd-Laplace mechanism



(b) Adjusted Mutual Information comparison for the Piecewise mechanism

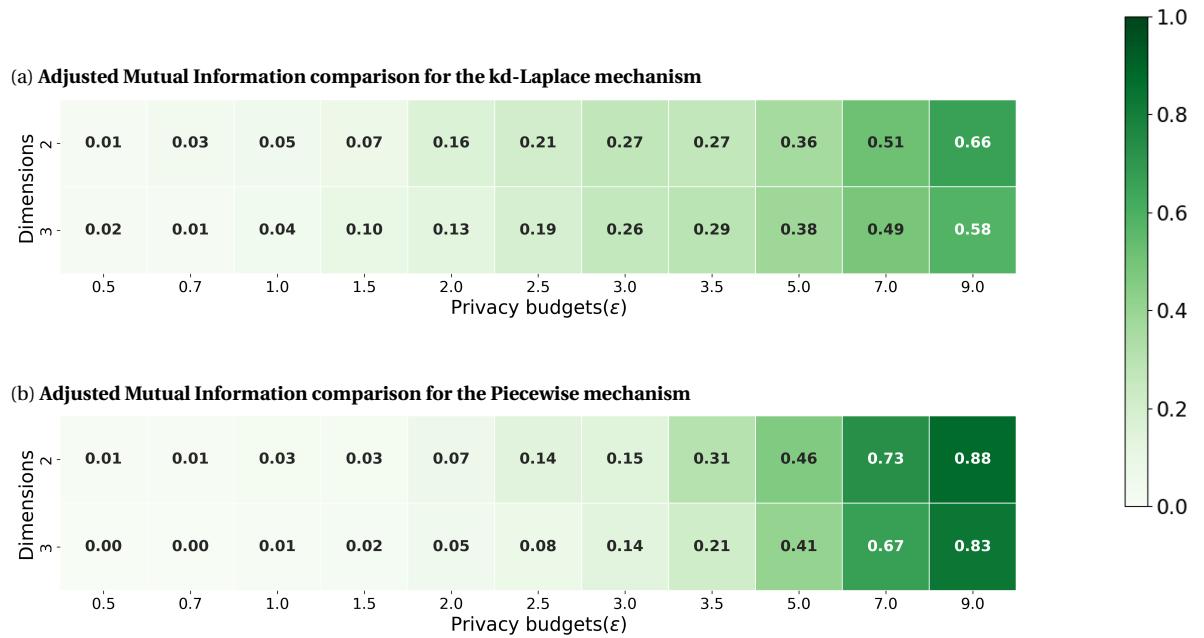


Up to privacy budget 3.5, the scores remain relatively similar for both mechanisms, but after that, they become better for Piecewise.

For kD-Laplace, the highest score is 0.63 AMI for privacy budget 9. For privacy budgets 5 and 7, the score is around 0.5 - 0.55. After that, the scores are no higher than 0.37.

Piecewise performs better, with a maximum of 0.90 AMI for privacy budget 9 for 2 dimensions. For both mechanisms, the dimensions do not significantly impact the score.

6.2.5. SKEWED-DATASET



The kD-Laplace mechanism performs slightly better from privacy budgets 2 to 5. However, Piecewise performs significantly better after that, achieving around 0.73 and 0.85 AMI for privacy budgets 7 and 9, respectively.

In contrast, kD-Laplace scores much lower in this range. Furthermore, it appears that the dimensions do not significantly impact the performance of the mechanisms in this context.

6.3. PRIVACY

6.3.1. SEEDS DATASET

(a) Heatmap showing adversary advantage for the kD-Laplace mechanism, per privacy budget & dimension for seeds-dataset.



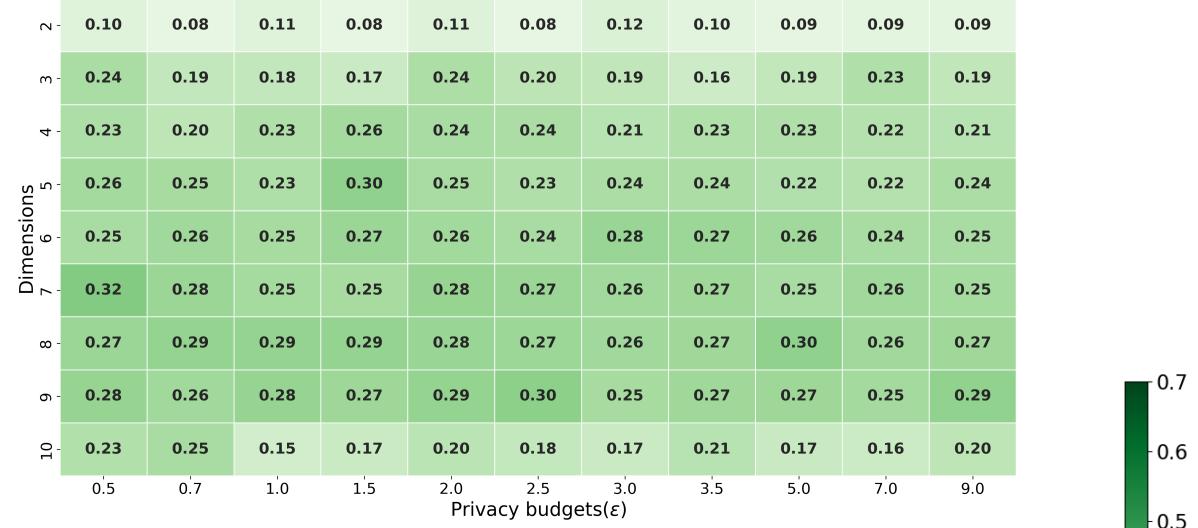
(b) Heatmap showing adversary advantage for the Piecewise mechanism, per privacy budget & dimension for seeds-dataset.



The heatmaps show the adversary advantage of kD-Laplace and Piecewise mechanisms. For kD-Laplace, the advantage slightly decreases with higher privacy budgets. Dimension 4 has a relatively high advantage for budgets 0.5 and 0.7. Piecewise generally has a higher advantage, especially for 2 dimensions (around +/- 0.5). Overall, dimensions don't have a significant impact on the advantage for both mechanisms.

6.3.2. HEART DATASET

(a) Heatmap showing adversary advantage for the kD-Laplace mechanism, per privacy budget & dimension for heart-dataset.

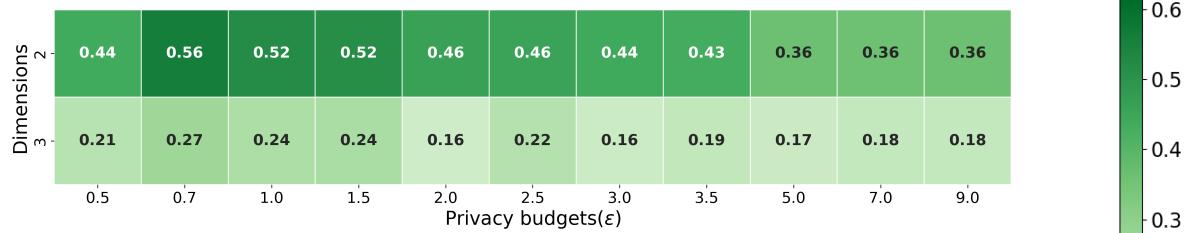


(b) Heatmap showing adversary advantage for the Piecewise mechanism, per privacy budget & dimension for heart-dataset.

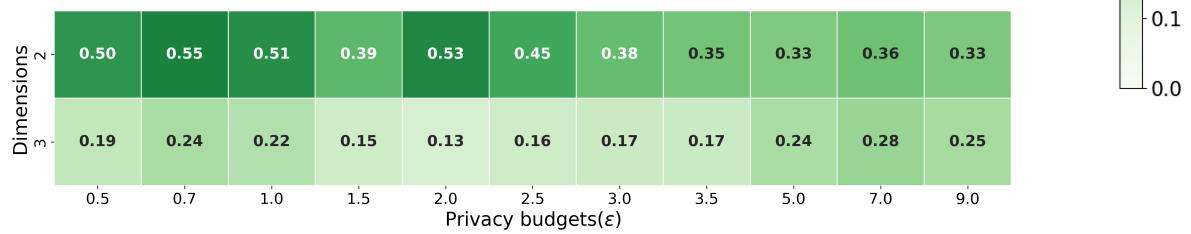


6.3.3. CIRCLE DATASET

(a) Heatmap showing adversary advantage for the kD-Laplace mechanism, per privacy budget & dimension for circle-dataset.

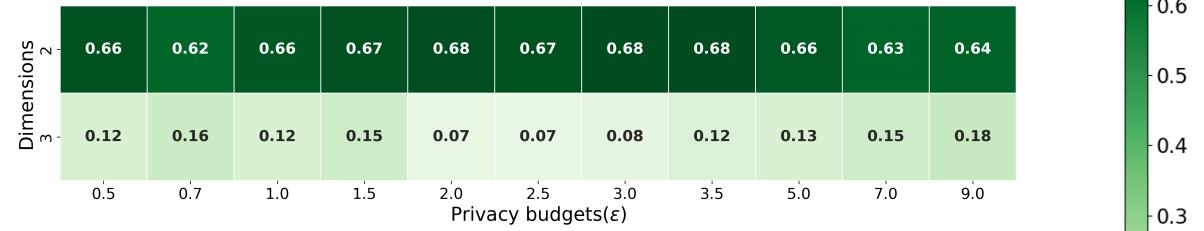


(b) Heatmap showing adversary advantage for the Piecewise mechanism, per privacy budget & dimension for seeds-dataset.

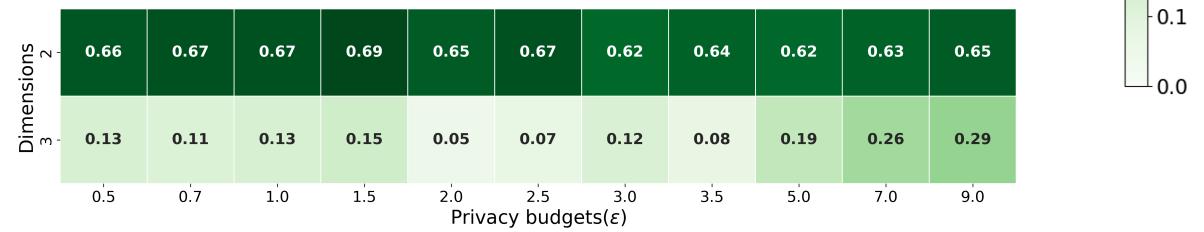


6.3.4. LINE DATASET

(a) Heatmap showing adversary advantage for the kD-Laplace mechanism, per privacy budget & dimension for seeds-dataset.

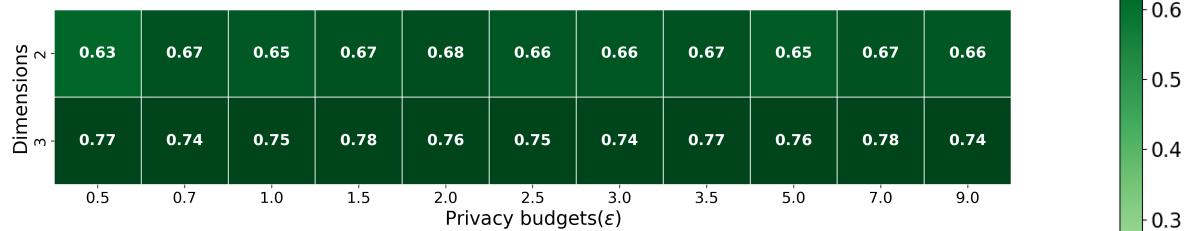


(b) Heatmap showing adversary advantage for the Piecewise mechanism, per privacy budget & dimension for seeds-dataset.

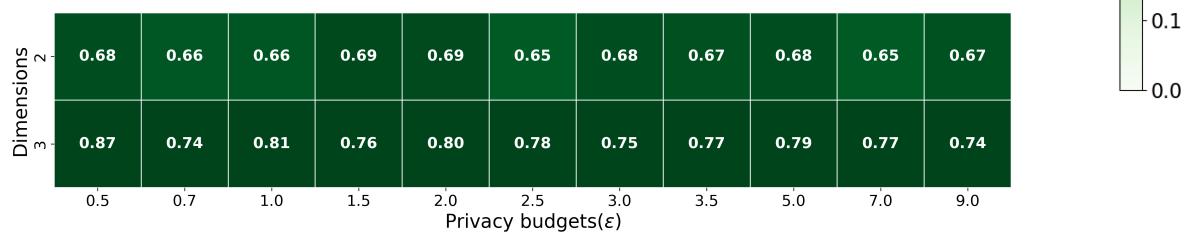


6.3.5. SKEWED DATASET

(a) Heatmap showing adversary advantage for the kD-Laplace mechanism, per privacy budget & dimension for seeds-dataset.



(b) Heatmap showing adversary advantage for the Piecewise mechanism, per privacy budget & dimension for seeds-dataset.



6.3.6. MECHANISM COMPARISON

In this section, we compare the different mechanisms for each dataset. For this purpose, we also include all the different variants of kd-Laplace to see if there is a difference between them. So, instead of comparing the mechanisms based on the number of dimensions, we compare them on the average scores for all dimensions per mechanism. We are most interested in the utility and performance, and to compare them, we only show the AMI and adversary advantage scores.

Also needs privacy distance comparison

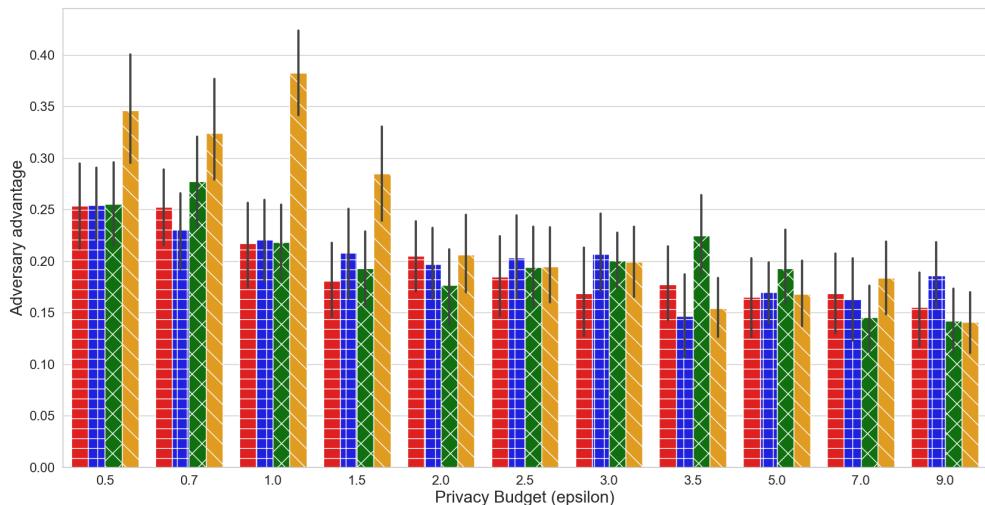
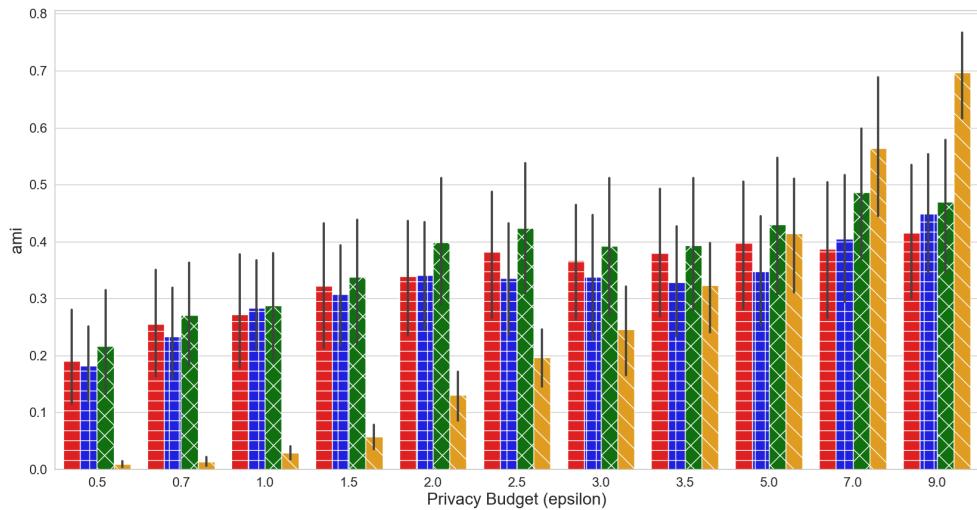


Figure 6.23: Average AMI (top) and Adversary Advantage (bottom) comparison for each mechanism for seeds-dataset (8 dimensions).

Add interpretation

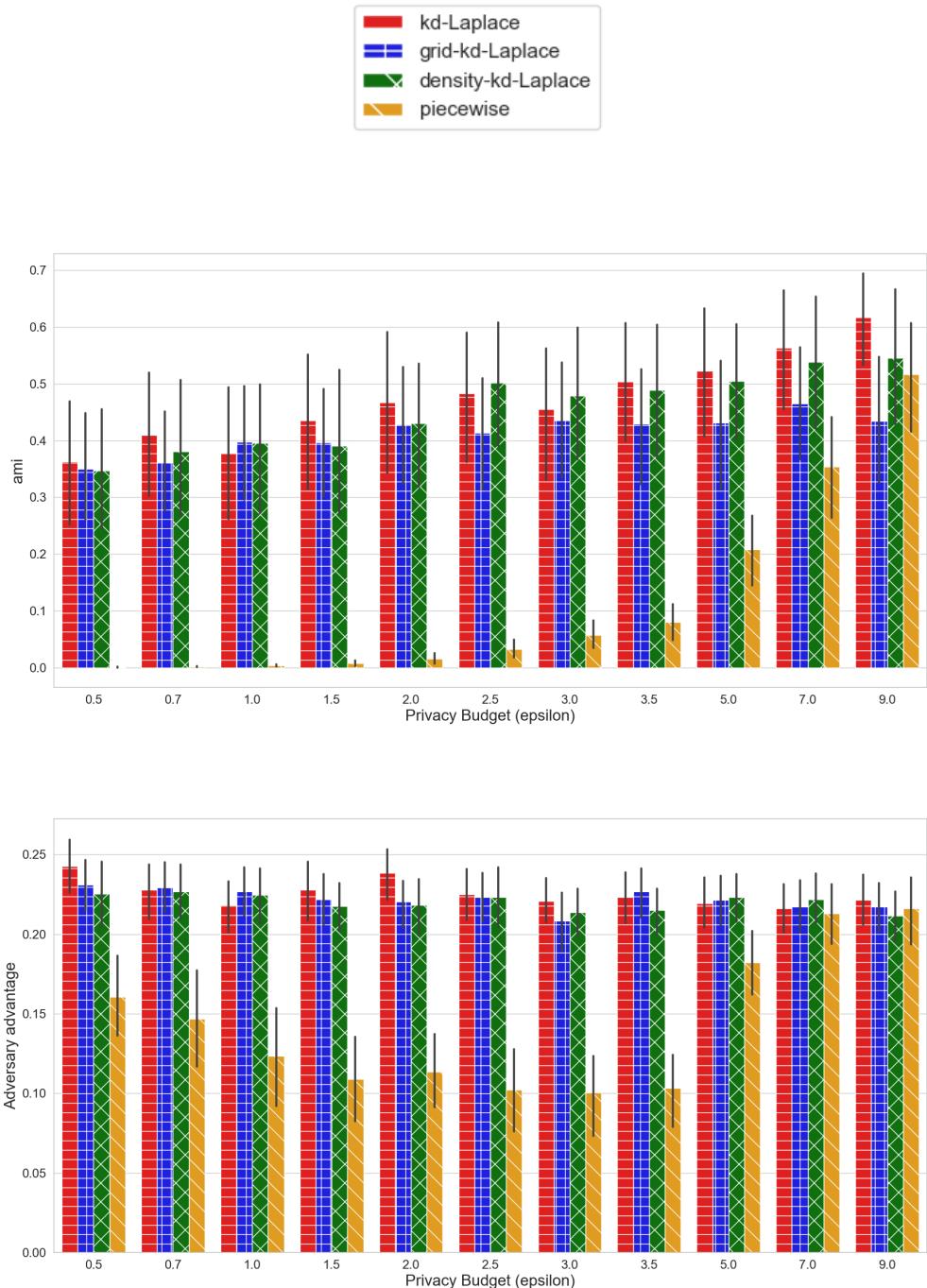


Figure 6.24: Average AMI (top) and Adversary Advantage (bottom) comparison for each mechanism for heart-dataset (10 dimensions).

Add interpretation

6.3.7. SHAPE DATASETS

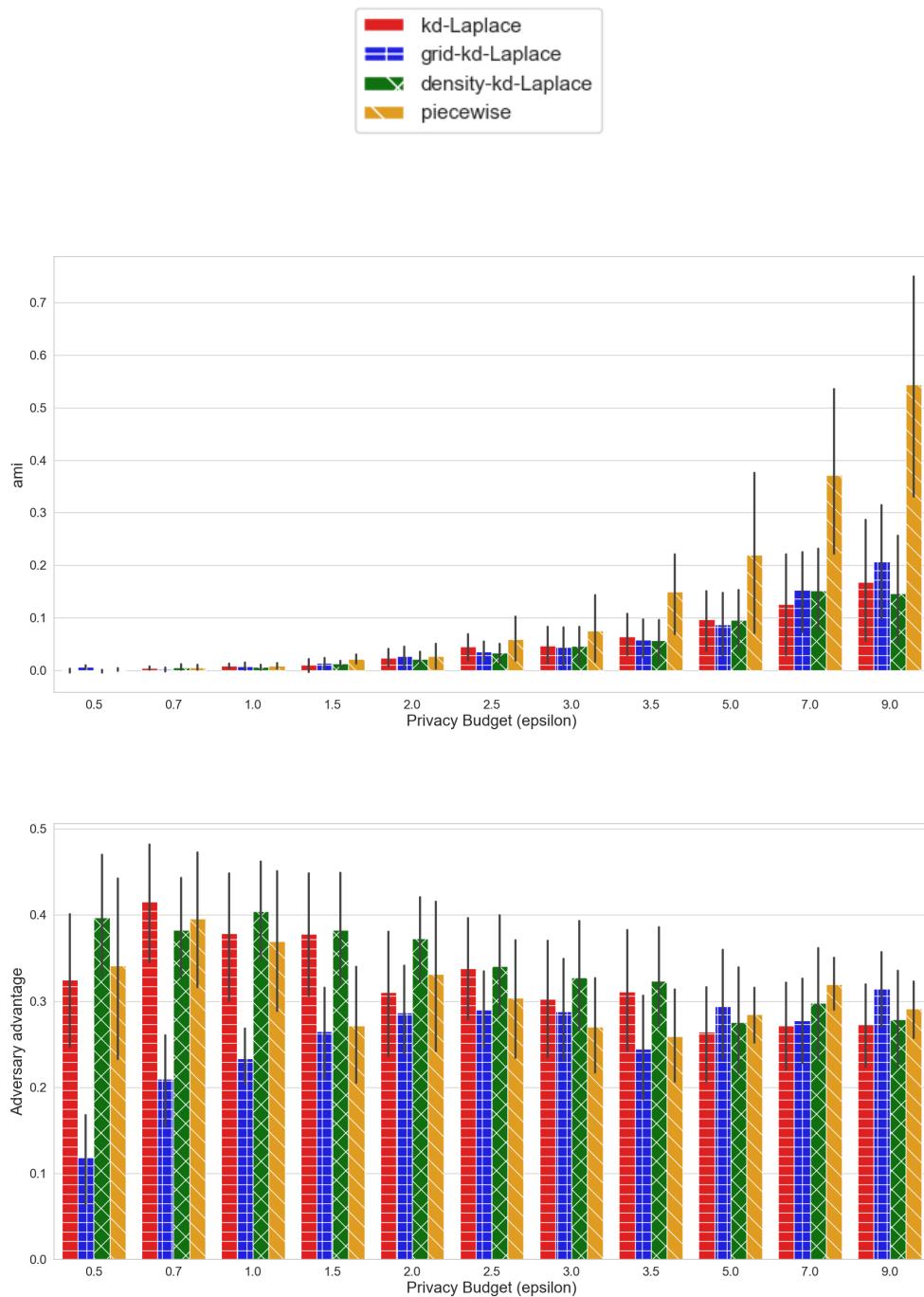


Figure 6.25: Average AMI (top) and Adversary Advantage (bottom) comparison for each mechanism for circle-dataset (3 dimensions).

Add interpretation

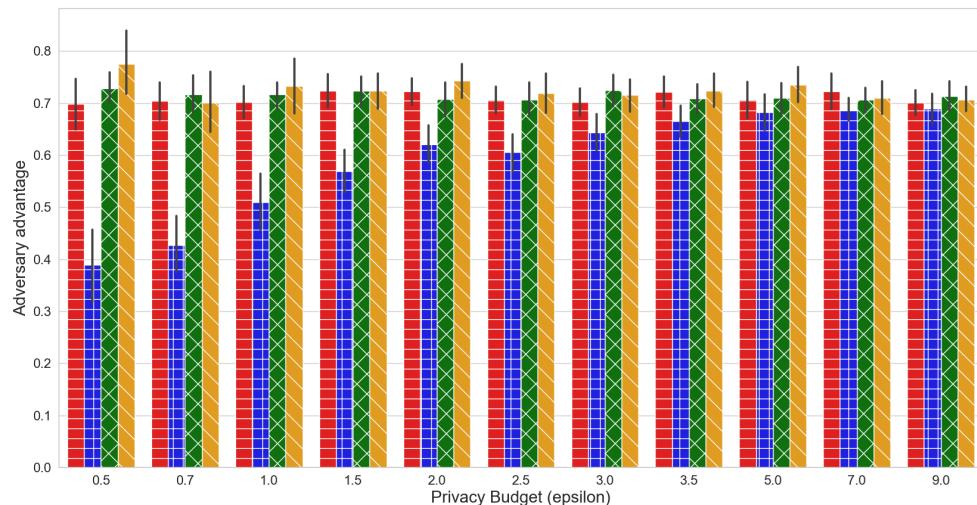
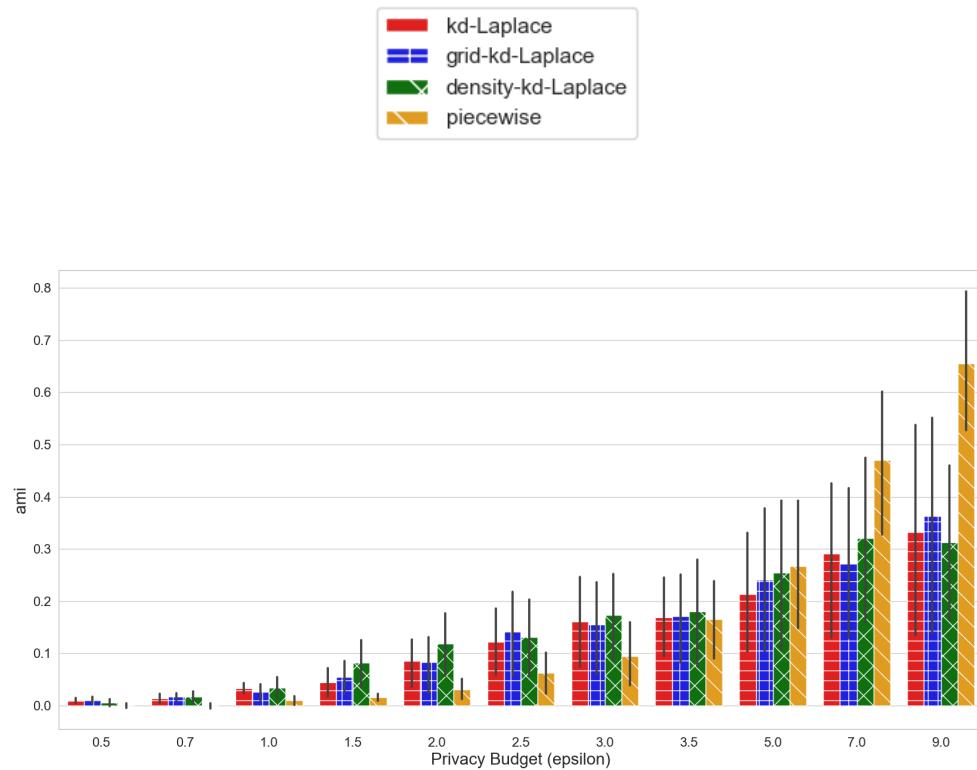


Figure 6.26: Average AMI (top) and Adversary Advantage (bottom) comparison for each mechanism for skewed-dataset (3 dimensions).

Add interpretation

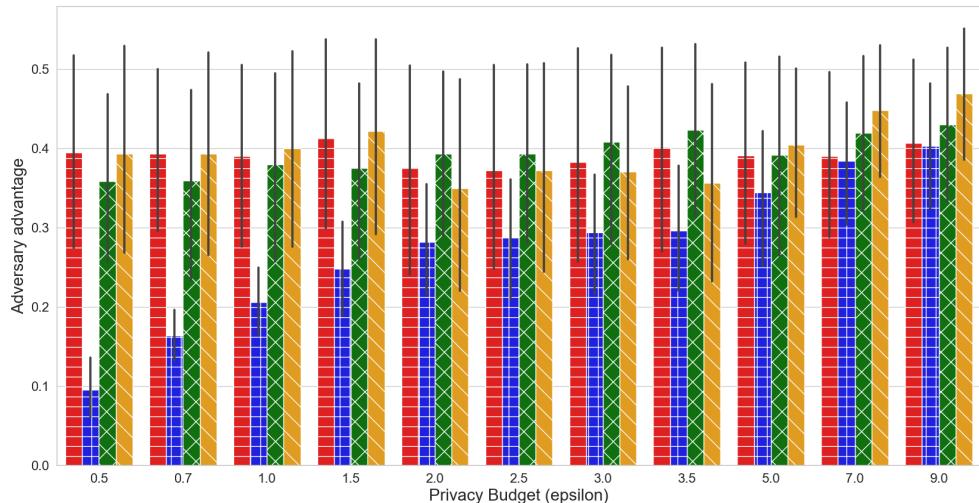
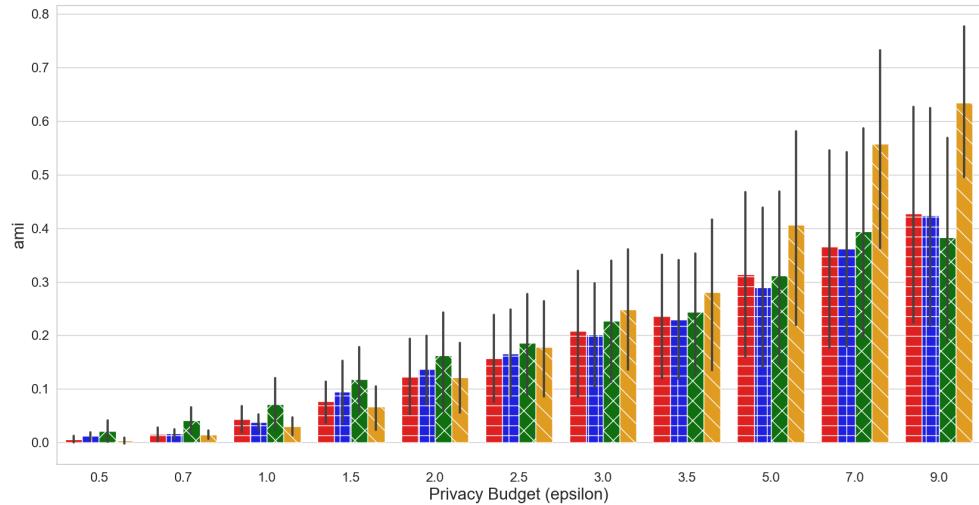


Figure 6.27: Average AMI (top) and Adversary Advantage (bottom) comparison for each mechanism for line-dataset (3 dimensions).

Add interpretation

7

DISCUSSION

1. Why does kd-Laplace perform poorly on shape datasets?
2. Why does OPTICS perform so poorly for clustering with both privacy mechanisms?
3. Why does the Heart dataset perform better than the Seeds dataset?

8

CONCLUSION

This thesis has explored the application of the kD-Laplace algorithm in training privacy-preserving clustering algorithms on distributed k-dimensional data. The research was guided by three research questions, which have been addressed as follows:

RQ1: How can 2D-Laplace be used to protect the privacy of 2-dimensional data employed for training clustering algorithms?

Implementing kD-Laplace on n-dimensional data has shown promising results, with the mechanism balancing data utility and privacy protection. For the Heart and Seeds datasets, the kD-Laplace mechanism scores better in **AMI** and adversary advantage for lower privacy budgets (0.1 - 3/5) between kD-Laplace and Piecewise. The Piecewise mechanism scores better in data utility for higher privacy budgets (5 - 9).

RQ2: How can 3D-Laplace be used to protect the privacy of 3-dimensional data employed for training clustering algorithms?

Results

RQ3: How can nD-Laplace be used to protect the privacy of n-dimensional data employed for training clustering algorithms?

This research question consists of three hypotheses, which are addressed as follows:

- H1: Adding remapping based on density improves utility without sacrificing privacy:

In progress

- H2: The privacy leakage (adversary advantage) and utility increases for more dimensions.

In progress

But especially for the higher privacy budgets.

- H3: The shape of the data negatively impacts the kd-Laplace mechanism in terms of privacy and utility. The kD-Laplace mechanism scores worse for **AMI** for the shape datasets in comparison to the real-world datasets (Heart and Seeds). Piecewise, conversely, scored more consistently and better in **AMI** for the shape datasets. Regarding

the adversary advantage, kD-Laplace scores higher than Piecewise. Upon closer examination, we observe that the True Positive Rate (TPR) is also higher for kD-Laplace. For both the Circle and Line datasets, kD-Laplace significantly outperforms Piecewise. Therefore, the shape of the data negatively impacts the kd-Laplace mechanism in terms of privacy and utility.

Still in progress

Our investigation into the utility and privacy differences among the three kd-Laplace variants and the Piecewise mechanism has revealed that the kd-Laplace mechanism can effectively protect the privacy of n-dimensional data. The kd-Laplace mechanism generally scores better in data utility and privacy than the Piecewise mechanism for lower privacy budgets (0.1 - 3/5). The findings of this research have significant implications for the field of privacy-preserving data analysis. This research approach presents a fresh take on a solution for protecting the privacy of n-dimensional data used in clustering algorithms. Also, this thesis presents a new take on evaluating privacy mechanisms using real-world data and attacks.

However, further research is needed to address the limitations identified in this study. In particular, the impact of the shape of the data on the mechanism's effectiveness, also for dimensions higher than 2-dimensions. In addition, it is also worth exploring the impact of the number of dimensions on the privacy and utility of the mechanism.

In conclusion, this thesis has contributed to understanding how the kd-Laplace algorithm can be applied in training privacy-preserving clustering algorithms on distributed k-dimensional data. The findings provide a foundation for future research in this area, with the potential to advance the field of privacy-preserving data analysis.

BIBLIOGRAPHY

EUR-Lex - 32018R1725 - EN - EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>, a. 1

Global big data industry market size 2011-2027. <https://www.statista.com/statistics/254266/global-big-data-market-forecast/>, b. 1

UCI Machine Learning Repository: Cardiotocography Data Set. <https://archive.ics.uci.edu/ml/datasets/cardiotocography>, c. 54

Mohiuddin Ahmed, Raihan Seraj, and Syed Mohammed Shamsul Islam. The k-means algorithm: A comprehensive survey and performance evaluation. *Electronics*, 9(8):1295, 2020. ISSN 2079-9292. 11

Muhammad Aitsam. Differential Privacy Made Easy, December 2021. 6

Miguel E. Andrés, Nicolás Emilio Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Geo-indistinguishability: Differential privacy for location-based systems. *CoRR*, abs/1212.1984, 2012. 2, 8, 26, 27, 28, 30, 34, 35, 38

Mihai Ankerst, Markus M Breunig, Hans-Peter Kriegel, and Jörg Sander. OPTICS: Ordering Points To Identify the Clustering Structure. 10

Samah Baraheem and Zhongmei Yao. A Survey on Differential Privacy with Machine Learning and Future Outlook, November 2022. 16

Raef Bassily and Adam Smith. Local, Private, Efficient Protocols for Succinct Histograms. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, pages 127–135, June 2015. doi: 10.1145/2746539.2746632. 18

Jon Louis Bentley. Multidimensional binary search trees used for associative searching. *Communications of the ACM*, 18(9):509–517, September 1975. ISSN 0001-0782. doi: 10.1145/361002.361007. 39

Avrim Blum, Cynthia Dwork, Frank McSherry, and Kobbi Nissim. *Practical Privacy: The SulQ Framework*. June 2005. doi: 10.1145/1065167.1065184. 19

Beyza Bozdemir, Sébastien Canard, Orhan Ermis, Helen Möllering, Melek Önen, and Thomas Schneider. Privacy-preserving Density-based Clustering. 21, 22

Hanbo Cai, Jinyan Wang, Xiaohong Liu, and Xianxian Li. DP-AP: Differential Privacy-Preserving Affinity Propagation Clustering. In *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, pages 73–79, Guangzhou, China, December 2020. IEEE. ISBN 978-1-66540-396-2. doi: 10.1109/BigDataSE50710.2020.00018. 20, 22

Tadeusz Caliński and Jerzy Harabasz. A dendrite method for cluster analysis. *Communications in Statistics-theory and Methods*, 3(1):1–27, 1974. ISSN 0090-3272. [13](#), [ix](#)

Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramer. Membership Inference Attacks From First Principles, April 2022. [50](#)

Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Marco Stronati. Constructing elastic distinguishability metrics for location privacy. *Proceedings on Privacy Enhancing Technologies*, 2015(2):156–170, June 2015. ISSN 2299-0984. doi: 10.1515/popets-2015-0023. [8](#), [29](#)

Konstantinos Chatzikokolakis, Ehab Elsalamouny, and Catuscia Palamidessi. Efficient utility improvement for location privacy. *Proceedings on Privacy Enhancing Technologies*, 2017(4):308–328, 2017. [28](#), [38](#), [40](#), [42](#), [43](#)

Jianbo Chen, Michael I. Jordan, and Martin J. Wainwright. HopSkipJumpAttack: A Query-Efficient Decision-Based Attack, April 2020. [48](#)

Christopher A. Choquette-Choo, Florian Tramer, Nicholas Carlini, and Nicolas Papernot. Label-Only Membership Inference Attacks, December 2021. [48](#), [50](#)

Toon Van Craenendonck and Hendrik Blockeel. Using Internal Validity Measures to Compare Clustering Algorithms. [13](#)

David L Davies and Donald W Bouldin. A cluster separation measure. *IEEE transactions on pattern analysis and machine intelligence*, (2):224–227, 1979. ISSN 0162-8828. [13](#)

Irit Dinur and Kobbi Nissim. Revealing information while preserving privacy. In *Proceedings of the Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pages 202–210, San Diego California, June 2003. ACM. ISBN 978-1-58113-670-8. doi: 10.1145/773153.773173. [49](#)

Freedom of Information Act (FOIA) Division. The Privacy Act. <https://www.hhs.gov/foia/privacy/index.html>, April 2007. [1](#)

Salim Dridi. *Unsupervised Learning - A Systematic Literature Review*. December 2021. doi: 10.13140/RG.2.2.16963.12323. [1](#)

John Duchi, Martin Wainwright, and Michael Jordan. Minimax Optimal Procedures for Locally Private Estimation, November 2017. [18](#), [23](#), [24](#)

John C. Duchi, Michael I. Jordan, and Martin J. Wainwright. Privacy Aware Learning, October 2013. [18](#)

Cynthia Dwork. Differential privacy. In *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II* 33, pages 1–12. Springer, 2006. ISBN 3-540-35907-9. [1](#), [6](#), [9](#), [18](#)

Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. Exposed! A Survey of Attacks on Private Data. *Annual Review of Statistics and Its Application*, 4(1):61–84, March 2017. ISSN 2326-8298, 2326-831X. doi: 10.1146/annurev-statistics-060116-054123. [49](#)

Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1054–1067, Scottsdale Arizona USA, November 2014. ACM. ISBN 978-1-4503-2957-6. doi: 10.1145/2660267.2660348. 9

Martin Ester, Hans-Peter Kriegel, and Xiaowei Xu. A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. 10

Adil Fahad, Najlaa Alshatri, Zahir Tari, Abdullah Alamri, Ibrahim Khalil, Albert Y. Zomaya, Sebti Foufou, and Abdelaziz Bouras. A Survey of Clustering Algorithms for Big Data: Taxonomy and Empirical Analysis. *IEEE Transactions on Emerging Topics in Computing*, 2(3):267–279, September 2014. ISSN 2168-6750. doi: 10.1109/TETC.2014.2330519. 10

Natasha Fernandes, Mark Dras, and Annabelle McIver. Generalised Differential Privacy for Text Document Processing, February 2019. 2, 35

Pasi Fränti, Mohammad Rezaei, and Qinpei Zhao. Centroid index: Cluster level similarity measure. *Pattern Recognition*, 47(9):3034–3045, September 2014. ISSN 00313203. doi: 10.1016/j.patcog.2014.03.017. 13

Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1322–1333, Denver Colorado USA, October 2015. ACM. ISBN 978-1-4503-3832-5. doi: 10.1145/2810103.2813677. 49

Brendan J. Frey and Delbert Dueck. Clustering by Passing Messages Between Data Points. *Science*, 315(5814):972–976, February 2007. ISSN 0036-8075, 1095-9203. doi: 10.1126/science.1136800. 10

Arik Friedman and Assaf Schuster. Data mining with differential privacy. In *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 493–502, Washington DC USA, July 2010. ACM. ISBN 978-1-4503-0055-1. doi: 10.1145/1835804.1835868. 6

Quan Geng and Pramod Viswanath. The Optimal Mechanism in Differential Privacy, October 2013. 23

Quan Geng, Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The staircase mechanism in differential privacy. *IEEE Journal of Selected Topics in Signal Processing*, 9(7):1176–1184, October 2015. ISSN 1932-4553, 1941-0484. doi: 10.1109/JSTSP.2015.2425831. 18, 23

Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. Differential Privacy Techniques for Cyber Physical Systems: A Survey, September 2019. 16

Marwan Hassani and Thomas Seidl. Using internal evaluation measures to validate the quality of diverse stream clustering algorithms. *Vietnam Journal of Computer Science*, 4(3):171–183, August 2017. ISSN 2196-8896. doi: 10.1007/s40595-016-0086-9. 13

Hongsheng Hu, Zoran Salcic, Lichao Sun, Gillian Dobbie, Philip S. Yu, and Xuyun Zhang. Membership Inference Attacks on Machine Learning: A Survey, February 2022. [47](#), [50](#)

D. Huang, X. Yao, S. An, and S. Ren. Private distributed K-means clustering on interval data. In *2021 IEEE International Performance, Computing, and Communications Conference (IPCCC)*, pages 1–9, Los Alamitos, CA, USA, October 2021. IEEE Computer Society. doi: [10.1109/IPCCC51483.2021.9679364](#). [2](#), [14](#), [20](#), [22](#), [24](#), [55](#)

Lawrence Hubert and Phipps Arabie. Comparing partitions. *Journal of classification*, 2: 193–218, 1985. ISSN 0176-4268. [13](#), [ix](#)

Bargav Jayaraman and David Evans. Evaluating Differentially Private Machine Learning in Practice. [47](#), [49](#)

Bargav Jayaraman and David Evans. Are Attribute Inference Attacks Just Imputation? In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 1569–1582, Los Angeles CA USA, November 2022. ACM. ISBN 978-1-4503-9450-5. doi: [10.1145/3548606.3560663](#). [49](#)

Marija Jegorova, Chaitanya Kaul, Charlie Mayor, Alison Q. O’Neil, Alexander Weir, Roderick Murray-Smith, and Sotirios A. Tsaftaris. Survey: Leakage and Privacy at Inference Time, September 2022. [49](#)

Zhanglong Ji, Zachary C. Lipton, and Charles Elkan. Differential Privacy and Machine Learning: A Survey and Review, December 2014. [16](#)

Matthew Joseph, Jieming Mao, Seth Neel, and Aaron Roth. The Role of Interactivity in Local Differential Privacy. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 94–105, Baltimore, MD, USA, November 2019. IEEE. ISBN 978-1-72814-952-3. doi: [10.1109/FOCS.2019.00015](#). [7](#)

Haim Kaplan and Uri Stemmer. Differentially Private k-Means with Constant Multiplicative Error, July 2018. [19](#)

Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. What Can We Learn Privately?, February 2010. [1](#)

Hannah Keller, Helen Möllering, Thomas Schneider, and Hossein Yalame. Balancing Quality and Efficiency in Private Clustering with Affinity Propagation:. In *Proceedings of the 18th International Conference on Security and Cryptography*, pages 173–184, Online Streaming, — Select a Country —, 2021. SCITEPRESS - Science and Technology Publications. ISBN 978-989-758-524-1. doi: [10.5220/0010547801730184](#). [10](#)

Trupti M Kodinariya and Prashant R Makwana. Review on determining number of Cluster in K-Means Clustering. *International Journal*, 1(6):90–95, 2013. [11](#), [12](#)

Jussi Lehtonen. The Lambert W function in ecological and evolutionary models. *Methods in Ecology and Evolution*, 7(9):1110–1118, 2016. ISSN 2041-210X. doi: [10.1111/2041-210X.12568](#). [27](#)

Zheng Li and Yang Zhang. Membership Leakage in Label-Only Exposures, September 2021.

48

Bo Liu, Ming Ding, Sina Shaham, Wenny Rahayu, Farhad Farokhi, and Zihuai Lin. When Machine Learning Meets Privacy: A Survey and Outlook. *ACM Computing Surveys*, 54(2): 1–36, March 2022. ISSN 0360-0300, 1557-7341. doi: 10.1145/3436755. 1

Jinfei Liu, Joshua Huang, Jun Luo, and Li Xiong. Privacy preserving distributed DBSCAN clustering. *Transactions on Data Privacy*, 6, March 2012. doi: 10.1145/2320765.2320819. 10

Yanchi Liu, Zhongmou Li, Hui Xiong, Xuedong Gao, and Junjie Wu. Understanding of internal clustering validation measures. In *2010 IEEE International Conference on Data Mining*, pages 911–916. IEEE, 2010. ISBN 1-4244-9131-2. 14

S. Lloyd. Least squares quantization in PCM. *IEEE Transactions on Information Theory*, 28 (2):129–137, 1982. doi: 10.1109/TIT.1982.1056489. 10

George Marsaglia. Choosing a point from the surface of a sphere. *The Annals of Mathematical Statistics*, 43(2):645–646, 1972. ISSN 0003-4851. 35

Xianrui Meng, Dimitrios Papadopoulos, Alina Oprea, and Nikos Triandopoulos. Private Hierarchical Clustering and Efficient Approximation. In *Proceedings of the 2021 on Cloud Computing Security Workshop*, pages 3–20, November 2021. doi: 10.1145/3474123. 3486760. 10

Minghui Min, Liang Xiao, Jiahao Ding, Hongliang Zhang, Shiyan Li, Miao Pan, and Zhu Han. 3D Geo-Indistinguishability for Indoor Location-Based Services. *IEEE Transactions on Wireless Communications*, 21(7):4682–4694, 2022. doi: 10.1109/TWC.2021.3132464. 2, 28, 31, 32, 35

Thông T. Nguyêñ, Xiaokui Xiao, Yin Yang, Siu Cheung Hui, Hyejin Shin, and Junbum Shin. Collecting and Analyzing Data from Smart Device Users with Local Differential Privacy, June 2016. 18, 20, 23, 24

Maria-Irina Nicolae, Mathieu Sinn, Minh Ngoc Tran, Beat Buesser, Ambrish Rawat, Martin Wistuba, Valentina Zantedeschi, Nathalie Baracaldo, Bryant Chen, Heiko Ludwig, Ian M. Molloy, and Ben Edwards. Adversarial Robustness Toolbox v1.0.0, November 2019. 49, 59

Kobbi Nissim and Uri Stemmer. Clustering Algorithms for the Centralized and Local Models. In *Proceedings of Algorithmic Learning Theory*, pages 619–653. PMLR, April 2018. 19, 22

Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 75–84, San Diego California USA, June 2007. ACM. ISBN 978-1-59593-631-8. doi: 10.1145/1250790.1250803. 9, 19, 22

Yuefeng Peng, Bo Zhao, and Hui Liu. Unsupervised Membership Inference Attacks Against Machine Learning Models. 48

William M Rand. Objective criteria for the evaluation of clustering methods. *Journal of the American Statistical association*, 66(336):846–850, 1971. ISSN 0162-1459. [13](#)

Maria Rigaki and Sebastian Garcia. A Survey of Privacy Attacks in Machine Learning, April 2021. [47](#), [48](#), [49](#), [50](#), [59](#)

Peter J Rousseeuw. Silhouettes: A graphical aid to the interpretation and validation of cluster analysis. *Journal of computational and applied mathematics*, 20:53–65, 1987. ISSN 0377-0427. [13](#), [14](#)

Maurice Roux. A comparative study of divisive hierarchical clustering algorithms, September 2015. [11](#), [12](#)

Jörg Sander, Martin Ester, Hans-Peter Kriegel, and Xiaowei Xu. Density-Based Clustering in Spatial Databases: The Algorithm GDBSCAN and Its Applications. *Data Mining and Knowledge Discovery*, 2(2):169–194, June 1998. ISSN 1573-756X. doi: 10.1023/A:1009745219419. [12](#)

Danny Matthew SAPUTRA, Daniel SAPUTRA, and Liniyanti D OSWARI. Effect of distance metrics in determining k-value in k-means clustering using elbow and silhouette method. In *Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)*, pages 341–346. Atlantis Press, 2020. ISBN 94-6252-963-9. [11](#)

Erich Schubert, Jörg Sander, Martin Ester, Hans Peter Kriegel, and Xiaowei Xu. DBSCAN Revisited, Revisited: Why and How You Should (Still) Use DBSCAN. *ACM Transactions on Database Systems*, 42(3):1–21, September 2017. ISSN 0362-5915, 1557-4644. doi: 10.1145/3068335. [10](#), [12](#)

Sreedhar Kumar Seetharaman, Madheswaran Muthusamy, Vinutha A, Manjunatha H, and Charan K V. A Brief Survey of Unsupervised Agglomerative Hierarchical Clustering Schemes. *International Journal of Engineering and Technology*, 8:29–37, January 2019. doi: 10.14419/ijet.v8i1.13971. [12](#)

Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership Inference Attacks against Machine Learning Models, March 2017. [48](#)

R. O. Sinnott, H. Duan, and Y. Sun. Chapter 15 - A Case Study in Big Data Analytics: Exploring Twitter Sentiment Analysis and the Weather. In Rajkumar Buyya, Rodrigo N. Calheiros, and Amir Vahid Dastjerdi, editors, *Big Data*, pages 357–388. Morgan Kaufmann, January 2016. ISBN 978-0-12-805394-2. doi: 10.1016/B978-0-12-805394-2.00015-5.

Jordi Soria-Comas and Josep Domingo-Ferrer. Optimal data-independent noise for differential privacy. *Information Sciences*, 250:200–214, November 2013. ISSN 0020-0255. doi: 10.1016/j.ins.2013.07.004. [18](#)

Uri Stemmer. Locally private k-means clustering. *The Journal of Machine Learning Research*, 22(1):7964–7993, 2021. ISSN 1532-4435. [19](#), [22](#)

Alexander Strehl and Joydeep Ghosh. Cluster ensembles—a knowledge reuse framework for combining multiple partitions. *Journal of machine learning research*, 3(Dec):583–617, 2002. [13](#)

Dong Su, Jianneng Cao, Ninghui Li, Elisa Bertino, and Hongxia Jin. Differentially Private k -Means Clustering, April 2015. [19](#), [20](#), [22](#)

Lin Sun, Jun Zhao, and Xiaojun Ye. Distributed Clustering in the Anonymized Space with Local Differential Privacy, June 2019. [2](#), [16](#), [22](#), [24](#)

Lin Sun, Guolou Ping, and Xiaojun Ye. PrivBV: Distance-aware encoding for distributed data with local differential privacy. *Tsinghua Science and Technology*, 27(2):412–421, April 2022. ISSN 1007-0214. doi: 10.26599/TST.2021.9010027. [13](#), [14](#), [22](#)

Latanya Sweeney. K-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, October 2002. ISSN 0218-4885, 1793-6411. doi: 10.1142/S0218488502001648. [1](#)

Robert Tibshirani, Guenther Walther, and Trevor Hastie. Estimating the number of clusters in a data set via the gap statistic. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 63(2):411–423, 2001. ISSN 1369-7412. [11](#)

Nguyen Xuan Vinh, Julien Epps, and James Bailey. Information Theoretic Measures for Clusterings Comparison: Variants, Properties, Normalization and Correction for Chance. [12](#), [13](#), [14](#)

Silke Wagner and Dorothea Wagner. Comparing Clusterings - An Overview. [13](#)

Ning Wang, Xiaokui Xiao, Yin Yang, Jun Zhao, Siu Cheung Hui, Hyejin Shin, Junbum Shin, and Ge Yu. Collecting and Analyzing Multidimensional Data with Local Differential Privacy, June 2019. [18](#), [23](#), [24](#)

Teng Wang, Xuefeng Zhang, Jingyu Feng, and Xinyu Yang. A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis. *Sensors*, 20(24), 2020. ISSN 1424-8220. doi: 10.3390/s20247030. [8](#), [44](#)

Tianhao Wang, Jeremiah Blocki, Ninghui Li, and Somesh Jha. Locally Differentially Private Protocols for Frequency Estimation. [18](#), [20](#)

Stanley L Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965. ISSN 0162-1459. [9](#)

Matthijs J. Warrens and Hanneke van der Hoef. Understanding the Adjusted Rand Index and Other Partition Comparison Indices Based on Counting Object Pairs. *Journal of Classification*, 39(3):487–509, November 2022. ISSN 1432-1343. doi: 10.1007/s00357-022-09413-z. [12](#), [13](#)

Washington. K-D Trees, February 2. [39](#), [40](#)

Chang Xia, Jingyu Hua, Wei Tong, and Sheng Zhong. Distributed K-Means clustering guaranteeing local differential privacy. *Computers & Security*, 90:101699, 2020. ISSN 0167-4048. [2](#), [13](#), [14](#), [20](#), [22](#), [24](#)

Xingxing Xiong, Shubo Liu, Dan Li, Zhaojun Cai, and Xiaoguang Niu. A Comprehensive Survey on Local Differential Privacy. *Security and Communication Networks*, 2020:8829523, October 2020a. ISSN 1939-0114. doi: 10.1155/2020/8829523. [7](#), [9](#)

Xingxing Xiong, Shubo Liu, Dan Li, Zhaojun Cai, and Xiaoguang Niu. A Comprehensive Survey on Local Differential Privacy. *Security and Communication Networks*, 2020:8829523, October 2020b. ISSN 1939-0114. doi: 10.1155/2020/8829523. [8](#), [44](#)

Dongkuan Xu and Yingjie Tian. A Comprehensive Survey of Clustering Algorithms. *Annals of Data Science*, 2(2):165–193, June 2015. ISSN 2198-5812. doi: 10.1007/s40745-015-0040-1. [10](#)

Mengmeng Yang, Lingjuan Lyu, Jun Zhao, Tianqing Zhu, and Kwok-Yan Lam. Local Differential Privacy and Its Applications: A Comprehensive Survey, August 2020. [1](#)

Samuel Yeom, Irene Giacomelli, Matt Fredrikson, and Somesh Jha. Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting. In *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, pages 268–282, Oxford, July 2018. IEEE. ISBN 978-1-5386-6680-7. doi: 10.1109/CSF.2018.00027. [48](#), [49](#), [50](#), [59](#)

Chunhui Yuan and Haitao Yang. Research on K-value selection method of K-means clustering algorithm. *J*, 2(2):226–235, 2019. ISSN 2571-8800. [11](#)

Liujie Yuan, Shaobo Zhang, Gengming Zhu, and Karim Alinani. Privacy-preserving mechanism for mixed data clustering with local differential privacy. *Concurrency and Computation: Practice and Experience*, July 2021. ISSN 1532-0626, 1532-0634. doi: 10.1002/cpe. 6503. [20](#), [22](#), [24](#)

Tian Zhang, Raghu Ramakrishnan, and Miron Livny. BIRCH: An efficient data clustering method for very large databases. *ACM SIGMOD Record*, 25(2):103–114, June 1996. ISSN 0163-5808. doi: 10.1145/235968.233324. [11](#)

Benjamin Zi Hao Zhao, Mohamed Ali Kaafar, and Nicolas Kourtellis. Not one but many Tradeoffs: Privacy Vs. Utility in Differentially Private Machine Learning. In *Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop*, pages 15–26, November 2020. doi: 10.1145/3411495.3421352. [59](#)

Benjamin Zi Hao Zhao, Aviral Agrawal, Catisha Coburn, Hassan Jameel Asghar, Raghav Bhaskar, Mohamed Ali Kaafar, Darren Webb, and Peter Dickinson. On the (In)Feasibility of Attribute Inference Attacks on Machine Learning Models, March 2021. [49](#)

GLOSSARY

Adjusted Mutual Information Comparable with **Adjusted Rand Index** this algorithm is modified to account to chance. This means it accounts for a higher MI for a higher amount of clusters between two cluster algorithms. Therefore, the calculations are strongly influenced by that of **Adjusted Rand Index** [?]. . 13

Adjusted Rand Index The Rand Index is improved and adjusted for chance [Hubert and Arabie, 1985]. This algorithm takes also into consideration the number of clusters and can be used to also compare different cluster algorithms [?]. ix, 13

Calinski-Harabasz Index This is a way to measure the similarity of clusters [Caliński and Harabasz, 1974]. It tells how well the clusters are separated from each other and how well the points are grouped.. 13

Mutual Information This metric can be used to explain the amount of information about a random variable if compared to another random variable. Therefore, it can also be used to compare two cluster similarities.. ix, 13

Normalized Mutual Information The normalized version is a scaled version of **Mutual Information** to always be a value between 0 (no correlation) and 1 (perfect correlation). This version of **Mutual Information** is not adjusted and therefore highly influenced by cluster amount [?]. So it suffers the same issue as with **Mutual Information**.. 13

ACRONYMS

AEE Average Estimated Error. *Glossary: Average Estimation Error*

AMI Adjusted Mutual Information. 13–15, 20, 60, 62, 63, 83, 90, *Glossary: Adjusted Mutual Information*

AP Affinity Propagation. 10, 14, 20, 56–58, 64, 65, 68

ARI Adjusted Rank Index. 13–15, 20, *Glossary: Adjusted Rand Index*

BIRCH Balanced Iterative Reducing and Clustering using Hierarchies. 11

CDF Cumulative Distribution Function. 27

CHI Calinski-Harabasz Index. 13, 14, *Glossary: Calinski-Harabasz Index*

DBSCAN Density-based spatial clustering of applications with noise. 10, 11, 13, 14, 19, 20

DP Differential Privacy. 2, 5, 6, 9, 14, 17

FPR False Positive Rate. 51

GI Geo-indistinguishability. 2, 8, 11, 26, 29, 52

LDP Local Differential Privacy. 1, 2, 7, 9, 17, 19, 24, 29, 52, 53

MI Mutual Information. [13](#), [15](#), *Glossary: Mutual Information*

MIA Membership Inference Attack. [48–51](#), [60](#)

NMI Normalized Mutual Information. [13](#), [14](#), *Glossary: Normalized Mutual Information*

OPTICS Ordering Points to Identify Clustering Structure. [10–14](#), [58](#)

PDF Probability Density Function. [17](#), [24](#), [27](#)

PM Piecewise Mechanism. [18](#)

SC Silhouette Coefficient. [13](#), [14](#), [57](#), [62](#)

SVM Support Vector Machine. [18](#)

TPR True Positive Rate. [51](#), [60](#), [90](#), [91](#)

HYPERPARAMETERS

.1. K-MEANS

For selecting the appropriate amount of clusters, we used an "elbow" plot in combination with the silhouette score.

1. Seeds dataset: 4 clusters (see figure: 1)
2. Heart dataset: TODO
3. Circle dataset: 5 clusters (see figure: 2)
4. Line dataset: 4 clusters (see figure: 3)
5. Skewed dataset: 4 clusters (see figure: 4)

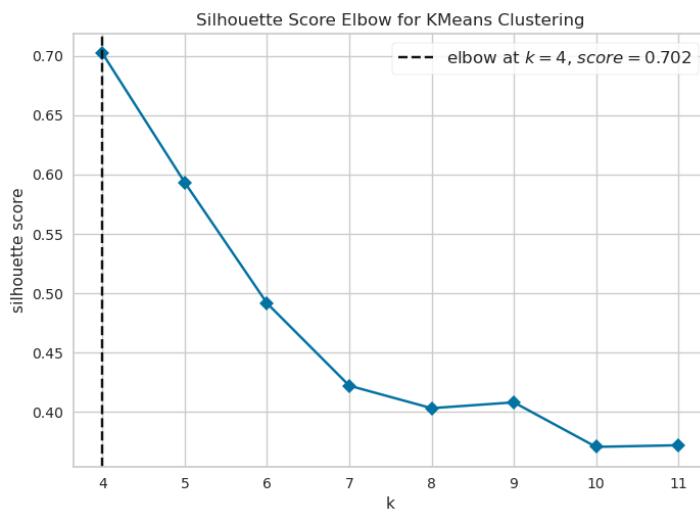


Figure 1: Selecting the k for K-Means for seeds dataset using the "elbow plot" using section 2.2.2

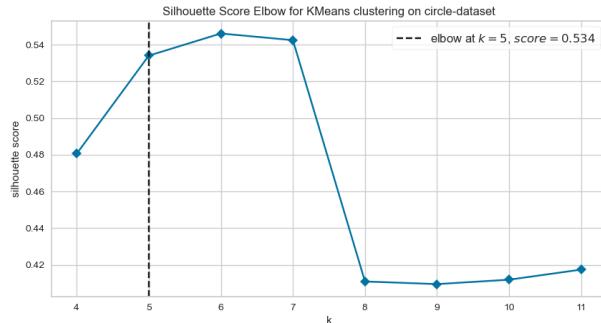


Figure 2: Selecting the k for K-Means for the circle dataset using the "elbow plot" using section 2.2.2

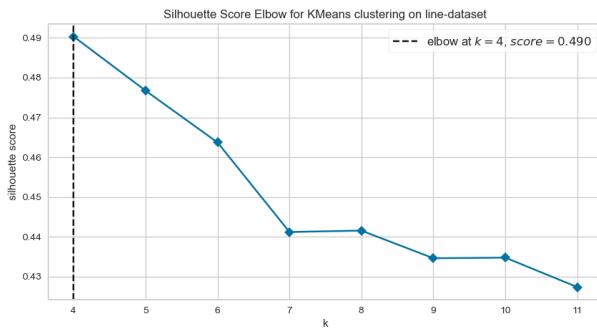


Figure 3: Selecting the k for K-Means for the line dataset using the "elbow plot" using section 2.2.2

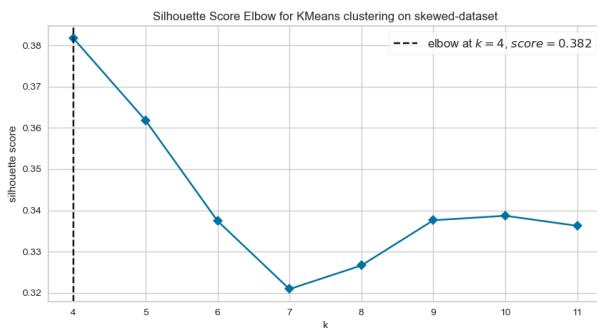


Figure 4: Selecting the k for K-Means for the skewed dataset using the "elbow plot" using section 2.2.2

.2. AGGLOMERATIVE CLUSTERING

.2.1. SEEDS DATASET

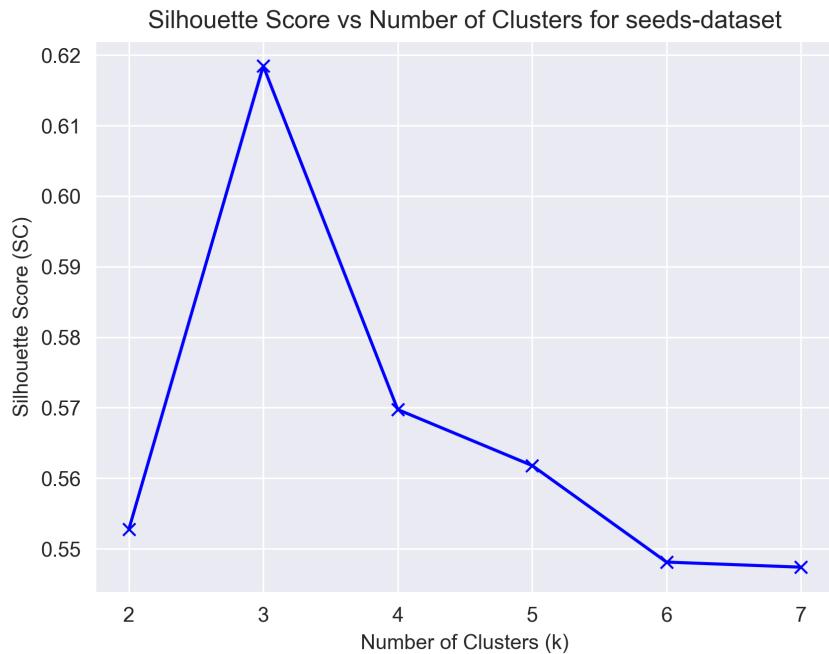


Figure 5: Selecting the k for Agglomerative clustering for seeds dataset (2 dimensions) using the "elbow plot."

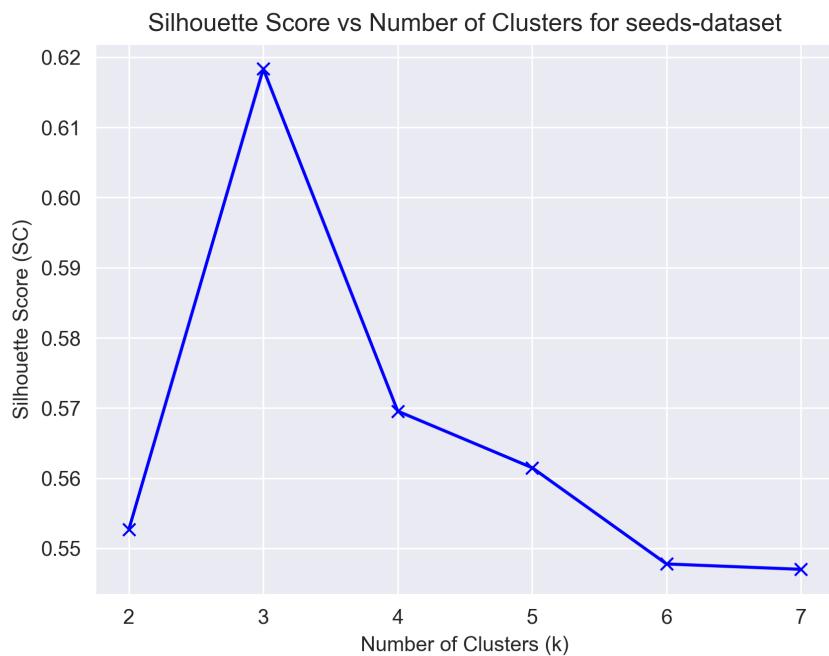


Figure 6: Selecting the k for Agglomerative clustering for seeds dataset (3 dimensions) using the "elbow plot."

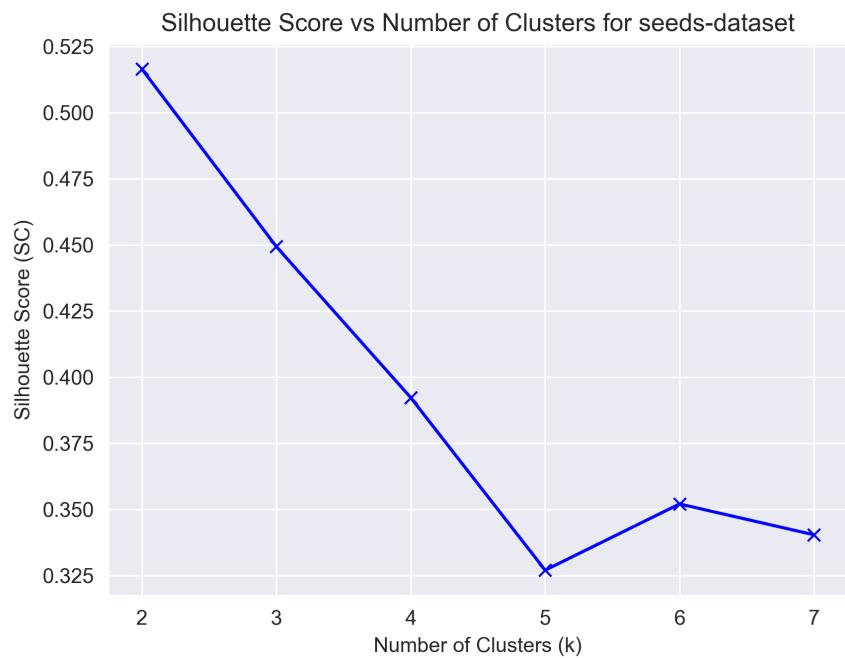


Figure 7: Selecting the k for Agglomerative clustering for seeds dataset (7 dimensions) using the "elbow plot."

.2.2. HEART DATASET

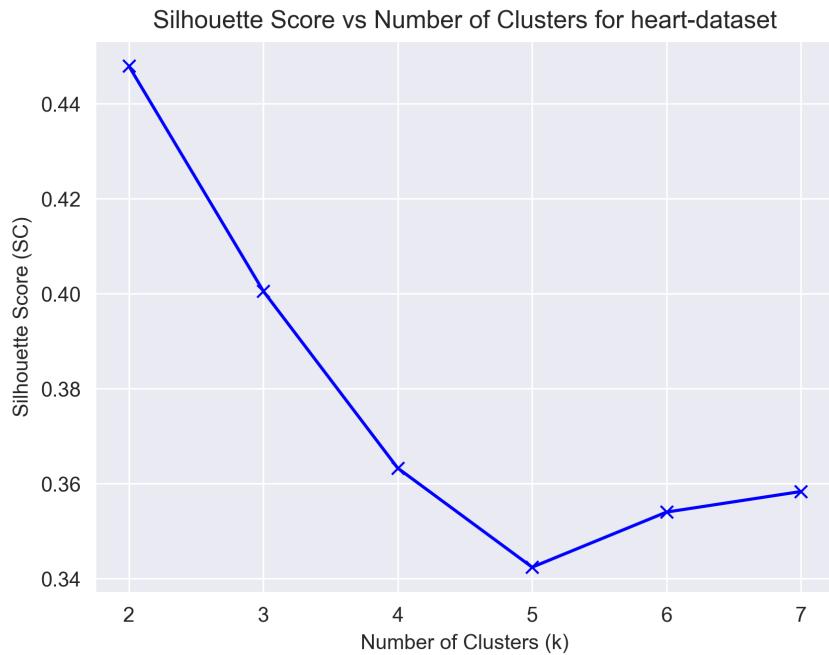


Figure 8: Selecting the k for Agglomerative clustering for Heart dataset (2 dimensions) using the "elbow plot."

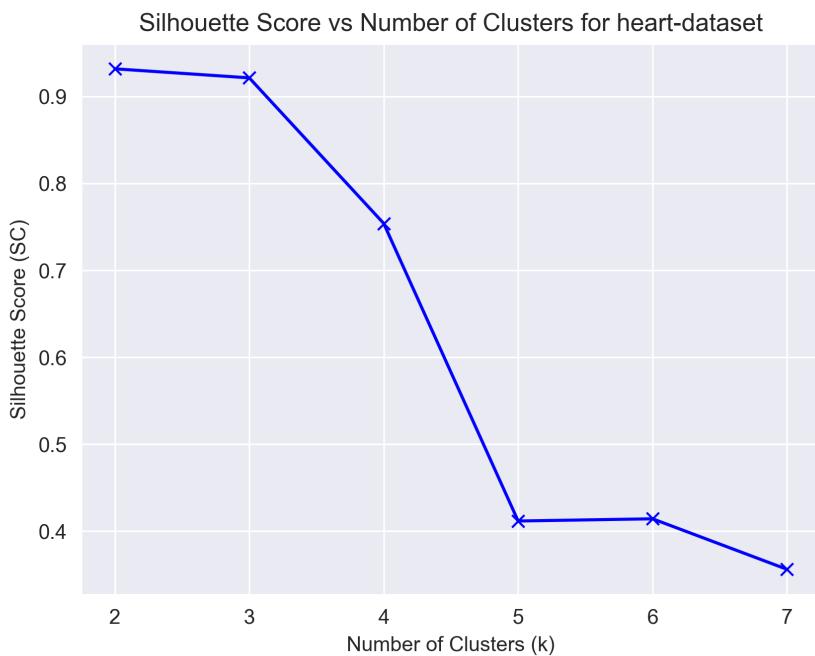


Figure 9: Selecting the k for Agglomerative clustering for Heart dataset (3 dimensions) using the "elbow plot."

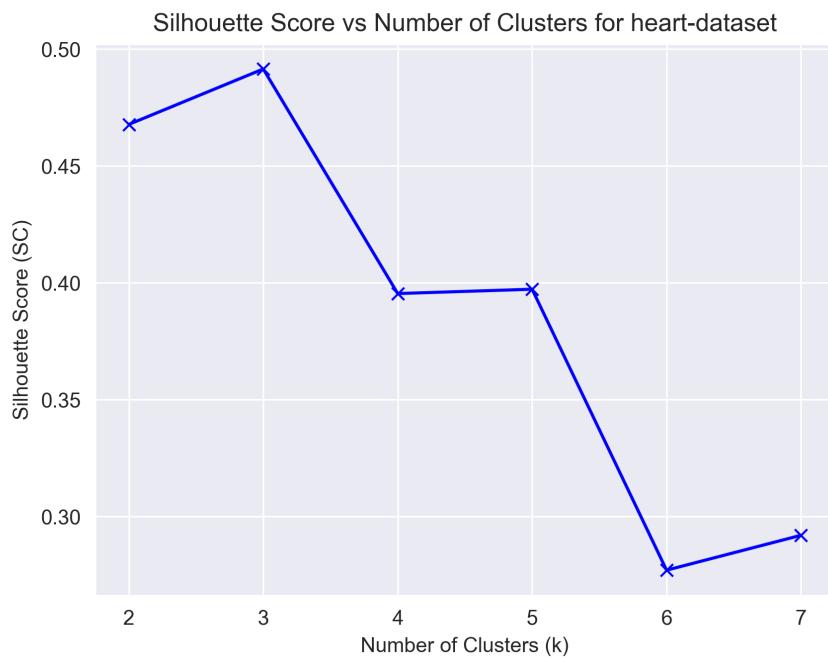


Figure 10: Selecting the k for Agglomerative clustering for Heart dataset (9 dimensions) using the "elbow plot."

2.3. CIRCLE DATASET

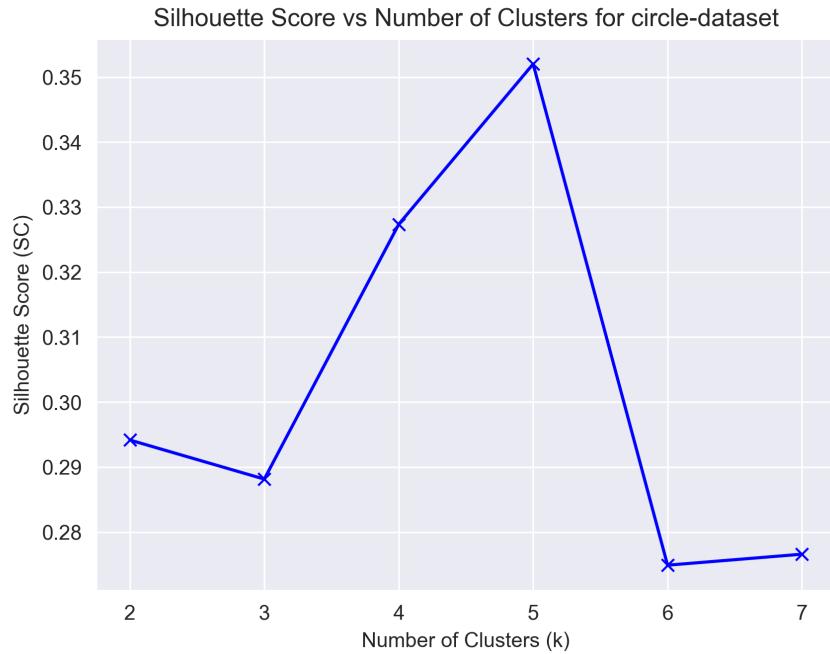


Figure 11: Selecting the k for Agglomerative clustering for circle dataset (2-dimensions) using the "elbow plot."

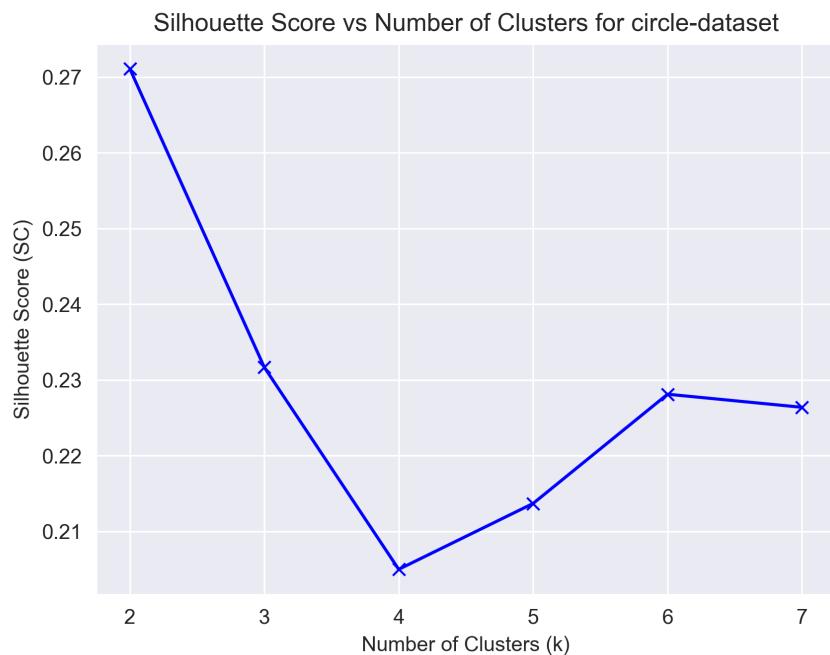


Figure 12: Selecting the k for Agglomerative clustering for circle dataset (3-dimensions) using the "elbow plot."

2.4. LINE DATASET

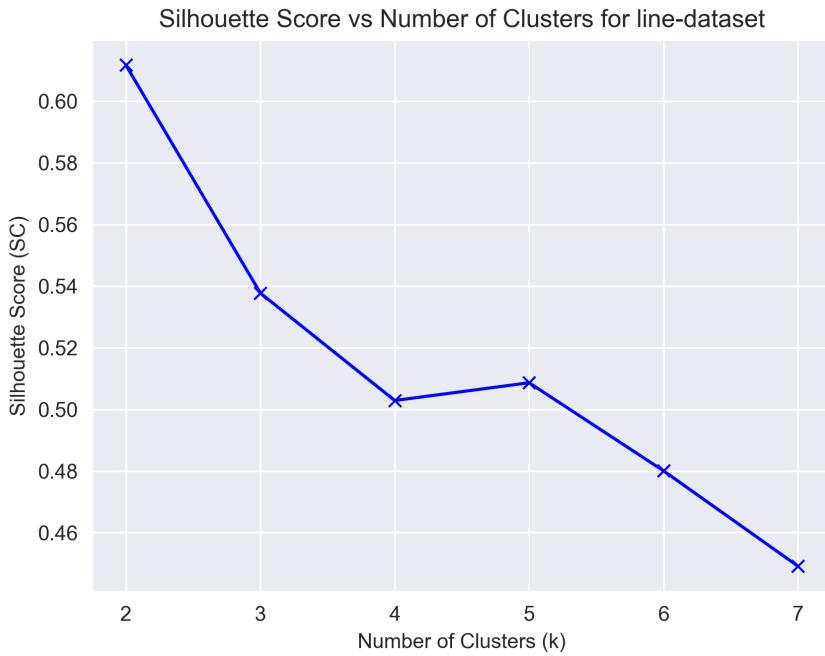


Figure 13: Selecting the k for Agglomerative clustering for line dataset (2-dimensions) using the "elbow plot."

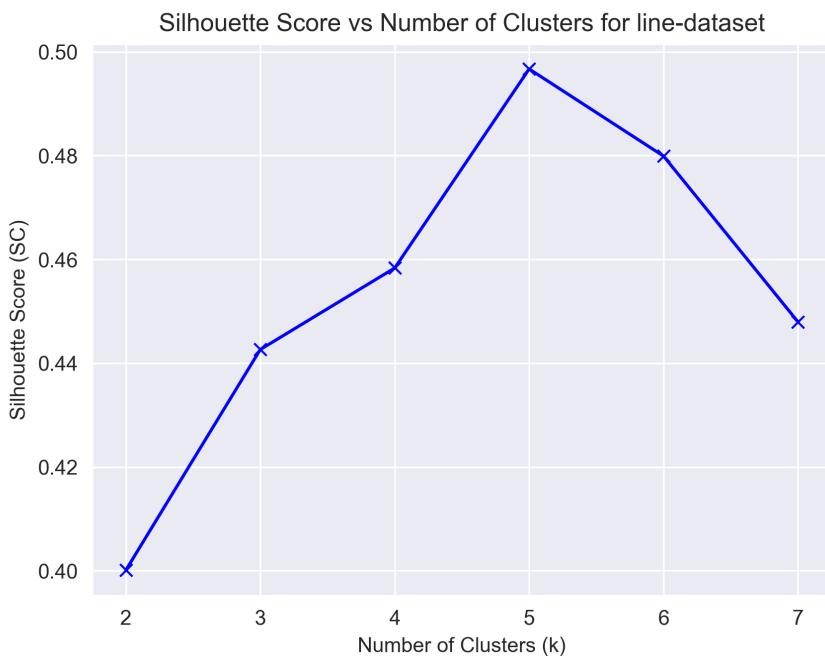


Figure 14: Selecting the k for Agglomerative clustering for line dataset (3-dimensions) using the "elbow plot."

.2.5. SKEWED DATASET

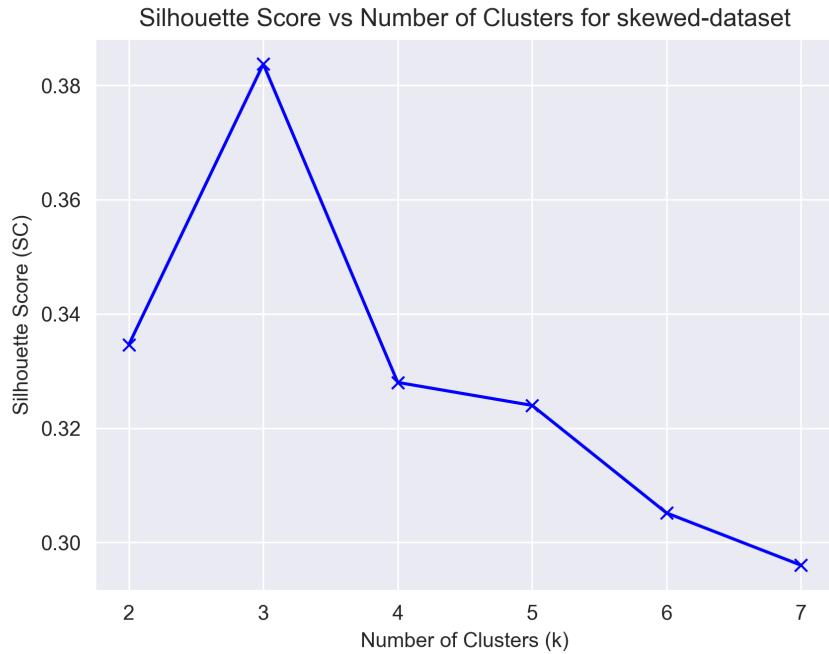


Figure 15: Selecting the k for Agglomerative clustering for skewed dataset (2-dimensions) using the "elbow plot."

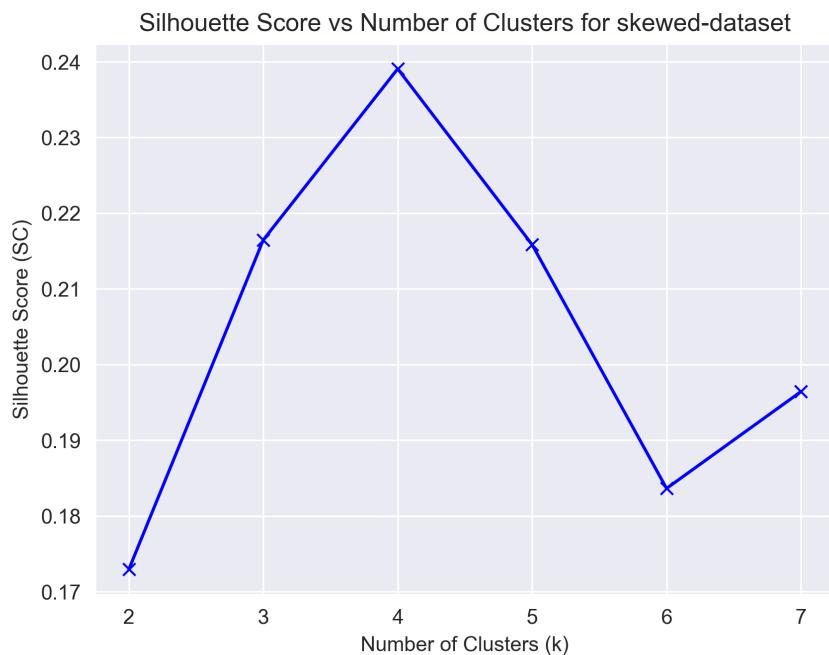


Figure 16: Selecting the k for Agglomerative clustering for skewed dataset (3-dimensions) using the "elbow plot."

THEORY

3. BIG O NOTATION

The big O notation is a common way to describe the complexity of an algorithm. It is used to describe the worst-case scenario of an algorithm. For example, if an algorithm has a complexity of $O(n)$, it means that the algorithm will take at most n steps to complete (source for figure: https://en.wikipedia.org/wiki/Big_O_notation):

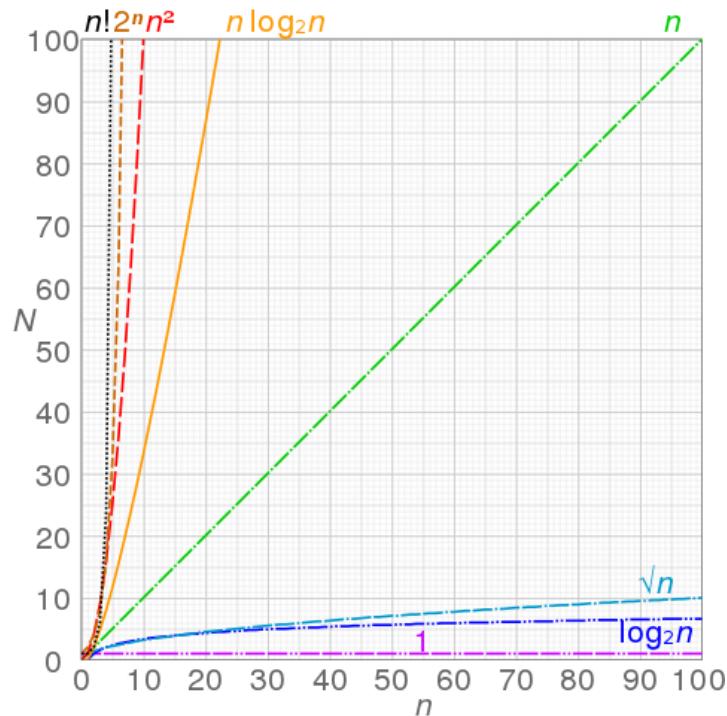


Figure 17: Graphical representation of the big O notation

RESULTS

.4. MECHANISM UTILITY

.4.1. SEEDS DATASET

(a) Adjusted Mutual Information comparison for the grid-kD-Laplace mechanism



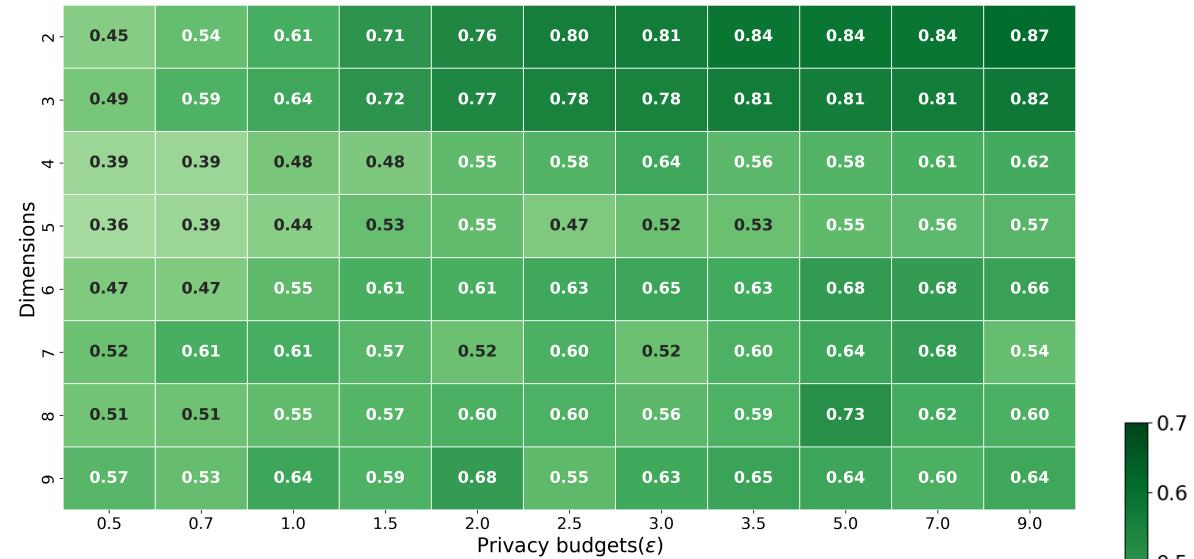
(b) Adjusted Mutual Information comparison for the density-kD-Laplace mechanism



Add comments

4.2. HEART DATASET

(a) Adjusted Mutual Information comparison for the grid-kD-Laplace mechanism



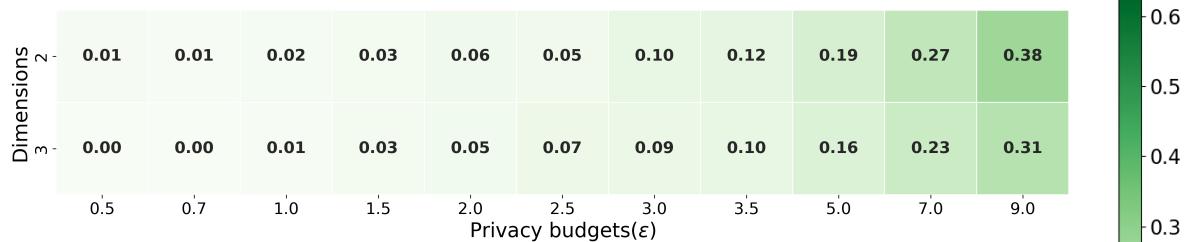
(b) Adjusted Mutual Information comparison for the density-kD-Laplace mechanism



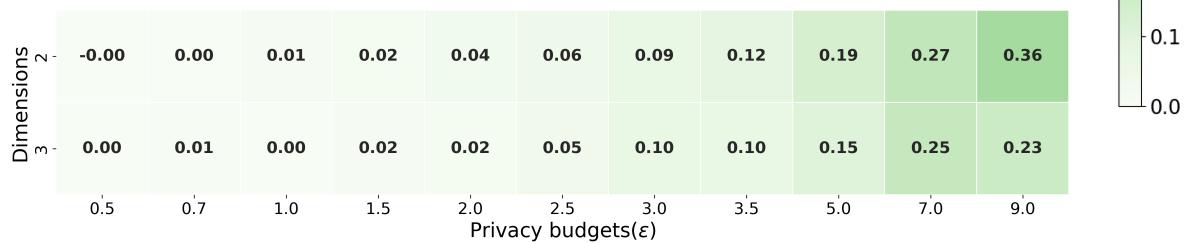
Add comments

4.3. CIRCLE DATASET

(a) Adjusted Mutual Information comparison for the grid-kD-Laplace mechanism



(b) Adjusted Mutual Information comparison for the density-kD-Laplace mechanism



Add comments

4.4. LINE DATASET

(a) Adjusted Mutual Information comparison for the grid-kD-Laplace mechanism



(b) Adjusted Mutual Information comparison for the density-kD-Laplace mechanism



Add comments

4.5. SKEWED DATASET

(a) Adjusted Mutual Information comparison for the grid-kD-Laplace mechanism



(b) Adjusted Mutual Information comparison for the density-kD-Laplace mechanism



Add comments

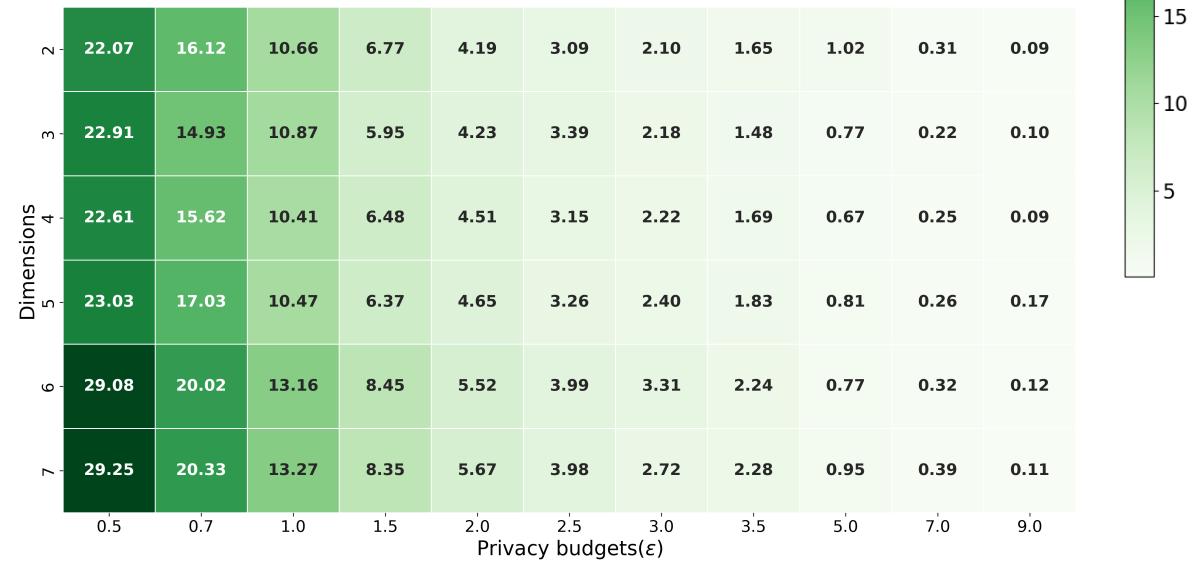
.5. PRIVACY

.5.1. SEEDS DATASET

(a) Heatmap showing disclosure risk for the kD-Laplace mechanism, per privacy budget & dimension for seeds-dataset.



(b) Heatmap showing disclosure risk for the Piecewise mechanism, per privacy budget & dimension for seeds-dataset.



Add comments

(a) Heatmap TPR for the kD-Laplace mechanism, per privacy budget & dimension for seeds-dataset.



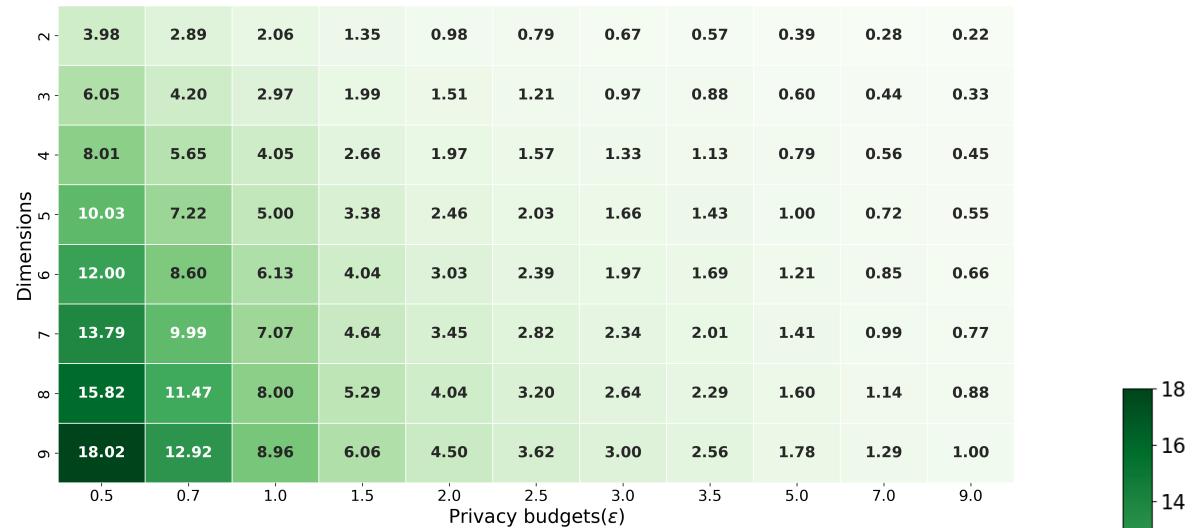
(b) Heatmap TPR for the Piecewise mechanism, per privacy budget & dimension for seeds-dataset.



Add comments

5.2. HEART DATASET

(a) Heatmap showing disclosure risk for the kD-Laplace mechanism, per privacy budget & dimension for heart-dataset.



(b) Heatmap showing disclosure risk for the Piecewise mechanism, per privacy budget & dimension for heart-dataset.



Add comments

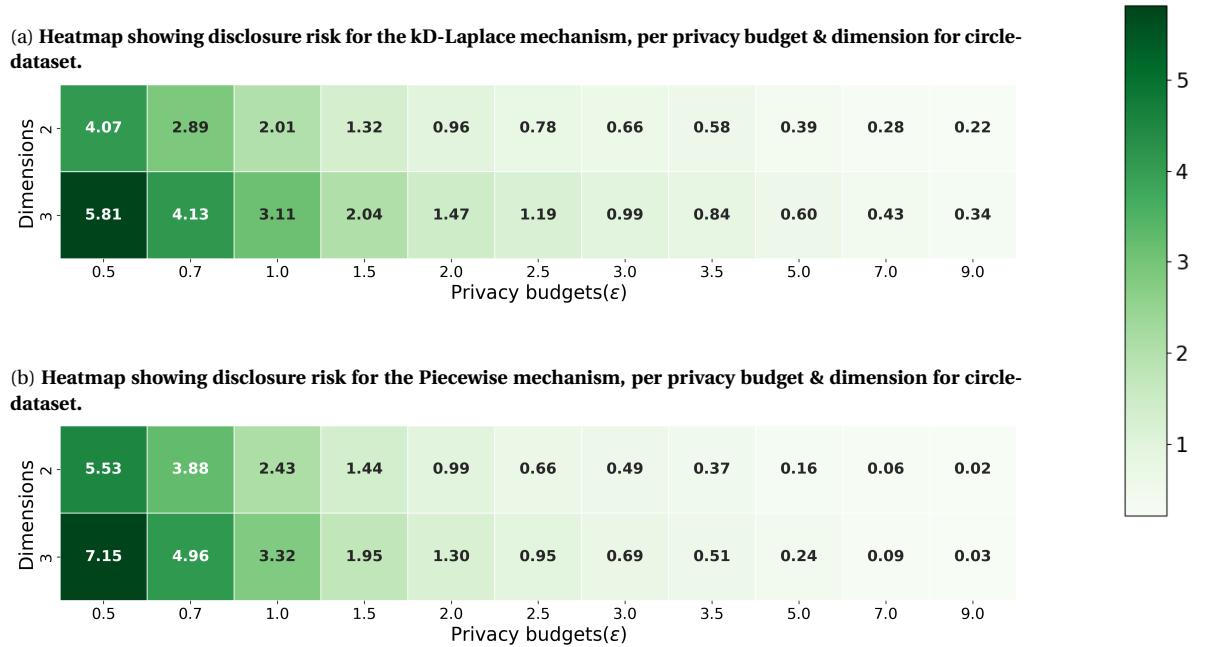
(a) Heatmap TPR for the kD-Laplace mechanism, per privacy budget & dimension for heart-dataset.



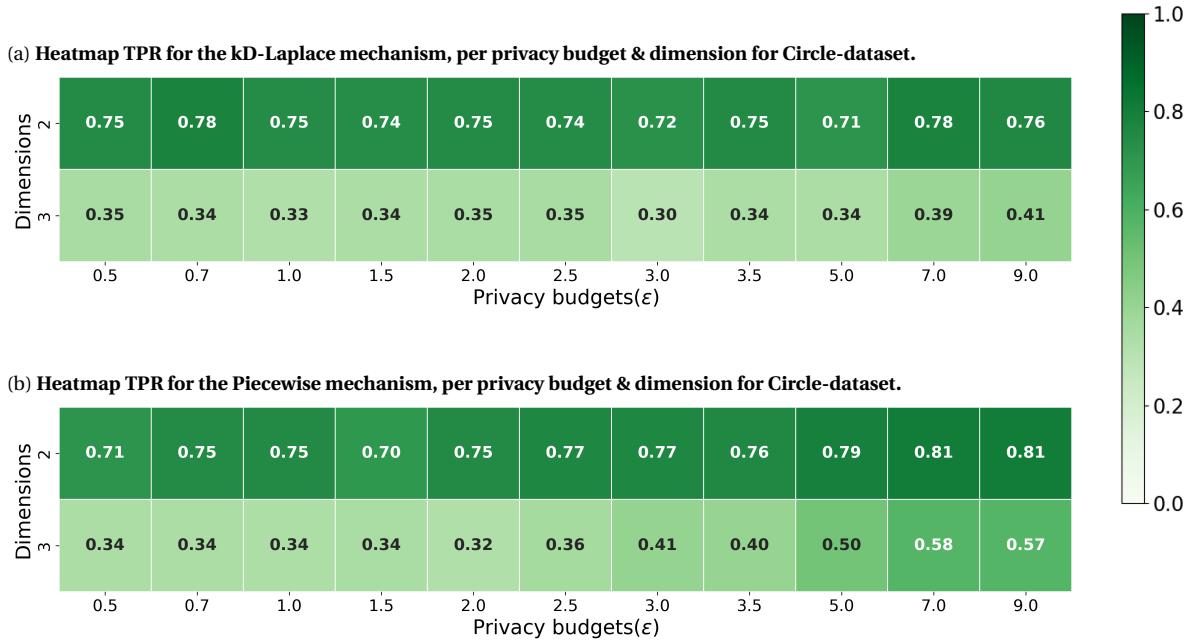
(b) Heatmap TPR for the Piecewise mechanism, per privacy budget & dimension for heart-dataset.



Add comments



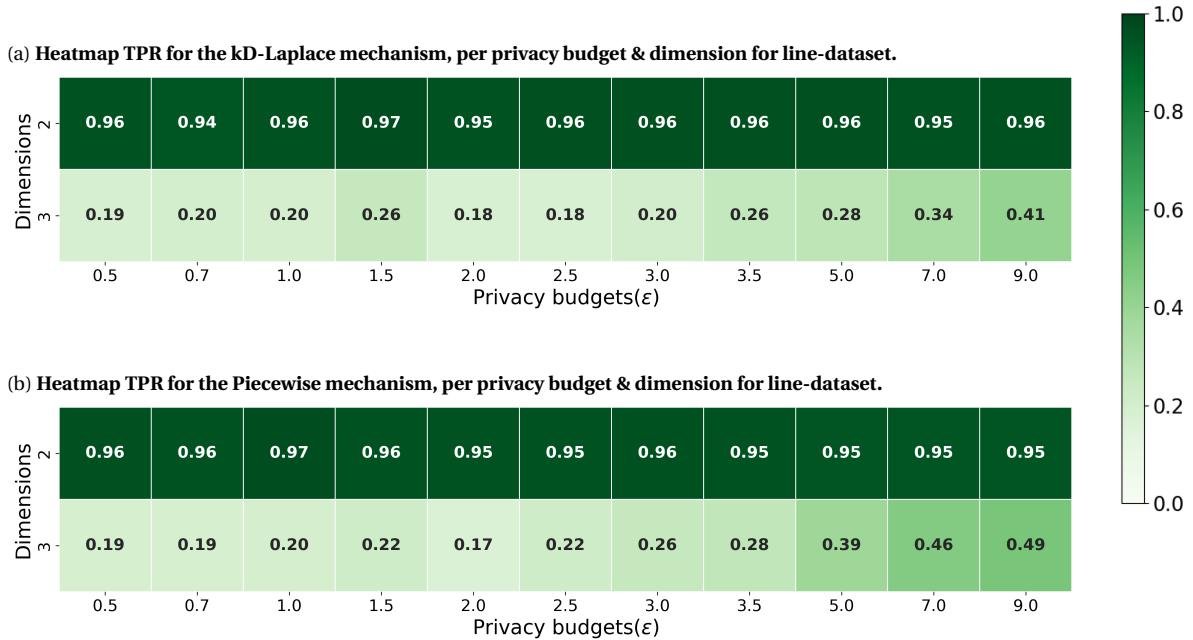
.5.3. CIRCLE DATASET



Add comments

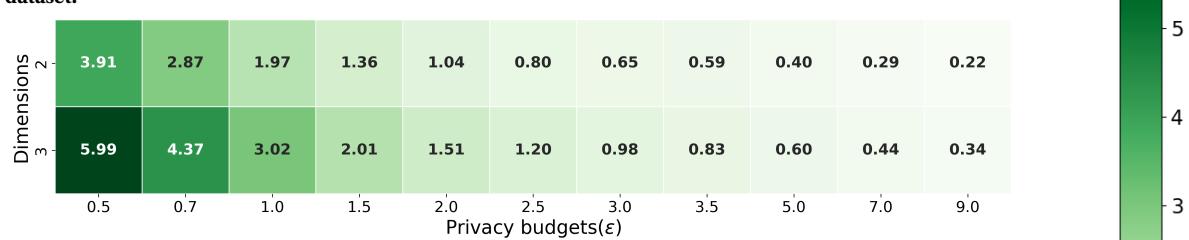


.5.4. LINE DATASET

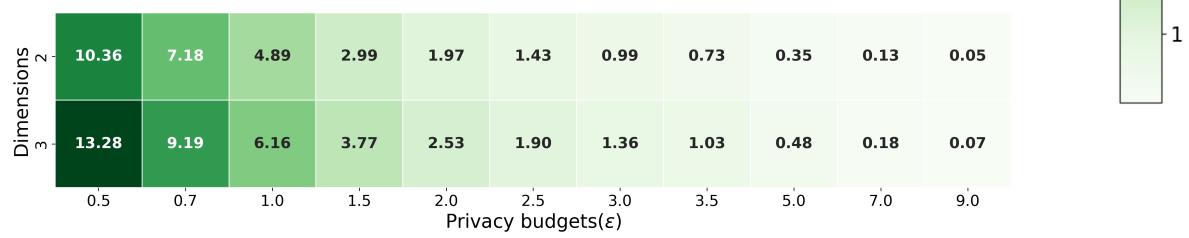


Add comments

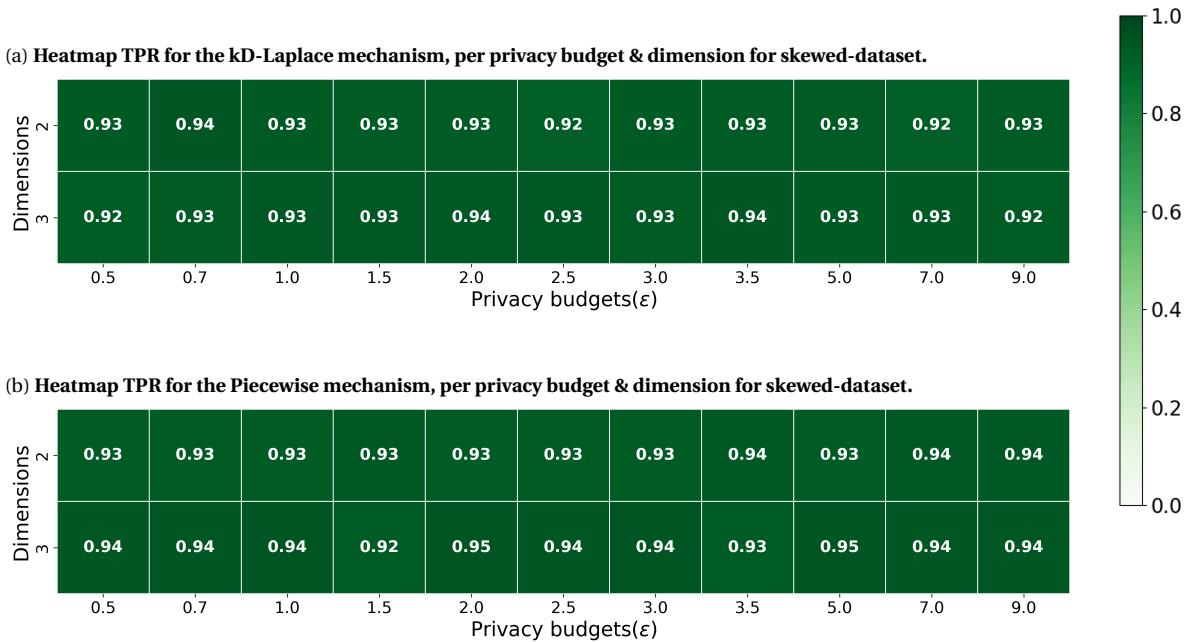
(a) Heatmap showing disclosure risk for the kD-Laplace mechanism, per privacy budget & dimension for skewed-dataset.



(b) Heatmap showing disclosure risk for the Piecewise mechanism, per privacy budget & dimension for skewed-dataset.



.5.5. SKEWED DATASET



Add comments