DIFFERENTIAL PRIVACY AT RISK

ASHISH DANDEKAR, DEBABROTA BASU, AND STÉPHANE BRESSAN

School of Computing, National University of Singapore, Singapore
e-mail address: (ashishdandekar,debabrota.basu)@u.nus.edu, steph@nus.edu.sg

Abstract. The calibration of noise for a privacy-preserving mechanism depends on the sensitivity of the query and on the prescribed privacy level. A data steward must make the non-trivial choice of a privacy level that balances the requirements of users and the monetary constraints of the business entity.

We propose *privacy at risk* that quantifies the probability with which a privacy-preserving mechanism satisfies differential privacy for any given privacy level. The probabilistic quantification depends on two sources of randomness, the explicit randomness induced by the noise distribution and the implicit randomness induced by the data-generation distribution, and thereby generalises probabilistic differential privacy and random differential privacy. Additionally, we study the effect of coupling between the two sources. We instantiate privacy at risk for the Laplace mechanism and provide analytical results.

We demonstrate the applicability of privacy at risk in two decision-making problems. Firstly, we empirically illustrate how a data steward finds the compromise between the privacy level and the desired utility requirement by implementing the Laplace mechanism for ridge regression. Secondly, we propose a cost model that bridges the gap between the privacy level and the compensation budget estimated by a GDPR compliant business entity. The cost model for privacy at risk being a convex function of the privacy level leads to unique privacy at risk level that minimises the compensation budget.

Thus, privacy at risk not only quantifies the privacy level for a given privacy-preserving mechanism but also facilitates decision-making in problems that focus on the privacy-utility trade-off and the compensation budget minimisation.

1. Introduction

Dwork et al. (2014) quantifies the privacy level ϵ in ϵ-differential privacy as an upper bound on the worst-case privacy loss incurred by a privacy-preserving mechanism. Generally, a privacy-preserving mechanism perturbs the results by adding the calibrated amount of random noise to them. The calibration of noise depends on the sensitivity of the query and the specified privacy level. In a real-world setting, a data steward must specify a privacy level that balances requirements of the users and monetary constraints of the business entity. Garfinkel et al. (2018) report the issues in deploying differential privacy as the privacy definition by the US census bureau. They highlight the lack of formal methods to choose the privacy level. Additionally, analytical computation of the sensitivity for any general query is not a simple task. For instance, the work by Chaudhuri et al. (2011) highlights

Key words and phrases: Differential privacy, Laplace mechanism, Cost model.

the rigour and non-triviality involved in the analytical calculation of the sensitivity of the optimal solution of an empirical risk minimisation problem.

We propose *privacy at risk* that quantifies the probability with which a privacy-preserving mechanism satisfies differential privacy for a specified privacy level (Section 3). The probabilistic quantification depends on two sources of randomness, the explicit randomness induced by the noise distribution and the implicit randomness induced by the data-generation distribution, and the coupling between the two. In its most general setting, privacy at risk is computed over the output space obtained by applying the privacy-preserving mechanism on the data-generation distribution. Thus, the proposed definition unifies and extends probabilistic differential privacy, proposed by Machanavajjhala et al. (2008), and random differential privacy, proposed by Hall et al. (2012). Probabilistic differential privacy considers the explicit randomness whereas random differential privacy considers the implicit randomness.

In order to analytically compute privacy at risk, we need to have at hand analytical forms of both the implicit and explicit sources of randomness as well as analytical form of the query. From the analytical form of the data-generation distribution and of the query, we could try and derive the distribution of the sensitivity of the query. From the analytical forms of the sensitivity distribution and of the noise distribution, we could try and derive the distribution of the privacy loss guaranteed by the calibrated noise. While this may be possible in some cases, it is generally challenging. We instantiate privacy at risk to three cases for the widely used Laplace mechanism proposed by Dwork et al. (2006b) that adds Laplacian noise.

Firstly, we compute privacy at risk under the effect of explicit randomness induced by the Laplacian noise (Section 3.1). In order to quantify this effect, we calculate the overlap between differently parametrised Laplace distributions under the constraint of the sensitivity of the query. This calculation leads us to the use of Bessel-K distribution in our analytical result.

Secondly, we compute the privacy at risk under the effect of implicit randomness induced by the data-generation distribution (Section 3.2). In order to quantify this effect, we statistically estimate the sensitivity of the query, which we call as the *sampled sensitivity* of the query, with the help of an empirical distribution over the sensitivities. The empirical distribution is generated using the sensitivities computed for the neighbouring datasets sampled from the data-generation distribution. We use DKW inequality to quantify the closeness of the sampled sensitivity to the true sensitivity of the query.

Lastly, we compute privacy at risk under the effect of both explicit and implicit randomness induced by the Laplace mechanism operating on the dataset that is modelled by a data-generation distribution (Section 3.3). In order to quantify this effect, we revise the analytical results from the earlier cases in light of the output space that is obtained by applying the privacy-preserving mechanism on the data-generation distribution. We find that the effect of the noise distribution, which is quantified by the Bessel-K distribution, is coupled with the effect of the data-generation distribution, which is quantified by the parameters in the DKW inequality. This coupling is evident in the analytical result that we derive for this case.

We demonstrate the applicability of privacy at risk in two decision-making problems. *First application* discusses how a data steward applies privacy at risk to choose a privacy level ϵ with confidence level γ (Section 4.1). We empirically illustrate design methods for the three cases for differentially private ridge regression proposed by Ligett et al. (2017).

In each of the three cases, we illustrate how a data steward finds the balance between the privacy level and the desired utility requirement. *Second application* discusses how a GDPR compliant business entity applies privacy at risk to minimise the compensation budget that it needs to maintain to pay back to the stakeholders in the unfortunate event of a personal data breach (Section 4.2). We propose a cost model that bridges the gap between the privacy level in differential privacy and the compensation budget as it is estimated by business entities. We adapt the proposed model for privacy at risk. The corresponding model for privacy at risk is a convex function of the privacy level. Hence, it leads to a unique privacy at risk level that minimises the compensation budget. We further illustrate a realistic scenario of a GDPR compliant health centre in a university that biannually publishes the health statistics of the staff using the Laplace mechanism. The illustration shows that the use of privacy at risk as a quantifier of privacy instead of *pure* differential privacy yields a significant reduction in the compensation budget.

In conclusion, the benefits of privacy at risk are twofold. It not only quantifies the privacy level for a given privacy-preserving mechanism but also facilitates decision-making in problems that focus on the privacy-utility trade-off and the compensation budget minimisation.

2. Background

We consider a universe of datasets $\mathcal{D}$. We explicitly mention when we consider that the datasets are sampled from a data-generation distribution $\mathcal{G}$ with support $\mathcal{D}$. Two datasets of equal cardinality x and y are said to be *neighbouring datasets* if they differ in one data point. A pair of neighbouring datasets is denoted by $x \sim y$. In this work, we focus on a specific class of queries called *numeric queries*. A numeric query is a function that maps a dataset into a real vector, i.e. $f : \mathcal{D} \to \mathbb{R}^k$. For instance, a sum query returns the sum of the values in a dataset.

In order to achieve a privacy guarantee, a *privacy-preserving mechanism*, which is a randomised algorithm, explicitly adds noise to the query from a given family of distributions. Thus, a privacy-preserving mechanism of a given family, $\mathcal{M}(f, \Theta)$, for the query f and the set of parameters Θ of the given noise distribution, is a function that maps a dataset into a real vector, i.e. $\mathcal{M}(f, \Theta) : \mathcal{D} \to \mathbb{R}^k$. We denote a privacy-preserving mechanism as $\mathcal{M}$, when the query and the parameters are clear from the context.

2.1. Differential privacy.

Definition 2.1 (**Differential privacy, Dwork et al. (2014)**)**.** A privacy-preserving mechanism $\mathcal{M}$, equipped with a query f and with parameters Θ, is ϵ-differentially private if for all $Z \subseteq \text{Range}(\mathcal{M})$ and $x, y \in \mathcal{D}$ such that $x \sim y$:

$$\log\left(\left|\frac{\mathbb{P}(\mathcal{M}(f,\Theta)(x) \in Z)}{\mathbb{P}(\mathcal{M}(f,\Theta)(y) \in Z)}\right|\right) \leq \epsilon.$$

A privacy-preserving mechanism provides perfect privacy if it yields indistinguishable outputs for all neighbouring input datasets. The privacy level ϵ quantifies the privacy guarantee provided by ϵ-differential privacy. For a given query, a smaller value of ϵ provides higher privacy. A randomised algorithm that is ϵ-differentially private is also ϵ'-differential private for any $\epsilon' > \epsilon$.

In order to satisfy ϵ-differential privacy, the parameters of a privacy-preserving mechanism require calculated calibration. The amount of noise required to achieve a specified privacy level depends on the query. If the output of the query does not change drastically for two neighbouring datasets, then less noise is required to achieve a given privacy level. The measure of such fluctuations is called the *sensitivity* of the query. The parameters of a privacy-preserving mechanism are calibrated using the sensitivity of the query.

Definition 2.2 (**Sensitivity, Dwork et al. (2014)**)**.** The sensitivity of a query $f : \mathcal{D} \to \mathbb{R}^k$ is defined as

$$\Delta_f \triangleq \max_{\substack{x,y \in \mathcal{D} \\ x \sim y}} \|f(x) - f(y)\|_1.$$

2.2. **Laplace mechanism.** The Laplace mechanism is a privacy-preserving mechanism that adds scaled noise sampled from a calibrated Laplace distribution to the numeric query.

Definition 2.3 (**Laplace distribution, Papoulis and Pillai (2002)**)**.** The Laplace distribution with mean zero and scale $b > 0$ is a probability distribution with probability density function

$$\text{Lap}(b) \triangleq \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right),$$

where $x \in \mathbb{R}$. We write $\text{Lap}(b)$ to denote a random variable $X \sim \text{Lap}(b)$

Definition 2.4 (**Laplace mechanism, Dwork et al. (2006b)**)**.** Given any function $f : \mathcal{D} \to \mathbb{R}^k$ and any $x \in \mathcal{D}$, the Laplace Mechanism is defined as

$$\mathcal{L}_\epsilon^{\Delta_f}(x) \triangleq \mathcal{M}\left(f, \frac{\Delta_f}{\epsilon}\right)(x) = f(x) + (L_1, ..., L_k),$$

where L_i is drawn from $\text{Lap}\left(\frac{\Delta_f}{\epsilon}\right)$ and added to the i^{th} component of $f(x)$.

Theorem 2.5 (**Dwork et al. (2006b)**)**.** *The Laplace mechanism, $\mathcal{L}_{\epsilon_0}^{\Delta_f}$, is ϵ_0-differentially private.*

In order to satisfy ϵ-differential privacy, the calibration of the Laplacian noise depends on the sensitivity of the query and the desired privacy level ϵ. Note that for the value of sensitivity Δ smaller than Δ_f, $\mathcal{L}_{\epsilon_0}^{\Delta}$ is not ϵ_0-differentially private.

3. Privacy at risk

The parameters of a privacy-preserving mechanism are calibrated using the privacy level and the sensitivity of the query. A data steward needs to choose appropriate privacy level (Lee and Clifton (2011) show that the choice of an actual privacy level by a data steward in regard to her business requirements is a non-trivial task). Recall that the privacy level in the definition of differential privacy corresponds to the worst case privacy loss. Business users are however used to taking and managing risk.

For instance, Jorion (2000) defines *Value at Risk* that is used by risk analysts to quantify the loss in investments for a given portfolio and an acceptable confidence bound. Motivated by the formulation of *Value at Risk*, we define *privacy at risk* as a privacy definition. For a given privacy-preserving mechanism, privacy at risk defines the privacy level ϵ with a

confidence level γ. For the sake of clarity, we refer to this privacy level ϵ as the privacy at risk level.

Definition 3.1 (**Privacy at risk**). For a given data generating distribution $\mathcal{G}$, a privacy-preserving mechanism $\mathcal{M}$, equipped with a query f and with parameters Θ, satisfies (ϵ, γ)-privacy at risk, if for all $Z \subseteq \text{Range}(\mathcal{M})$ and x, y sampled from $\mathcal{G}$ such that $x \sim y$:

$$\mathbb{P}\left[\log\left|\frac{\mathbb{P}(\mathcal{M}(f,\Theta)(x) \in Z)}{\mathbb{P}(\mathcal{M}(f,\Theta)(y) \in Z)}\right| > \epsilon\right] \leq \gamma, \tag{3.1}$$

where the outer probability is calculated with respect to the probability space $\text{Range}(\mathcal{M} \circ \mathcal{G})$ obtained by applying the privacy-preserving mechanism $\mathcal{M}$ on the data-generation distribution $\mathcal{G}$.

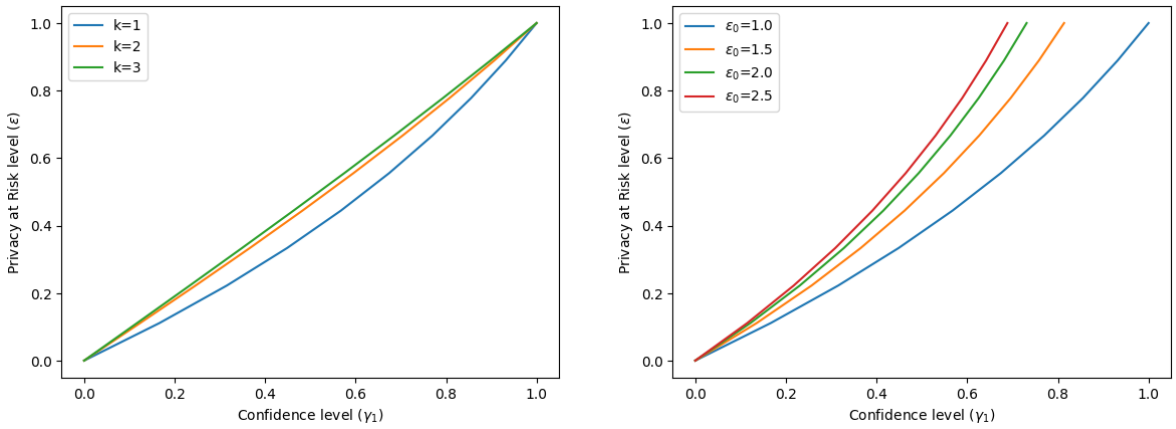
If a privacy-preserving mechanism is ϵ_0-differentially private for a given query f and parameters Θ, its privacy at risk level coincides with the privacy level ϵ_0 with confidence level 1. Our interest is to study the effect of both the randomness induced by the noise and that of the data-generation distribution to help a data steward calibrate the privacy-preserving mechanism as per a desired privacy level and a desired confidence level.

Unifying Probabilistic and Random Differential Privacy. Interestingly, privacy at risk unifies the notions of probabilistic differential privacy and random differential privacy by accounting for both sources of randomness in a privacy-preserving mechanism. Machanavajjhala et al. (2008) define probabilistic differential privacy that incorporates the explicit randomness of the noise distribution of the privacy-preserving mechanism. In probabilistic differential privacy, the outer probability is computed over the sample space of $\text{Range}(\mathcal{M})$ and all datasets are equally probable. Thus, if we consider a uniform data-generation distribution in Equation 3.1, Definition 3.1 leads to the definition of probabilistic differential privacy. Hall et al. (2012) define random differential privacy that incorporates the implicit randomness of the data-generation distribution. In random differential privacy, the outer probability is calculated with respect to the support of the data-generation distribution $\mathcal{G}$. Thus, if we consider a specific data-generation distribution $\mathcal{G}$ in Equation 3.1, Definition 3.1 leads to the definition of random differential privacy.

Now, we instantiate privacy at risk for the Laplace mechanism for three cases: two cases involving two sources of randomness and third case involving the coupled effect. Three different cases correspond to three different interpretations of the confidence level, represented by the parameter γ, corresponding to three interpretation of the support of the outer probability in Definition 3.1. In order to highlight this nuance, we denote the confidence levels corresponding to the three cases and their three sources of randomness as γ_1, γ_2 and γ_3, respectively.

3.1. **The Case of Explicit Randomness.** In this section, we study privacy at risk of the Laplace mechanism by considering effect of the explicit randomness induced by the Laplacian distribution. We assume that the sensitivity of the query is known a priori. We study the privacy at risk at a given confidence level, γ_1, on the noise distribution induced by the Laplace mechanism.

For a Laplace mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$ calibrated with sensitivity Δ_f and privacy level ϵ_0, we present the analytical formula relating privacy at risk level ϵ and the confidence level γ_1 in Theorem 3.2. The proof is available in Appendix A.



(A) (B)

FIGURE 1. Privacy at risk level ϵ for varying confidence level γ_1 for Laplace mechanism $\mathcal{L}^{1.0}_{\epsilon_0}$. In Figure 1a, we use $\epsilon_0 = 1.0$ and different values of k. In Figure 1b, for $k = 1$ and different values of ϵ_0.

Theorem 3.2. *The confidence level $\gamma_1 \in [0, 1]$ of achieving a privacy at risk level $\epsilon \geq 0$ by a Laplace Mechanism $\mathcal{L}^{\Delta_f}_{\epsilon_0}$ is given by*

$$\gamma_1 = \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \epsilon_0)}, \tag{3.2}$$

where T is a random variable dependent on the Laplace noise $\text{Lap}(\frac{\Delta_f}{\epsilon_0})$, and follows the $\text{BesselK}\left(k, \frac{\Delta_f}{\epsilon_0}\right)$ distribution.

Figure 1a shows the plot of the privacy at risk level against confidence level for different values of k and for a Laplace mechanism $\mathcal{L}^{1.0}_{1.0}$. As the value of k increases, the amount of noise added in the output of numeric query increases. Therefore, for a fixed value of the confidence level, the privacy at risk level increases with the value of k.

The analytical formula representing γ_1 as a function of ϵ is bijective. We need to invert it to obtain the privacy at risk level ϵ for a given confidence level γ_1. However the analytical closed form for such an inverse function is not explicit. We use a numerical approach to compute privacy at risk level for a given confidence level from the analytical formula of Theorem 3.2. This corresponds to inverting the analytical formula for γ_1 by reading the relevant plot in Figure 1a from the y-axis to the x-axis.

Result for real-valued query. For the case $k = 1$, the computation of the confidence level is comparatively straightforward because it only involves *Laplace* and *exponential distributions*, and does not require *gamma* and *BesselK-distribution*. In this case, privacy at risk level is given by the following result. Privacy at risk level ϵ for a Laplace Mechanism $\mathcal{L}^{\Delta_f}_{\epsilon_0}$ for a query $f : \mathcal{D} \to \mathbb{R}$ and a confidence level γ_1 is given by Equation 3.3.

$$\epsilon = \ln\left(\frac{1}{1 - \gamma_1(1 - e^{-\epsilon_0})}\right) \tag{3.3}$$

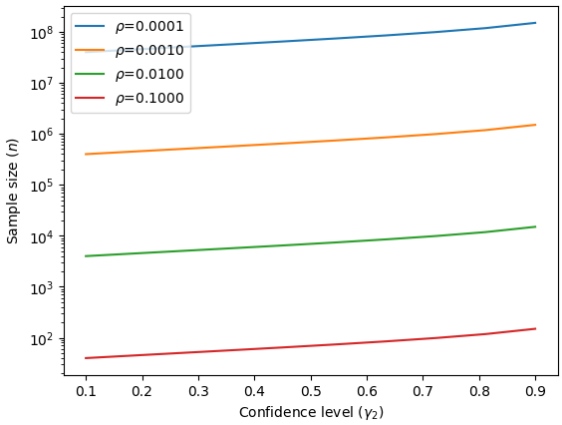


FIGURE 2. Number of samples n for varying confidence level of γ_2 for different accuracy parameter ρ.

Comment on ϵ_0. For $k = 1$, Figure 1b shows the plot of privacy at risk level ϵ versus confidence level γ_1 for the Laplace mechanism $\mathcal{L}^{1.0}_{\epsilon_0}$. As the value of ϵ_0 increases, the probability of Laplace mechanism generating higher value of noise reduces. Therefore, we observe that for a fixed confidence level, privacy at risk level increases with the value of ϵ_0. The same observation is made for $k > 1$.

3.2. **The Case of Implicit Randomness.** In this section, we study privacy at risk of the Laplace mechanism by considering effect of the implicit randomness induced by the data-generation distribution. We do not assume the knowledge of the sensitivity of the query. We study privacy at risk at a given confidence level, γ_2, on the sensitivity distribution computed using the data-generation distribution.

If we have access to an analytical form of the data-generation distribution and to the query, we could analytically derive the sensitivity distribution for the query. In general, we have access to the datasets, but not the data-generation distribution that generates them. Although we know the query, it rarely takes an analytical form suitable for the derivations needed. We, therefore, statistically estimate sensitivity by constructing an empirical distribution. We call the sensitivity value obtained for a given confidence level from the empirical cumulative distribution of sensitivity the *sampled sensitivity* (Definition 3.4). However, the value of sampled sensitivity is not the exact value of the sensitivity for a specified confidence level. In order to capture this additional uncertainty introduced by the estimation from the empirical sensitivity rather than the sensitivity distribution, we compute a lower bound on the accuracy of this estimation. This lower bound yields a probabilistic lower bound on the specified confidence level. We refer to it as *empirical privacy at risk*. For a given confidence level γ_2, we denote by $\hat{\gamma_2}$ the confidence level for empirical privacy at risk.

For the Laplace mechanism $\mathcal{L}_{\epsilon}^{\Delta_{S_f}}$ calibrated with sampled sensitivity Δ_{S_f} and privacy at risk level ϵ, we evaluate the confidence level $\hat{\gamma_2}$. We present the result in Theorem 3.3. The proof is available in Appendix B.

Theorem 3.3. *Analytical bound on the confidence level for empirical privacy at risk,* $\hat{\gamma_2}$*, for Laplace mechanism* $\mathcal{L}_{\epsilon}^{\Delta_{S_f}}$ *with privacy at risk level* ϵ *and sampled sensitivity* Δ_{S_f} *for a*

query $f : \mathcal{D} \to \mathbb{R}^k$ *is*

$$\hat{\gamma_2} \geq \gamma_2(1 - 2e^{-2\rho^2 n}) \tag{3.4}$$

where n *is the number of samples used for estimation of the sampled sensitivity and* ρ *is the accuracy parameter.* γ_2 *denotes the confidence level for the privacy at risk.*

The accuracy parameter ρ represents the closeness between the empirical cumulative distribution of the sensitivity to the true cumulative distribution of the sensitivity. Lower the value of the accuracy, closer is the empirical cumulative distribution to the true cumulative distribution. Figure 2 shows the plot of number of samples as a function of the confidence interval and the accuracy parameter. We observe that as the value of the accuracy reduces the number of samples in order to achieve the same confidence level exponentially increases. Let us now present the details of the derivation of the analytical bound on the confidence level for empirical privacy risk in Theorem 3.5.

If the analytical form of the data-generation distribution is not known a priori, the empirical distribution of sensitivity can be estimated in two ways. The first way is to fit a known distribution on the available data and later use it to build an empirical distribution of the sensitivities. The second way is to sub-sample from a large dataset in order to build an empirical distribution of the sensitivities. In both of these ways, the empirical distribution of sensitivities captures the inherent randomness in the data-generation distribution. The first way suffers from the goodness of the fit of the known distribution to the available data. An ill-fit distribution does not reflect the true data-generation distribution and hence introduces errors in the sensitivity estimation. Since the second way involves subsampling, it is immune to this problem. The quality of sensitivity estimates obtained by sub-sampling the datasets depend on the availability of large population to sample from.

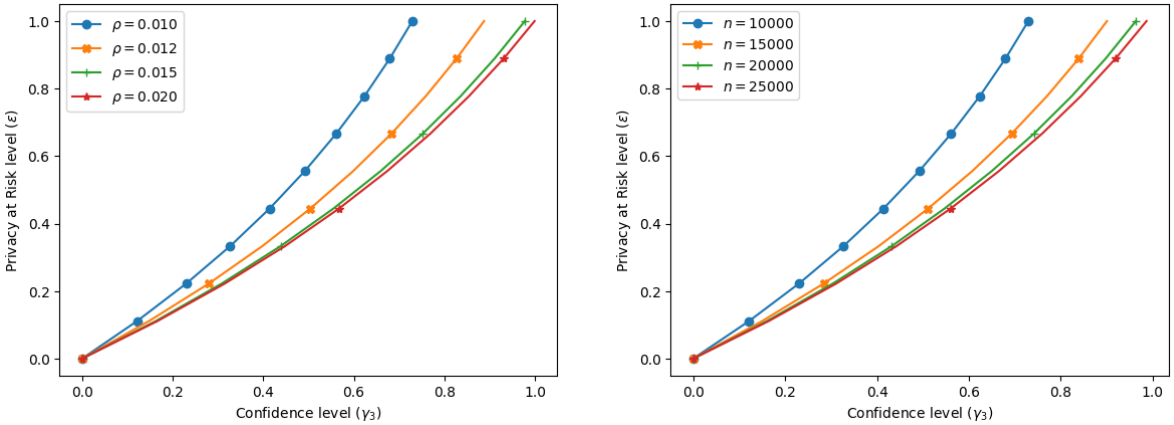
Let, $\mathcal{G}$ denotes the data-generation distribution that is realised using either of the two ways. We adopt the procedure of Rubinstein and Aldà (2017) to sample two neighbouring datasets with p data points each. We sample $p-1$ data points from $\mathcal{G}$ that are common to both of these datasets. We sample two more data points from $\mathcal{G}$ and allot one data point to each of the two datasets.

Let, $S_f = \|f(x) - f(y)\|_1$ denotes the sensitivity random variable for a given query f, where x and y are two neighbouring datasets sampled from $\mathcal{G}$. Using n pairs of neighbouring datasets sampled from $\mathcal{G}$, we construct the empirical cumulative distribution, F_n, for the sensitivity random variable.

Definition 3.4 (**Sampled sensitivity**)**.** For a given query f and for a specified confidence level γ_2, sampled sensitivity, Δ_{S_f}, is defined as the value of sensitivity random variable that is estimated using its empirical cumulative distribution function, F_n, constructed using n pairs of neighbouring datasets sampled from the data-generation distribution $\mathcal{G}$.

$$\Delta_{S_f} \triangleq F_n^{-1}(\gamma_2)$$

If we knew analytical form of the data generation distribution, we could analytically derive the cumulative distribution function of the sensitivity, F, and find the sensitivity of the query as $\Delta_f = F^{-1}(1)$. Therefore, in order to have the sampled sensitivity close to the sensitivity of the query, we require the empirical cumulative distributions to be close to the cumulative distribution of the sensitivity. We use this insight to derive the analytical bound in the Theorem 3.3.



(A) Privacy at risk level ϵ for varying confidence levels γ_3 for different accuracy parameters ρ. We fix the number of samples to 10000.

(B) Privacy at risk level ϵ for varying confidence levels γ_3 for different sample sizes n. We fix the accuracy parameter to 0.01

FIGURE 3. Dependence of accuracy and number of samples on the privacy at risk for Laplace mechanism $\mathcal{L}_{1.0}^{\Delta_{S_f}}$. For the figure on the left hand side, we fix the number of samples to 10000. For the Figure 3b we fix the accuracy parameter to 0.01.

3.3. **The case of Explicit and Implicit Randomness.** In this section, we study the combined effect of both explicit randomness induced by the noise distribution and implicit randomness in the data-generation distribution respectively, on the privacy at risk. We do not assume the knowledge of the sensitivity of the query. We study privacy at risk at a given confidence level γ_3 on the joint support of the noise distribution and the data-generation distribution.

We estimate sensitivity using the empirical cumulative distribution of sensitivity. We construct the empirical distribution over the sensitivities using the sampling technique presented in Section 3.2. Since we use the sampled sensitivity (Definition 3.4) to calibrate the Laplace mechanism, we evaluate the confidence level for *empirical privacy at risk* $\hat{\gamma_3}$.

For the Laplace mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}$ calibrated with sampled sensitivity Δ_{S_f} and privacy level ϵ_0, we present the analytical bound on the confidence level $\hat{\gamma_3}$ in Theorem 3.5. The proof is available in Appendix C.

Theorem 3.5. *Analytical bound on the confidence level for empirical privacy at risk* $\hat{\gamma_3} \in [0, 1]$ *to achieve a Privacy at Risk level* $\epsilon > 0$ *for Laplace mechanism* $\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}$ *with sampled sensitivity* Δ_{S_f} *of a query* $f : \mathcal{D} \to \mathbb{R}^k$ *is*

$$\hat{\gamma_3} \geq \gamma_3(1 - 2e^{-2\rho^2 n}) \tag{3.5}$$

where n *is the number of samples used for estimating the sensitivity,* ρ *is the accuracy parameter.* γ_3 *denotes the confidence level for the privacy at risk.*

The accuracy parameter ρ controls the closeness between the empirical cumulative distribution of the sensitivity to the true cumulative distribution of the sensitivity. Figure 3 shows the dependence of the accuracy parameter on the number of samples on the privacy

at risk. In Figure 3a, we observe that the for a fixed number of samples and a privacy at risk level, the confidence level decreases with the value of accuracy parameter. For a fixed number of samples, smaller values of the accuracy parameter reduce the probability of similarity between the empirical cumulative distribution of sensitivity and the true cumulative distribution. Therefore, we observe the reduction in the confidence level for a fixed privacy at risk level. In Figure 3b, we observe that for a fixed value of accuracy parameter and a fixed level of privacy at risk, the confidence level increases with the number of samples. For a fixed value of the accuracy parameter, larger values of the sample size increase the probability of similarity between the empirical cumulative distribution of sensitivity and the true cumulative distribution. Therefore, we observe the increase in the confidence level for a fixed privacy at risk level.

Effect of the consideration of implicit and exlict randomness is evident in the analytical expression for γ_3 in Equation 3.6. Proof is available in Appendix C. The confidence level is composed of two factors. The second term is the confidence level that accounts for inherent randomness. The first term takes into account the implicit randomness of the Laplace distribution along with a coupling coefficient η. We define η as the ratio of the true senstivity of the query to its sampled sensitivity.

$$\gamma_3 \triangleq \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \eta\epsilon_0)} \cdot \gamma_2 \tag{3.6}$$

4. Applications of Privacy at Risk

In this section, we demonstrate the application of privacy at risk in solving two real-world decision-making problems.

4.1. **Balancing utility and privacy.**

In this section, we empirically illustrate and discuss the steps that a data steward needs to take and the issues that she needs to consider in order to realize a required privacy at risk level ϵ for a confidence level γ when seeking to disclose the result of a query.

We consider a query that returns the parameter of a ridge regression [Murphy (2012)] for an input dataset. It is a basic and widely used statistical analysis tool. We use the privacy-preserving mechanism presented by Ligett et al. (2017) for ridge regression. It is a Laplace mechanism that induces noise in the output parameters of the ridge regression. The authors provide a theoretical upper bound on the sensitivity of the ridge regression, which we refer as *sensitivity*, in the experiments.

4.1.1. ***Dataset.***

We conduct experiments on a subset of the 2000 US census dataset published by Ruggles et al. (2015) under Minnesota Population Center in its Integrated Public Use Microdata Series. The census dataset consists of 1% sample of the original census data. It spans over 1.23 million households with records of 2.8 million people. The value of several attributes is not necessarily available for every household. We have therefore selected $212,605$ records, corresponding to the household heads, and 6 attributes, namely, *Age, Gender, Race, Marital Status, Education, Income*, whose values are available for the $212,605$ records.

In order to satisfy the constraint in the derivation of the sensitivity of ridge regression Ligett et al. (2017), we, without loss of generality, normalise the dataset in the following

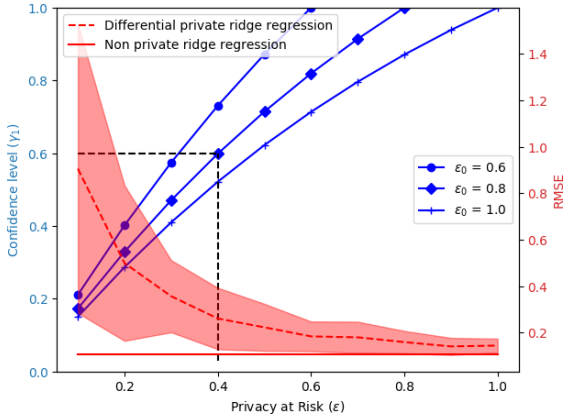


FIGURE 4. Utility, measured by RMSE (right y-axis), and privacy at risk for selected Laplace mechanism (left y-axis) for varying confidence levels

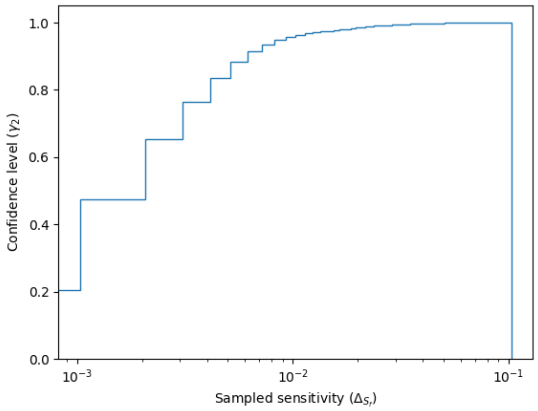


FIGURE 5. Empirical cumulative distribution of sensitivities of ridge regression queries constructed using 15000 samples of neighboring datasets.

way. We normalise *Income* attribute such that the values lie in $[0, 1]$. We normalise other attributes such that l_2 norm of each data point is unity.

4.1.2. ***Experimental Setup***. All experiments are run on Linux machine with 12-core 3.60GHz Intel® Core i7™processor with 64GB memory. Python® 2.7.6 is used as the scripting language.

4.1.3. ***Result Analysis***. We train ridge regression model to predict *Income* using other attributes as predictors. We split the dataset into the training dataset (80%) and testing dataset (20%). We compute the *root mean squared error (RMSE)* of ridge regression, that is trained with the regularisation parameter set to 0.01, on the testing dataset. We use it as the metric of *utility loss*. Smaller the value of RMSE, smaller is the loss in utility. For a given value of privacy at risk level, we conduct 50 runs of an experiment of a differentially private ridge regression and report the means over the 50 runs of the experiment.

Let us now provide illustrative scenarios under the three different cases. In every scenario, the data steward is given a privacy at risk level ϵ and the confidence level γ and wants to disclose the parameters of a ridge regression model that she trains on the census dataset. She needs to calibrate the Laplace mechanism to achieve the privacy at risk required the ridge regression query.

The Case of Explicit Randomness (cf. Section 3.1) In this scenario, the data steward knows the sensitivity for the ridge regression. She needs to compute the privacy level, ϵ_0, to calibrate the Laplace mechanism. She uses Equation 3.2 that links the desired privacy at risk level ϵ, the confidence level γ_1 and the privacy level of noise ϵ_0. Specifically, for given values of ϵ and γ_1, she computes ϵ_0 by solving the equation:

$$\gamma_1 \mathbb{P}(T \leq \epsilon_0) - \mathbb{P}(T \leq \epsilon) = 0.$$

Since the equation does not give an analytical formula for ϵ_0, the data steward uses a root finding algorithm such as Newton-Raphson method, illustrated in Press (2007), to solve the above equation. For instance, if she needs to achieve a privacy at risk level $\epsilon = 0.4$ with confidence level $\gamma_1 = 0.6$, she can substitute these values in the above equation and solve the equation to get the privacy level of noise $\epsilon_0 = 0.8$.

Figure 4 shows the variation of privacy at risk level ϵ and confidence level γ_1. It also depicts the variation of utility loss for different privacy at risk levels in Figure 4. In accordance to the data steward's problem, if she needs to achieve a privacy at risk level $\epsilon = 0.4$ with confidence level $\gamma_1 = 0.6$, she obtains the privacy level of noise to be $\epsilon_0 = 0.8$. Additionally, we observe that the choice of privacy level 0.8 instead of 0.4 to calibrate the Laplace mechanism gives lower utility loss for the data steward. This is the benefit drawn from the risk taken under the control of privacy at risk.

Thus, she uses privacy level ϵ_0 and the sensitivity of the function to calibrate Lapalce mechanism.

The Case of Implicit Randomness (cf. Section 3.2) In this scenario, the data steward does not know the sensitivity of ridge regression. She assesses that she can afford to sample at most n times from the population dataset. She understands the effect of the uncertainty introduced by the statistical estimation of the sensitivity. Therefore, she uses the confidence level for empirical privacy at risk $\hat{\gamma_2}$.

Given the value of n, she chooses the value of the accuracy parameter using Figure 2. For instance, if the number of samples that she can draw is $10,000$, she chooses the value of the accuracy parameter $\rho = 0.01$. Next, she uses Equation 4.1 to determine the value of probabilistic tolerance, α, for the sample size n. For instance, if the data steward is not allowed to access more than $15,000$ samples, for the accuracy of 0.01 the probabilistic tolerance is 0.9.

$$\alpha = 1 - 2e^{(-2\rho^2 n)} \tag{4.1}$$

She constructs an empirical cumulative distribution over the sensitivities as described in Section 3.2. Such an empirical cumulative distribution is shown in Figure 5. Using the computed probabilistic tolerance and desired confidence level $\hat{\gamma_2}$, she uses equation in Theorem 3.3 to determine γ_2. She computes the sampled sensitivity using the empirical distribution function and the confidence level for privacy Δ_{S_f} at risk γ_2. For instance, using the empirical cumulative distribution in Figure 5 she calculates the value of the sampled sensitivity to be approximately 0.001 for $\gamma_2 = 0.4$ and approximately 0.01 for $\gamma_2 = 0.85$

Thus, she uses privacy level ϵ, sets the number of samples to be n and computes the sampled sensitivity Δ_{S_f} to calibrate the Laplace mechanism.

The Case of Explicit and Implicit Randomness (cf. Section 3.3) In this scenario, the data steward does not know the sensitivity of ridge regression. She is not allowed to sample more than n times from a population dataset. For a given confidence level γ_2 and the privacy at risk ϵ, she calibrates the Laplace mechanism using illustration for Section 3.3. The privacy level in this calibration yields utility loss that is more than her requirement. Therefore, she wants to re-calibrate the Laplace mechanism in order to reduce utility loss.

For the recalibration, the data steward uses privacy level of the pre-calibrated Laplace mechanism, i.e. ϵ, as the privacy at risk level and she provides a new confidence level for empirical privacy at risk $\hat{\gamma_3}$. Using Equation C.4 and Equation C.2, she calculates:

$$\hat{\gamma_3}\mathbb{P}(T \leq \eta\epsilon_0) - \alpha\gamma_2\ \mathbb{P}(T \leq \epsilon) = 0$$

She solves such an equation for ϵ_0 using the root finding technique such as Newton-Raphson method in Press (2007). For instance, if she needs to achieve a privacy at risk level $\epsilon = 0.4$ with confidence levels $\hat{\gamma}_3 = 0.9$ and $\gamma_2 = 0.9$, she can substitute these values and the values of tolerance parameter and sampled sensitivity, as used in the previous experiments, in the above equation. Then, solving the equation leads to the privacy level of noise $\epsilon_0 = 0.8$.

Thus, she recalibrates the Laplace mechanism with privacy level ϵ_0, sets the number of samples to be n and sampled sensitivity Δ_{S_f}.

4.2. **Minimising compensation budget.** Many service providers collect users' data to enhance user experience. In order to avoid misuse of this data, we require a legal framework that not only limits the use of the collected data but also proposes reparative measures in case of a data leak. General Data Protection Regulation (GDPR)[1] is such a legal framework. Starting from May 2018, every business entity that holds or processes data of EU citizens, irrespective of the geographical location of the entity itself, must comply with GDPR.

Section 82 in GDPR states that any person who suffers from material or non-material damage as a result of a personal data breach has the right to demand compensation from the data processor. Therefore, every GDPR compliant business entity that either holds or processes personal data needs to secure a certain budget in the worst case scenario of the personal data breach. In order to reduce the risk of such an unfortunate event, the business entity may use privacy-preserving mechanisms that provide provable privacy guarantees while publishing their results. In order to calculate the compensation budget for a business entity, we devise a cost model that maps the privacy guarantees provided by differential privacy and privacy at risk to monetary costs. The discussions demonstrate the usefulness of privacy at risk over differential privacy to reduce expenditure.

4.2.1. ***Cost model for differential privacy.*** Let E be the compensation budget that a business entity has to pay to every stakeholder in case of a personal data breach when the data is processed without any provable privacy guarantees. Let E_ϵ^{dp} be the compensation budget that a business entity has to pay to every stakeholder in case of a personal data breach when the data is processed with privacy guarantees in terms of ϵ-differential privacy.

Privacy level, ϵ, in ϵ-differential privacy is the quantifier of indistinguishability of the outputs of a privacy-preserving mechanism when two neighbouring datasets are provided as inputs. When the privacy level is zero, the privacy-preserving mechanism outputs all results with equal probability. The indistinguishability reduces with increase in the privacy level. Thus, privacy level of zero bears the lowest risk of personal data breach and the risk increases with the privacy level. E_ϵ^{dp} needs to be commensurate to such a risk and, therefore, it needs to satisfy the following constraints.

- For all $\epsilon \in \mathbb{R}^{\geq 0}$, $E_\epsilon^{dp} \leq E$.
- E_ϵ^{dp} is a monotonically increasing function of ϵ.
- As $\epsilon \to 0$, $E_\epsilon^{dp} \to E_{min}$ where E_{min} is the unavoidable cost that business entity might need to pay in case of personal data breach even after the privacy measures are employed.
- As $\epsilon \to \infty$, $E_\epsilon^{dp} \to E$.

[1] https://eugdpr.org/

There are various functions that satisfy these constraints. In absence of any further constraints, we model E_ϵ^{dp} as defined in Equation 4.2.

$$E_\epsilon^{dp} \triangleq E_{min} + Ee^{-\frac{c}{\epsilon}} \tag{4.2}$$

E_ϵ^{dp} has two parameters, namely $c > 0$ and $E_{min} \geq 0$. c controls the rate of change in the cost as the privacy level changes and E_{min} is a privacy level independent bias. For this study, we use a simplified model with $c = 1$ and $E_{min} = 0$.

4.2.2. ***Cost model for privacy at risk.*** Let, $E_{\epsilon_0}^{par}(\epsilon, \gamma)$ be the compensation that a business entity has to pay to every stakeholder in case of a personal data breach when the data is processed with an ϵ_0-differentially private privacy-preserving mechanism but a (ϵ, γ)-privacy at risk guarantee is provided.

In Section 3, we define privacy at risk as a refinement over the existing privacy definition of differential privacy. Privacy at risk provides a quantifiable probabilistic privacy guarantees for a privacy-preserving mechanism. Any ϵ_0-differentially private privacy-preserving mechanism that satisfies (ϵ, γ)-privacy at risk is ϵ-differentially private with probability at most γ and ϵ_0-differentially private with probability $(1 - \gamma)$. Thus, we calculate $E_{\epsilon_0}^{par}$ using Equation 4.3.

$$E_{\epsilon_0}^{par}(\epsilon, \gamma) \triangleq \gamma E_\epsilon^{dp} + (1 - \gamma)E_{\epsilon_0}^{dp} \tag{4.3}$$

4.2.3. ***Existence of minimum compensation budget.*** We want to find the privacy at risk level, say ϵ_{min}, that yields the lowest compensation budget. We do that by minimising Equation 4.3 with respect to ϵ.

Lemma 4.1. *$E_{\epsilon_0}^{par}(\epsilon, \gamma)$ is a convex function of ϵ.*

By Lemma 4.1, there exists a unique ϵ_{min} that minimises the compensation budget for a given privacy level ϵ_0. Since the confidence level γ in Equation 4.3 is a function of privacy at risk level ϵ, analytical calculation of ϵ_{min} is not possible in the most general case. When the output of the query is a real number, we derive the analytic form (Equation 3.3) to compute the confidence level under the consideration of explicit randomness. In such a case, ϵ_{min} is calculated by differentiating Equation 4.3 with respect to ϵ and equating it to zero. It gives us Equation 4.4 that we solve using any root finding technique such as Newton-Raphson method[Press (2007)] to compute ϵ_{min}.

$$\frac{1}{\epsilon} - \ln\left(1 - \frac{1 - e^\epsilon}{\epsilon^2}\right) = \frac{1}{\epsilon_0} \tag{4.4}$$

4.2.4. ***Illustration.*** Suppose that the health centre in a university that complies to GDPR publishes statistics of its staff health checkup, such as obesity statistics, twice in a year. In January 2018, the health centre publishes that 34 out of 99 faculty members suffer from obesity. In July 2018, the health centre publishes that 35 out of 100 faculty members suffer from obesity. An intruder, perhaps an analyst working for an insurance company, checks the staff listings in January 2018 and July 2018, which are publicly available on website of the university. The intruder does not find any change other than the recruitment of John Doe in April 2018. Thus, with high probability, the intruder deduces that John Doe suffers from obesity. In order to avoid such a privacy breach, the health centre decides to publish the

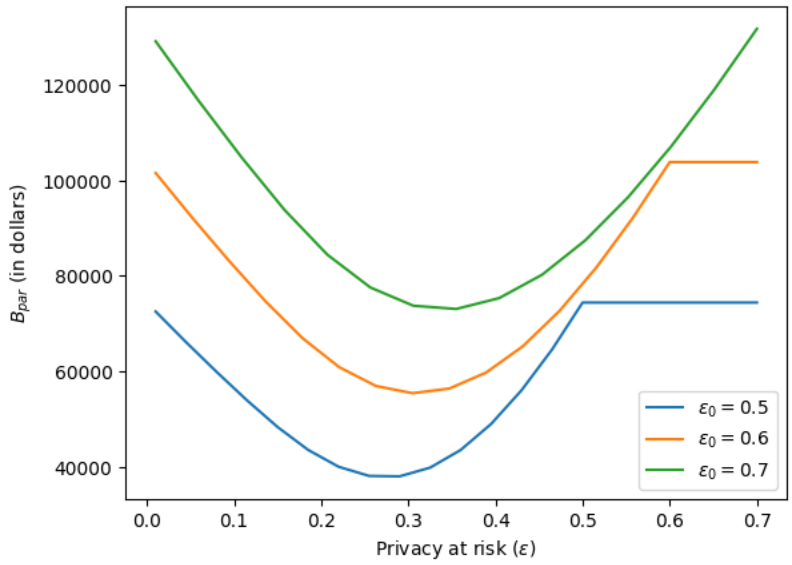


FIGURE 6. Variation in the budget for Laplace mechanism $\mathcal{L}^1_{\epsilon_0}$ under privacy at risk considering explicit randomness in the Laplace mechanism for the illustration in Section 4.2.4.

results using the Laplace mechanism. In this case, the Laplace mechanism operates on the count query.

In order to control the amount of noise, the health centre needs to appropriately set the privacy level. Suppose that the health centre decides to use the expected mean absolute error, defined in Equation 4.5, as the measure of *effectiveness* for the Laplace mechanism.

$$\mathbb{E}\left[|\mathcal{L}^1_\epsilon(x) - f(x)|\right] = \frac{1}{\epsilon} \tag{4.5}$$

Equation 4.5 makes use of the fact that the sensitivity of the count query is one. Suppose that the health centre requires the expected mean absolute error of at most two in order to maintain the quality of the published statistics. In this case, the privacy level has to be at least 0.5.

In order to compute the budget, the health centre requires an estimate of E. Moriarty et al. (2012) show that the incremental cost of premiums for the health insurance with morbid obesity ranges between \$5467 to \$5530. With reference to this research, the health centre takes \$5500 as an estimate of E. For the staff size of 100 and the privacy level 0.5, the health centre uses Equation 4.2 in its simplified setting to compute the total budget of \$74434.40.

Is it possible to reduce this budget without degrading the effectiveness of the Laplace mechanism? In Section 3, we study privacy at risk of an ϵ_0-differentially private Laplace mechanism. Under the consideration of the explicit randomness introduced by the Laplace noise distribution, we show that ϵ_0-differentially private Laplace mechanism satisfies (ϵ, γ)-privacy at risk. γ is computed using the formula in Theorem 3.2. In Figure 6, we plot the budget for various privacy at risk levels. We observe that the privacy at risk level 0.274, which is same as ϵ_{min} computed by solving Equation 4.4, yields the lowest compensation

budget of $37805.86. Thus, by using privacy at risk, the health centre is able to save $36628.532 without sacrificing the quality of the published results.

4.2.5. ***Bounds on the privacy at risk level.*** For a fixed budget, say B, re-arrangement of Equation 4.3 gives us an upper bound on the privacy at risk level ϵ. We use the cost model with $c = 1$ and $E_{min} = 0$ to derive the upper bound. If we have a maximum permissible expected mean absolute error T, we use Equation 4.5 to obtain a lower bound on the privacy at risk level. Equation 4.6 illustrates the upper and lower bounds that dictate the permissible range of ϵ that a data publisher can promise depending on the budget and the permissible error constraints.

$$\frac{1}{T} \leq \epsilon \leq \left[\ln \left(\frac{\gamma E}{B - (1-\gamma) E_{\epsilon_0}^{dp}} \right) \right]^{-1} \tag{4.6}$$

Thus, the privacy at risk is constrained by the effectiveness requirement from below and by the monetary budget from above. Hsu et al. (2014) calculate upper and lower bound on the privacy level in the differential privacy. They use a different cost model owing to the scenario of research study that compensates its participants for their data and releases the results in a differentially private manner. Their cost model is different than our GDPR inspired modelling.

5. Related Work

Researchers have proposed different privacy-preserving mechanisms to make different queries differentially private. These mechanisms can be broadly classified into two categories. In one category, the mechanisms explicitly add calibrated noise, such as Laplace noise in the work of Dwork et al. (2006c) or Gaussian noise in the work of Dwork et al. (2014), to the outputs of the query. In the other category, Acs et al. (2012); Chaudhuri et al. (2011); Hall et al. (2013); Zhang et al. (2012) propose mechanisms that alter the query function so that the modified function satisfies differentially privacy. Privacy-preserving mechanisms in both of these categories perturb the original output of the query and make it difficult for a malicious data analyst to recover the original output of the query. These mechanisms induce randomness using the explicit noise distribution. Calibration of these mechanisms require the knowledge of the sensitivity of the query. Nissim et al. (2007) consider the implicit randomness in the data-generation distribution to compute an estimate of the sensitivity. The authors propose the smooth sensitivity function that is an envelope over the local sensitivities for all individual datasets. Local sensitivity of a dataset is the maximum change in the value of the query over all of its neighboring datasets. In general, it is not easy to analytically estimate the smooth sensitivity function for a general query. Rubinstein and Aldà (2017) also study the inherent randomness in the data-generation algorithm. They do not use the local sensitivity. We adopt their approach of sampling the sensitivity from the empirical distribution of the sensitivity. They use order statistics to choose a particular value of the sensitivity. We use the confidence level, which provides a mediation tool for business entities to assess the actual business risks, on the sensitivity distribution to estimate the sensitivity.

In order to account for both sources of randomness, refinements of ϵ-differential privacy are proposed in order to bound the probability of occurrence of worst case scenarios. Machanavajjhala et al. (2008) propose probabilistic differential privacy that considers

upper bounds of the worst case privacy loss for corresponding confidence levels on the noise distribution. Definition of probabilistic differential privacy incorporates the explicit randomness induced by the noise distribution and bounds the probability over the space of noisy outputs to satisfy the ϵ-differential privacy definition. Dwork and Rothblum (2016) propose Concentrated differential privacy that considers the expected values of the privacy loss for the corresponding confidence levels on the noise distribution. Definition of concentrated differential privacy incorporates the explicit randomness induced by the noise distribution but considering only the expected value of privacy loss satisfying ϵ-differential privacy definition instead of using the confidence levels limits its scope.

Hall et al. (2013) propose random differential privacy that considers the privacy loss for corresponding confidence levels on the implicit randomness in the data-generation distribution. Definition of random differential privacy incorporates the implicit randomness induced by the data-generation distribution and bounds the probability over the space of datasets generated from the given distribution to satisfy the ϵ-differential privacy definition. Dwork et al. (2006a) define approximate differential privacy by adding a constant bias to the privacy guarantee provided by the differential privacy. It is not a probabilistic refinement of the differential privacy.

In this work, we consider the widely used Laplace mechanism proposed by Dwork et al. (2006c). The Laplace mechanism adds Laplacian noise to the query output. Acs et al. (2012); Xiao et al. (2011); Zhang et al. (2012) use Laplace mechanism by providing the calibration by computing senstivity of the query.

Chen et al. (2016); Ghosh and Roth (2015) propose game theoretic methods that provide the means to evaluate the monetory cost of differential privacy. Our approach is inspired by the approach by the work of Hsu et al. (2014). They model the cost under a scenario of a research study wherein the participants are reimbursed for their participation. Our cost modelling is driven by the scenario of securing a compensation budget in compliance with GDPR. Our requirement differs from the requirements for the scenario in the work of Hsu et al. (2014). In our case, there is no monetary incentive for participants to share their data.

6. Conclusion and Future Works

We propose privacy at risk that quantifies the probability with which a privacy-preserving mechanism satisfies differential privacy for a specified privacy level. The probabilistic quantification depends on two sources of randomness, the explicit randomness induced by the noise distribution and the implicit randomness induced by the data-generation distribution, and the coupling between the two. We instantiate privacy at risk for the Laplace mechanism.

We demonstrate the applicability of privacy at risk in two decision-making problems. Firstly, we illustrate the use of privacy at risk by a data steward to balance the privacy-utility trade-off. Secondly, we propose a cost model that bridges the gap between the privacy level and the compensation budget estimated by a GDPR compliant business entity. We show the existence of a privacy level that yields the minimum compensation budget under the cost model of privacy at risk. Thus, privacy at risk not only quantifies privacy level for a given privacy-preserving mechanism but also facilitates minimisation of monetary risk under the proposed cost model.

Privacy at risk may be fully analytically computed in cases where the data-generation, or the sensitivity distribution, the noise distribution and the query are analytically known and take convenient forms. We are now looking at such convenient but realistic cases.

Acknowledgement

This project is supported by the National Research Foundation, Singapore Prime Minister's Office under its Corporate Laboratory@University Scheme between National University of Singapore and Singapore Telecommunications Ltd.

References

Acs, G., Castelluccia, C., and Chen, R. (2012). Differentially private histogram publishing through lossy compression. In *Data Mining (ICDM), 2012 IEEE 12th International Conference on*, pages 1–10. IEEE.

Askey, R. and Daalhuis, A. O. (2010). Generalized hypergeometric functions and meijer g-function. *NIST handbook of mathematical functions*, pages 403–418.

Chaudhuri, K., Monteleoni, C., and Sarwate, A. D. (2011). Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12(Mar):1069–1109.

Chen, Y., Chong, S., Kash, I. A., Moran, T., and Vadhan, S. (2016). Truthful mechanisms for agents that value privacy. *ACM Transactions on Economics and Computation (TEAC)*, 4(3):13.

Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., and Naor, M. (2006a). Our data, ourselves: Privacy via distributed noise generation. In *Eurocrypt*, volume 4004, pages 486–503. Springer.

Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006b). Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference*, pages 265–284. Springer.

Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006c). *Calibrating Noise to Sensitivity in Private Data Analysis*, pages 265–284. Springer Berlin Heidelberg, Berlin, Heidelberg.

Dwork, C., Roth, A., et al. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407.

Dwork, C. and Rothblum, G. N. (2016). Concentrated differential privacy. *arXiv preprint arXiv:1603.01887*.

Garfinkel, S. L., Abowd, J. M., and Powazek, S. (2018). Issues encountered deploying differential privacy. *arXiv preprint arXiv:1809.02201*.

Ghosh, A. and Roth, A. (2015). Selling privacy at auction. *Games and Economic Behavior*, 91:334–346.

Hall, R., Rinaldo, A., and Wasserman, L. (2012). Random differential privacy. *Journal of Privacy and Confidentiality*, 4(2):43–59.

Hall, R., Rinaldo, A., and Wasserman, L. (2013). Differential privacy for functions and functional data. *Journal of Machine Learning Research*, 14(Feb):703–727.

Hsu, J., Gaboardi, M., Haeberlen, A., Khanna, S., Narayan, A., Pierce, B. C., and Roth, A. (2014). Differential privacy: An economic method for choosing epsilon. In *Computer Security Foundations Symposium (CSF), 2014 IEEE 27th*, pages 398–410. IEEE.

Jorion, P. (2000). Value at risk: The new benchmark for managing financial risk.

Lee, J. and Clifton, C. (2011). How much is enough? choosing ε for differential privacy. In *International Conference on Information Security*, pages 325–340. Springer.

Ligett, K., Neel, S., Roth, A., Waggoner, B., and Wu, S. Z. (2017). Accuracy first: Selecting a differential privacy level for accuracy constrained erm. In *Advances in Neural Information Processing Systems*, pages 2563–2573.

Machanavajjhala, A., Kifer, D., Abowd, J., Gehrke, J., and Vilhuber, L. (2008). Privacy: Theory meets practice on the map. In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*, pages 277–286. IEEE.

Massart, P. et al. (1990). The tight constant in the dvoretzky-kiefer-wolfowitz inequality. *The annals of Probability*, 18(3):1269–1283.

Moriarty, J. P., Branda, M. E., Olsen, K. D., Shah, N. D., Borah, B. J., Wagie, A. E., Egginton, J. S., and Naessens, J. M. (2012). The effects of incremental costs of smoking and obesity on health care costs among adults: a 7-year longitudinal study. *Journal of Occupational and Environmental Medicine*, 54(3):286–291.

Murphy, K. P. (2012). *Machine Learning: A Probabilistic Perspective*. The MIT Press.

Nissim, K., Raskhodnikova, S., and Smith, A. (2007). Smooth sensitivity and sampling in private data analysis. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 75–84. ACM.

Papoulis, A. and Pillai, S. U. (2002). *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education.

Press, W. H. (2007). *Numerical recipes 3rd edition: The art of scientific computing*. Cambridge university press.

Rubinstein, B. I. and Aldà, F. (2017). Pain-free random differential privacy with sensitivity sampling. In *International Conference on Machine Learning*, pages 2950–2959.

Ruggles, S., Genadek, K., Goeken, R., Grover, J., and Sobek, M. (2015). Integrated public use microdata series: Version 6.0 [dataset].

Xiao, X., Wang, G., and Gehrke, J. (2011). Differential privacy via wavelet transforms. *IEEE Transactions on Knowledge and Data Engineering*, 23(8):1200–1214.

Zhang, J., Zhang, Z., Xiao, X., Yang, Y., and Winslett, M. (2012). Functional mechanism: regression analysis under differential privacy. *Proceedings of the VLDB Endowment*, 5(11):1364–1375.

Appendix A. Proof of Theorem 3.2

Although a Laplace mechanism $\mathcal{L}_{\epsilon}^{\Delta_f}$ induces higher amount of noise on average than a Laplace mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$ for $\epsilon < \epsilon_0$, there is a non-zero probability that $\mathcal{L}_{\epsilon}^{\Delta_f}$ induces noise commensurate to $\mathcal{L}_{\epsilon_0}^{\Delta_f}$. This non-zero probability guides us to calculate the confidence level γ_1 for the privacy at risk level ϵ. In order to get an intuition, we illustrate the calculation of the overlap between two Laplace distributions as an estimator of similarity between the two distributions.

Definition A.1 (**Overlap of Distributions, Papoulis and Pillai (2002)**)**.** The overlap, O, between two probability distributions P_1, P_2 with support $\mathcal{X}$ is defined as

$$O = \int_{\mathcal{X}} \min[P_1(x), P_2(x)]\ dx.$$

Lemma A.2. *The overlap O between two probability distributions,* $\text{Lap}(\frac{\Delta_f}{\epsilon_1})$ *and* $\text{Lap}(\frac{\Delta_f}{\epsilon_2})$*, such that $\epsilon_2 \leq \epsilon_1$, is given by*

$$O = 1 - (\exp(-\mu\epsilon_2/\Delta_f) - \exp(-\mu\epsilon_1/\Delta_f)),$$

where $\mu = \frac{\Delta_f \ln(\epsilon_1/\epsilon_2)}{\epsilon_1 - \epsilon_2}$.

Using the result in Lemma A.2, we note that the overlap between two distributions with $\epsilon_0 = 1$ and $\epsilon = 0.6$ is 0.81. Thus, $\mathcal{L}_{0.6}^{\Delta_f}$ induces noise that is more than 80% times similar to the noise induced by $\mathcal{L}_{1.0}^{\Delta_f}$. Therefore, we can loosely say that at least 80% of the times a Laplace Mechanism $\mathcal{L}_{1.0}^{\Delta_f}$ will provide the same privacy as a Laplace Mechanism $\mathcal{L}_{0.8}^{\Delta_f}$.

Although the overlap between Laplace distributions with different scales offers an insight into the relationship between different privacy level and the privacy at risk level, it does not capture the constraint induced by the *sensitivity*. For a given query f, the amount of noise required to satisfy differential privacy is commensurate to the sensitivity of the query. This calibration puts a constraint on the noise that is required to be induced on a pair of neighbouring datasets. We state this constraint in Lemma A.3, which we further use to prove that the Laplace Mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$ satisfies (ϵ, γ_1)-privacy at risk.

Lemma A.3. *For a Laplace Mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$, the difference in the absolute values of noise induced on a pair of neighbouring datasets is upper bounded by the sensitivity of the query.*

Proof. Suppose that two neighbouring datasets x and y are given input to a numeric query $f : \mathcal{D} \to \mathbb{R}^k$. For any output $z \in \mathbb{R}^k$ of the Laplace Mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$,

$$\begin{aligned}\sum_{i=1}^{k} (|f(y_i) - z_i| - |f(x_i) - z_i|) &\leq \sum_{i=1}^{k} (|f(x_i) - f(y_i)|) \\ &\leq \Delta_f.\end{aligned}$$

We use triangular inequality in the first step and Definition 2.2 of sensitivity in the second step. □

We write $\text{Exp}(b)$ to denote a random variable sampled from an *exponential distribution* with scale $b > 0$. We write $\text{Gamma}(k, \theta)$ to denote a random variable sampled from a *gamma distribution* with shape $k > 0$ and scale $\theta > 0$.

Lemma A.4 (**Papoulis and Pillai (2002)**). *If a random variable X follows Laplace Distribution with mean zero and scale b, $|X| \sim \text{Exp}(b)$.*

Lemma A.5 (**Papoulis and Pillai (2002)**). *If $X_1, ..., X_n$ are n i.i.d. random variables each following the Exponential Distribution with scale b, $\sum_{i=1}^{n} X_i \sim$ Gamma(n, b).*

Lemma A.6. *If X_1 and X_2 are two i.i.d. Gamma(n, θ) random variables, the probability density function for the random variable $T = |X_1 - X_2|/\theta$ is given by*

$$P_T(t) = \frac{2^{2-n} t^{n-\frac{1}{2}} K_{n-\frac{1}{2}}(t)}{\sqrt{2\pi}\Gamma(n)}$$

where $K_{n-\frac{1}{2}}$ is the modified Bessel function of second kind.

Proof. Let X_1 and X_2 be two i.i.d. Gamma(n, θ) random variables. Characteristic function of a Gamma random variable is given as

$$\phi_{X_1}(z) = \phi_{X_2}(z) = (1 - \iota z\theta)^{-n}.$$

Therefore,

$$\phi_{X_1 - X_2}(z) = \phi_{X_1}(z)\phi^*_{X_2}(z) = \frac{1}{(1 + (z\theta)^2)^n}$$

Probability density function for the random variable $X_1 - X_2$ is given by,

$$\begin{aligned} P_{X_1 - X_2}(x) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{-\mathrm{i}zx} \phi_{X_1 - X_2}(z) dz \\ &= \frac{2^{1-n} |\frac{x}{\theta}|^{n-\frac{1}{2}} K_{n-\frac{1}{2}}(|\frac{x}{\theta}|)}{\sqrt{2\pi}\Gamma(n)\theta} \end{aligned}$$

where $K_{n-\frac{1}{2}}$ is the Bessel function of second kind. Let, $T = |\frac{X_1 - X_2}{\theta}|$. Therefore,

$$P_T(t) = \frac{2^{2-n} t^{n-\frac{1}{2}} K_{n-\frac{1}{2}}(t)}{\sqrt{2\pi}\Gamma(n)}$$

We denote this probability distribution as $\text{BesselK}(n, \theta)$. □

Lemma A.7. *If X_1 and X_2 are two i.i.d. Gamma(n, θ) random variables and $|X_1 - X_2| \leq M$, then $T' = |X_1 - X_2|/\theta$ follows Truncated BesselK(n, θ, M) distribution with probability density function:*

$$P_{T'}(t') = \frac{P_T(t')}{P_T(T \leq M)},$$

where P_T is the probability density function of $\text{BesselK}(n, \theta)$.

Lemma A.8. *For Laplace Mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$ with query $f : \mathcal{D} \to \mathbb{R}^k$ and for any output $Z \subseteq$ Range$(\mathcal{L}_{\epsilon_0}^{\Delta_f})$, $\epsilon \leq \epsilon_0$,*

$$\gamma_1 \triangleq \mathbb{P}\left[\log\left|\frac{\mathbb{P}(\mathcal{L}_{\epsilon_0}^{\Delta_f}(x) \in Z)}{\mathbb{P}(\mathcal{L}_{\epsilon_0}^{\Delta_f}(y) \in Z)}\right| \leq \epsilon\right] = \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \epsilon_0)},$$

where T follows $\text{BesselK}(k, \Delta_f/\epsilon_0)$.

Proof. Let, $x \in \mathcal{D}$ and $y \in \mathcal{D}$ be two datasets such that $x \sim y$. Let $f : \mathcal{D} \to \mathbb{R}^k$ be some numeric query. Let $\mathbb{P}_x(z)$ and $\mathbb{P}_y(z)$ denote the probabilities of getting the output z for Laplace mechanisms $\mathcal{L}_{\epsilon_0}^{\Delta_f}(x)$ and $\mathcal{L}_{\epsilon_0}^{\Delta_f}(y)$ respectively. For any point $z \in \mathbb{R}^k$ and $\epsilon \neq 0$,

$$\begin{aligned}\frac{\mathbb{P}_x(z)}{\mathbb{P}_y(z)} &= \prod_{i=1}^{k} \frac{\exp\left(\frac{-\epsilon_0|f(x_i)-z_i|}{\Delta_f}\right)}{\exp\left(\frac{-\epsilon_0|f(y_i)-z_i|}{\Delta_f}\right)} \\ &= \prod_{i=1}^{k} \exp\left(\frac{\epsilon_0(|f(y_i)-z_i| - |f(x_i)-z_i|)}{\Delta_f}\right) \\ &= \exp\left(\epsilon\left[\frac{\epsilon_0 \sum_{i=1}^{k}(|f(y_i)-z_i| - |f(x_i)-z_i|)}{\epsilon\Delta_f}\right]\right). \end{aligned} \tag{A.1}$$

By Definition 2.4,

$$(f(x)-z), (f(y)-z) \sim \text{Lap}(\Delta_f/\epsilon_0). \tag{A.2}$$

Application of Lemma A.4 and Lemma A.5 yields,

$$\sum_{i=1}^{k} (|f(x_i)-z_i|) \sim \text{Gamma}(k, \Delta_f/\epsilon_0). \tag{A.3}$$

Using Equations A.2, A.3, and Lemma A.3, A.7, we get

$$\left(\frac{\epsilon_0}{\Delta_f}\sum_{i=1}^{k} |(|f(y_i)-z| - |f(x_i)-z|)|\right) \sim \text{TruncatedBesselK}(k, \Delta_f/\epsilon_0, \Delta_f). \tag{A.4}$$

since, $\sum_{i=1}^{k} |(|f(y_i)-z| - |f(x_i)-z|)| \leq \Delta_f$. Therefore,

$$\mathbb{P}\left(\left[\frac{\epsilon_0}{\Delta_f}\sum_{i=1}^{k} |(|f(y_i)-z| - |f(x_i)-z|)|\right] \leq \epsilon\right) = \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \epsilon_0)}, \tag{A.5}$$

where T follows $\text{BesselK}(k, \Delta_f/\epsilon_0)$. Analytically,

$$\mathbb{P}(T \leq x) \propto \left[{}_1F_2(\frac{1}{2}; \frac{3}{2}-k, \frac{3}{2}; \frac{x^2}{4})\sqrt{\pi}4^k x - 2{}_1F_2(k; \frac{1}{2}+k, k+1; \frac{x^2}{4})x^{2k}\Gamma(k)\right],$$

where ${}_1F_2$ is the regularised generalised hypergeometric function as defined in Askey and Daalhuis (2010). From Equation A.1 and A.5,

$$\mathbb{P}\left[\log\left|\frac{\mathbb{P}(\mathcal{L}_{\epsilon_0}(x) \in S)}{\mathbb{P}(\mathcal{L}_{\epsilon_0}(y) \in S)}\right| \leq \epsilon\right] = \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \epsilon_0)}.$$

□

This completes the proof of Theorem 3.2.

Corollary A.9. *Laplace Mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_f}$ with $f : \mathcal{D} \to \mathbb{R}^k$ is (ϵ, δ)-probabilistically differentially private where*

$$\delta = \begin{cases} 1 - \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \epsilon_0)} & \epsilon \leq \epsilon_0 \\ 0 & \epsilon > \epsilon_0 \end{cases}$$

and T follows $\text{BesselK}(k, \Delta_f/\epsilon_0)$.

Appendix B. Proof of Theorem 3.3

Proof. Let, x and y be any two neighbouring datasets sampled from the data generating distribution $\mathcal{G}$. Let, Δ_{S_f} be the sampled sensitivity for query $f : \mathcal{D} \to \mathbb{R}^k$. Let, $\mathbb{P}_x(z)$ and $\mathbb{P}_y(z)$ denote the probabilities of getting the output z for Laplace mechanisms $\mathcal{L}_\epsilon^{\Delta_{S_f}}(x)$ and $\mathcal{L}_\epsilon^{\Delta_{S_f}}(y)$ respectively. For any point $z \in \mathbb{R}^k$ and $\epsilon \neq 0$,

$$\begin{aligned}
\frac{\mathbb{P}_x(z)}{\mathbb{P}_y(z)} &= \prod_{i=1}^{k} \frac{\exp\left(\frac{-\epsilon|f(x_i)-z_i|}{\Delta_{S_f}}\right)}{\exp\left(\frac{-\epsilon|f(y_i)-z_i|}{\Delta_{S_f}}\right)} \\
&= \exp\left(\frac{\epsilon \sum_{i=1}^{k}(|f(y_i)-z_i| - |f(x_i)-z_i|)}{\Delta_{S_f}}\right) \\
&\leq \exp\left(\frac{\epsilon \sum_{i=1}^{k}|f(y_i)-f(x_i)|}{\Delta_{S_f}}\right) \\
&= \exp\left(\frac{\epsilon\|f(y)-f(x)\|_1}{\Delta_{S_f}}\right) \qquad \text{(B.1)}
\end{aligned}$$

We used triangle inequality in the penultimate step.

Using the trick in the work of Rubinstein and Aldà (2017), we define following events. Let, $B^{\Delta_{S_f}}$ denotes the set of pairs neighbouring dataset sampled from $\mathcal{G}$ for which the sensitivity random variable is upper bounded by Δ_{S_f}. Let, $C_\rho^{\Delta_{S_f}}$ denotes the set of sensitivity random variable values for which F_n deviates from the unknown cumulative distribution of S, F, at most by the accuracy value ρ. These events are defined in Equation B.2.

$$\begin{aligned}
B^{\Delta_{S_f}} &\triangleq \{x, y \sim \mathcal{G} \text{ such that } \|f(y)-f(x)\|_1 \leq \Delta_{S_f}\} \\
C_\rho^{\Delta_{S_f}} &\triangleq \left\{\sup_{\Delta} |F_S^n(\Delta) - F_S(\Delta)| \leq \rho\right\} \qquad \text{(B.2)}
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}(B^{\Delta_{S_f}}) &= \mathbb{P}(B^{\Delta_{S_f}}|C_\rho^{\Delta_{S_f}})\mathbb{P}(C_\rho^{\Delta_{S_f}}) + \mathbb{P}(B^{\Delta_{S_f}}|\overline{C\rho^{\Delta_{S_f}}})\mathbb{P}(\overline{C_\rho^{\Delta_{S_f}}}) \\
&\geq \mathbb{P}(B^{\Delta_{S_f}}|C_\rho^{\Delta_{S_f}})\mathbb{P}(C_\rho^{\Delta_{S_f}}) \\
&= F_n(\Delta_{S_f})\mathbb{P}(C_\rho^{\Delta_{S_f}}) \\
&\geq \gamma_2 \cdot (1 - 2e^{-2\rho^2 n}) \qquad \text{(B.3)}
\end{aligned}$$

In the last step, we use the definition of the sampled sensitivity to get the value of the first term. The last term is obtained using DKW-inequality, as defined in Massart et al. (1990), where the n denotes the number of samples used to build empirical distribution of the sensitivity, F_n.

From Equation B.1, we understand that if $\|f(y) - f(x)\|_1$ is less than or equals to the sampled sensitivity then the Laplace mechanism $\mathcal{L}_\epsilon^{\Delta_{S_f}}$ satisfies ϵ-differential privacy. Equation B.3 provides the lower bound on the probability of the event $\|f(y)-f(x)\|_1 \leq \Delta_{S_f}$. Thus, combining Equation B.1 and Equation B.3 completes the proof. □

Appendix C. Proof of Theorem 3.5

In addition to the events defined in Equation B.2, we define an additional event $A_{\epsilon_0}^{\Delta_{S_f}}$, defined in Equation C.1, as a set of outputs of Laplace mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}$ that satisfy the constraint of ϵ-differential privacy for a specified privacy at risk level ϵ.

$$A_{\epsilon_0}^{\Delta_{S_f}} \triangleq \left\{ z \sim \mathcal{L}_{\epsilon_0}^{\Delta_{S_f}} \ : \ \log \left| \frac{\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}(x)}{\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}(y)} \right| \leq \epsilon, x, y \sim \mathcal{G} \right\} \tag{C.1}$$

Corollary C.1.

$$\mathbb{P}(A_{\epsilon_0}^{\Delta_{S_f}} | B^{\Delta_{S_f}}) = \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \eta\epsilon_0)}$$

where T *follows* $\text{BesselK}(k, \Delta_{S_f}/\epsilon_0)$ *and* $\eta = \frac{\Delta_f}{\Delta_{S_f}}$.

Proof. We provide the sketch of the proof. Proof follows from the proof of Lemma A.8. For a Laplace mechanism calibrated with the sampled sensitivity Δ_{S_f} and privacy level ϵ_0, Equation A.4 translates to,

$$\left(\frac{\epsilon_0}{\Delta_{S_f}} \sum_{i=1}^{k} |(|f(y_i) - z| - |f(x_i) - z|)| \right) \sim \text{Truncated BesselK}(k, \Delta_{S_f}/\epsilon_0, \Delta_f).$$

since, $\sum_{i=1}^{k} |(|f(y_i) - z| - |f(x_i) - z|)| \leq \Delta_f$. Using Lemma A.7 and Equation A.5,

$$\mathbb{P}(A_{\epsilon_0}^{\Delta_{S_f}}) = \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \eta\epsilon_0)}$$

where T follows $\text{BesselK}(k, \Delta_{S_f}/\epsilon_0)$ and $\eta = \frac{\Delta_f}{\Delta_{S_f}}$. □

In this section, we do not assume the knowledge of the sensitivity of the query. Using the empirical estimation presented in Section 3.2, if we choose the sampled sensitivity for confidence level $\gamma_2 = 1$, we obtain an approximation for η.

Lemma C.2. *For a given value of accuracy parameter* ρ,

$$\frac{\Delta_f}{\Delta_{S_f}^*} = 1 + \mathcal{O}\left(\frac{\rho}{\Delta_{S_f}^*} \right)$$

where $\Delta_{S_f}^* = F_n^{-1}(1)$. $\mathcal{O}\left(\frac{\rho}{\Delta_{S_f}^*} \right)$ *denotes order of* $\frac{\rho}{\Delta_{S_f}^*}$, *i.e.,* $\mathcal{O}\left(\frac{\rho}{\Delta_{S_f}^*} \right) = k\frac{\rho}{\Delta_{S_f}^*}$ *for some* $k \geq 1$.

Proof. For a given value of accuracy parameter ρ and any $\Delta > 0$,

$$F_n(\Delta) - F(\Delta) \leq \rho$$

Since above inequality is true for any value of Δ, let $\Delta = F^{-1}(1)$. Therefore,

$$\begin{aligned} F_n(F^{-1}(1)) - F(F^{-1}(1)) &\leq \rho \\ F_n(F^{-1}(1)) &\leq 1 + \rho \end{aligned} \tag{C.2}$$

Since a cumulative distribution function is 1-Lipschitz [Papoulis and Pillai (2002)],

$$|F_n(F_n^{-1}(1)) - F_n(F^{-1}(1))| \leq |F_n^{-1}(1) - F^{-1}(1)|$$
$$|F_n(F_n^{-1}(1)) - F_n(F^{-1}(1))| \leq |\Delta^*_{S_f} - \Delta_f|$$
$$\rho \leq \Delta_f - \Delta^*_{S_f}$$
$$1 + \frac{\rho}{\Delta^*_{S_f}} \leq \frac{\Delta_f}{\Delta^*_{S_f}}$$

where we used result from Equation C.2 in step 3. Introducing $\mathcal{O}\left(\frac{\rho}{\Delta^*_{S_f}}\right)$ completes the proof. □

Lemma C.3. *For Laplace Mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}$ with sampled sensitivity Δ_{S_f} of a query $f : \mathcal{D} \to \mathbb{R}^k$ and for any $Z \subseteq Range(\mathcal{L}_{\epsilon}^{\Delta_{S_f}})$,*

$$\mathbb{P}\left[\log\left|\frac{\mathbb{P}(\mathcal{L}_{\epsilon_0}(x) \in Z)}{\mathbb{P}(\mathcal{L}_{\epsilon_0}(y) \in Z)}\right| \leq \epsilon\right] \geq \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \eta\epsilon_0)}\gamma_2(1 - 2e^{-2\rho^2 n})$$

where n is the number of samples used to find sampled sensitivity, $\rho \in [0, 1]$ is a accuracy parameter and $\eta = \frac{\Delta_f}{\Delta_{S_f}}$. The outer probability is calculated with respect to support of the data-generation distribution $\mathcal{G}$.

Proof. The proof follows from the proof of Lemma A.8 and Lemma C.3. Consider,

$$\mathbb{P}(A_{\epsilon_0}^{\Delta_{S_f}}) \geq \mathbb{P}(A_{\epsilon_0}^{\Delta_{S_f}}|B^{\Delta_{S_f}})\mathbb{P}(B^{\Delta_{S_f}}|C_\rho^{\Delta_{S_f}})\mathbb{P}(C_\rho^{\Delta_{S_f}})$$
$$\geq \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \eta\epsilon_0)} \cdot \gamma_2 \cdot (1 - 2e^{-2\rho^2 n}) \tag{C.3}$$

The first term in the final step of Equation C.3 follows from the result in Corollary C.1 where T follows BesselK$(k, \frac{\Delta_{S_f}}{\epsilon_0})$. It is the probability with which the Laplace mechanism $\mathcal{L}_{\epsilon_0}^{\Delta_{S_f}}$ satisfies ϵ-differential privacy for a given value of sampled sensitivity. □

Probability of occurrence of event $A_{\epsilon_0}^{\Delta_{S_f}}$ calculated by accounting for both explicit and implicit sources of randomness gives the confidence level for privacy at risk level ϵ. Thus, the proof of Lemma C.3 completes the proof for Theorem 3.5.

Comparing the equations in Theorem 3.5 and Lemma C.3, we observe that

$$\gamma_3 \triangleq \frac{\mathbb{P}(T \leq \epsilon)}{\mathbb{P}(T \leq \eta\epsilon_0)} \cdot \gamma_2 \tag{C.4}$$

The confidence level for privacy at risk, as defined in Equation C.4, is free from the term that accounts for the accuracy of sampled estimate. If we know cumulative distribution of the sensitivity, we do not suffer from the uncertainty of introduced by sampling from the empirical distribution.