Context Aware Laplacian Mechanism for Local Information Privacy

Mohamed Seif Ravi Tandon Ming Li
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ, 85721
Email: {*mseif, tandonr, lim*}@email.arizona.edu

***Abstract*—In this paper, we consider the problem of designing additive noise mechanisms for data release subject to a local information privacy constraint. While there has been significant prior work on devising additive noise mechanisms for differential privacy (such as Laplacian and Gaussian mechanisms), for the notion of information privacy, which accounts for prior-knowledge about the data, there are no such general purpose additive noise mechanisms. To this end, we devise a prior-aware Laplacian noise mechanism, which satisfies local information privacy. We show that adding context awareness (i.e., via the knowledge of prior of the data) improves the tradeoff between utility and privacy when compared to context-unaware mechanisms.**

I. Introduction

Differential privacy (DP) [1] has been considered a *de facto* standard notion for private data analysis and aggregation. Intuitively, in DP, an adversary *can not* infer the presence or the absence of an individual contributing to the released output. DP notion has been considered in two contexts: 1) centralized setting, where a trusted service provider releases data; and 2) the localized setting, where a user can locally perturb and disclose the data to an *untrusted* data curator/aggregator. Recently, local privacy setting has gained attention in the literature. Randomized response (RR) [2] was the earliest privacy preserving mechanism used for the local setting. However, the original RR mechanism does not have formal privacy guarantees. To this end, *local differential privacy* (LDP) was proposed as a local variant of DP. In the literature, many schemes were proposed under the LDP notion for private data aggregation such as [3]–[5].

It is worth noting that both localized and centralized DP are context-free privacy notions, i.e., there is no assumption on the underlying prior on data of the users, and thus the privacy guarantees are strong and hold for worst-case settings (any realization of the data). In contrast, context-aware privacy notions such as *mutual information privacy* (MIP) and *information privacy* [6] and *local information privacy* (LIP) [7] consider the priors of users' data in their definitions (also see [8] for a data-driven context-aware privacy definition and references therein). In fact, context-aware notions can lead to mechanisms with better utility-privacy tradeoff by incorporating the priors of users' data. In many applications, prior knowledge about the data is often publicly available, for instance, location data in location-based services and periodic surveys [9].

This work was supported in part by the U.S. NSF through grants CNS-1715947, CAREER-1651492, and CNS-1731164.

For DP, there are well-known *general* purpose mechanisms such as Laplacian [1], exponential [10] and randomized response [3] which have been widely adopted in practice. To the best of our knowledge, general purpose *context-aware* mechanisms have not been explored in the existing literature.

Contributions: The contributions of this paper are summarized as follows: 1) We discuss the approximate case of LIP and its relationship to the approximate LDP. We formally show that (ϵ, δ)-LDP implies (ϵ, δ)-LIP. Conversely, we show that (ϵ, δ)-LIP implies $\left(2\epsilon, \frac{(e^{\epsilon}+1)\delta}{P_{\min}}\right)$-LDP, where $P_{\min} = \min_x P_X(x)$, is the minimum probability over the given data prior. Thus, LIP relaxes LDP notion for the approximate case as well. 2) We then present a context-aware Laplacian mechanism which satisfies $(\epsilon, 0)$-LIP for the *local* privacy setting. The notion of context-awareness is incorporated by taking into account the prior knowledge of user's data. More specifically, the additive Laplace noise is made dependent on the prior distribution by making its variance inversely proportional to $P_{\min}$. Intuitively, this is because a smaller $P_{\min}$ means that the data distribution is skewed, and rare instances can potentially leak more information. Therefore, for smaller $P_{\min}$, the noise variance is large, i.e., we add more noise. On the other extreme, when $P_{\min} = \frac{1}{|\mathcal{X}|}$ (i.e., uniform prior), we add the least amount of noise.

II. Privacy Definitions and Properties

We consider the problem of local privacy-preserving data release, where a user perturbs his input data $X \in \mathcal{D}, \mathcal{D} = \{x_1, x_2, \ldots, x_m\}$ and outputs Y to an *untrusted* data aggregator. For the scope of this paper, we consider two context-aware privacy metrics, namely mutual information privacy, and information privacy. We next define these metrics, along with local differential privacy, and briefly discuss the inter-relationships between these metrics.

A. Context-free privacy notion

Definition 1: (ϵ-Local Differential Privacy (LDP) [3]). A randomized mechanism $\mathcal{M} : X \to Y$ which takes an input X and outputs Y satisfies ϵ-LDP for some $\epsilon \in \mathbb{R}^+$, if for any $x, x' \in \mathcal{D}$ and for all $\mathcal{S}_{\text{out}} \in \text{Range}(\mathcal{M})$, we have

$$\Pr(Y \in \mathcal{S}_{\text{out}} | X = x) \leq e^{\epsilon} \Pr(Y \in \mathcal{S}_{\text{out}} | X = x'). \quad (1)$$

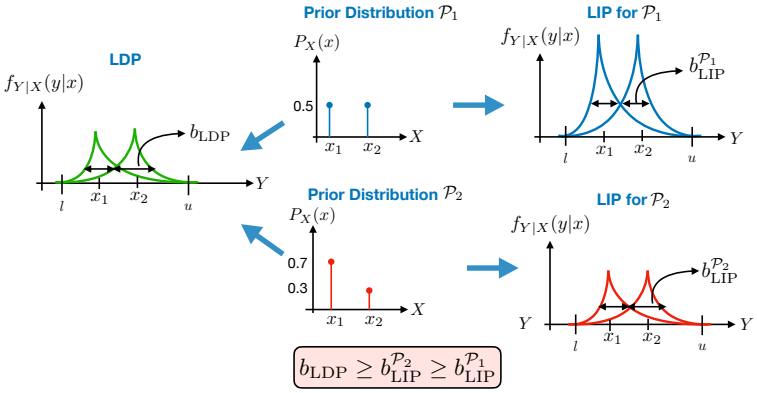

Fig. 1: Comparison between context-free mechanism and context-aware mechanism under the same privacy level ϵ.

LDP guarantees that each user's perturbed data has a similar output probability for any two input instances, $x, x' \in \mathcal{D}$.

B. Context-aware privacy notions

Definition 2: (ϵ-Mutual Information Privacy (MIP) [6]). A randomized mechanism $\mathcal{M} : X \to Y$ which takes an input X and outputs Y satisfies ϵ-MIP for some $\epsilon \in \mathbb{R}^+$, if the mutual information between X and Y, i.e., $I(X;Y)$ satisfies

$$I(X;Y) \leq \epsilon. \tag{2}$$

Definition 3: (ϵ-Local Information Privacy (LIP) [7]). A randomized mechanism $\mathcal{M} : X \to Y$ which takes an input X and outputs Y satisfies ϵ-LIP for some $\epsilon \in \mathbb{R}^+$, if for any $x \in \mathcal{D}$ and for all sets $\mathcal{S}_{\text{out}} \subseteq \text{Range}(\mathcal{M})$, we have

$$e^{-\epsilon} \leq \frac{\Pr(X = x, Y \in \mathcal{S}_{\text{out}})}{P_X(x)\Pr(Y \in \mathcal{S}_{\text{out}})} \leq e^{\epsilon}, \tag{3}$$

where $P_X(x)$ denotes the prior of input data X taking value x. Using Bayes' rule, the above definition can be re-written as

$$e^{-\epsilon} \leq \frac{\Pr(X = x | Y \in \mathcal{S}_{\text{out}})}{P_X(x)} \leq e^{\epsilon}. \tag{4}$$

Remark 1: From the above, it is clear that LIP essentially guarantees that the ratio of posterior (upon observing Y) to prior is bounded. Hence, having the knowledge of a user's prior, an adversary can *not* infer too much additional information about any input X by observing any output Y.

Remark 2: Since MI is the expected value of the ratio of posterior and prior distributions, thus, it is immediate that LIP is a stronger privacy notion than MIP. In essence, MIP provides an average privacy guarantee while LIP provides a privacy guarantee for every pair of input and output realizations.

Remark 3: With regards to the relationship between LDP and LIP, it was shown in [7] that ϵ-LIP implies 2ϵ-LDP while ϵ-LDP implies ϵ-LIP. To conclude, LIP is stronger than MIP but weaker than LDP and thus a stronger candidate for context-aware privacy guarantees.

Next, we define the approximate LIP as follows.

Definition 4: ((ϵ, δ)-Local Information Privacy (LIP)). A randomized mechanism $\mathcal{M} : X \to Y$ which takes an input X and outputs Y satisfies (ϵ, δ)-LIP for some $\epsilon \in \mathbb{R}^+$, if for any $x \in \mathcal{D}$ and for all sets $\mathcal{S}_{\text{out}} \subseteq \text{Range}(\mathcal{M})$, we have

$$\Pr(Y \in \mathcal{S}_{\text{out}}, X = x) \leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}})P_X(x) + \delta, \tag{5}$$

$$\Pr(Y \in \mathcal{S}_{\text{out}})P_X(x) \leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}}, X = x) + \delta. \tag{6}$$

In the following Proposition, we show the relationship between approximate LDP and approximate LIP.

Proposition 1: If a mechanism $\mathcal{M}$ satisfies (ϵ, δ)-LDP, then it also satisfies (ϵ, δ)-LIP. Conversely, if $\mathcal{M}$ satisfies (ϵ, δ)-LIP, then it satisfies $\left(2\epsilon, \frac{(e^{\epsilon}+1)\delta}{P_{\min}}\right)$-LDP, where $P_{\min} > 0$.

Proof: We start proving the first part. If a mechanism $\mathcal{M}$ satisfies (ϵ, δ)-LDP, then we have

$$\Pr(Y \in \mathcal{S}_{\text{out}} | X = x') \leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}} | X = x) + \delta.$$

Now we have the following:

$$\begin{aligned}\Pr(Y \in \mathcal{S}_{\text{out}}) &= \sum_{x'} \Pr(Y \in \mathcal{S}_{\text{out}} | X = x')P_X(x') \\ &\leq \sum_{x'} \left(e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}} | X = x) + \delta\right) P_X(x') \\ &= e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}} | X = x) + \delta,\end{aligned}$$

which yields,

$$\begin{aligned}\Pr(Y \in \mathcal{S}_{\text{out}})P_X(x) &\leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}}, X = x) + P_X(x)\delta \\ &\leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}}, X = x) + \delta.\end{aligned}$$

By switching the inputs, we can readily prove that

$$\Pr(Y \in \mathcal{S}_{\text{out}}, X = x) \leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}})P_X(x) + \delta,$$

which implies that the mechanism $\mathcal{M}$ also satisfies (ϵ, δ)-LIP.

Now we prove the second part. If $\mathcal{M}$ satisfies (ϵ, δ)-LIP, then from Definition 4, we have

$$\begin{aligned}\Pr(Y \in \mathcal{S}_{\text{out}}) &\leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}} | X = x') + \delta / P_X(x') \\ &\leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}} | X = x') + \delta / P_{\min}.\end{aligned} \tag{7}$$

Furthermore, from Definition 4, we also have

$$\Pr(Y \in \mathcal{S}_{\text{out}} | X = x) \leq e^{\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}}) + \delta / P_{\min}.$$

Hence, from the above equation, we have

$$\Pr(Y \in \mathcal{S}_{\text{out}}) \geq e^{-\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}}|X = x) - e^{-\epsilon}\delta/P_{\min}. \quad (8)$$

Plugging (8) in (7), we obtain the following,

$$\Pr(Y \in \mathcal{S}_{\text{out}}|X = x) \leq e^{2\epsilon}\Pr(Y \in \mathcal{S}_{\text{out}}|X = x') + \frac{(e^{\epsilon}+1)\delta}{P_{\min}},$$

which completes the proof of Proposition 1. ■

Remark 4: This result can be viewed as the generalization of the results in [6], [7], which show that ϵ-LIP implies 2ϵ-LDP. In contrast to the pure case ($\delta = 0$), the above proposition shows that the relationship between approximate LIP and approximate LDP depends on the underlying prior of the data.

III. Preliminaries on Laplacian Mechanism

Consider the setting when a single user has to release the local data X to an *untrusted* data curator. To achieve privacy, we perturb the data X by adding independent random noise N drawn from Laplacian distribution. The noise-adding mechanism will output

$$Y = X + N, \quad (9)$$

where $N \sim \text{Lap}(0, b)$ is a random variable with probability density function

$$f_N(n) = \frac{1}{2b}e^{-\frac{|n|}{b}}, \quad (10)$$

where b is the noise parameter that describes the Laplacian distribution. Note that b controls the width of the distribution, and the variance is $2b^2$. It has been shown in [1] that if we pick the noise parameter b as

$$b_{\text{LDP}} = \frac{\Delta X}{\epsilon} \quad (11)$$

satsifies ϵ-LDP, where ΔX is the query sensitivity. Formally, the local sensitivity, ΔX is defined as follows.

Definition 5: (Local Sensitivity). Let an input $X \in [x_{\min}, x_{\max}]$. Then, for a real-valued query $f(X) = X$ (i.e., identity query), the sensitivity of X is defined as

$$\Delta X \triangleq \max_{x_i, x_j} |X_i - X_j| \quad (12)$$

$$= x_{\max} - x_{\min}. \quad (13)$$

As the support of the Laplacian mechanism is infinite, the output of the Laplacian mechanism can have *undesired* values (e.g., the value of the output falls outside a certain specified range). To circumvent this issue, for the scope of this work, we focus on the *bounded* Laplacian mechanism [11].

Definition 6: (Bounded Laplacian Mechanism [11]). Given $b > 0$ and a domain interval $[l, u] \subset \mathbb{R}$, $l \leq u$. The bounded Laplacian mechanism $\mathcal{M}_B : X \to Y$, $\forall y \in [l, u]$ is given by the following conditional density function:

$$f_{Y|X}(y|x) = \begin{cases} 0, & \text{if } y \notin [l, u], \\ \frac{1}{C_x(b)}\frac{1}{2b}e^{-\frac{|y-x|}{b}}, & \text{if } y \in [l, u], \end{cases} \quad (14)$$

where $C_x(b) = \int_l^u \frac{1}{2b}e^{\frac{-|y-x|}{b}}dy$ is a normalization constant which depends on X.

Remark 5: We set $\Delta X = u - l$, however, in the most general case $[l, u]$ is a powerset of $[x_{\min}, x_{\max}]$.

Next, we present two Lemmas concerning $C_x(b)$ presented in [11], where these Lemmas will be useful in the design of the noise parameter b.

Lemma 1: The normalization constant $C_x(b)$ is written as follows:

$$C_x(b) = 1 - \frac{1}{2}\left(e^{-\frac{x-l}{b}} + e^{-\frac{u-x}{b}}\right). \quad (15)$$

It can be readily shown that the result of the integration yields (15). It is worth noting that for a fixed b, the minimum value of C_x is attained when $x = l$ or $x = u$.

Lemma 2: Let $C_x(b)$ be given by Definition 6. Then for a fixed b and $\Delta X = u - l$, we have

$$\max_{x,x'} \frac{C_x(b)}{C_{x'}(b)}e^{\frac{|x'-x|}{b}} = \max_{x',z} \frac{C_{x'+z}(b)}{C_{x'}(b)}e^{\frac{z}{b}} = e^{\frac{\Delta X}{b}}. \quad (16)$$

Outline of the proof: By the symmetry of $C_x(b)$ around $x = \frac{l+u}{2}$, we can assume that $x \geq x'$. Also, as shown in [11], $\frac{\partial}{\partial z}\left(\frac{C_{x'+z}}{C_{x'}}e^{\frac{z}{b}}\right) \geq 0$ whenever $x' + z \leq u$. Therefore, the value of z that maximize the ratio is ΔX. Also, $\frac{\partial}{\partial x'}\left(\frac{C_{x'+z}}{C_{x'}}e^{\frac{z}{b}}\right) \leq 0$ and the minimum value of x' is l.

Remark 6: For the context-free *bounded* Laplacian mechanism, it has been shown in [11] that when $\Delta X = u - l$, the noise obtained in (11) satisfies ϵ-LDP. In the next Section, we present our main results.

We note that the definition of LDP is independent of the priors, in which we can *not* adjust the perturbation parameters based on the priors. In the next Section, we show the advantage of devising mechanisms that are dependent on the priors which satisfy LIP. Fig. 1 gives an illustration of the differences between context-free and context-aware mechanisms.

IV. Main Results and Discussions

In this Section, we present our main result on context-aware Laplacian mechanism which satisfies (ϵ, 0)-LIP. In particular, we show how to design the noise parameter b as a function of the prior knowledge about the user's input data X[1] in the following Theorem. Before presenting the result, we highlight that for the context-aware Laplacian mechanism design, there are two methodologies to design the noise parameter b: 1) first case, which we term as *instance independent*, where we design b as a function of the prior distribution, however, each instance is perturbed by the same amount of noise. 2) second case being *instance dependent*, where we design the functional $b(x)$ as a function of the prior of every input instance x such that we add less noise for the high probability instances, and vice versa (see Fig. 2). For the scope of this paper, we focus on the first case, and the second setting of instant dependent mechanism design is left for future work.

[1]Note that the adversary may have inaccurate prior knowledge about user's data inputs. This scenario is left as a future work.

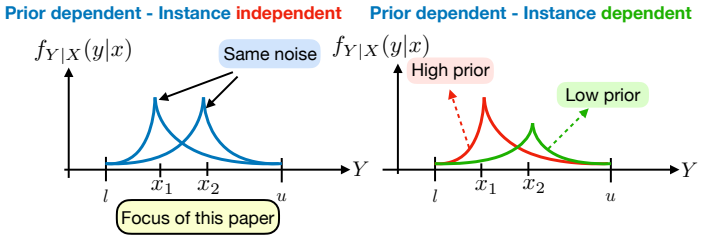

Fig. 2: Instance independent vs. Instance dependent context aware mechanisms.

Theorem 1: Let $\mathcal{M}_B$ be the bounded Laplacian mechanism given in Definition 6 and let $\epsilon \geq 0$ and $\delta = 0$. Then, $\{\mathcal{M}_B(x)|y \in [l,u]\}$ satisfies ϵ-LIP if

$$b_{\text{LIP}} = \begin{cases} \frac{\Delta X}{\log\left(\frac{e^{\epsilon}-P_{\min}}{1-P_{\min}}\right)}, & \epsilon < \log(\frac{1}{P_{\min}}) \\ \frac{\Delta X}{\epsilon}, & \text{otherwise}, \end{cases} \tag{17}$$

where $P_{\min}$ is the minimum probability value of the distribution $P_X(x)$.

The proof of Theorem 1 is presented in the Appendix. From Theorem 1, we make the following observations: the noise parameter b_{LIP} is picked as a function of $P_{\min} = \min_x P_X(x)$, the minimum probability over the data prior. Furthermore, for $\epsilon < \log(\frac{1}{P_{\min}})$, we observe that context-aware mechanism satisfying LIP adds less noise compared to context-unaware Laplacian mechanism satisfying LDP. Finally, we note that both mechanisms become equivalent in the limit $P_{\min} \to 0$.

Remark 7: (Comparison of Utility). We numerically compare the performance of context-free and context-aware Laplacian mechanisms for different probability distributions. To assess the performance i.e., utility, we define the following cost function[2]:

$$\text{MSE} \triangleq \mathbb{E}\left[(Y-X)^2\right] \tag{18}$$

$$= \sum_{x\in\mathcal{D}} \frac{P_X(x)}{2bC_x(b)} \int_{l-x}^{u-x} n^2 e^{-\frac{|n|}{b}} dn. \tag{19}$$

The expected cost is a function of the prior distribution $\mathcal{P}_X$, the noise distribution f_N and the bounds on the released output l, u. If the output support is unbounded, i.e., $l \to -\infty$ and $u \to \infty$, then $\text{MSE} = \mathbb{E}\left[N^2\right] = 2b^2$. We used MATLAB in order to compute the expression in (19).

Remark 8: (Numerical Comparison). In Fig. 3, we plot the utility function of context-free Laplacian mechanism and the context-aware Laplacian mechanism. We can see that our mechanism outperforms the conventional Laplacian mechanism, this is due to the relaxed definition of LIP where the noise parameter b is adjusted to the priors, i.e., as $P_{\min}$ increases, we require less noise. If $|\mathcal{X}| = m$, then $P_{\min} \leq \frac{1}{m}$. We note that the best utility is attained when $P_{\min} = \frac{1}{m}$, i.e., the priors are uniformly distributed.

[2]The details are skipped due to space limitation.

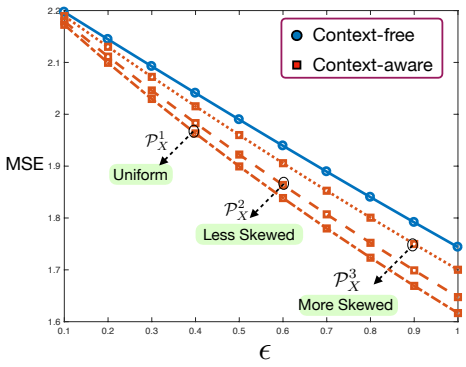

Fig. 3: MSE vs. ϵ for $X = \{0, 1.5, 3\}$, where $\Delta X = 3$, $|\mathcal{X}| = 3$ and $[l,u] = [0,3]$. We consider two distributions: $\mathcal{P}_X^1 = \{\frac{5}{15}, \frac{5}{15}, \frac{5}{15}\}$ and $\mathcal{P}_X^2 = \{\frac{6}{15}, \frac{5}{15}, \frac{4}{15}\}$, and $\mathcal{P}_X^3 = \{\frac{8}{15}, \frac{5}{15}, \frac{2}{15}\}$.

V. Conclusion

In this paper, we considered the problem of mechanism design under local information privacy constraints. We discussed the approximate case of local information privacy and showed its relationship to local differential privacy. We proposed a context-aware Laplacian mechanism which satisfies local information privacy. We showed better utility-privacy tradeoff for the proposed mechanism compared to the context-free Laplacian mechanism. There are several interesting directions for future work. First, it would be interesting to devise instance dependent Laplacian mechanisms which satisfy LIP constraints. Second, an interesting scenario is where the knowledge about the underlying prior distribution is limited.

References

[1] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[2] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," *Journal of the American Statistical Association*, vol. 60, no. 309, pp. 63–69, 1965.

[3] P. Kairouz, S. Oh, and P. Viswanath, "Extremal mechanisms for local differential privacy," in *Advances in neural information processing systems*, 2014, pp. 2879–2887.

[4] Ú. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. ACM, 2014, pp. 1054–1067.

[5] S. Xiong, A. D. Sarwate, and N. B. Mandayam, "Randomized requantization with local differential privacy," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, March 2016, pp. 2189–2193.

[6] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, October 2012, pp. 1401–1408.

[7] B. Jiang, M. Li, and R. Tandon, "Context-aware data aggregation with localized information privacy," *IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, May 2018.

[8] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Context-aware generative adversarial privacy," *Entropy*, vol. 19, no. 12, 2017.

[9] Y. Cao, M. Yoshikawa, Y. Xiao, and L. Xiong, "Quantifying differential privacy under temporal correlations," in *Data Engineering (ICDE), 2017 IEEE 33rd International Conference on*, April 2017, pp. 821–832.

[10] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science, FOCS'07.*, October 2007, pp. 94–103.

[11] N. Holohan, S. Antonatos, S. Braghin, and P. Mac Aonghusa, "The bounded Laplace mechanism in differential privacy," *arXiv preprint arXiv:1808.10410*, 2018.

APPENDIX

In this Section, we present the main steps behind the proof of the Theorem 1 in Section IV. We derive the minimum amount of noise needed to ensure ϵ-LIP for any input data $X \in \mathcal{D}$. We can write the LIP definition as

$$\frac{\Pr(Y \in \mathcal{S}_{\text{out}})P_X(x)}{\Pr(Y \in \mathcal{S}_{\text{out}}, X = x)} = \frac{\Pr(Y \in \mathcal{S}_{\text{out}})}{\Pr(Y \in \mathcal{S}_{\text{out}}|X = x)}.$$

For any arbitrary $\mathcal{S}_{\text{out}} \subseteq \text{Range}(\mathcal{M})$, and any pair x, x', we have the following sequence of inequalities:

$$\frac{\Pr(Y \in \mathcal{S}_{\text{out}})}{\Pr(Y \in \mathcal{S}_{\text{out}}|X = x)} = \frac{\sum_{x'} \Pr(Y \in \mathcal{S}_{\text{out}}|X = x')P_X(x')}{\Pr(Y \in \mathcal{S}_{\text{out}}|X = x)} \tag{20}$$

$$= \frac{\sum_{x'} P_X(x') \int_{\mathcal{S}_{\text{out}}} \frac{1}{C_{x'}} \frac{1}{2b} e^{-\frac{|y-x'|}{b}} dy}{\int_{\mathcal{S}_{\text{out}}} \frac{1}{C_x} \frac{1}{2b} e^{-\frac{|y-x|}{b}} dy}$$

$$= P_X(x) + \sum_{x' \neq x} P_X(x') \frac{C_x}{C_{x'}} \frac{\int_{\mathcal{S}_{\text{out}}} e^{-\frac{|y-x'|}{b}} dy}{\int_{\mathcal{S}_{\text{out}}} e^{-\frac{|y-x'+x'-x|}{b}} dy}$$

$$\overset{(a)}{\leq} P_X(x) + \sum_{x' \neq x} P_X(x') \frac{C_x}{C_{x'}} \frac{\int_{\mathcal{S}_{\text{out}}} e^{-\frac{|y-x'|}{b}} dy}{\int_{\mathcal{S}_{\text{out}}} e^{-\frac{|x'-x|}{b}} e^{-\frac{|y-x'|}{b}} dy}$$

$$= P_X(x) + \sum_{x' \neq x} P_X(x') \frac{C_x}{C_{x'}} e^{\frac{|x'-x|}{b}}$$

$$\overset{(b)}{\leq} P_X(x) + \sum_{x' \neq x} P_X(x') e^{\frac{\Delta X}{b}}$$

$$= P_X(x) + e^{\frac{\Delta X}{b}}(1 - P_X(x)),$$

where (a) follows from triangle inequality and (b) follows directly from Lemma 2. In order to upper bound the ratio $\frac{\Pr(Y \in \mathcal{S}_{\text{out}})}{\Pr(Y \in \mathcal{S}_{\text{out}}|X=x)}$ by e^{ϵ}, we have

$$P_X(x) + e^{\frac{\Delta X}{b}}(1 - P_X(x)) \leq e^{\epsilon} \Rightarrow e^{\frac{\Delta X}{b}} \leq \frac{e^{\epsilon} - P_X(x)}{1 - P_X(x)}.$$

We choose the same noise parameter b_{LIP} for every input data X. Here, we pick the worst b_{LIP} in order to satisfy ϵ-LIP for every X. Therefore, we pick the noise parameter b_{LIP} as follows:

$$b_{\text{LIP}} \geq \max_{P_X(x)} \frac{\Delta X}{\log\left(\frac{e^{\epsilon} - P_X(x)}{1 - P_X(x)}\right)}. \tag{21}$$

We note that $\frac{e^{\epsilon} - P_X(x)}{1 - P_X(x)}$ is an increasing function in $P_X(x)$, i.e.,

$$\frac{\partial}{\partial P_X(x)} \left(\frac{e^{\epsilon} - P_X(x)}{1 - P_X(x)}\right) = \frac{e^{\epsilon} - 1}{(1 - P_X(x))^2} \geq 0.$$

Therefore, we pick $P_X(x)$ that minimize the denominator of (21). Hence, from the above argument, we arrive at the following choice of the noise parameter b_{LIP}:

$$b_{\text{LIP}} = \frac{\Delta X}{\log\left(\frac{e^{\epsilon} - P_{\min}}{1 - P_{\min}}\right)}. \tag{22}$$

Now, we derive another lower bound for the amount of noise needed to satisfy ϵ-LIP. Starting from (20), we have the following sequence of inequalities:

$$\frac{\Pr(Y \in \mathcal{S}_{\text{out}})}{\Pr(Y \in \mathcal{S}_{\text{out}}|X = x)} = \frac{\sum_{x'} P_X(x') \int_{\mathcal{S}_{\text{out}}} \frac{1}{C_{x'}} \frac{1}{2b} e^{-\frac{|y-x'|}{b}} dy}{\int_{\mathcal{S}_{\text{out}}} \frac{1}{C_x} \frac{1}{2b} e^{-\frac{|y-x|}{b}} dy}$$

$$= P_X(x) + \sum_{x' \neq x} P_X(x') \frac{C_x}{C_{x'}} \frac{\int_{\mathcal{S}_{\text{out}}} e^{-\frac{|y-x+x-x'|}{b}} dy}{\int_{\mathcal{S}_{\text{out}}} e^{-\frac{|y-x|}{b}} dy}$$

$$\overset{(a)}{\geq} P_X(x) + \sum_{x' \neq x} P_X(x') \frac{C_x}{C_{x'}} e^{\frac{-|x-x'|}{b}}$$

$$\overset{(b)}{\geq} P_X(x) + \sum_{x' \neq x} P_X(x') e^{\frac{-\Delta X}{b}} \tag{23}$$

$$= P_X(x) + e^{\frac{-\Delta X}{b}}(1 - P_X(x)),$$

where (a) follows from triangle inequality and (b) follows directly from Lemma 2. In order to lower bound the ratio $\frac{\Pr(Y \in \mathcal{S}_{\text{out}})}{\Pr(Y \in \mathcal{S}_{\text{out}}|X=x)}$ by $e^{-\epsilon}$, we have

$$P_X(x) + e^{\frac{-\Delta X}{b}}(1 - P_X(x)) \geq e^{-\epsilon} \Rightarrow e^{\frac{-\Delta X}{b}} \geq \frac{e^{-\epsilon} - P_X(x)}{1 - P_X(x)}.$$

Therefore, we pick the noise parameter b_{LIP} as follows:

$$b_{\text{LIP}} \geq \max_{P_X(x)} \frac{\Delta X}{\log\left(\frac{1 - P_X(x)}{e^{-\epsilon} - P_X(x)}\right)}. \tag{24}$$

We note that $\frac{1 - P_X(x)}{e^{-\epsilon} - P_X(x)}$ is an increasing function in $P_X(x)$, i.e.,

$$\frac{\partial}{\partial P_X(x)} \left(\frac{1 - P_X(x)}{e^{-\epsilon} - P_X(x)}\right) = \frac{1 - e^{-\epsilon}}{(e^{-\epsilon} - P_X(x))^2} \geq 0.$$

Therefore, we pick $P_X(x)$ that minimizes the denominator of (24). This leads to the following choice for the noise parameter b_{LIP}:

$$b_{\text{LIP}} = \frac{\Delta X}{\log\left(\frac{1 - P_{\min}}{e^{-\epsilon} - P_{\min}}\right)}. \tag{25}$$

We pick the parameter b_{LIP} as the maximum of (22) and (25). Therefore, we get the following:

$$b_{\text{LIP}} = \frac{\Delta X}{\min\left[\log\left(\frac{e^{\epsilon} - P_{\min}}{1 - P_{\min}}\right), \log\left(\frac{1 - P_{\min}}{e^{-\epsilon} - P_{\min}}\right)\right]}. \tag{26}$$

Now, we wan check which term in the denominator of (26) is smaller by computing the following:

$$\left(\frac{e^{\epsilon} - P_{\min}}{1 - P_{\min}}\right) - \left(\frac{1 - P_{\min}}{e^{-\epsilon} - P_{\min}}\right) = \frac{(2 - e^{\epsilon} - e^{-\epsilon})P_{\min}}{(1 - P_{\min})(e^{-\epsilon} - P_{\min})}. \tag{27}$$

Note that $e^a + e^{-a} \geq 2$ for all $a \in \mathbb{R}$. Therefore, $(2 - e^{\epsilon} - e^{-\epsilon}) \leq 0$. To this end, (27) is negative when $(e^{-\epsilon} - P_{\min}) > 0$, i.e., $\epsilon < \log(\frac{1}{P_{\min}})$.

Next, we check the difference between the denominators in the expressions of (11) and (26). It is easy to see that $b_{\text{LIP}} \leq b_{\text{LDP}}$ for $\epsilon < \log\left(\frac{1}{P_{\min}}\right)$.

This completes the proof of Theorem 1.