Supplementary Document: Context-Aware Local Information Privacy

Bo Jiang*, *Student Member, IEEE,* Mohamed Seif*, *Student Member, IEEE,* Ravi Tandon, *Senior Member, IEEE,* and Ming Li, *Senior Member, IEEE*

Appendix A
Proof of Theorem 1 and Proposition 1

We first derive the upper bound of $\mathsf{LR}(y,x',x)$ for all $x,x' \in \mathcal{X}$, $y \in \mathcal{Y}$ when ϵ-LIP holds. If a mechanism $\mathcal{M}$ satisfies ϵ-LIP, we have $\forall x \in \mathcal{X}, y \in \mathcal{Y}$:

$$e^{-\epsilon} \leq \frac{P_Y(y)}{P_{Y|X}(y|x)} \leq e^{\epsilon}. \tag{1}$$

The privacy metric can be further expressed as

$$\begin{aligned} &\frac{\sum_{x'\in\mathcal{X}} P_{Y|X}(y|x')P_X(x')}{P_{Y|X}(y|x)} \\ =&P_X(x) + \frac{\sum_{x'\neq x} P_{Y|X}(y|x')P_X(x')}{P_{Y|X}(y|x)} \\ =&P_X(x) + \sum_{x'\neq x} \mathsf{LR}(y,x',x)P_X(x'). \end{aligned} \tag{2}$$

Bounding the leakage of LDP is equivalent to deriving the maximal value of $\mathsf{LR}(y,x',x)$ over all $x,x' \in \mathcal{X}$, $y \in \mathcal{Y}$, such that (2) is bounded by $[e^{-\epsilon}, e^{\epsilon}]$.

Note that $\mathsf{LR}(y,x',x') = 1$; $\mathsf{LR}(y,x',x) = \frac{1}{\mathsf{LR}(y,x,x')}$; $\mathsf{LR}(y,x',x) = \frac{\mathsf{LR}(y,x',j)}{\mathsf{LR}(y,x,j)}$, $\forall j \in \mathcal{X}$. Then, the constraints in (1) can be expressed as (3).

Dividing the i-th row by $\mathsf{LR}(y,1,i)$ yields (4). Denote $W(y) = P_X(1) + \mathsf{LR}(y,2,1)P_X(2) + \cdots + \mathsf{LR}(y,|\mathcal{X}|,1)P_X(|\mathcal{X}|)$. Using these, (3) can be rewritten as follows:

$$\begin{aligned} e^{-\epsilon} \leq& W(y) \leq e^{\epsilon}, \\ e^{-\epsilon}\mathsf{LR}(y,2,1) \leq& W(y) \leq e^{\epsilon}\mathsf{LR}(y,2,1), \\ &\vdots \\ e^{-\epsilon}\mathsf{LR}(y,|\mathcal{X}|,1) \leq& W(y) \leq e^{\epsilon}\mathsf{LR}(y,|\mathcal{X}|,1). \end{aligned} \tag{5}$$

It is worth noting that, the problem of bounding the leakage of LDP is equivalent to finding the maximum of the ratio of $\mathsf{LR}(y,x,1)/\mathsf{LR}(y,x',1)$ such that (5) is satisfied, which can also be expressed as the form in Theorem 1.

We next derive the loose bound presented in Proposition 1. For an arbitrary, fixed $y' \in \mathcal{Y}$, denote $x_u^* = \underset{x}{\text{argmax}}\mathsf{LR}(y',x,1)$ and $x_l^* = \underset{x}{\text{argmin}}\mathsf{LR}(y',x,1)$, then $\forall y' \in \mathcal{Y}$, there is:

$$e^{-\epsilon}\mathsf{LR}(y',x_u^*,1) \leq W(y') \leq e^{\epsilon}\mathsf{LR}(y',x_l^*,1). \tag{6}$$

*co-first authors. Bo Jiang, Mohamed Seif, Ravi Tandon and Ming Li are with the Department of Electrical and Computer Engineering, University of Arizona, AZ, 85718. Email:{bjiang, mseif, tandonr, lim}@email.arizona.edu

It is readily seen that the maximum value of $\mathsf{LR}(y',x',x)$ can be expressed as: $\max_{x,x'\in\mathcal{X}} \mathsf{LR}(y',x',x) = \mathsf{LR}(y',x_u^*,x_l^*) = \frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)}$. Divide (6) by $\mathsf{LR}(y',x_l^*,1)$ and denote $W'(y') = W(y')/\mathsf{LR}(y',x_l^*,1)$, which is shown in (7). Then, (6) becomes:

$$e^{-\epsilon}\frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)} \leq W'(y') \leq e^{\epsilon}.$$

For the first inequality, we have:

$$e^{-\epsilon}\frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)} \leq \frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)}(1-P_X(x_l^*)) + P_X(x_l^*),$$

which implies that when $e^{-\epsilon} - 1 + P_X(x_l^*) \geq 0$:

$$\frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)} \leq \frac{P_X(x_l^*)}{e^{-\epsilon}-1+P_X(x_l^*)} \leq \frac{P_{\min}}{e^{-\epsilon}-1+P_{\min}}. \tag{8}$$

Then, divide (6) by $\mathsf{LR}(y',x_u^*,1)$, and denoting $W^*(y')$ as $W(y')/\mathsf{LR}(y',x_u^*,1)$, then $W^*(y')$ becomes (9).

Therefore, (6)/$\mathsf{LR}(y',x_u^*,1)$ yields the following:

$$e^{-\epsilon} \leq W^*(y') \leq e^{\epsilon}\frac{\mathsf{LR}(y',x_l^*,1)}{\mathsf{LR}(y',x_u^*,1)}.$$

For the second inequality, we have

$$e^{\epsilon}\frac{\mathsf{LR}(y',x_l^*,1)}{\mathsf{LR}(y',x_u^*,1)} \geq \frac{\mathsf{LR}(y',x_l^*,1)}{\mathsf{LR}(y',x_u^*,1)}(1-P_X(x_u^*)) + P_X(x_u^*), \tag{10}$$

which implies:

$$\frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)} \leq \frac{e^{\epsilon}-1+P_X(x_u^*)}{P_X(x_u^*)} \leq \frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}. \tag{11}$$

Combining (8) and (11) we have

$$\mathsf{LR}(y',x_u^*,x_l^*) \leq \min\left\{\frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}, \frac{P_{\min}}{e^{-\epsilon}-1+P_{\min}}\right\}. \tag{12}$$

Comparing the two bounds in (12), we have

$$\begin{aligned} &\frac{e^{\epsilon}-1+P_{\min}}{P_{\min}} - \frac{P_{\min}}{e^{-\epsilon}-1+P_{\min}} \\ =&\frac{(e^{-\epsilon}-1+P_{\min})(e^{\epsilon}-1+P_{\min}) - (P_{\min})^2}{P_{\min}(e^{-\epsilon}-1+P_{\min})} \\ =&\frac{(1-P_{\min})(2-e^{\epsilon}-e^{-\epsilon})}{P_{\min}(e^{-\epsilon}-1+P_{\min})} \leq 0. \end{aligned} \tag{13}$$

To this end, (12) can be simplified as:

$$\mathsf{LR}(y',x_u^*,x_l^*) \leq \frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}. \tag{14}$$

$$\begin{aligned}
&e^{-\epsilon} \leq P_X(1) + \mathsf{LR}(y,2,1)P_X(2) + ... + \mathsf{LR}(y,|\mathcal{X}|,1)P_X(|\mathcal{X}|) \leq e^{\epsilon},\\
&e^{-\epsilon} \leq \mathsf{LR}(y,1,2)P_X(1) + P_X(2) + ... + \mathsf{LR}(y,|\mathcal{X}|,2)P_X(|\mathcal{X}|) \leq e^{\epsilon},\\
&...\\
&e^{-\epsilon} \leq \mathsf{LR}(y,1,|\mathcal{X}|)P_X(1) + \mathsf{LR}(y,2,|\mathcal{X}|)P_X(2) + ... + P_X(|\mathcal{X}|) \leq e^{\epsilon}.
\end{aligned} \tag{3}$$

$$e^{-\epsilon}\mathsf{LR}(y,i,1) \leq P_X(1) + \mathsf{LR}(y,2,1)P_X(2) + ... + \mathsf{LR}(y,|\mathcal{X}|,1)P_X(|\mathcal{X}|) \leq e^{\epsilon}\mathsf{LR}(y,i,1). \tag{4}$$

$$W'(y') = \frac{P_X(1)}{\mathsf{LR}(y',x_l^*,1)} + ... \frac{\mathsf{LR}(y',x_u^*,1)}{\mathsf{LR}(y',x_l^*,1)}P_X(x_u^*) + ...P_X(x_l^*) + \frac{\mathsf{LR}(y',|\mathcal{X}|,1)}{\mathsf{LR}(y',x_l^*,1)}P_X(|\mathcal{X}|). \tag{7}$$

$$W^*(y') = \frac{P_X(1)}{\mathsf{LR}(y',x_u^*,1)} + ...P_X(x_u^*) + ... \frac{\mathsf{LR}(y',x_l^*,1)}{\mathsf{LR}(y',x_u^*,1)}P_X(x_l^*) + \frac{\mathsf{LR}(y',|\mathcal{X}|,1)}{\mathsf{LR}(y',x_u^*,1)}P_X(|\mathcal{X}|). \tag{9}$$

From our prior work in [32], we know that $\mathsf{LR}(y', x_u^*, x_l^*) \leq e^{2\epsilon}$. We can also compare our new result with the new bound of (14) as follows:

$$\frac{e^{\epsilon} - 1 + P_{\min}}{P_{\min}} - e^{2\epsilon} = \frac{(e^{\epsilon}-1)(1-P_{\min}-P_{\min}e^{\epsilon})}{P_{\min}},$$

which implies when $\epsilon \geq \ln(\frac{1-P_{\min}}{P_{\min}})$, $\frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}$ is a tighter bound than $e^{2\epsilon}$, otherwise, $e^{2\epsilon}$ is a tighter bound.

Note that $\mathsf{LR}(y', x_u^*, x_l^*) \leq \min\{e^{2\epsilon}, \frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}\}$ can be applied to all $y' \in \mathcal{Y}$, which means,

$$\max_{x,x'\in\mathcal{X},y\in\mathcal{Y}} \mathsf{LR}(y,x',x) \leq \min\left\{e^{2\epsilon}, \frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}\right\}.$$

We next show ϵ-LDP implies $\ln(P_{\min} + e^{\epsilon}(1-P_{\min}))$-LIP. Suppose a mechanism $\mathcal{M}$ satisfies ϵ-LDP, then $\forall x, x' \in \mathcal{X}$, $y \in \mathcal{Y}$, then we have:

$$\frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \leq e^{\epsilon}. \tag{15}$$

Our goal is to find a bound $e^{\epsilon'}$ for the leakage of LIP, such that (15) is satisfied. Using Bayes rule, we have:

$$\max_{x\in\mathcal{X},y\in\mathcal{Y}} \frac{P_Y(y)}{P_{Y|X}(y|x)} \leq e^{\epsilon'}, \tag{16}$$

$$\max_{x\in\mathcal{X},y\in\mathcal{Y}} \frac{P_{Y|X}(y|x)}{P_Y(y)} \leq e^{\epsilon'}. \tag{17}$$

When ϵ-LDP holds, the left hand side of (16) can be further simplified as follows:

$$\begin{aligned}
&\frac{\sum_{x'\in\mathcal{X}} P_{Y|X}(y|x')P_X(x')}{P_{Y|X}(y|x)}\\
&= \frac{P_{Y|X}(y|x)P_X(x) + \sum_{x'\neq x} P_{Y|X}(y|x')P_X(x')}{P_{Y|X}(y|x)}\\
&= P_X(x) + \frac{\sum_{x'\neq x} P_{Y|X}(y|x')P_X(x')}{P_{Y|X}(y|x)}\\
&\leq P_X(x) + \sum_{x\neq x'} e^{\epsilon}P_X(x')\\
&= P_X(x) + e^{\epsilon}(1-P_X(x))\\
&\leq P_{\min} + e^{\epsilon}(1-P_{\min}).
\end{aligned} \tag{18}$$

Similarly, the left hand side of (17) is upper bounded by

$$\frac{1}{P_{\min} + e^{-\epsilon}(1-P_{\min})}. \tag{19}$$

Therefore, we have the following

$$\begin{aligned}
&\max_{x\in\mathcal{X},y\in\mathcal{Y}} \left\{\frac{P_X(x)}{P_{X|Y}(x|y)}, \frac{P_{X|Y}(x|y)}{P_X(x)}\right\}\\
&\leq \max\left\{P_{\min} + e^{\epsilon}(1-P_{\min}), \frac{1}{P_{\min} + e^{-\epsilon}(1-P_{\min})}\right\}\\
&\overset{(a)}{=} P_{\min} + e^{\epsilon}(1-P_{\min}),
\end{aligned} \tag{20}$$

where in step (a), $P_{\min} + e^{\epsilon}(1-P_{\min})$ is no smaller than (19), i.e.,

$$\begin{aligned}
&P_{\min} + e^{\epsilon}(1-P_{\min}) - \frac{1}{P_{\min} + e^{-\epsilon}(1-P_{\min})}\\
&= \frac{(1-P_{\min})P_{\min}(e^{\epsilon}+e^{-\epsilon}-2)}{P_{\min} + e^{-\epsilon}(1-P_{\min})} \geq 0.
\end{aligned}$$

This completes the proof of the statement in Proposition that if a mechanism satisfies ϵ-LDP, it satisfies $\ln(P_{\min} + e^{\epsilon}(1-P_{\min}))$-LIP.

Appendix B
Proof of Theorem 2

When ϵ-LDP holds, from (18), the leakage under BP-LIP can is upper bounded by

$$P_X(x) + e^{\epsilon}(1-P_X(x)),$$

which is upper bounded by

$$\begin{aligned}
&\max_{x\in\mathcal{X},\mathbf{P}\in\mathscr{P}_{\mathcal{X}}^{bp}} \{P_X(x) + e^{\epsilon}(1-P_X(x))\}\\
&= \min_{\mathbf{P}\in\mathscr{P}_{\mathcal{X}}^{bp}} P_{\min}^{bp} + e^{\epsilon}\left(1 - \min_{\mathbf{P}\in\mathscr{P}_{\mathcal{X}}^{bp}} P_{\min}^{bp}\right),
\end{aligned}$$

where $\min P^{bp}_{\min} = \min_{x\in\mathcal{X}, P\in\mathscr{P}^{bp}_{\mathcal{X}}} P_X(x)$. Conversely, from (14), we have

$$\mathsf{LR}(y', x^*_u, x^*_l) \leq \frac{e^\epsilon - 1 + P_X(x)}{P_X(x)}.$$

Notice that, for any fixed prior $\mathbf{P}$,

$$\mathsf{LR}(y', x^*_u, x^*_l) \leq \max_{x\in\mathcal{X}} \left\{ \frac{e^\epsilon - 1 + P_X(x)}{P_X(x)} \right\} = \frac{e^\epsilon - 1 + P_{\min}}{P_{\min}}.$$

For uncertain prior case, the leakage under any prior within $\mathscr{P}^{bp}_{\mathcal{X}}$ must be bounded, then we have

$$\begin{aligned}\mathsf{LR}(y', x^*_u, x^*_l) &\leq \min_{\mathbf{P}\in\mathscr{P}^{bp}_{\mathcal{X}}} \left\{ \frac{e^\epsilon - 1 + P_{\min}}{P_{\min}} \right\} \\ &= \frac{e^\epsilon - 1 + \max P^{bp}_{\min}}{\max P^{bp}_{\min}},\end{aligned}$$

where $\max P^{bp}_{\min} = \max_{\mathbf{P}\in\mathscr{P}_{\mathcal{X}}} \min^{bp}_{x\in\mathcal{X}} P_X(x)$.

Combined with the bound of 2ϵ, we have that when ϵ-BP-LIP holds, the maximum $\mathsf{LR}(y, x', x) \leq \min\left\{2\epsilon, \frac{e^\epsilon - 1 + \max P^{bp}_{\min}}{\max P^{bp}_{\min}}\right\}$. This completes the proof of Theorem 2.

Appendix C
Proof of Theorem 3

(1) LIP v.s. DI: When ϵ-LIP holds, the privacy leakage under DI can be expressed as:

$$\begin{aligned}\frac{P_{Y|X}(y|x)P_X(x)}{P_{Y|X}(y|x')P_X(x')} &\leq \frac{P_Y(y)P_X(x)e^\epsilon}{P_Y(y)P_X(x')e^{-\epsilon}} \\ &= e^{2\epsilon}\frac{P_X(x)}{P_X(x')} \\ &\leq e^{2\epsilon + D_\infty(\mathbf{P})}.\end{aligned}$$

For the other direction, when ϵ-DI holds, we have $\forall x, x' \in \mathcal{X}$:

$$\frac{P_{Y|X}(y|x)P_X(x)}{P_{Y|X}(y|x')P_X(x')} \leq e^\epsilon,$$

which implies

$$\frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \leq e^{\epsilon + D_\infty(\mathbf{P})}.$$

For the metric of LIP:

$$\begin{aligned}\frac{P_Y(y)}{P_{Y|X}(y|x)} &= P_X(x) + \sum_{x'\neq x} \frac{P_{Y|X}(y|x')P_X(x')}{P_{Y|X}(y|x)} \\ &\leq P_X(x) + [1 - P_X(x)]e^{\epsilon + D_\infty(\mathbf{P})} \\ &\leq P_{\min} + [1 - P_{\min}]e^{\epsilon + D_\infty(\mathbf{P})}.\end{aligned}$$

(2) LIP v.s. MIP: When ϵ-LIP is satisfied, by Bayes rule, we have that $\forall x, y \in \mathcal{X}$:

$$e^{-\epsilon} \leq \frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)} \leq e^\epsilon. \tag{21}$$

Substituting (21) into the definition of mutual information, we get:

$$I(X,Y) \leq \epsilon \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} P_{X,Y}(x,y) = \epsilon,$$

where $\sum_{x\in\mathcal{X}, y\in\mathcal{Y}} P_{X,Y}(x,y) = 1$.

(3) LIP v.s. MIL: The local maximal leakage between X and Y is defined as:

$$\mathcal{L}_{\mathsf{MIL}}(X;Y) = \ln \sum_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} P_{Y|X}(y|x).$$

When ϵ-LIP holds, we have:

$$\max_{x\in\mathcal{X}} P_{Y|X}(y|x) \leq P_Y(y)e^\epsilon,$$

which further implies:

$$\mathcal{L}_{\mathsf{MIL}}(X;Y) \leq \epsilon.$$

This completes the proof of Theorem 3.

Appendix D
Proofs of Lemma 1

Using Bayes rule, we have

$$\frac{P_X(x)}{P_{X|Y}(x|y)} = \frac{P_Y(y)}{P_{Y|X}(y|x)} = \frac{\sum_{x\in\mathcal{X}} P_X(x)P_{Y|X}(y|x)}{P_{Y|X}(y|x)}. \tag{22}$$

The first three properties mentioned in Lemma 1 are straightforward and the proof is omitted for brevity. We focus on presenting the proof of post-processing and linkage properties.

Post-processing: For $X \to Y \to Z$ that forms a Markov chain, we have the following set of steps:

$$\begin{aligned}\mathcal{L}_{\mathsf{LIP}}(X;Z) &= \max_{x\in\mathcal{X}, z\in\mathcal{Z}} \left| \ln \frac{P_{X|Z}(x|z)}{P_X(x)} \right| \\ &= \max_{x\in\mathcal{X}, z\in\mathcal{Z}} \left| \ln \sum_y \frac{P_{X|Y}(x|y)P_{Y|Z}(y|z)}{P_X(x)} \right| \\ &= \max_{x\in\mathcal{X}, z\in\mathcal{Z}} \left| \ln E_{Y|Z} \frac{P_{X|Y}(x|y)}{P_X(x)} \right| \\ &\leq \max_{x\in\mathcal{X}, y\in\mathcal{Z}} \left| \ln \frac{P_{X|Y}(x|y)}{P_X(x)} \right| \\ &= \mathcal{L}_{\mathsf{LIP}}(X;Y).\end{aligned}$$

Linkage: We know that LIP is a symmetric privacy measure, i.e., $\mathcal{L}_{\mathsf{LIP}}(X;Y) = \mathcal{L}_{\mathsf{LIP}}(Y;X)$ (i.e., the privacy measure remains unchanged when swapping the roles of the released output and the sensitive input). Suppose we have $S \to X \to Y$ forms a Markov chain. If we swap the roles of S and Y, we have $Y \to X \to S$ forms a Markov chain. Then, using the post-processing property we get the following:

$$\begin{aligned}&\mathcal{L}_{\mathsf{LIP}}(Y;X) \geq \mathcal{L}_{\mathsf{LIP}}(Y;S) \\ \Rightarrow\ &\mathcal{L}_{\mathsf{LIP}}(X;Y) \geq \mathcal{L}_{\mathsf{LIP}}(S;Y), \text{ (due to symmetry of LIP).}\end{aligned}$$

Note that if the latent variable S is independent of X, then the leakage $\mathcal{L}_{\mathsf{LIP}}(S;Y) = 0$. We prove this as follows:

$$\begin{aligned}\mathcal{L}_{\mathsf{LIP}}(S;Y) &= \sup_{s\in\mathcal{S}, y\in\mathcal{Y}} \left| \ln \frac{P_{S|Y}(s|y)}{P_S(s)} \right| \\ &= \sup_{s\in\mathcal{S}, y\in\mathcal{Y}} \left| \ln \frac{P_{Y|S}(y|s)}{P_Y(y)} \right| \\ &= \sup_{s\in\mathcal{S}, y\in\mathcal{Y}} \left| \ln \frac{\sum_x P_{Y|X}(y|x)P_{X|S}(x|s)}{\sum_x P_{Y|X}(y|x)P_X(x)} \right|.\end{aligned}$$

Therefore, $\mathcal{L}_{\text{LIP}}(S;Y)=0$ when $P_{X|S}(x|s)=P_X(x)$, i.e., X and S are independent. This completes the proof of the Lemma.

APPENDIX E
PROOF OF LEMMA 2

In this Section, we prove the modular property of LIP for the continuous case. The discrete case can be derived in a similar manner. W.L.O.G., we prove the case for two mixed distributions, i.e., $K=2$. Now, consider a prior mixture distribution f_X as follows:

$$f_X(x)=\alpha_1 f_1(x)+\alpha_2 f_2(x), \tag{23}$$

where $\alpha_i\in[0,1]$ and $\alpha_1+\alpha_2=1$. The marginal distribution of the mechanism output Y is obtained as

$$\begin{aligned} f_Y(y)&=\int_x f_{X,Y}(x,y)dx\\ &=\int_x f_{Y|X}(y|x)\left[\alpha_1 f_1(x)+\alpha_2 f_2(x)\right]dx\\ &=\alpha_1\int_x f_{Y|X}(y|x)f_1(x)dx+\alpha_2\int_x f_{Y|X}(y|x)f_2(x)dx\\ &=\alpha_1 g_1(y)+\alpha_2 g_2(y), \end{aligned}\tag{24}$$

where $g_i(y)$ is the marginal distribution of the output mechanism Y averaged on $f_i(x)$.

Therefore, we have

$$\begin{aligned} \Pr_{f_Y}(Y\in\mathcal{S}_y)&=\int_{y\in\mathcal{S}_y} f_Y(y)dy\\ &=\alpha_1\Pr_{g_1}(Y\in\mathcal{S}_y)+\alpha_2\Pr_{g_2}(Y\in\mathcal{S}_y), \end{aligned}\tag{25}$$

where $\Pr_{g_i}(Y\in\mathcal{S}_y)=\int_{y\in\mathcal{S}_y} g_i(y)dy$ is taken over the randomness of distribution g_i.

We know that the mechanism $\mathcal{M}$ satisfies (ϵ,δ)-LIP for each prior $f_i(x)$, i.e.,

$$\begin{aligned} \Pr_{g_1}(Y\in\mathcal{S}_y)&\le e^{\epsilon}\Pr_{\mathcal{M}}(Y\in\mathcal{S}_y|X\in\mathcal{S}_x)+\delta,\\ \Pr_{g_2}(Y\in\mathcal{S}_y)&\le e^{\epsilon}\Pr_{\mathcal{M}}(Y\in\mathcal{S}_y|X\in\mathcal{S}_x)+\delta, \end{aligned}\tag{26}$$

where $\Pr_{\mathcal{M}}(Y\in\mathcal{S}_y|X\in\mathcal{S}_x)$ is taken over the randomness of the perturbation mechanism $\mathcal{M}$. Plugging (26) into (25) proves the first result of Lemma 2, i.e.,

$$\Pr_{f_Y}(Y\in\mathcal{S}_y)\le e^{\epsilon}\Pr_{\mathcal{M}}(Y\in\mathcal{S}_y|X\in\mathcal{S}_x)+\delta. \tag{27}$$

The other direction can be proved using similar arguments, thus completing the proof of the Lemma.

APPENDIX F
PROOF OF THEOREM 4

We simplify the expression of leakage after n queries as follows:

$$\begin{aligned} \frac{P_X(x)}{P_{X|\mathbf{Y}_1^n}(x|\mathbf{y}_1^n)}&=\frac{P_{\mathbf{Y}_1^n}(\mathbf{y}_1^n)}{P_{\mathbf{Y}_1^n|X}(\mathbf{y}_1^n|x)}\\ &=\frac{\sum_{x'\in\mathcal{X}}P_{\mathbf{Y}_1^n|X}(\mathbf{y}_1^n|x')P_X(x')}{\prod_{i=1}^n P_{Y_i|X}(y_i|x)}\\ &=\frac{\sum_{x'\in\mathcal{X}}\prod_{j=1}^n P_{Y_j|X}(y_j|x')P_X(x')}{\prod_{i=1}^n P_{Y_i|X}(y_i|x)}\\ &=P_X(x)+\sum_{x'\neq x}\prod_{i=1}^n\frac{P_{Y_i|X}(y_i|x')P_X(x')}{P_{Y_i|X}(y_i|x)}. \end{aligned}$$

Using the property that if a mechanism satisfies ϵ-LIP, it satisfies $\min\left\{2\epsilon,\ln\frac{e^{\epsilon}-1+P_{\min}}{P_{\min}}\right\}$-LDP, we have:

$$\begin{aligned} &P_X(x)+\sum_{x'\neq x}\prod_{i=1}^n\frac{P_{Y_i|X}(y_i|x')P_X(x')}{P_{Y_i|X}(y_i|x)}\\ \le&P_X(x)+\sum_{x'\neq x}e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}P_X(x')\\ =&P_X(x)+e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}(1-P_X(x))\\ \le&P_{\min}+e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}(1-P_{\min}). \end{aligned}$$

Similarly, we can derive a lower bound on the leakage as follows:

$$P_{\min}+e^{-\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}(1-P_{\min}).$$

Thus the maximum leakage is bounded by:

$$\begin{aligned} &\ln\max\left\{P_{\min}+e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}(1-P_{\min})\right.\\ &\left.,\frac{1}{P_{\min}+e^{-\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}(1-P_{\min})}\right\}\\ =&\ln\left\{P_{\min}+e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P_{\min}}{P_{\min}}\right\}}(1-P_{\min})\right\}. \end{aligned}$$

This completes the proof of the Theorem.

APPENDIX G
PROOF OF LEMMA 3

For any arbitrary pmf $\mathbf{P}_2$ on $\mathcal{X}$, it can be verified that

$$P_2(x)\le P_1(x)+\frac{1}{2}\|\mathbf{P}_1-\mathbf{P}_2\|_1,\forall x\in\mathcal{X}. \tag{28}$$

This follows from the following fact

$$\begin{aligned} \frac{1}{2}\|\mathbf{P}_1-\mathbf{P}_2\|_1&=\max_{\mathcal{S}}|\mathbf{P}_1(\mathcal{S})-\mathbf{P}_2(\mathcal{S})|\\ &\ge|\mathbf{P}_1(\mathcal{S})-\mathbf{P}_2(\mathcal{S})|. \end{aligned}$$

Using the above we also have:

$$\frac{1}{2}\|\mathbf{P}_1-\mathbf{P}_2\|_1\ge|P_1(x)-P_2(x)|,\forall x\in\mathcal{X}. \tag{29}$$

Therefore, we have

$$\begin{aligned}\frac{P_2(x)}{P_1(x)} &\leq \max_x \frac{P_2(x)}{P_1(x)} \\ &\leq \max_x \frac{P_1(x)+\frac{1}{2}\|\mathbf{P}_1-\mathbf{P}_2\|_1}{P_1(x)} \\ &= \max_x 1+\frac{\|\mathbf{P}_1-\mathbf{P}_2\|_1}{2P_1(x)} \\ &= 1+\frac{\|\mathbf{P}_1-\mathbf{P}_2\|_1}{2P^1_{\min}} \triangleq \delta_1.\end{aligned}$$

Similarly, we can show that

$$\frac{P_1(x)}{P_2(x)} \leq 1+\frac{\|\mathbf{P}_1-\mathbf{P}_2\|_1}{2P^2_{\min}} \triangleq \delta_2.$$

Combining these bounds we have

$$\max\left(\frac{P_1(x)}{P_2(x)},\frac{P_2(x)}{P_1(x)}\right) \leq \max(\delta_1,\delta_2).$$

Also,

$$\begin{aligned}&\max\left(\frac{P_1(x)}{P_2(x)},\frac{P_2(x)}{P_1(x)}\right) \geq \min\left(\frac{P_1(x)}{P_2(x)},\frac{P_2(x)}{P_1(x)}\right) \\ &\geq \min(1/\delta_1,1/\delta_2) = \frac{1}{\max(\delta_1,\delta_2)}.\end{aligned}$$

Now we have the following upper bound on $P_Y^{(2)}(y)$:

$$\begin{aligned}P_Y^{(2)}(y) &= \sum_{x'}\frac{P_2(x')}{P_1(x')}P_1(x')P_{Y|X}(y|x') \\ &\leq \max(\delta_1,\delta_2)\sum_{x'}P_1(x')P_{Y|X}(y|x') \\ &= \max(\delta_1,\delta_2)P_Y^{(1)}(y).\end{aligned}$$

Also, $P_Y^{(2)}(y)$ can be lower bounded as

$$\begin{aligned}P_Y^{(2)}(y) &= \sum_{x'}\frac{P_2(x')}{P_1(x')}P_1(x')P_{Y|X}(y|x') \\ &\geq \frac{1}{\max(\delta_1,\delta_2)}\sum_{x'}P_1(x')P_{Y|X}(y|x') \\ &= \frac{1}{\max(\delta_1,\delta_2)}P_Y^{(1)}(y).\end{aligned}$$

Dividing the above equation by $P_{Y|X}(y|x)$ on both sides, we get the following:

$$\frac{1}{\max(\delta_1,\delta_2)}\times\frac{P_Y^{(1)}(y)}{P_{Y|X}(y|x)} \leq \frac{P_Y^{(2)}(y)}{P_{Y|X}(y|x)} \tag{30}$$

$$\frac{P_Y^{(2)}(y)}{P_{Y|X}(y|x)} \leq \max(\delta_1,\delta_2)\times\frac{P_Y^{(1)}(y)}{P_{Y|X}(y|x)}. \tag{31}$$

Now, we have the following:

$$\begin{aligned}&\max\left(\frac{P_Y^{(2)}(y)}{P_{Y|X}(y|x)},\frac{P_{Y|X}(y|x)}{P_Y^{(2)}(y)}\right) \\ &\leq \max(\delta_1,\delta_2)\times\max\left(\frac{P_Y^{(1)}(y)}{P_{Y|X}(y|x)},\frac{P_{Y|X}(y|x)}{P_Y^{(1)}(y)}\right).\end{aligned}$$

Therefore, by taking $\ln(\cdot)$ and $\sup_{x\in\mathcal{X},y\in\mathcal{Y}}$ for both sides, we have

$$\begin{aligned}&\sup_{x\in\mathcal{X},y\in\mathcal{Y}}\ln\left[\max\left(\frac{P_Y^{(2)}(y)}{P_{Y|X}(y|x)},\frac{P_{Y|X}(y|x)}{P_Y^{(2)}(y)}\right)\right] \\ &\leq \ln\left[\max(\delta_1,\delta_2)\right] \\ &\quad+\sup_{x\in\mathcal{X},y\in\mathcal{Y}}\ln\left[\max\left(\frac{P_Y^{(1)}(y)}{P_{Y|X}(y|x)},\frac{P_{Y|X}(y|x)}{P_Y^{(1)}(y)}\right)\right].\end{aligned} \tag{32}$$

Hence, we arrive at the following bound:

$$\mathcal{L}_{\mathsf{LIP}}(\mathcal{M}(\mathbf{P}_1),\mathbf{P}_2) \leq \ln\left[\max(\delta_1,\delta_2)\right]+\mathcal{L}_{\mathsf{LIP}}(\mathcal{M}(\mathbf{P}_1),\mathbf{P}_1).$$

Similarly, we can show that,

$$\mathcal{L}_{\mathsf{LIP}}(\mathcal{M}(\mathbf{P}_1),\mathbf{P}_2) \geq -\ln\left[\max(\delta_1,\delta_2)\right]+\mathcal{L}_{\mathsf{LIP}}(\mathcal{M}(\mathbf{P}_1),\mathbf{P}_1).$$

We can further simplify the term $\max(\delta_1,\delta_2)$ as follows:

$$\begin{aligned}\max(\delta_1,\delta_2) &= 1+\frac{\|\mathbf{P}_1-\mathbf{P}_2\|_1}{2\min\left[P^1_{\min},P^2_{\min}\right]} \\ &\overset{(a)}{=} 1+\frac{D_{\mathsf{TV}(\mathbf{P}_1,\mathbf{P}_2)}}{\min\left[P^1_{\min},P^2_{\min}\right]} \\ &\overset{(b)}{=} 1+\frac{D_{\mathsf{TV}(\mathbf{P}_1,\mathbf{P}_2)}}{c},\end{aligned}$$

where (a) follows from the fact that $D_{\mathsf{TV}}(\mathbf{P}_1,\mathbf{P}_2)=\frac{1}{2}\|\mathbf{P}_1-\mathbf{P}_2\|_1$, while in (b), we defined c as $c \triangleq \min\left[P^1_{\min},P^2_{\min}\right]$. This completes the proof of Lemma 3.

Appendix H
Proof of Corollary 3

It was shown in [1] under the plug-in estimator defined in:

$$\hat{P}_X(x) \triangleq \frac{1}{n}\sum_{i=1}^{n}\mathbb{1}_{\{x_i=x\}}, \tag{33}$$

the ℓ_1 distance between P_X and $\hat{P}_X$ is upper bounded by

$$D_{\ell_1}(P_X,\hat{P}_X) \leq \sqrt{\frac{2}{n}(|\mathcal{X}|-\ln\beta)}, \tag{34}$$

w.p. $1-\beta$. Therefore, by using the results from Lemma 3, we have

$$\ln\left(1+\frac{D_{\ell_1}(P_X,\hat{P}_X)}{2c}\right) \leq \ln\left(1+\frac{1}{2c}\sqrt{\frac{2}{n}(|\mathcal{X}|-\ln\beta)}\right),$$

w.p. $1-\beta$. This completes the proof of the Corollary.

Appendix I
Proof of Proposition 2

The likelihood $f_{Y|X}$ can be expressed as follows:

$$f_{Y|X}(y|x) = \lambda\delta(y-x)+(1-\lambda)f_X(y).$$

Using the above, we can compute the following probability:

$$\begin{aligned}&\Pr(Y\in\mathcal{S}_y,X\in\mathcal{S}_x) = \int_{\mathcal{S}_y}\int_{\mathcal{S}_x}f_X(x)f_{Y|X}(y|x)dxdy \\ &= \int_{\mathcal{S}_y}\int_{\mathcal{S}_x}f_X(x)\left[\lambda\delta(y-x)+(1-\lambda)f_X(y)\right]dxdy \\ &= \int_{\mathcal{S}_y}\left[\lambda\mathbb{1}_{\{y\in\mathcal{S}_x\}}f_X(y)+(1-\lambda)f_X(y)\Pr(X\in\mathcal{S}_x)\right]dy \\ &= \lambda\Pr(Y\in\mathcal{S}_x\cap\mathcal{S}_y)+(1-\lambda)\Pr(X\in\mathcal{S}_x)\Pr(Y\in\mathcal{S}_y).\end{aligned} \tag{35}$$

The marginal distribution f_Y is obtained as follows

$$\begin{aligned} f_Y(y) &= \lambda f_X(y) + (1-\lambda) f_X(y) \\ &= f_X(y), \end{aligned}$$

which means under the sampling mechanism, the marginal probability of Y is identical to that of X. Then, from (35) we have

$$\Pr(Y \in \mathcal{S}_y | X \in \mathcal{S}_x) \quad (36)$$

$$= \lambda \Pr(X \in \mathcal{S}_y | X \in \mathcal{S}_x) + (1-\lambda)\Pr(Y \in \mathcal{S}_y). \quad (37)$$

Note that the value of the conditional probability of $\Pr(X \in \mathcal{S}_y | X \in \mathcal{S}_x)$ is between $[0,1]$, which means (36) is bounded by

$$[(1-\lambda)\Pr(Y \in \mathcal{S}_y), \lambda + (1-\lambda)\Pr(Y \in \mathcal{S}_y)].$$

Observe that, the definition of (ϵ,δ)-LIP can be expressed as

$$e^{-\epsilon}(\Pr(Y \in \mathcal{S}_y) - \delta) \leq \Pr(Y \in \mathcal{S}_y | X \in \mathcal{S}_x) \leq e^{\epsilon}(\Pr(Y \in \mathcal{S}_y) + \delta). \quad (38)$$

A sufficient condition of (ϵ,δ)-LIP is the following:

$$e^{-\epsilon}\Pr(Y \in \mathcal{S}_y) - e^{-\epsilon}\delta \leq (1-\lambda)\Pr(Y \in \mathcal{S}_y), \quad (39)$$

$$\lambda + (1-\lambda)\Pr(Y \in \mathcal{S}_y) \leq e^{\epsilon}\Pr(Y \in \mathcal{S}_y) + e^{\epsilon}\delta. \quad (40)$$

From (39), we have

$$\lambda \leq 1 - e^{-\epsilon} + \frac{\delta e^{-\epsilon}}{\Pr(Y \in \mathcal{S}_y)}.$$

A sufficient condition is

$$\lambda \leq \min_{\Pr(Y \in \mathcal{S}_y)} 1 - e^{-\epsilon} + \frac{\delta e^{-\epsilon}}{\Pr(Y \in \mathcal{S}_y)} = 1 - e^{-\epsilon} + \delta e^{-\epsilon}.$$

Thus, we have $\lambda \leq 1 - e^{-\epsilon} + \delta e^{-\epsilon}$. From (40), we have

$$\lambda \leq \frac{(e^{\epsilon}-1)\Pr(Y \in \mathcal{S}_y) + \delta e^{\epsilon}}{1 - \Pr(Y \in \mathcal{S}_y)},$$

which is monotonically decreasing with $\Pr(Y \in \mathcal{S}_y)$. Therefore, in order to satisfy (40), we pick λ as

$$\lambda \leq \min_{\Pr(Y \in \mathcal{S}_y)} \frac{(e^{\epsilon}-1)\Pr(Y \in \mathcal{S}_y) + \delta e^{\epsilon}}{1 - \Pr(Y \in \mathcal{S}_y)} = \delta e^{\epsilon}.$$

Combining with the result from (39), we get

$$\lambda \leq \min\{\delta e^{\epsilon}, 1 - e^{-\epsilon} + \delta e^{-\epsilon}\}.$$

This completes the proof of the Proposition.

APPENDIX J
PROOF OF PROPOSITION 3

For any $0 \leq \gamma \leq 1$ and two distributions f and g, we have

$$\begin{aligned} 1-\gamma &= \int_{\mathcal{Y}} (f(y) - \gamma g(y))dy \\ &= \int_{\{y: f(y) \geq \gamma g(y)\}} (f(y) - \gamma g(y))dy \\ &\quad + \int_{\{y: f(y) \leq \gamma g(y)\}} (f(y) - \gamma g(y))dy \\ &= E_\gamma(f||g) - \gamma \int_{\{y: f(y) \leq \gamma g(y)\}} (g(y) - \frac{1}{\gamma} f(y))dy \\ &= E_\gamma(f||g) - \gamma \int_{\{y: g(y) \geq f(y)/\gamma\}} (g(y) - \frac{1}{\gamma} f(y))dy \\ &= E_\gamma(f||g) - \gamma E_{\frac{1}{\gamma}}(g||f). \end{aligned}$$

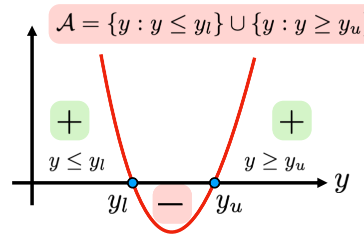

Fig. 1: Feasible regions for the quadratic equation, y_l, y_u are the roots of the equation for $\sigma_1 \geq \sigma_2$.

By setting $\gamma = e^{-\epsilon}$, we have

$$E_{e^{-\epsilon}}(f||g) - e^{-\epsilon} E_{e^{\epsilon}}(g||f) = 1 - e^{-\epsilon},$$

which means

$$E_{e^{\epsilon}}(g||f) = e^{\epsilon} E_{e^{-\epsilon}}(f||g) - e^{\epsilon} + 1.$$

By setting $f = f_Y$ and $g = f_{Y|X}$, this completes the proof of the Proposition.

APPENDIX K
PROOF OF LEMMA 4

Consider two Gaussian distributions, $f = \mathcal{N}(\mu_1, \sigma_1^2)$ and $g = \mathcal{N}(\mu_2, \sigma_2^2)$ where $\sigma_1 > \sigma_2$. Then, we have the following:

$$\begin{aligned} E_\gamma(f||g) &= \int_{\mathcal{Y}} \max\left[\frac{f(y)}{g(y)} - \gamma, 0\right] g(y)dy \\ &= \int_{\mathcal{A}=\{y: f(y) > \gamma g(y)\}} (f(y) - \gamma g(y))dy. \end{aligned}$$

Notice that $f(y) > \gamma g(y)$ when

$$\frac{(y-\mu_2)^2}{2\sigma_2^2} - \frac{(y-\mu_1)^2}{2\sigma_1^2} > \ln\left(\frac{\gamma\sigma_1}{\sigma_2}\right).$$

Therefore,

$$\begin{aligned} & y^2\left(\frac{1}{2\sigma_2^2} - \frac{1}{2\sigma_1^2}\right) - y\left(\frac{\mu_2}{\sigma_2^2} - \frac{\mu_1}{\sigma_1^2}\right) \\ & + \left(\frac{\mu_2^2}{2\sigma_2^2} - \frac{\mu_1^2}{2\sigma_1^2}\right) - \ln\left(\frac{\gamma\sigma_1}{\sigma_2}\right) \geq 0. \end{aligned}$$

The solution of this quadratic equation is

$$\begin{aligned} y_u &= \frac{\sigma_1^2\mu_2 - \sigma_2^2\mu_1 + \sigma_1\sigma_2\sqrt{B}}{\sigma_1^2 - \sigma_2^2}, \\ y_l &= \frac{-(\sigma_2^2\mu_1 - \sigma_1^2\mu_2 + \sigma_1\sigma_2\sqrt{B})}{\sigma_1^2 - \sigma_2^2}, \end{aligned}$$

where,

$$B = 2(\sigma_1^2 - \sigma_2^2)\ln\left(\frac{\gamma\sigma_1}{\sigma_2}\right) + (\mu_1 - \mu_2)^2.$$

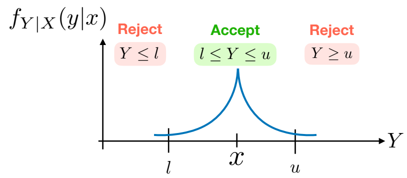

Fig. 2: An illustration for the truncated Laplcian mechanism.

Therefore, by integrating over the defined region $\mathcal{A}$ (depicted in Fig. 1), we have

$$\begin{aligned}E_\gamma(f||g) &= \int_{\mathcal{A}} (f(y) - \gamma g(y))dy \\ &= 1 + Q\left(\frac{y_u - \mu_1}{\sigma_1}\right) - Q\left(\frac{y_l - \mu_1}{\sigma_1}\right) \\ &\quad - \gamma\left[1 + Q\left(\frac{y_u - \mu_2}{\sigma_2}\right) - Q\left(\frac{y_l - \mu_2}{\sigma_2}\right)\right].\end{aligned}$$

This completes the proof of the Lemma.

Appendix L
Proof of Theorem 6

We pick the parameter $b_{\text{LIP}}(x)$ to have the following functional form:

$$b_{\text{LIP}}(x) = \frac{\Delta X}{\alpha_\epsilon P_X(x) + \beta_\epsilon}, \forall x \in \mathcal{X},$$

where α_ϵ and β_ϵ are constants given a privacy level ϵ. The functional form must be chosen carefully to satisfy LIP. Hence, the context-aware mechanism works as follows in this case: We pick the noise parameter $b_{\text{LIP}}(x)$ such that we add less to a high probability instance and vice versa. Now, our goal is to find the function the parameters of $b_{\text{LIP}}(x)$, i.e., α_ϵ and β_ϵ.

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, we truncate the output of the Laplcian mechanism. In this approach, we have a deterministic mapping to the upper and lower bounds of the output domain, when the value falls outside (see Fig. 2).

For any arbitrary output y, and any pair x, x', we have the following sequence of inequalities:

$$\begin{aligned}\frac{f_Y(y)}{f_{Y|X}(y|x)} &= \frac{\sum_{x'} f_{Y|X}(y|x')P_X(x')}{f_{Y|X}(y|x)} \\ &= \frac{\sum_{x'} P_X(x')\frac{1}{2b(x')}e^{-\frac{|y-x'|}{b(x')}}dy}{\frac{1}{2b(x)}e^{-\frac{|y-x|}{b(x)}}dy} \\ &= P_X(x) + \sum_{x' \neq x} P_X(x')\frac{b(x)}{b(x')}\frac{e^{-\frac{|y-x'|}{b(x')}}dy}{e^{-\frac{|y-x|}{b(x)}}dy} \\ &= P_X(x) + \sum_{x' \neq x} P_X(x')\frac{b(x)}{b(x')}\exp\left[\frac{|y-x|}{b(x)} - \frac{|y-x'|}{b(x')}\right] \\ &\overset{(a)}{\le} P_X(x) + \sum_{x' \neq x} P_X(x')\frac{b(x)}{b(x')}\exp\left[\frac{\Delta X}{b(x)}\right] \\ &= P_X(x) + \sum_{x' \neq x} P_X(x')\left[\frac{\alpha_\epsilon P_X(x') + \epsilon}{\alpha_\epsilon P_X(x) + \beta_\epsilon}\right]e^{\alpha_\epsilon P_X(x) + \beta_\epsilon},\end{aligned}$$

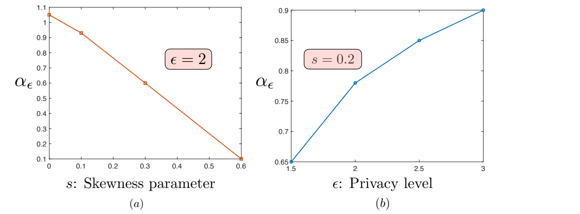

Fig. 3: (a): Effect of skewness parameter s on α_ϵ for $\epsilon = 2$. (b): Effect of the privacy parameter ϵ on α_ϵ. The prior distribution is $\mathscr{P}_X = \{\frac{1}{3} + \frac{s}{2}, \frac{1}{3}, \frac{1}{3} - \frac{s}{2}\}$ and $s = 0.2$.

where step (a) is due to the output truncation of the Laplace mechanism. Now, in order to bound the ratio $\frac{f_Y(y)}{f_{Y|X}(y|x)}$ by e^ϵ, we have to satisfy

$$P_{\min} + \sum_{x' \neq x} P_X(x')\left[\frac{\alpha_\epsilon P_X(x') + \beta_\epsilon}{\alpha_\epsilon P_X(x) + \beta_\epsilon}\right]e^{\alpha_\epsilon P_X(x) + \beta_\epsilon} \le e^\epsilon.$$

On the other hand, we have

$$\begin{aligned}\frac{f_Y(y)}{f_{Y|X}(y|x)} &\ge P_X(x) + \sum_{x' \neq x} P_X(x')\frac{b(x)}{b(x')}\exp\left[\frac{-\Delta X}{b(x')}\right] \\ &\ge P_X(x) + \sum_{x' \neq x} P_X(x')\left[\frac{\alpha_\epsilon P_X(x') + \beta_\epsilon}{\alpha_\epsilon P_X(x) + \beta_\epsilon}\right]e^{-(\alpha_\epsilon P_X(x') + \beta_\epsilon)}.\end{aligned}$$

In order to lower bound $\frac{f_Y(y)}{f_{Y|X}(y|x)}$ by $e^{-\epsilon}$, we have the following sufficient condition:

$$P_{\min} + \sum_{x' \neq x} P_X(x')\left[\frac{\alpha_\epsilon P_X(x') + \beta_\epsilon}{\alpha_\epsilon P_X(x) + \beta_\epsilon}\right]e^{-(\alpha_\epsilon P_X(x') + \beta_\epsilon)} \ge e^{-\epsilon}.$$

Now, we do a grid search for α_ϵ and β_ϵ such that the bounds on $\frac{f_Y(y)}{f_{Y|X}(y|x)}$ are satisfied. From the search, we found that β_ϵ is too close to ϵ, therefore we set $\beta_\epsilon = \epsilon$. We pick the maximum allowable α_ϵ that satisfies both bounds on $\frac{f_Y(y)}{f_{Y|X}(y|x)}$. In Fig. 3 we plot the feasible values of the parameter α_ϵ. We first show the impact of the skewness of the prior distribution of P_X, as we see in Fig. 3 (a), for a given privacy level ϵ, more skewness requires more perturbation, i.e., higher values of α_ϵ since low probability instances can potentially leak more information.

We next compare between the denominators of the functional forms in

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

and

$$b_{\text{LIP}}^{\text{dep.}}(x) = \frac{\Delta X}{\alpha_\epsilon P_X(x) + \epsilon}, \forall x \in \mathcal{X}.$$

Therefore, we have

$$\begin{aligned}&\alpha_\epsilon P_X(x)+\epsilon \geq \ln\left(\frac{e^\epsilon - P_{\min}}{1-P_{\min}}\right)\\ &\Rightarrow \alpha_\epsilon P_X(x) \geq \ln\left(\frac{e^\epsilon - P_{\min}}{1-P_{\min}}\right)-\epsilon\\ &\Rightarrow \alpha_\epsilon P_X(x) \geq \ln\left(\frac{e^\epsilon - P_{\min}}{1-P_{\min}}\right)-\ln\left(e^\epsilon\right)\\ &\Rightarrow \alpha_\epsilon \geq \frac{1}{P_X(x)}\times \ln\left(\frac{e^\epsilon - P_{\min}}{1-P_{\min}}\times\frac{1}{e^\epsilon}\right).\end{aligned}$$

Therefore, it is sufficient if

$$\alpha_\epsilon \geq \frac{1}{P_{\min}}\times \ln\left(\frac{e^\epsilon - P_{\min}}{1-P_{\min}}\times\frac{1}{e^\epsilon}\right).$$

This completes the proof of the Theorem.

Appendix M
Proof of Corollary 5

The second term in the leakage metric after time n can be expressed as follows:

$$\begin{aligned}\frac{P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)}{P_{\mathbf{X}_1^n|\mathbf{Y}_1^n}(\mathbf{x}_1^n|\mathbf{y}_1^n)} =&\frac{P_{\mathbf{Y}_1^n}(\mathbf{y}_1^n)}{P_{\mathbf{Y}_1^n|\mathbf{X}_1^n}(\mathbf{y}_1^n|\mathbf{x}_1^n)}\\ =&\frac{\sum_{\mathbf{x}_1^n\in\mathcal{X}^n} P_{\mathbf{Y}_1^n|\mathbf{X}_1^n}(\mathbf{y}_1^n|\mathbf{x}_1^n)P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)}{\prod_{i=1}^n P_{Y_i|X_i}(y_i|x_i)}\\ =&\frac{\sum_{\mathbf{x}_1^n\in\mathcal{X}^n} \prod_{j=1}^n P_{Y_j|X_j}(y_j|x_j)P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)}{\prod_{i=1}^n P_{Y_i|X_i}(y_i|x_i)}\\ =&P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)+\sum_{\bar{\mathbf{x}}_1^n\neq\mathbf{x}_1^n}\prod_{i=1}^n\frac{P_{Y_i|X_i}(y_i|\bar{x}_i)P_{\mathbf{X}_1^n}(\bar{\mathbf{x}}_1^n)}{P_{Y_i|X_i}(y_i|x_i)}.\end{aligned}$$

Using the property that if a mechanism satisfies ϵ-LIP, it satisfies $\min\left\{2\epsilon, \ln\frac{e^\epsilon-1+P_{\min}}{P_{\min}}\right\}$-LDP, we have:

$$\begin{aligned}&P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)+\sum_{\bar{\mathbf{x}}_1^n\neq\mathbf{x}_1^n}\prod_{i=1}^n\frac{P_{Y_i|X_i}(y_i|\bar{x}_i)P_{\mathbf{X}_1^n}(\bar{\mathbf{x}}_1^n)}{P_{Y_i|X_i}(y_i|x_i)}\\ \leq& P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)+\sum_{\bar{\mathbf{x}}_1^n\neq\mathbf{x}_1^n} e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P^k_{\min}}{P^k_{\min}}\right\}}P_{\mathbf{X}_1^n}(\bar{\mathbf{x}}_1^n)\\ =&P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)+e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P^k_{\min}}{P^k_{\min}}\right\}}(1-P_{\mathbf{X}_1^n}(\bar{\mathbf{x}}_1^n))\\ \leq& P^{\min}_{\mathbf{X}_1^n}+e^{\sum_{k=1}^n\min\left\{2\epsilon_k,\ln\frac{e^{\epsilon_k}-1+P^k_{\min}}{P^k_{\min}}\right\}}(1-P^{\min}_{\mathbf{X}_1^n}),\end{aligned}$$

where $P^{\min}_{\mathbf{X}_1^n} = \min_{\mathbf{x}_1^n\in\mathcal{X}^n} P_{\mathbf{X}_1^n}(\mathbf{x}_1^n)$, $P^k_{\min} = \min_{x\in\mathcal{X}} P_{X_k}(x)$. This completes the proof of the Corollary.

Appendix N
Proof of Corollary 6

We provide special cases: First, it can be readily verified that $2\epsilon \leq \frac{e^\epsilon-1+P^1_{\min}}{P^1_{\min}}$ when $P^1_{\min} \leq \frac{e^\epsilon-1}{2\epsilon-1}$ and $\epsilon > 1/2$. We next compare the bound on LIP leakage with the ones for LDP as follows:

- Case 1:

$$\begin{aligned}&\eta+\epsilon\leq 2\epsilon\\ \Rightarrow&\eta\leq\epsilon\\ \Rightarrow&\log\left[1+\frac{D_{\text{TV}}(\mathbf{P}_1,\mathbf{P}_2)}{\min(P^1_{\min},P^2_{\min})}\right]\leq\epsilon\\ \Rightarrow&\min(P^1_{\min},P^2_{\min})\geq\frac{D_{\text{TV}}(\mathbf{P}_1,\mathbf{P}_2)}{e^\epsilon-1}\\ \Rightarrow&D_{\text{TV}}(\mathbf{P}_1,\mathbf{P}_2)\leq\min(P^1_{\min},P^2_{\min})(e^\epsilon-1).\end{aligned}$$

- Case 2:

$$\begin{aligned}&\eta+\epsilon\leq\frac{e^\epsilon-1+P^1_{\min}}{P^1_{\min}}\\ \Rightarrow&\eta\leq\frac{e^\epsilon-1+P^1_{\min}}{P^1_{\min}}-\epsilon\triangleq\Phi\\ \Rightarrow&D_{\text{TV}}(\mathbf{P}_1,\mathbf{P}_2)\leq\min(P^1_{\min},P^2_{\min})(e^\Phi-1).\end{aligned}$$

Combining both bounds, we get the following:

$$D_{\text{TV}}(\mathbf{P}_1,\mathbf{P}_2)\leq\min(P^1_{\min},P^2_{\min})(e^{\min(\epsilon,\Phi)}-1)$$

This completes the proof of the Corollary.

References

[1] Tsachy Weissman, Erik Ordentlich, Gadiel Seroussi, Sergio Verdu, and Marcelo J Weinberger. Inequalities for the ℓ_1 deviation of the empirical distribution. *Hewlett-Packard Labs, Tech. Rep*, 2003.