Differential Privacy Mechanism for `Prio3` and `PureDpDiscreteLaplace`

July 15, 2024

Recall the definitions of pure differential privacy and the discrete Laplace distribution from [1].

Definition 1. A randomized algorithm $M : \mathcal{X}^n \to \mathcal{Y}$ satisfies ε-differential privacy if, for all $x, x' \in \mathcal{X}^n$ differing on a single element and all events $E \subset \mathcal{Y}$, we have $\mathbb{P}\left[M\left(x\right) \in E\right] \leq e^{\varepsilon} \cdot \mathbb{P}\left[M\left(x'\right) \in E\right]$.

Definition 2. The discrete Laplace distribution, with scale parameter t, is defined by the following probability density function, supported on the integers.

$$\forall x \in \mathbb{Z}, \underset{X \leftarrow \mathrm{Lap}_{\mathbb{Z}}(t)}{\mathbb{P}}\left[X = x\right] = \frac{e^{1/t} - 1}{e^{1/t} + 1} \cdot e^{-|x|/t}$$

The following differential privacy mechanism is implemented for the combination of the `PureDpDiscreteLaplace` strategy and the `Prio3Histogram` or `Prio3SumVec` VDAFs. Let $f\left(x\right)$ be the VDAF's aggregation function, operating over the integers. The aggregation function produces a query result $q = f\left(x\right) \in \mathcal{Y}$. Without loss of generality, we assume the domain $\mathcal{Y}$ is a vector of integers, $\mathcal{Y} = \mathbb{Z}^d$. Let GS_f be the global sensitivity of $f\left(x\right)$, using the replacement definition of neighboring datasets. Let $\mathbb{F}_p$ be field of prime order over which Prio3 operates. Noise is sampled from the discrete Laplace distribution $\mathrm{Lap}_{\mathbb{Z}}\left({GS_f}/{\varepsilon}\right)$, projected into the field, and added to each coordinate of aggregate share field element vectors. Let $\pi_{\mathbb{F}_p} : \mathbb{Z} \to \mathbb{F}_p$ and $\pi_{\mathbb{Z}} : \mathbb{F}_p \to \mathbb{Z}$ be the natural projections between the integers and field elements, where $\pi_{\mathbb{Z}}$ maps field elements to $[0, p)$. Let $q^* = f^*\left(x\right) \in \mathbb{F}_p^d$ be the element-wise projections of q and f into the field using $\pi_{\mathbb{F}_p}$. The un-noised aggregate shares produced by Prio3 are secret shares of the query result, $q^* = q^{(0)} + q^{(1)}$. Each aggregator samples noise from the discrete Laplace distribution and adds it to the un-noised aggregate shares, and then sends the sum as their aggregate share to the collector. If we pessimistically assume that only one honest aggregator out of the two aggregators is adding differential privacy noise, then the mechanism produces $M\left(x\right) = q^{(0)} + q^{(1)} + \pi_{\mathbb{F}_p}\left(Z\right) = q^* + \pi_{\mathbb{F}_p}\left(Z\right)$, where $Z_j \leftarrow \mathrm{Lap}_{\mathbb{Z}}\left({GS_f}/{\varepsilon}\right)$ is drawn independently for all $1 \leq j \leq d$.

Theorem 3. *$M\left(x\right) = \pi_{\mathbb{F}_p}\left(f\left(x\right)\right) + \pi_{\mathbb{F}_p}\left(Z\right), Z_j \leftarrow Lap_{\mathbb{Z}}\left({GS_f}/{\varepsilon}\right)$ satisfies ε-differential privacy.*

Proof. We will show Definition 1 holds for singleton events, where E is a set of cardinality one, then other events will follow by a union bound.

Let $q = f(x)$, $q' = f(x')$, and $q^* = \vec{\pi}_{\mathbb{F}_p}(f(x))$, and let q_j, q_j^*, and Z_j denote the j-th component of the respective vectors. Then $M_j(x) = q_j^* + \pi_{\mathbb{F}_p}(Z_j)$. Applying the probability density function of the discrete Laplace distribution, we have:

$$\begin{aligned}
\forall j \in [d], y_j \in \mathbb{F}_p, \mathbb{P}[M_j(x) = y_j] &= \mathbb{P}\left[\pi_{\mathbb{F}_p}(Z_j) = y_j - q_j^*\right] \\
&= \sum_{k=-\infty}^{\infty} \mathbb{P}[Z_j = \pi_{\mathbb{Z}}(y_j) - q_j + kp] \\
&= \sum_{k=-\infty}^{\infty} \frac{e^{\varepsilon/GS_f} - 1}{e^{\varepsilon/GS_f} + 1} e^{-\varepsilon|\pi_{\mathbb{Z}}(y_j) - q_j + kp|/GS_f} \\
&= \frac{e^{\varepsilon/GS_f} - 1}{e^{\varepsilon/GS_f} + 1} \sum_{k=-\infty}^{\infty} e^{-\varepsilon|\pi_{\mathbb{Z}}(y_j) - q_j + kp|/GS_f}
\end{aligned}$$

Since each Z_j is drawn independently, the probability of the mechanism returning some result can be found by taking the product of the probabilities for each dimension of the result vector.

$$\mathbb{P}[M(x) = y] = \left(\frac{e^{\varepsilon/GS_f} - 1}{e^{\varepsilon/GS_f} + 1}\right)^d \prod_{j=1}^{d} \sum_{k=-\infty}^{\infty} e^{-\varepsilon|\pi_{\mathbb{Z}}(y_j) - q_j + kp|/GS_f}$$

$$\mathbb{P}[M(x') = y] = \left(\frac{e^{\varepsilon/GS_f} - 1}{e^{\varepsilon/GS_f} + 1}\right)^d \prod_{j=1}^{d} \sum_{k=-\infty}^{\infty} e^{-\varepsilon\left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right|/GS_f}$$

By the definition of global sensitivity, we know $\|q - q'\|_{\ell_1} \leq GS_f$. We can break up the ℓ_1 distance between q and q' by dimension, and relate this sum of absolute values of differences to the product of multiplicative factors of $e^{\left|q_j - q_j'\right|}$, in order to get the bound we need. Let $\delta_j = q_j - q_j'$. By the triangle inequality, $|\pi_{\mathbb{Z}}(y_j) - q_j + kp| \leq \left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right| + |\delta_j|$. Since $\varepsilon > 0$ and $GS_f > 0$, then,

$$-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j) - q_j + kp| \geq -\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right| - \frac{\varepsilon}{GS_f}|\delta_j|$$

$$\begin{aligned}
e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j) - q_j + kp|} &\geq e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right| - \frac{\varepsilon|\delta_j|}{GS_f}} \\
e^{\frac{\varepsilon|\delta_j|}{GS_f}} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j) - q_j + kp|} &\geq e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right|} \\
e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right|} &\leq e^{\frac{\varepsilon|\delta_j|}{GS_f}} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j) - q_j + kp|}
\end{aligned}$$

Since the above holds for a fixed y, q and q', and any j and k, we can first add and then multiply inequalities together.

$$\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j) - q_j' + kp\right|} \leq e^{\frac{\varepsilon|\delta_j|}{GS_f}} \sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j) - q_j + kp|}$$

$$\prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j)-q'_j+kp\right|} \leq \prod_{j=1}^{d} e^{\frac{\varepsilon|\delta_j|}{GS_f}} \sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j)-q_j+kp|}$$

$$\prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j)-q'_j+kp\right|} \leq e^{\frac{\varepsilon\sum_{j=1}^{d}|\delta_j|}{GS_f}} \prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j)-q_j+kp|}$$

$$\prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j)-q'_j+kp\right|} \leq e^{\frac{\varepsilon}{GS_f}\left\|q-q'\right\|_{\ell_1}} \prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j)-q_j+kp|}$$

Then, since $\|q-q'\|_{\ell_1} \leq GS_f$,

$$\prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j)-q'_j+kp\right|} \leq e^{\frac{\varepsilon}{GS_f}GS_f} \prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j)-q_j+kp|}$$

$$\prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}\left|\pi_{\mathbb{Z}}(y_j)-q'_j+kp\right|} \leq e^{\varepsilon} \prod_{j=1}^{d}\sum_{k=-\infty}^{\infty} e^{-\frac{\varepsilon}{GS_f}|\pi_{\mathbb{Z}}(y_j)-q_j+kp|}$$

This shows that $\mathbb{P}\left[M\left(x'\right)=y\right] \leq e^{\varepsilon} \cdot \mathbb{P}\left[M\left(x\right)=y\right]$. By applying union bounds, then $\mathbb{P}\left[M\left(x'\right)\in E\right] \leq e^{\varepsilon} \cdot \mathbb{P}\left[M\left(x\right)\in E\right]$ as well, and thus $M\left(x\right)$ satisfies ε-differential privacy. □

References

[1] Canonne, C. L., Kamath, G., and Steinke, T., “The Discrete Gaussian for Differential Privacy”, 2020, <https://arxiv.org/abs/2004.00010>.