The Optimal Mechanism in Additive Differential Privacy

Quan Geng, Wei Ding, Ruiqi Guo, and Sanjiv Kumar

Google AI

Gmail: {qgeng, vvei, guorq, sanjivk}@google.com

Abstract

We derive the optimal **(0, δ)**-differentially private query-output independent noise-adding mechanism for single real-valued query function.

We show that the optimal noise probability distribution is a uniform distribution with a probability mass at the origin.

Background on Differential Privacy

A randomized mechanism K satisfies **(ε, δ)-differential privacy** if for any two neighboring datasets D_1 and D_2 differing by one element, and all $S \subset Range(K)$

$$Pr[\mathcal{K}(D_1) \in S] \le e^{\epsilon}\ Pr[\mathcal{K}(D_2) \in S] + \delta.$$

In the special case ε=0, the constraint for **(0, δ)-differential privacy** is

$$\boxed{\Pr[\mathcal{K}(D_1) \in S] \le \Pr[\mathcal{K}(D_2) \in S] + \delta.}$$

Problem Formulation

Query sensitivity $\quad \Delta := \max_{D_1, D_2 \in \mathcal{D}} |q(D_1) - q(D_2)|$

Query-output independent noise-adding mechanisms

K(D) = q(D) + noise

Constraint on the noise probability distribution **P**

$$\mathcal{P}(S) \le \mathcal{P}(S+d) + \delta, \forall\ |d| \le \Delta, \text{measurable set } S \subset \mathbb{R}.$$

Cost model on the additive noise

Symmetric cost function on the noise: $\quad \ell(\cdot) : \mathcal{R} \to \mathcal{R}$

Expected cost: $\quad \int_{x \in \mathbb{R}} \mathcal{L}(x)\mathcal{P}(dx).$

Optimization problem to solve

$$\boxed{\begin{array}{c} \underset{\mathcal{P}}{\text{minimize}} \int_{x \in \mathbb{R}} \mathcal{L}(x)\mathcal{P}(dx) \\ \text{subject to } \forall \text{ measurable set } S \subseteq \mathbb{R},\ \forall |d| \le \Delta. \\ |\mathcal{P}(S) - \mathcal{P}(S+d)| \le \delta \end{array}}$$

Main Result

As the loss function L is symmetric, without loss of generality, assume P is symmetric.

Assuming L is monotonically increasing for x ≥ 0.

Consider the class of symmetric noise distributions **SP** whose "p.d.f." monotonically decreases for x ≥ 0,

$$\boxed{\inf_{\mathcal{P} \in \mathcal{SP}} \int_{x \in \mathbb{R}} \mathcal{L}(x)\mathcal{P}(dx) = \inf_{\alpha \in [0,\delta)} \int_{x \in \mathbb{R}} \mathcal{L}(x)\mathcal{P}_\alpha(dx).}$$

The optimal parameter α depends on the privacy parameters δ and loss function L

where $\mathcal{P}_\alpha$ is defined as

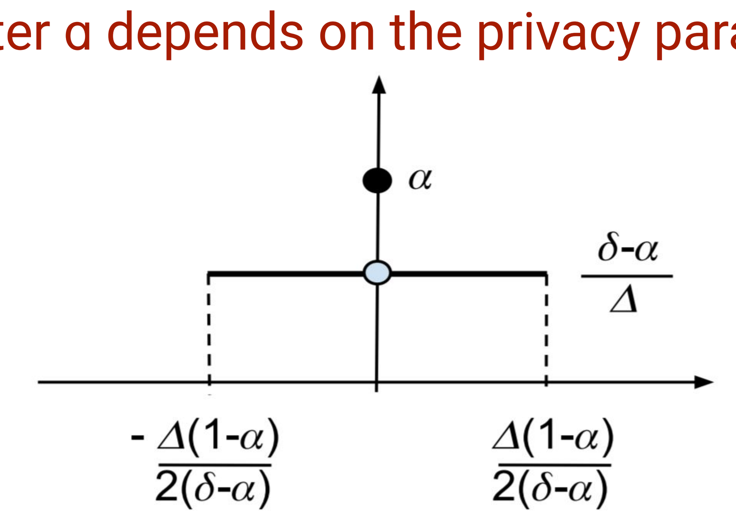


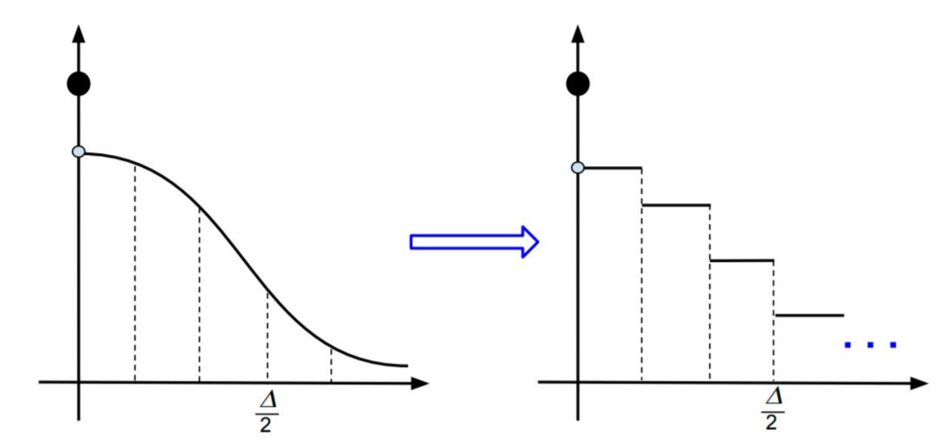
Figure 1: Probability distribution of $\mathcal{P}_\alpha$. $\mathcal{P}_\alpha$ has a probability mass $\alpha \in [0, \delta)$ at the origin, and has a uniform distribution over $[-\frac{1-\alpha}{\delta-\alpha}\frac{\Delta}{2}, \frac{1-\alpha}{\delta-\alpha}\frac{\Delta}{2}] \setminus \{0\}$ with probability density $\frac{\delta-\alpha}{\Delta}$.

Proof Ideas

Sufficient and necessary condition for preserving (0, δ)-differential privacy (assuming P is symmetric and monotonic)

$$\boxed{\mathcal{P}([-\frac{\Delta}{2}, \frac{\Delta}{2}]) \le \delta.}$$

Step 1: Discretize the probability distribution



Step 2: Rearrange the tail distribution

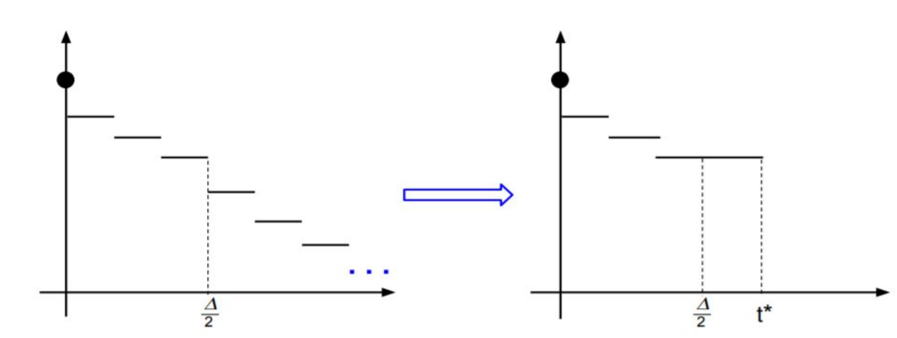


Figure 3: Re-arrange the probability distribution in $[\frac{\Delta}{2}, +\infty)$ to be a step.

Step 3: Rearrange the distribution in [0, Δ/2]

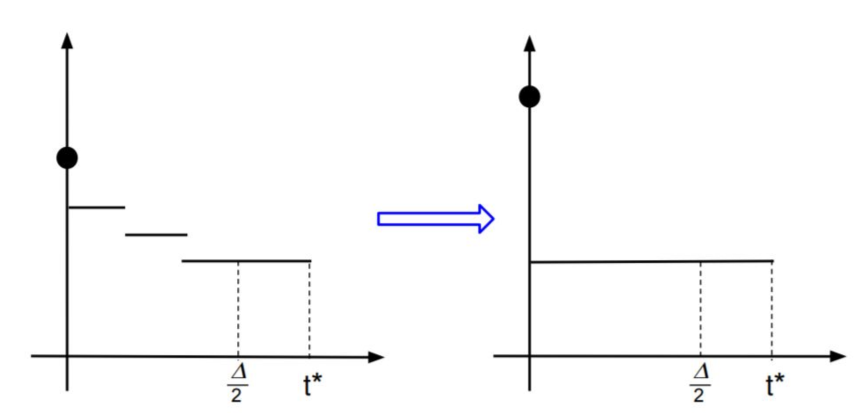


Figure 4: Re-arrange the probability distribution in $(0, \frac{\Delta}{2})$ to be uniform and put the extra probability mass at the origin.

Applications

Let $V(\mathcal{P}) := \int_{x \in \mathbb{R}} \mathcal{L}(x)\mathcal{P}(dx)$, i.e., $V(\mathcal{P})$ denote the expectation of the cost given the noise probability distribution $\mathcal{P}$ for the cost function $\mathcal{L}(\cdot)$.

Theorem 3. *Given $0 < \delta < 1$ and the query sensitivity $\Delta > 0$. For the general momentum cost function $\ell^p(x) := |x|^p$, where $p > 0$, the optimal noise probability distribution to preserve $(0, \delta)$-differential privacy with query sensitivity Δ is $\mathcal{P}_{\alpha^*}$ with*

$$\alpha^* = \begin{cases} 0, & \text{for } \delta \in (0, \frac{p}{p+1}] \\ (p+1)\delta - p, & \text{for } \delta \in (\frac{p}{p+1}, 1) \end{cases}$$

and the minimum cost is

$$V(\mathcal{P}_{\alpha^*}) = \begin{cases} \frac{\Delta^p}{2^p(p+1)\delta^p}, & \text{for } \delta \in (0, \frac{p}{p+1}] \\ \frac{(p+1)^p}{2^p p^p}(1-\delta)\Delta^p, & \text{for } \delta \in (\frac{p}{p+1}, 1) \end{cases}$$

Corollary: Optimal Noise Magnitude

$$\boxed{\begin{cases} \frac{\Delta}{4\delta}, & \text{for } \delta \in (0, \frac{1}{2}] \\ (1-\delta)\Delta, & \text{for } \delta \in (\frac{1}{2}, 1) \end{cases}}$$

Corollary: Optimal Noise Power

$$\boxed{\begin{cases} \frac{\Delta^2}{12\delta^2}, & \text{for } \delta \in (0, \frac{2}{3}] \\ \frac{9}{16}(1-\delta)\Delta^2, & \text{for } \delta \in (\frac{2}{3}, 1) \end{cases}}$$

Paper link https://arxiv.org/abs/1809.10224