Tight Analysis of Privacy and Utility Tradeoff in Approximate Differential Privacy

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

Google AI

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

ISIT 2019 PARIS JULY 7-12, 2019

Abstract

We characterize the minimum noise amplitude and power for query-output independent noise-adding mechanisms in (ε, δ)-differential privacy (DP) for single real-valued query function.

- We derive new **lower bounds** using the duality of linear programming.
- We derive new **upper bounds** by analyzing a special class of truncated Laplacian mechanisms.
- We show that the **multiplicative gap** of the lower bounds and upper bounds **goes to zero** in various high privacy regimes, proving the tightness of the lower and upper bounds.
- In particular, our results close the previous constant multiplicative gap in the discrete setting.
- Numeric experiments show the improvement of the truncated Laplacian mechanism over the optimal Gaussian mechanism in all privacy regimes.

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 $S \subset Range(K)$

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

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**

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

Minimum noise amplitude and noise power under DP constraint

$$V_1^* := \inf_{\mathcal{P} \in \mathcal{P}_{\epsilon,\delta}} \int_{x \in \mathbb{R}} |x| \mathcal{P}(dx) \quad \text{(minimum noise amplitude)},$$

$$V_2^* := \inf_{\mathcal{P} \in \mathcal{P}_{\epsilon,\delta}} \int_{x \in \mathbb{R}} x^2 \mathcal{P}(dx) \quad \text{(minimum noise power)}.$$

Goal: derive tight lower and upper bounds

$$V_1^{low} \le V_1^* \le V_1^{upp} \text{ and } V_2^{low} \le V_2^* \le V_2^{upp}$$

Upper Bounds: Truncated Laplacian Mechanism

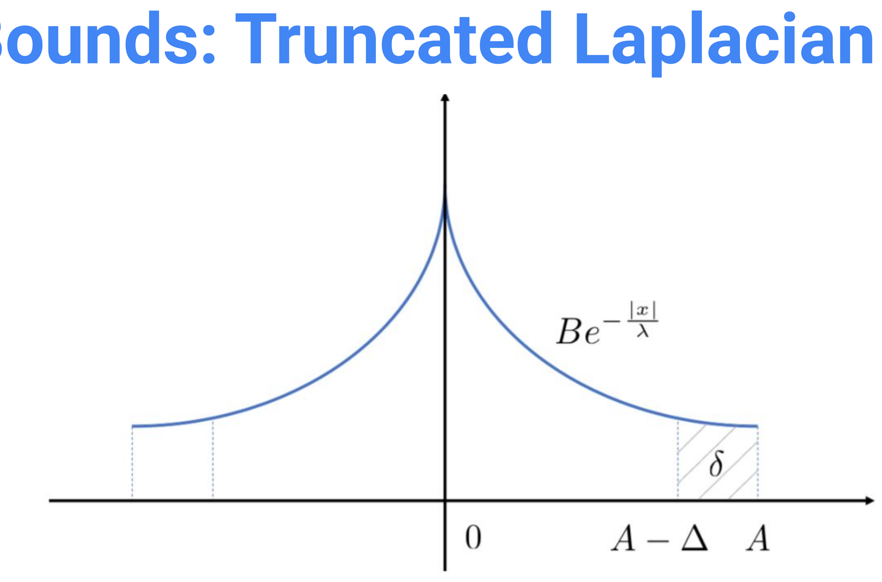


Figure 1: Noise probability density function f_{TLap} of the truncated Laplacian mechanism. f_{TLap} is a symmetric truncated exponentinal function with a probability mass δ in the last interval with length Δ in the support of f_{TLap}, i.e., the interval $[A-\Delta, A]$. The decay rate $\frac{f_{\text{TLap}}(x)}{f_{\text{TLap}}(x+\Delta)}$ is exactly e^{ϵ} for $x \in [0, A-\Delta)$. The parameters A and B are then derived by solving the equations that $\int_{x\in\mathbb{R}} f_{\text{TLap}}(x)dx = 1$ and $\int_{A-\Delta}^{A} f_{\text{TLap}}(x)dx = \delta$.

Theorem 1. *The truncated Laplacian mechanism preserves (ϵ, δ)-differential privacy.*

Upper bounds on minimum noise amplitude and noise power

$$V_1^* \le V_1^{upp} := \frac{\Delta}{\epsilon}\left(1 - \frac{\log(1 + \frac{e^{\epsilon}-1}{2\delta})}{\frac{e^{\epsilon}-1}{2\delta}}\right).$$

$$V_2^* \le V_2^{upp} := \frac{2\Delta^2}{\epsilon^2}\left(1 - \frac{\frac{1}{2}\log^2(1 + \frac{e^{\epsilon}-1}{2\delta}) + \log(1 + \frac{e^{\epsilon}-1}{2\delta})}{\frac{e^{\epsilon}-1}{2\delta}}\right).$$

Lower Bounds: Duality of Linear Programming

Define

$$a := \frac{\delta + \frac{e^{\epsilon}-1}{2}}{e^{\epsilon}}, \qquad b := e^{-\epsilon}.$$

To avoid integer rounding issues, assume that there exists an integer n such that $\sum_{k=0}^{n-1} ab^k = \frac{1}{2}$.

Theorem 4 (Lower Bound on Minimum Noise Amplitude).

$$V_1^* \ge V_1^{low} := 2a \sum_{k=0}^{n-1} b^k k \Delta = 2a \left(\frac{b - b^n}{(1-b)^2} - \frac{(n-1)b^n}{1-b} \right) \Delta.$$

Theorem 5 (Lower Bound on Minimum Noise Power). *Define*

$$\begin{aligned} V_2^{low} &:= 2 \sum_{k=0}^{n-1} ab^k k^2 \Delta^2 \\ &= \frac{2a\Delta^2}{1-b}\left[-b + 2\left(\frac{b(1-b^{n-1})}{(1-b)^2} - \frac{(n-1)b^n}{1-b}\right) - \frac{b^2(1-b^{n-2})}{1-b} - (n-1)^2 b^n\right]. \end{aligned}$$

We have

$$V_2^* \ge V_2^{low}.$$

Tightness of the Lower and Upper Bounds

$$\lim_{\epsilon \to 0} \frac{V_1^{low}}{V_1^{upp}} \ge 1 - 2\delta.$$

$$\lim_{\delta \to 0} \frac{V_1^{low}}{V_1^{upp}} \ge \frac{\epsilon}{e^{\epsilon} - 1} = 1 - \frac{\epsilon}{2} + O(\epsilon^2).$$

$$\lim_{\epsilon = \delta \to 0} \frac{V_1^{low}}{V_1^{upp}} = 1.$$

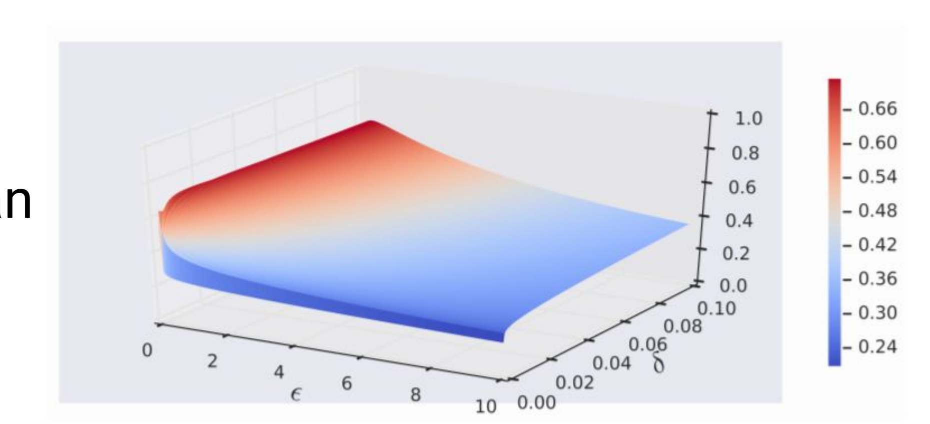
$$\lim_{\epsilon \to 0} \frac{V_2^{low}}{V_2^{upp}} \ge (1-\delta)(1-2\delta) = 1 - 3\delta + 2\delta^2.$$

$$\lim_{\delta \to 0} \frac{V_2^{low}}{V_2^{upp}} \ge \frac{\epsilon^2(1+e^{\epsilon})}{2(e^{\epsilon}-1)^2} = 1 - \frac{\epsilon}{2} + O(\epsilon^2).$$

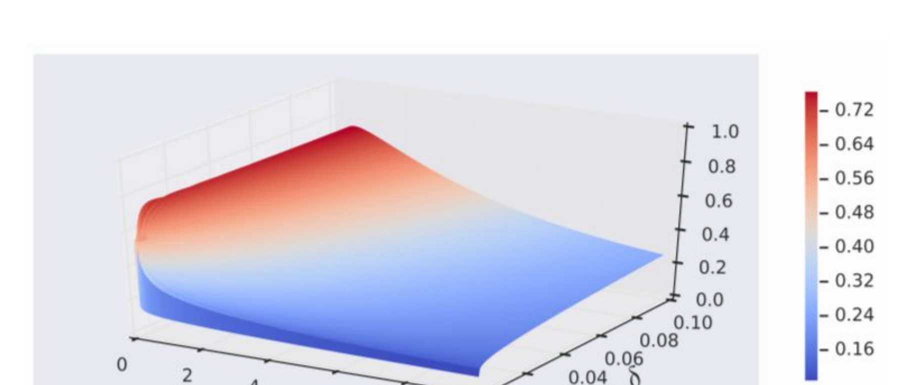
$$\lim_{\epsilon = \delta \to 0} \frac{V_2^{low}}{V_2^{upp}} = 1.$$

Comparison with the Optimal Gaussian Mechanism

Ratio of the noise amplitude and power between truncated Laplacian mechanism and the Optimal Gaussian Mechanism.



Top: Noise Amplitude
Bottom: Noise power



Paper link https://arxiv.org/abs/1810.00877