Harvard Privacy Tools Project

Reasoning About Utility of the Snapping Mechanism

Christian Covington

August 5, 2019

1 Snapping Mechanism Introduction

The snapping mechanism is a differentially-private mechanism introduced in Mironov (2012) that avoids the vulnerabilities[1] of the Laplace mechanism that were first demonstrated in the same paper. Our goal is to assess (both empirically and theoretically) the utility loss of using the snapping mechanism as opposed to the Laplace mechanism.

2 Definitions

2.1 Laplace Mechanism

Let f be a function computed on a dataset D with sensitivity Δ_f and ϵ be the desired privacy parameter. Further, let $\lambda = \frac{\Delta_f}{\epsilon}$ the Laplace Mechanism is defined as:

$$M_L(D, f(\cdot), \lambda) = f(D) + Y$$

where $Y \sim Laplace(\lambda)$.

2.2 Snapping Mechanism

Let B be a user-chosen quantity that reflects beliefs about reasonable bounds on $f(D)$ and Λ be the smallest power of two at least as large as λ. Using the same notation as above, the snapping mechanism is defined as:

$$M_S(D, f(\cdot), \lambda, B) = clamp_B\left(\lfloor clamp_B\left(f(D)\right) \oplus Y \rceil_\Lambda\right).$$

where $clamp_B(\cdot)$ restricts output to the interval $[-B, B]$ and $\lfloor \cdot \rceil_\Lambda$ rounds to the nearest multiple of Λ, with ties resolved toward $+\infty$. We will also make use of $\lfloor \cdot \rceil^*_\Lambda$, which rounds to the nearest multiple of Λ, with ties resolved toward $-\infty$.

[1] due to sampling from floating-point numbers rather than the reals

2.3 Utility

This remains undefined for now.

3 Mechanism Comparison

3.1 Distance

We first examine the distance between output from the Laplace and Snapping Mechanisms. We define the distance as follows:

$$d_{M_L,M_S}(D, f(\cdot), \lambda, B) = \left|M_L(\cdot) - M_S(\cdot)\right|$$

which we will refer to as *dist* for ease of notation.

Let D, f, λ be fixed. We will assume that $f(D) > 0$, but letting $f(D) \leq 0$ changes only the strictness of equality at certain points.[2] We consider different circumstances with respect to B:

3.1.1 Case 1: $clamp_B$ never binding

Consider the case in which both $f(D)$ and $\lfloor f(D) + Y \rceil_\Lambda$ lie in the interval $[-B, B]$. Then $clamp_B$ is never binding and we can ignore it. Then we have:

$$dist_1 = \left|f(D) + Y - \lfloor f(D) + Y \rceil_\Lambda\right|$$

We know that $f(D) + Y$ is, at most, $\frac{\Lambda}{2}$ away from the nearest multiple of Λ. Furthermore, we have $\Lambda = 2^m$ for some $m \in \mathbb{Z}$ so that $2^{m-1} < \lambda \leq 2^m$. Thus, we know:

$$\begin{aligned} dist_1 &= \left|f(D) + Y - \lfloor f(D) + Y \rceil_\Lambda\right| \\ &\leq \frac{\Lambda}{2} \\ &= \frac{2^m}{2} \\ &= 2^{m-1} \\ &< \lambda. \end{aligned}$$

We can now consider the expectation.

3.1.2 Case 2: inner $clamp_B$ binding

Consider the case in which $f(D) \notin [-B, B]$ but $\lfloor clamp_B\,(f(D)) + Y \rceil_\Lambda \in [-B, B]$. Because we assume $f(D) > 0$, we know that $f(D) > B$. We keep the inner clamp and ignore the outer and get:

$$\begin{aligned} dist_2 &= \left|f(D) + Y - \lfloor clamp_B\,(f(D)) + Y \rceil_\Lambda\right| \\ &= \left|f(D) + Y - \lfloor B + Y \rceil_\Lambda\right| \end{aligned}$$

Similar to Case 1, we know that $\lfloor B + Y \rceil_\Lambda$ is at most $\frac{\Lambda}{2}$ away from $B + Y$. More precisely, we know

$$B + Y - \frac{\Lambda}{2} < \lfloor B + Y \rceil_\Lambda \leq B + Y + \frac{\Lambda}{2}$$

[2] I think ...

so we can use this to bound $dist_2$:

$$\begin{aligned}
dist_2 &= \left| f(D) + Y - \lfloor B + Y \rceil_\Lambda \right| \\
&< \left| f(D) + Y - \left(B + Y - \frac{\Lambda}{2} \right) \right| \\
&= \left| f(D) - B + \frac{\Lambda}{2} \right| \\
&= f(D) - B + \frac{\Lambda}{2} \\
&< f(D) - B + \lambda
\end{aligned}$$

3.1.3 Case 3: outer $clamp_B$ binding

Now we consider the case in which $f(D) \in [-B, B]$ but $\lfloor f(D) + Y \rceil_\Lambda \notin [-B, B]$. We know then that $clamp_B \left(\lfloor f(D) + Y \rceil_\Lambda \right) \in \{-B, B\}$. So we have:

$$\begin{aligned}
dist_3 &= \left| f(D) + Y - clamp_B \left(\lfloor f(D) + Y \rceil_\Lambda \right) \right| \\
&= \left| f(D) + Y \pm B \right|
\end{aligned}$$

This is technically unbounded because Y is unbounded, so we should probably return to this and try another approach (e.g. getting the expectation or bounding with high probability).

3.1.4 Case 4: both $clamp_B$ binding

Finally, we consider the case in which $f(D) \notin [-B, B]$ and $\lfloor clamp_B (f(D)) + Y \rceil_\Lambda \notin [-B, B]$. Because $f(D) > 0$, we know that $clamp_B (f(D)) = B$. So,

$$\begin{aligned}
dist_4 &= \left| f(D) + Y - clamp_B \left(\lfloor clamp_B (f(D)) + Y \rceil_\Lambda \right) \right| \\
&= \left| f(D) + Y - clamp_B \left(\lfloor B + Y \rceil_\Lambda \right) \right| \\
&= \left| f(D) + Y \pm B \right|
\end{aligned}$$

As for Case 3, this is unbounded.