Verifying Snapping Mechanism

October 9, 2019

1 Formalization - without Clamping

Definition 1 ($\mathsf{Snap}(\mu, a) : \mathsf{Distr}(U) \to A \to \mathsf{Distr}(B)$)
The ideal Snapping mechanism without clamp operation is defined as:

$$\mathsf{Snap}(\mu, a) = u \leftarrow \mu; \lfloor f(a) + \frac{S \cdot \log(u)}{\epsilon} \rceil_\Lambda$$

where f is the query function over input $a \in A$, ϵ is the privacy budget and S sampled from $\{-1, +1\}$ with $\mathsf{Bernoulli}(0.5)$.

Definition 2 (ϵ **- dilation**)
.

Let $\epsilon \geq 0$. The ϵ-dilation $D_\epsilon(\mu_1, \mu_2)$ between two sub-distributions $\mu_1 \in \mathsf{Distr}(U)$, $\mu_2 \in \mathsf{Distr}(U)$is defined as:

$$\sup_{E \in U} \Big(\Pr_{x \leftarrow \mu_1}[x \in E] - \exp(\epsilon) \Pr_{x \leftarrow \mu_2}[x \in \exp(-\epsilon) \cdot E]] \Big)$$

Proposition 1 (**(ϵ, δ)-differential privacy**)
For every pair of sub-distributions $\mu_1 \in \mathsf{Distr}(U)$, $\mu_2 \in \mathsf{Distr}(U)$, s.t.

$$D_\epsilon(\mu_1, \mu_2) \leq \delta,$$

The snapping mechanism $\mathsf{Snap}(\mu, a) : \mathsf{Distr}(U) \to A \to \mathsf{Distr}(B)$ is (ϵ, δ) - differentially private w.r.t. an adjacency relation Φ for every two adjacent inputs a, a' and μ_1, μ_2

Proof. Followed directly by unfolding the Snap mechanism.

$$\begin{array}{rcl}
\Pr_{x \leftarrow \mathsf{Snap}(\mu_1, a)}[x = e] & = & \Pr_{u \leftarrow \mu_1}[\lfloor f(a) + \frac{S \cdot \log(u)}{\epsilon} \rceil_\Lambda = e] \\
& = & \Pr_{u \leftarrow \mu_1}[u \in [\frac{\exp((e - \frac{\Lambda}{2} - f(a))\epsilon)}{S}, \frac{\exp((e + \frac{\Lambda}{2} - f(a))\epsilon)}{S})] \\
& \leq & \exp(\epsilon) \Pr_{u \leftarrow \mu_2}[u \in \exp(-\epsilon)[\frac{\exp((e - \frac{\Lambda}{2} - f(a))\epsilon)}{S}, \frac{\exp((e + \frac{\Lambda}{2} - f(a))\epsilon)}{S})] \\
& = & \exp(\epsilon) \Pr_{u \leftarrow \mu_2}[\lfloor f(a') + \frac{S \cdot \log(u)}{\epsilon} \rceil_\Lambda = e] \\
& = & \exp(\epsilon) \Pr_{x \leftarrow \mathsf{Snap}(\mu_2, a')}[x = e]
\end{array}$$

□

Definition 3 (**(ϵ, δ) - Dilation lifting**)
Two sub-distributions $\mu_1 \in \mathsf{Distr}(U_1)$, $\mu_2 \in \mathsf{Distr}(U_2)$are related by the (ϵ, δ) - dilation lifting of $\Psi \subseteq U_1 \times U_2$, written $\mu_1 \Psi^{\#(\epsilon,\delta)} \mu_2$, if there exist two witness sub-distributions $\mu_L \in \mathsf{Distr}(U_1 \times U_2)$ and $\mu_R \in \mathsf{Distr}(U_1, U_2)$ s.t.:

1. $\pi_1(\mu_L) = \mu_1$ and $\pi_2(\mu_R) = \mu_2$;
2. $\mathsf{supp}(\mu_L) \subseteq \Psi$ and $\mathsf{supp}(\mu_R) \subseteq \Psi$; and

3. $D_\epsilon(\mu_L, \mu_R) \leq \delta$.

It is easy to see that two sub-distributions μ_1 and μ_2 are related by $=^{\#(\epsilon,\delta)}$ iff $D_\epsilon(\mu_1, \mu_2) \leq \delta$. Therefore, the Snap mechanism $\mathsf{Distr}(U) \to A \to \mathsf{Distr}(B)$ is $(\epsilon,\delta)-$ differentially private w.r.t. and adjacency relation Φ and μ_1, μ_2 iff:

$$\mu_1 =^{\#(\epsilon,\delta)} \mu_2$$

for every two adjacent inputs a and a'.

2 Formalization - with Clamping

Definition 4 ($\mathsf{Snap}(\mu, a) : \mathsf{Distr}(U) \to A \to \mathsf{Distr}(B)$)
The ideal Snapping mechanism is defined as:

$$\mathsf{Snap}(\mu, a) = u \leftarrow \mu; \mathsf{clamp}_B(\lfloor \mathsf{clamp}_B(f(a)) + \frac{S \cdot \log(u)}{\epsilon} \rfloor_\Lambda)$$

where f is the query function over input $a \in A$, ϵ is the privacy budget and S sampled from $\{-1, +1\}$ with $\mathsf{Bernoulli}(0.5)$.

Definition 5 (ϵ **- dilation**)
.

Let $\epsilon \geq 0$. The ϵ-dilation $D_\epsilon(\mu_1, \mu_2)$ between two sub-distributions $\mu_1 \in \mathsf{Distr}(U)$, $\mu_2 \in \mathsf{Distr}(U)$is defined as:

$$\underset{E \in U}{sup}\Big(\Pr_{x \leftarrow \mu_1}[x \in E] - \exp(\epsilon) \Pr_{x \leftarrow \mu_2}[x \in \exp(-\epsilon) \cdot E]\Big)$$

Proposition 2 (**(ϵ, δ)-differential privacy**)
For every pair of sub-distributions $\mu_1 \in \mathsf{Distr}(U)$, $\mu_2 \in \mathsf{Distr}(U)$, s.t.

$$D_\epsilon(\mu_1, \mu_2) \leq \delta,$$

The snapping mechanism $\mathsf{Snap}(\mu, a) : \mathsf{Distr}(U) \to A \to \mathsf{Distr}(B)$ is (ϵ, δ) - differentially private w.r.t. an adjacency relation Φ for every two adjacent inputs a, a' and μ_1, μ_2

Proof. Followed directly by unfolding the Snap mechanism.

$$\begin{aligned}
\Pr_{x \leftarrow \mathsf{Snap}(\mu_1, a)}[x = e] &= \Pr_{u \leftarrow \mu_1}[\lfloor f(a) + \tfrac{S \cdot \log(u)}{\epsilon} \rfloor_\Lambda = e] \\
&= \Pr_{u \leftarrow \mu_1}[u \in [\tfrac{\exp((e - \frac{\Lambda}{2} - f(a))\epsilon)}{S}, \tfrac{\exp((e + \frac{\Lambda}{2} - f(a))\epsilon)}{S})] \\
&\leq \exp(\epsilon) \Pr_{u \leftarrow \mu_2}[u \in \exp(-\epsilon)[\tfrac{\exp((e - \frac{\Lambda}{2} - f(a))\epsilon)}{S}, \tfrac{\exp((e + \frac{\Lambda}{2} - f(a))\epsilon)}{S})] \\
&= \exp(\epsilon) \Pr_{u \leftarrow \mu_2}[\lfloor f(a') + \tfrac{S \cdot \log(u)}{\epsilon} \rfloor_\Lambda = e] \\
&= \exp(\epsilon) \Pr_{x \leftarrow \mathsf{Snap}(\mu_2, a')}[x = e]
\end{aligned}$$

□

Definition 6 (**(ϵ, δ) - Dilation lifting**)
Two sub-distributions $\mu_1 \in \mathsf{Distr}(U_1)$, $\mu_2 \in \mathsf{Distr}(U_2)$are related by the (ϵ, δ) - dilation lifting of $\Psi \subseteq U_1 \times U_2$, written $\mu_1 \Psi^{\#(\epsilon,\delta)} \mu_2$, if there exist two witness sub-distributions $\mu_L \in \mathsf{Distr}(U_1 \times U_2)$ and $\mu_R \in \mathsf{Distr}(U_1, U_2)$ s.t.:

1. $\pi_1(\mu_L) = \mu_1$ and $\pi_2(\mu_R) = \mu_2$;
2. $\mathsf{supp}(\mu_L) \subseteq \Psi$ and $\mathsf{supp}(\mu_R) \subseteq \Psi$; and
3. $D_\epsilon(\mu_L, \mu_R) \leq \delta$.

It is easy to see that two sub-distributions μ_1 and μ_2 are related by $=^{\#(\epsilon,\delta)}$ iff $D_\epsilon(\mu_1,\mu_2) \leq \delta$. Therefore, the Snap mechanism $\mathsf{Distr}(U) \to A \to \mathsf{Distr}(B)$ is $(\epsilon,\delta)-$ differentially private w.r.t. and adjacency relation Φ and μ_1, μ_2 iff:

$$\mu_1 =^{\#(\epsilon,\delta)} \mu_2$$

for every two adjacent inputs a and a'.