The Optimal Mechanism in (ϵ, δ)-Differential Privacy

Quan Geng

University of Illinois at Urbana Champaign

- (ϵ, δ)-differential privacy

$$\mathbf{Pr(K(D_1) \in S) \leq e^{\epsilon} Pr(K(D_2) \in S) + \delta}$$

- Two special cases:
  - $(\boldsymbol{\epsilon}, \mathbf{0})$-differential privacy
    - well studied in the literature: Laplacian Mechanism, Staircase Mechanism
  - $(\mathbf{0}, \boldsymbol{\delta})$-differential privacy

$$\|P_{K(D_1)} - P_{K(D_2)}\|_{\mathrm{TV}} \leq \delta$$

(ϵ,δ)-Differential Privacy

- (ϵ, δ)-differential privacy

$$\mathbf{Pr}(\mathbf{K}(\mathbf{D_1}) \in \mathbf{S}) \leq \mathbf{e}^{\epsilon}\, \mathbf{Pr}(\mathbf{K}(\mathbf{D_2}) \in \mathbf{S}) + \boldsymbol{\delta}$$

- Assuming instance-independent noise-adding mechanisms, what is the **optimal** noise probability distribution?

- **Our Results**:
  - $(0, \delta)$-DP

    Optimality of **Uniform Noise Mechanism**

  - (ϵ, δ)-DP

    Near-Optimality of **Laplacian** and **Uniform Noise Mechanism** in high privacy regime as $(\epsilon, \delta) \to (0,0)$,

    Error bound: $\Theta(\min\left(\frac{1}{\epsilon}, \frac{1}{\delta}\right)),$

Problem Formulation

$$V^* := \min_{P} \sum_{i=-\infty}^{+\infty} L(i)P(i)$$

$$\text{s.t.} \quad P(S) \le e^{\epsilon} P(S + d) + \delta,$$
$$\forall S \subset Z, d \in Z, |d| \le \Delta$$

$\boldsymbol{L}: Z \to Z$ cost function on the noise

$\boldsymbol{P}$: noise probability mass function

$\boldsymbol{\Delta}$: global sensitivity

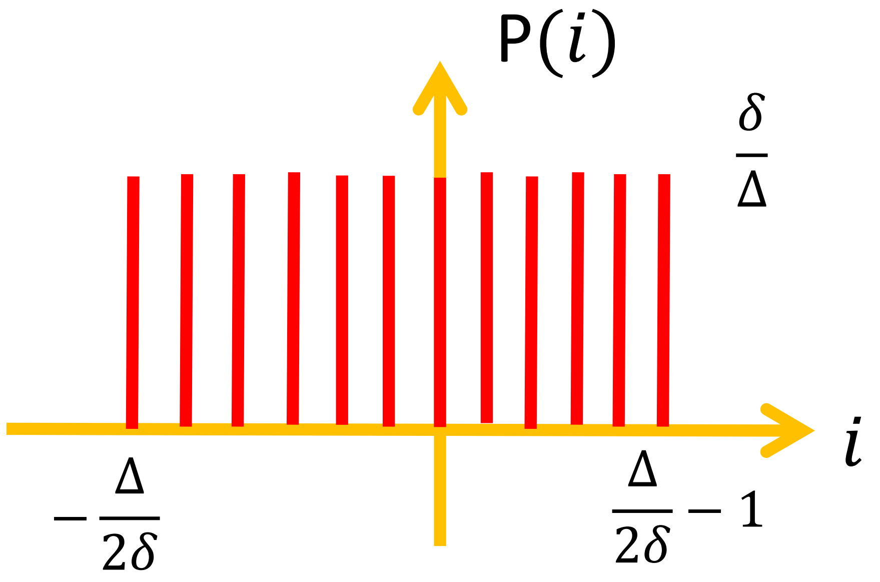
$(0,\delta)$-DP: General $\boldsymbol{\Delta}$

$$V^* := \min \sum_{i=-\infty}^{+\infty} L(i)P(i)$$

$$\text{s.t.} \quad P(S) \le P(S+d) + \delta, \quad \forall S \subset Z, d \in Z, |d| \le \Delta$$

- **Upper Bound:** Uniform Noise Mechanism

$$V^* \le V_{UB} := 2\sum_{i=1}^{\frac{\delta}{2\Delta}-1} \frac{\delta}{\Delta} L(i) + \frac{\delta}{\Delta} L(\frac{\Delta}{2\delta})$$



$(0,\delta)$-DP: General Δ

$$V^* := \min \sum_{i=-\infty}^{+\infty} L(i)P(i)$$

$$\text{s.t.} \quad P(S) \leq P(S+d) + \delta, \quad \forall S \subset Z, d \in Z, |d| \leq \Delta$$

- **Lower Bound:** Duality of Linear Programming

choose $S = S_k = \{l: l \geq k\}$, then $\sum_{i=k}^{k+\Delta-1} P(i) \leq \delta, \forall k$

$$\begin{aligned}
V_{LB} := \min \quad & 2\sum_{k=1}^{\infty} \mathcal{L}(k)\mathcal{P}_k \\
\text{such that} \quad & \mathcal{P}_k \geq 0 \quad \forall k \in N \\
& \frac{\mathcal{P}_0}{2} + \sum_{k=1}^{\infty} \mathcal{P}_k \geq \frac{1}{2} \\
-\sum_{\ell=0}^{\Delta-1} \mathcal{P}_{k+\ell} \geq -\delta, & \quad \forall k \in \mathbb{N}.
\end{aligned}$$

$$V_{LB} = 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} L(1+i\Delta)$$

$(0,\delta)$-DP: Comparison of V_{LB}, V_{UB}

- $L(i) = |i|$

$$V_{LB} = \frac{\Delta}{4\delta} + 1 - \frac{\Delta}{2},$$
$$V_{UB} = \frac{\Delta}{4\delta},$$

Additive gap goes to 0

- $L(i) = |i|^2$

$$V_{LB} = \frac{\Delta^2}{12\delta^2} - \frac{\Delta^2}{4\delta} + \Delta(\frac{1}{2\delta} - 1) + \frac{\Delta^2}{6} + 1,$$
$$V_{UB} = \frac{\Delta^2}{12\delta^2} + \frac{1}{6},$$

- $L(i) = |i|^m$

$$\lim_{\delta \to 0} \frac{V_{UB}}{V_{LB}} = 1.$$

Multiplicative gap goes to 0

(ϵ,δ)-DP: Upper Bound

$$V^* := \min \sum_{i=-\infty}^{+\infty} L(i)P(i)$$

$$\text{s.t.} \quad P(S) \leq e^{\epsilon} P(S+d) + \delta, \quad \forall S \subset Z, d \in Z, |d| \leq \Delta$$

- Both **(ϵ,0)**-DP and **(0,δ)**-DP imply (ϵ,δ)-DP

$$\boldsymbol{V^* \leq min\,(V_{Lap}, V_{Uniform})}$$

(ϵ,δ)-DP: Comparison of $\boldsymbol{V_{LB}}, \boldsymbol{V_{UB}}$

- $\boldsymbol{L(i)} = |\boldsymbol{i}|$, as $(\epsilon,\delta) \rightarrow (0,0)$

$$\Theta\left(\min\left(\frac{1}{\epsilon},\frac{1}{\delta}\right)\right) \leq V_{LB} \leq V^* \leq V_{UB} = \Theta(\min\left(\frac{1}{\epsilon},\frac{1}{\delta}\right))$$

- $\boldsymbol{L(i)} = |\boldsymbol{i}|^2$, as $(\epsilon,\delta) \rightarrow (0,0)$

$$\Theta\left(\min\left(\frac{1}{\epsilon^2},\frac{1}{\delta^2}\right)\right) \leq V_{LB} \leq V^* \leq V_{UB} = \Theta(\min\left(\frac{1}{\epsilon^2},\frac{1}{\delta^2}\right))$$

Conclusion

- Near-Optimality of Uniform Noise Mechanism in $(0, \delta)$-DP

- Trade-off between $\boldsymbol{\epsilon}$ and $\boldsymbol{\delta}$

$$\mathrm{V}^* = \Theta(\min\left(\frac{1}{\epsilon}, \frac{1}{\delta}\right)), \quad \text{for noise magnitude}$$
$$\mathrm{V}^* = \Theta(\min\left(\frac{1}{\epsilon^2}, \frac{1}{\delta^2}\right)), \quad \text{for noise power}$$

Reference

Quan Geng, Pramod Viswanath,
The optimal mechanism in (epsilon,delta)-differential privacy,
available at http://arxiv.org/abs/1305.1330

Thank you!