Theory of Differential Privacy

Lecture 13:

Rényi DP, zCDP, Privacy Accounting

EN.601.438/638 Fall 2026

Lydia Zakynthinou
Johns Hopkins University

Oct 14, 2026

PLRV

Distributions P, Q, where p, q their density functions:

$$L(y) = \log \frac{p(y)}{q(y)} \qquad \forall y \in \mathcal{Y}$$

$$L(Y) = \log \frac{p(Y)}{q(Y)} \leftarrow \text{when } Y \text{ is r.v.}$$

$L(Y)$ is r.v.

Gaussian mechanism: $M(x) = f(x) + N(0, \sigma^2 \mathbb{I}_d)$, $f : \mathcal{X}^n \to \mathbb{R}^d$.

Denote $f(x) = \mu$, $f(x') = \mu'$.

$M(x) : P = N(\mu, \sigma^2 \mathbb{I}_d)$, $Q = N(\mu', \sigma^2 \mathbb{I}_d) : M(x')$

$$L(Y) = \log \frac{p(Y)}{q(Y)} \quad \text{for} \quad Y \sim P$$

$$\Rightarrow \quad L(Y) = \frac{\|Y-\mu'\|_2^2 - \|Y-\mu\|_2^2}{2\sigma^2} \quad (\|Y-\mu'\|_2 = \|Z+v\|,\ \|Y-\mu\|_2 = \|Z\|)$$

. Replace $Y = \mu + Z$, $Z \sim N(0, \sigma^2 \mathbb{I}_d)$

If $\mu - \mu' = v$, then $L(Y) = \frac{\|v\|_2^2}{2\sigma^2} + \frac{\langle Z, v \rangle}{2\sigma^2}$.

Then $L(Y) \sim N(\rho_v, 2\rho_v)$, where $\rho_v = \frac{\|v\|^2}{2\sigma^2}$

$$\mathbb{E}_{Y\sim P}\left[e^{\lambda L(Y)}\right] = e^{\lambda(\lambda+1)\rho_v}$$ [MGF of PLRV of Gaussian mech.]

using

Fact: $\mathbb{E}_{X\sim N(\mu,\sigma^2)}\left[e^{\lambda X}\right] = e^{\lambda\mu + \lambda^2\sigma^2/2} \quad \forall \lambda > 0.$

Def. Zero-Concentrated DP:

A mechanism M is ρ-zCDP if for every pair of neighboring datasets x, x', and every $\lambda > 0$:

$$\mathbb{E}_{Y \sim M(x)}\left[\exp\left(\lambda \log \frac{P_x(Y)}{P_{x'}(Y)}\right)\right] \leq e^{\rho\lambda(\lambda+1)}$$

where $P_x, P_{x'}$ are the pdfs of $M(x), M(x')$ respectively.

If $L(y) = \log \frac{P_x(y)}{P_{x'}(y)}$ then equivalently:

$$\boxed{\mathbb{E}_{Y \sim M(x)}\left[e^{\lambda L(Y)}\right] \leq e^{\rho\lambda(\lambda+1)}}$$

$$\Leftrightarrow \quad \mathbb{E}_{Y \sim M(x)}\left[e^{\lambda(L(Y)-\rho)}\right] \leq e^{\rho\lambda^2}$$

➢ If f has sensitivity Δ, then the Gaussian mechanism $f(x) + N(0, \sigma^2 I_d)$ is $\frac{\Delta^2}{2\sigma^2}$-zCDP (by MGF of PLRV of Gaussian mech. above)

Adaptive Composition for zCDP:

Suppose round t, conditional on every previous transcript, is ρ_t-zCDP. Then

$$(Y_1, Y_2, \ldots, Y_T) \text{ is } \left(\sum_{t=1}^{T} \rho_t\right)\text{-zCDP}.$$

Recall, $Y_t \sim M_t(x, Y_{t-1}, \ldots, Y_1)$ is the output of the t-th mechanism.

ρ_{total}

Proof.

Fix neighboring datasets $x \sim x'$. Let P_x be the distribution of $H_T = (Y_1, \ldots, Y_T)$ on input x, $P_{x'}$ ... on x'. $H_{t-1} = (Y_1, \ldots, Y_{t-1})$.

$Y_t \mid H_{t-1}$: $L_t = \log \frac{P_X(Y_t \mid H_{t-1})}{P_{X'}(Y_t \mid H_{t-1})}$ PLRV of $Y_t \mid H_{t-1}$.

$(Y_1, \ldots, Y_T)$: $L_{1:T} = \log \frac{P_X(Y_1, \ldots, Y_T)}{P_{X'}(Y_1, \ldots, Y_T)} = \sum_{t=1}^{T} L_t$ (1)

$= \log \frac{P_X(Y_1) \cdot P_X(Y_2 \mid Y_1) \cdots P_X(Y_T \mid H_{T-1})}{P_{X'}(Y_1) \cdot P_{X'}(Y_2 \mid Y_1) \cdots P_{X'}(Y_T \mid H_{T-1})}$

← Recall, we proved this to prove advanced composition.

Each M_t is ρ_t-zCDP $\Rightarrow$ $\mathbb{E}_{P_X}[e^{\lambda L_t} \mid H_{t-1}] \le e^{\rho_t \lambda(\lambda+1)}$ (2)

$\mathbb{E}_{P_X}[e^{\lambda L_{1:T}}] \overset{(1)}{=} \mathbb{E}_{P_X}[e^{\lambda \sum_{t=1}^{T} L_t}] = \mathbb{E}_{P_X}[e^{\lambda \sum_{t=1}^{T-1} L_t} \cdot e^{\lambda L_T}]$

$= \mathbb{E}_{P_X}[e^{\lambda \sum_{t=1}^{T-1} L_t} \cdot \mathbb{E}_{P_X}[e^{\lambda L_T} \mid H_{T-1}]] \overset{(2) \text{ for } t=T}{\le} \mathbb{E}_{P_X}[e^{\lambda \sum_{t=1}^{T-1} L_t} \cdot e^{\rho_T \lambda(\lambda+1)}]$

$Y_T \mid H_{T-1}$

$= \dots = e^{\left(\sum_{t=1}^{T} \rho_t\right) \cdot \lambda(\lambda+1)} = e^{\rho_{\text{total}} \lambda(\lambda+1)}$. So the whole adaptive composition transcript $(Y_1, \dots, Y_T)$ is ρ_{total}-zCDP.

Converting zCDP to approx. DP

for every $\delta \in (0,1)$: ρ-zCDP $\Rightarrow$ $\left(\overbrace{\rho + 2\sqrt{\rho \log(1/\delta)}}^{\varepsilon'}, \delta\right)$-DP.

Proof sketch.

It suffices to prove,

$$\Pr_{Y \sim M(x)}\left[L(Y) > \varepsilon' \right] \le \delta$$

$$\Pr_{Y \sim M(x)}\left[L(Y) > \varepsilon' \right] \le \underbrace{\mathbb{E}\left[e^{\lambda L(Y)}\right]}_{\text{by } \rho\text{-zCDP}} \cdot e^{-\lambda \varepsilon'} \le e^{\rho \lambda(\lambda+1)} \cdot e^{-\lambda \varepsilon'}$$

Pure/Approx. and zero-Concentrated DP comparison

Adapt. Comp.

- $(\varepsilon_0, \delta_0)$-DP in T rounds $\longrightarrow$ $\left(T\varepsilon_0(e^{\varepsilon_0}-1) + \sqrt{2T\varepsilon_0^2 \log(1/(T\delta+\delta_0))},\ T\delta+\delta\right)$-DP
- ρ_0-DP " " " $\longrightarrow$ $\left(T\rho_0 + 2\sqrt{T\rho_0 \log(1/\delta)}, \delta\right)$-DP.

ε-DP $\Rightarrow$ $\frac{\varepsilon^2}{2}$-zCDP $\Rightarrow$ $\left(\frac{\varepsilon^2}{2} + \sqrt{2\log(1/\delta)}\cdot\varepsilon, \delta\right)$-DP

Rényi DP

Rényi divergence for $\alpha > 1$, and $P \ll Q$

$$D_\alpha(P\|Q) = \frac{1}{\alpha-1}\log \mathbb{E}_{Y\sim P}\left[\left(\frac{P(Y)}{Q(Y)}\right)^{\alpha-1}\right].$$

Writing $L(Y) = \log\left(\frac{P(Y)}{Q(Y)}\right)$:

$$D_\alpha(P\|Q) = \frac{1}{\alpha-1}\log \mathbb{E}_{Y\sim P}\left[e^{(\alpha-1)L(Y)}\right].$$

M is $(\alpha, \varepsilon_\alpha)$-RDP if $\forall\, x\sim x'$ $D_\alpha(M(x)\|M(x')) \le \varepsilon_\alpha$.

ρ-zCDP $\Longleftrightarrow$ $(\alpha, \underbrace{\rho\alpha}_{\varepsilon_\alpha})$-RDP.

Adaptive Composition

$(\alpha, \varepsilon_{\alpha,t})$-RDP M_t for $t = 1, \ldots, T$

$$\varepsilon_\alpha^{tot} = \sum_{t=1}^{T} \varepsilon_{\alpha,t}$$

RDP to Approx. DP conversion

If M is $(\alpha, \varepsilon_\alpha)$-RDP then M is $\left(\varepsilon_\alpha + \frac{\log(1/\delta)}{\alpha - 1}, \delta\right)$-DP.

$\Rightarrow$ M is $\left(\inf_{\alpha > 1}\left(\varepsilon_\alpha + \frac{\log(1/\delta)}{\alpha - 1}\right), \delta\right)$-DP.