Variants of Differential Privacy

March 13, 2019

Basic Definitions

The following all admit the Gaussian mechanism with the specified noise variance σ^2.

Definition	Gaussian mech.	Seq. Comp.	Advanced comp.	Conv. to (ϵ, δ)-DP
(ϵ, δ)-DP	$\sigma^2 = \frac{2\Delta^2 \log(1.25/\delta)}{\epsilon^2}$	$(\epsilon_1 + \epsilon_2, \delta_1 + \delta_2)$	$(2\epsilon\sqrt{2k\log(1/\delta')}, k\delta + \delta')$	n/a
Moments acct.	(same as DP)	(same as DP)	$(4\epsilon\sqrt{2k\log(1/\delta)}, \delta)$	n/a
(α, ϵ)-RDP	$\sigma^2 = \frac{\Delta^2 \alpha}{(2\epsilon)}$	$(\alpha, \epsilon_1 + \epsilon_2)$	n/a	$(\epsilon + \frac{\log(1/\delta)}{\alpha - 1}, \delta)$
ρ-zCDP	$\sigma^2 = \frac{\Delta^2}{(2\rho)}$	$\rho_1 + \rho_2$	n/a	$(\rho + 2\sqrt{\rho \log(1/\delta)}, \delta)$

tCDP

The *arsinh* mechanism for a query q with L_2 sensitivity Δ provides $(16\rho, \frac{A}{8\Delta})$-tCDP:

$$M(x) \leftarrow q(x) + A \operatorname{arsinh}(\frac{1}{A}\,\mathcal{N}(\frac{\Delta^2}{2\rho}))$$

where $\operatorname{arsinh}(x) = \log(x + \sqrt{x^2 + 1})$.

Another way to phrase this (without A) is: adding noise sampled from

$$8\Delta\omega \operatorname{arsinh}\Big(\frac{1}{8\Delta\omega}\,\mathcal{N}\Big(\frac{8\Delta^2}{\rho}\Big)\Big)$$

preserves (ρ, ω)-tCDP.

Amplification by Subsampling

Here, we uniformly sample a size-n subset of a size-N dataset. We let $s = n/N$.

Definition	Sampling bound
(ϵ, δ)-DP	$(\log(1 + s(e^\epsilon - 1)), s\delta)$-DP
(α, ϵ)-RDP	see below
ρ-zCDP	N/A
(ρ, ω)-tCDP	$(13s^2\rho, \frac{\log(1/s)}{4\rho})$-tCDP

For $(\alpha, \epsilon(\alpha))$-RDP, when the Gaussian mechanism is used, a not-quite-tight bound is $(\alpha, \epsilon'(\alpha))$, where:

$$\epsilon'(\alpha) = \frac{1}{\alpha - 1} \log\Big(1 + \sum_{j=2}^{\alpha} 2s^j \binom{\alpha}{j} e^{(j-1)\epsilon(j)}\Big)$$

The tight bound is available in Wang et al. (2018).

We can loosen the bound slightly more and avoid expressing ϵ as a function of α. By Mironov, proposition 8 (monotonicity of Rényi divergence), we know that for any RDP mechanism and positive integer $k < \alpha$, $\epsilon(\alpha - k) \le \epsilon(\alpha)$. Thus,

$$\epsilon'(\alpha) \le \frac{1}{\alpha - 1} \log\Big(1 + \sum_{j=2}^{\alpha} 2s^j \binom{\alpha}{j} e^{(j-1)\epsilon(\alpha)}\Big)$$

So given an (α, ϵ)-RDP mechanism, running the mechanism on a subsampled dataset yields at least (α, ϵ')-RDP, where:

$$\epsilon' = \frac{1}{\alpha - 1} \log\Big(1 + \sum_{j=2}^{\alpha} 2s^j \binom{\alpha}{j} e^{(j-1)\epsilon}\Big)$$