Harvard Privacy Tools Project

Gaussian Mechanism Accuracy

April 25, 2020

Definition 1. Let z be the true value of the statistic and let X be the random variable the noisy release is drawn from. Let α be the statistical significance level, and let $Y = |X - z|$. Then, accuracy a for a given $\alpha \in [0, 1]$ is the a s.t.

$$\alpha = \Pr[Y > a].$$

Theorem 1. *The accuracy of an (ϵ, δ)-differentially private release from the Gaussian mechanism on a function with ℓ_2-sensitivity Δ_2 at statistical significance level α is*

$$a = \frac{2\Delta_2}{\epsilon}\sqrt{\ln\left(\frac{1.25}{\delta}\right)}\, erf^{-1}(1-\alpha).$$

Proof. Note that

$$\begin{aligned}
\alpha &= 1 - P[Y \leq a] \\
&= 1 - 2\int_0^a f(y)dy \\
&= 1 - \frac{2}{\sigma\sqrt{2\pi}}\int_0^a e^{-\frac{1}{2}\left(\frac{y}{\sigma}\right)^2} dy \\
&= 1 - \operatorname{erf}\left(\frac{a}{\sigma\sqrt{2}}\right).
\end{aligned}$$

,
where the last two lines are taken from the definitions of the Gaussian distribution.
Recall from the definition of the Gaussian mechanism that it adds Gaussian noise to queries with standard deviation $\sigma \geq c\Delta_2/\epsilon$, where $c^2 \geq 2\ln\left(\frac{1.25}{\delta}\right)$ [DR+14].[1] Setting σ into its minimum value, plugging it into the above expression and solving for a then gives

[1] In the formulation of the Gaussian mechanism in Dwork & Roth, they say that $c^2 \geq 2\ln\left(\frac{1.25}{\delta}\right)$. However, this bound comes from a tighter bound in their proof on p.264, which requires that $c^2 > 2\ln(\sqrt{2e^{8/9}/\pi}(1/\delta))$. Since $\sqrt{2e^{8/9}/\pi} < 1.25$, the bound can safely be made tight.

$$
\begin{aligned}
a &= \sigma\sqrt{2}\,\mathrm{erf}^{-1}(1-\alpha) \\
&= \frac{\Delta_2\sqrt{2}}{\epsilon}\sqrt{2\ln\left(\frac{1.25}{\delta}\right)}\,\mathrm{erf}^{-1}(1-\alpha) \\
&= \frac{2\Delta_2}{\epsilon}\sqrt{\ln\left(\frac{1.25}{\delta}\right)}\,\mathrm{erf}^{-1}(1-\alpha)
\end{aligned}
$$

□

References

[DR+14] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.