Effectively Using Public Data in Privacy Preserving Machine Learning

Milad Nasr, Saeed Mahloujifar, Xinyu Tang, Prateek Mittal, Amir Houmansadr

miladnasr@google.com, sfar@princeton.edu, xinyut@princeton.edu, pmittal@princeton.edu, amir@cs.umass.edu

We Are Wasting The Public Data!

- State of the art differentially private models use public data! (and it is necessary in some settings!*)
- Places we can use public data:

Is this the *optimal* way of using the public data ?

Public Data is Scarce!

- We should utilize the public data as much as possible!
- Augmentation helps! Let's do it better!
- Leverage generative models trained on public datasets for a powerful data augmentation strategy. Notably, diffusion models show exceptional performance, even when trained on smaller datasets
- Use *augmented* public data to improve:
  - Pre-training (**warm-aug**),
  - private training (**extended**).

Setting	Test Acc (%)
Baseline (WRN16-4) (cold)	64.9
+ Pretraining on the public data (warm)	68.1
+ Pretraining on the generated data using public data (**warm-aug**)	72.0
+ Including the generated data in the training dataset (**extended**)	73.7

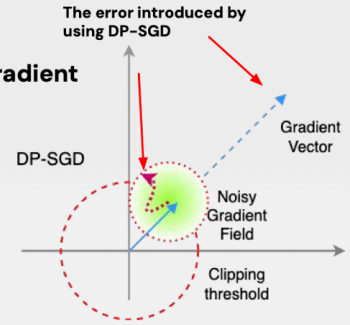
How To Use Public Data To Improve The Private Training?

How does DP-SGD work?

Step 1
Take the per example gradient

Step 2
Clip the gradient

Step 3
Add noise



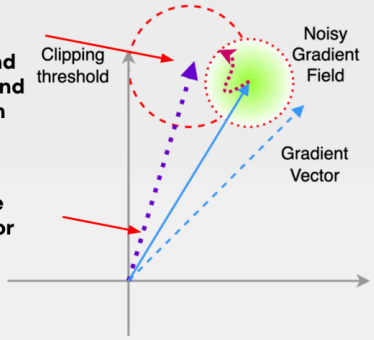
Proposition Let X and Θ be example and model spaces and let ℓ be a $\mathcal{L}$-lipschitz and r-concentrated loss function for X and Θ. DOPE-SGD achieves $(c\frac{rq}{\sigma}\sqrt{T\ln(1/\delta)\ln(T/\delta)}), \delta)$-DP, where as DP-SGD achieves $(c\frac{\mathcal{L}q}{\sigma}\sqrt{T\ln(1/\delta)\ln(T/\delta)})$, $\delta)$-DP, for a constant c, sampling rate q, and number of iterations T and sufficiently large σ .

Epsilon	DP-SGD (pretraining)	DOPE-SGD (ours)
1	60.1%	**72.1%**
2	68.1%	**75.1%**
4	72.4%	**77.9%**
6	77.1%	**80.0%**

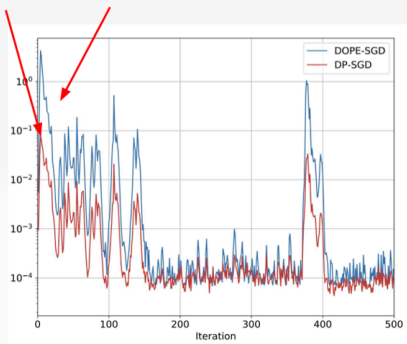
DOPE-SGD

2. Instead of clipping around zero, clip around the estimation

1. Estimate the gradient vector



Significantly less noise compared to the original gradient with using DOPE-SGD



*Catch our other work: Ganesh, Arun, Mahdi Haghifam, Milad Nasr, Sewoong Oh, Thomas Steinke, Om Thakkar, Abhradeep Guha Thakurta, and Lun Wang. "Why Is Public Pretraining Necessary for Private Model Training?" ICML'23

Read our work in detail:

Google DeepMind PRINCETON UNIVERSITY ICML International Conference On Machine Learning