Compare with plaintext

- Tensorflow library
- IBM library

Tensorflow library

MNIST dataset	Accuracy
Plaintext	0.92
DP (ϵ = 5)	0.74
DP/Plaintext	80 %

APS dataset	Accuracy	Recall	Precision	AUC
Plaintext	0.98	0.31	0.71	0.66
DP (ϵ = 6)	0.97	0.19	0.31	0.58
DP/plaintext	99 %	61 %	44 %	88 %

IBM library

MNIST dataset	Accuracy
Plaintext	0.92
DP (ϵ = 5)	0.42
DP/Plaintext	46 %

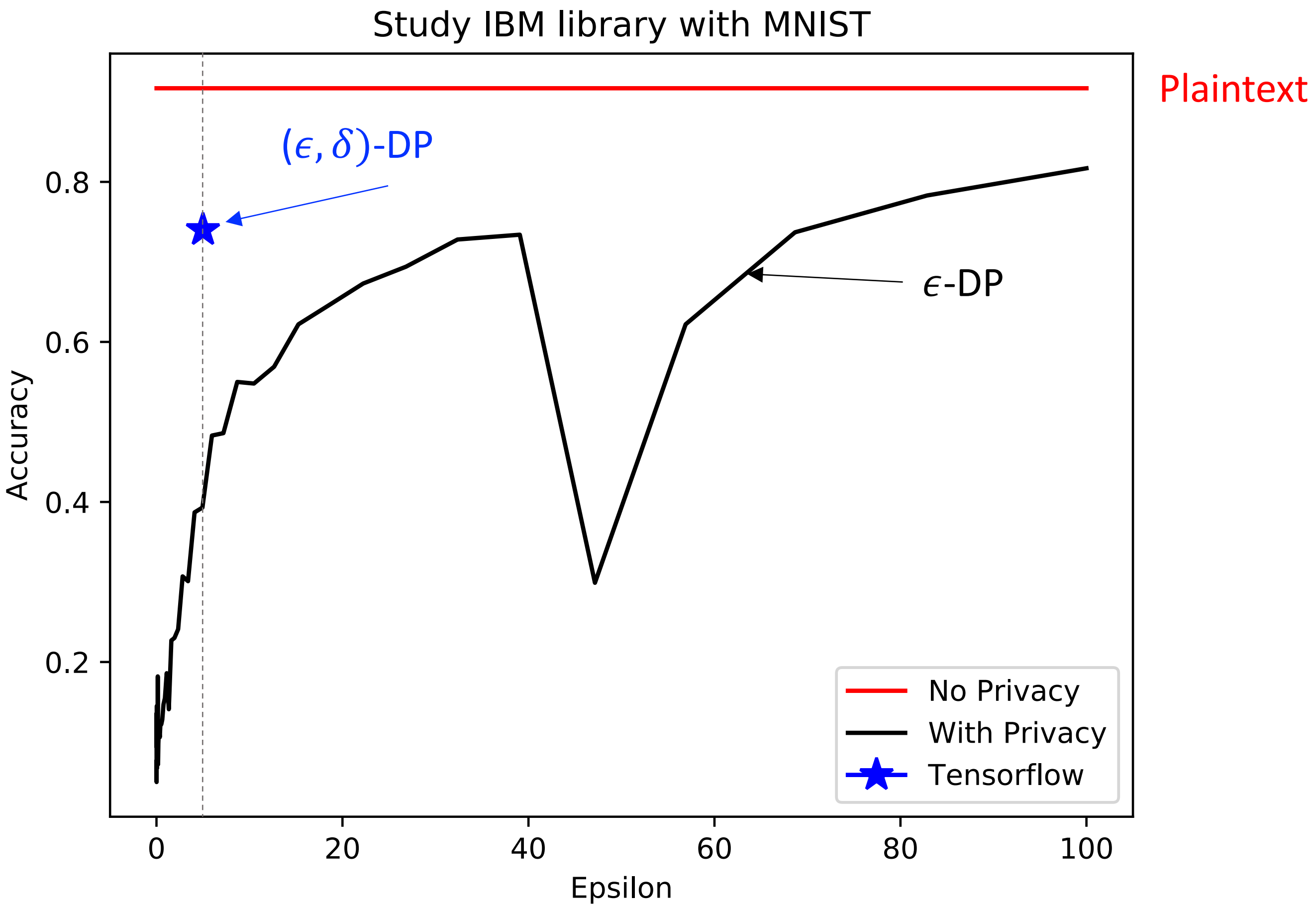
APS dataset	Accuracy	Recall	Precision	AUC
Plaintext	0.99	0.64	0.82	0.82
DP (ϵ = 5)	0.88	0.42	0.06	0.65
DP/plaintext	88 %	66 %	7 %	79 %

Accuracy vs Epsilon with Tensorflow library

Accuracy	ϵ
0.8	991217
0.78	234
0.76	11.7
0.74	4.9
0.64	0.8
0.44	0.4

Which one to choose?: as high accuracy as possible && as low ϵ as possible

Train with IBM library



Evaluate Differential Privacy in Practice (*)

- Naïve Differential Privacy and Relaxed Differential Privacy: (ϵ)-DP, (ϵ, δ)-DP
  - Relaxed DP: result in lower noise added, hence it can get lower ϵ and good utility (accuracy) but also come with additional privacy risk

	Loss	# exposed	ϵ
ϵ-DP	0.1	328	500
(ϵ, δ)−DP	0.09	329	10

Where # exposed is the number of individuals (out of 10000) exposed by membership inference attack

➢ Conclusion: privacy does not come for free, the thing matter is how much noise we added in.

- Reference: https://arxiv.org/pdf/1902.08874.pdf

(*) result on this slide is from the paper, with logistic regression on CIFAR-100 dataset