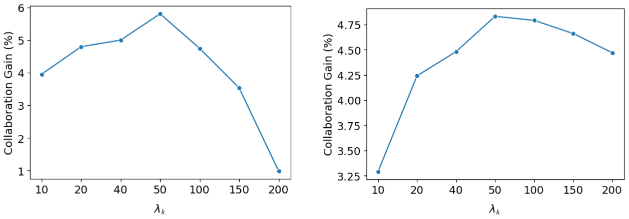
CaPriDe Learning: Confidential and Private Decentralized Learning based on Encryption-friendly Distillation Loss
Supplementary Material

Nurbek Tastan   Karthik Nandakumar
Mohamed bin Zayed University of Artificial Intelligence, UAE
{nurbek.tastan,karthik.nandakumar}@mbzuai.ac.ae

1. Impact of Weight Factor λ_k

We conduct an experiment to analyze the sensitivity of CaPriDe learning algorithm to the weight factor λ_k. We choose weight factor values in the following range $\lambda_k \in [10, 200]$ and report the collaboration gain in Figure 1. This study has been conducted with $K = 10$ participants on CIFAR-10 and $K = 2$ participants on CIFAR-100 in a homogeneous setting. The best collaboration gain in both scenarios is obtained when $\lambda_k = 50$.



(a) CIFAR-10: 10 participants

(b) CIFAR-100: 2 participants

Figure 1. Impact of weight factor on collaboration gain for CIFAR-10 (a) and CIFAR-100 (b) in homogeneous (iid) setting.

2. FedAvg + DP

FedAvg algorithm with local differential privacy is sensitive to the amount of noise added to the gradients, which determines the trade-off between privacy and the accuracy of the given model. Therefore, we conduct an experiment on CIFAR-100 with $K = 2$ participants in a homogeneous setting with different values of standard deviation (σ_g) parameter and the results are shown in Figure 2. Smaller values of σ_g in the Gaussian mechanism indicate weaker privacy, but improves the accuracy. We observe that even very small values of σ_g lead to much lower accuracy than FedAvg and CaPriDe learning.

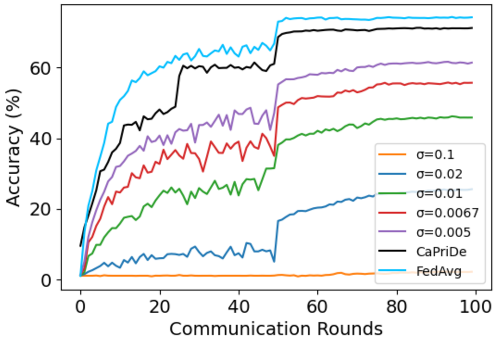


Figure 2. FedAvg algorithm with Local Differential Privacy on CIFAR-100 with 2 participants.

3. Distillation Loss

As discussed in Section 3.3 of the main paper, both L2 distance and approximate KL divergence can be used as encryption-friendly distillation loss. Table 1 summarizes the results obtained for these two loss functions under various settings. The CaPriDe algorithm with L2 distillation loss did not lead to any significant collaboration gain compared to stand-alone training. In contrast, the proposed approximate KL divergence loss leads to significant collaboration gain for all the settings.

Setting	K	Individual	CaPriDe (KL)	CaPriDe (L2)
Homogeneous	2	91.050	**92.155**	91.025
Homogeneous	5	81.770	**85.194**	82.710
Homogeneous	10	68.065	**72.580**	68.272
Heterogeneous	2	87.485	**88.424**	87.320
Heterogeneous	5	77.336	**81.324**	76.070
Heterogeneous	10	64.320	**70.520**	65.010

Table 1. Accuracy of CaPriDe learning algorithm with the proposed approximate KL loss in comparison with the L2 loss.

4. Number of Participants

Results of experiments with different number of participants $K = 2, 5, 10$ on CIFAR-10 and CIFAR-100 datasets based on the heterogeneous setting are shown in Figure 3. Similar to the homogeneous setting, the collaboration gain increases with the number of participants, even though the final accuracy is lower. This is because the training samples per participant become less when there are more participants, consequently resulting in lower individual accuracy.

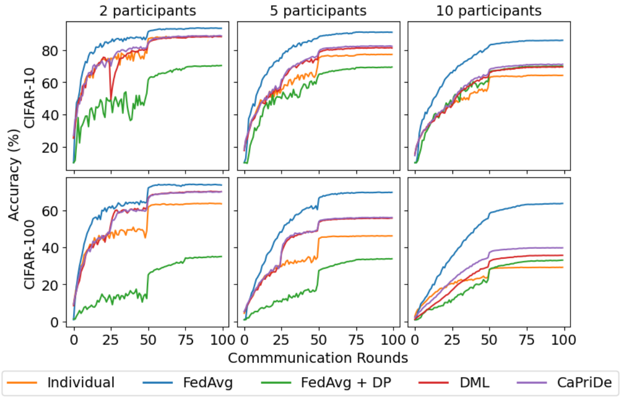


Figure 3. Accuracy with different number of participants K based on the heterogeneous partition (non-iid) setting.