IntraShuffler: A Privacy Preserving Framework for Heterogeneous Differential Privacy (HDP)-Federated Learning (FL)

Scientific Achievement

- IntraShuffler: middleware that buckets clients by privacy budget and performs parameter-level shuffling within each bucket, while preserving epsilon-aware aggregation.
- New Privacy Inference Attack on HDP-FL: an honest-but-curious server uses epsilon-aware denoising and a surrogate model to infer client attributes and link updates across rounds, even under local DP (LDP) and message-level shuffling.

Significance and Impact

- Cuts gradient recoverability by over 60% and surrogate inference accuracy from 0.78 → 0.33, with near-random cross-round linkage and utility on par with Shuffle-DP.
- Drop-in for FedAvg / FedOpt / FedProx - no changes to client training or server optimizer.
- Enables privacy-preserving collaboration across DOE labs, hospitals, and utilities with mixed privacy budgets budgets.

Technical Approach

- Privacy-aware bucketing groups clients by privacy budget and merges small groups with the nearest neighbor to guarantee a minimum anonymity set.
- Parameter-level shuffling per bucket breaks per-client vectors while LDP is preserved by post-processing.

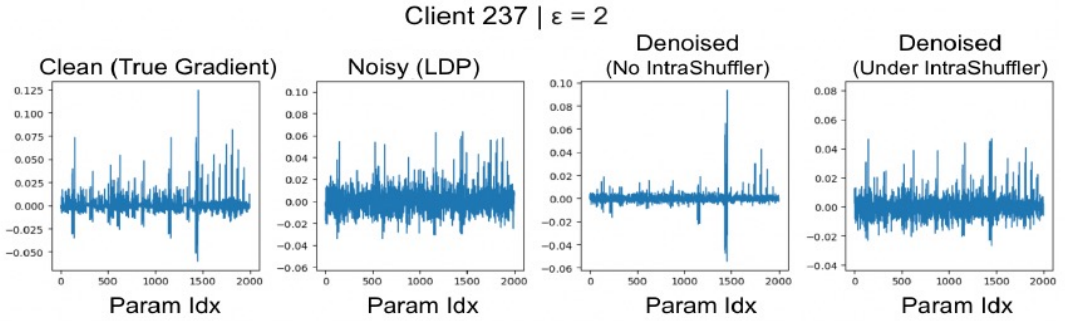

Fig. 1: Effect of IntraShuffler on gradient recovery. Without shuffling, denoising partially restores gradients; IntraShuffler disrupts alignment and prevents recovery even at higher privacy budget.

Method	CosAUC	ΔCos	Sur. Acc.	ARI
No Shuff + DP	0.42	0.21	0.78	0.41
Shuffler-DP	0.36	0.18	0.69	0.30
IntraShuffler (ours)	**0.15**	**0.05**	**0.33**	**0.06**

Table 1: Comparison of privacy leakage under defenses.

PI(s)/Facility Lead(s): K. Kim (PI), O. Kotevska (ORNL's PI)
ASCR Program: AI for Science
ASCR PM: Xujing Davis
Publication(s) for this work: Riya, F., Kotevska, O., Sun, Y. (2026). IntraShuffler: A Privacy Preserving Framework for Heterogeneous DP Federated Learning. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. x-y). Cham: Springer Nature Switzerland.