**Differentially Private Learning**

An algorithm $A$ is said to be $(\epsilon, \delta)$-differentially private (DP) if

$$P(A(S_1) \in Q) \leq \exp(\epsilon)P(A(S_2) \in Q) + \delta$$

for all neighbouring datasets $S_1, S_2$ and output sets $Q$.

**Existing Results**: Sample complexity of DP algorithms are dimension-dependent in the worst case.

In Semi-Private learning [1], the learner accesses

- Private Labelled dataset,
- Public Unlabelled dataset from nearby distribution

**This work**: Design Semi-Private learner for linear half-spaces that

1. Is Computationally Efficient
2. Admits Dimension Independent sample complexity
3. Performs well in Challenging Practical Applications

---

**Theoretical Results**

We exploit two properties of data distribution $\mu$ (covariance $\Sigma$)

- (A) Large Margin: $\mu$ admits a classifier $w^*$ with margin $\gamma$
- (A2) Low Rank: Large Proj. of $w^*$ on top-$k$ components of $\Sigma$.

**PILLAR** Unlabelled dataset $(X_U, \epsilon)$, Labelled dataset $(X_L, Y_L, k)$,

1. $\Sigma \leftarrow \sum_{x \in S_l} xx^T, A_k \leftarrow$ top-$k$ principal components of $\Sigma$.
2. $X_L^{(proj)} \leftarrow$ Project $X_L$ on $A_k$.
3. $\hat{w}_{\epsilon, \delta} \leftarrow$ Run Noisy-SGD on $(X_L^{(proj)}, Y_L)$ with privacy parameters $\epsilon, \delta$.

**Guarantees on $\hat{w}_{\epsilon, \delta}$**

- **Privacy**: $\hat{w}_{\epsilon, \delta}$ is $(\epsilon, \delta)$-DP.
- **Accuracy**: For $\alpha, \beta \geq 0$, $|X_U| = O\left(\frac{1}{\epsilon^2}\right)$ and $|X_L| = O\left(\frac{\sqrt{n}}{\alpha \epsilon}\right)$,

$$P[\text{Error}(\hat{w}_{\epsilon, \delta}) \leq \alpha] \geq 1 - \beta$$

---

**Experiments I: Reducing Dimensions**

- **Takeaway**:
  - **Strict privacy ($\epsilon = 0.1$)**: Dimension $\downarrow$ $\Rightarrow$ Accuracy $\uparrow$.
  - **Without privacy ($\epsilon = \infty$)**: Dimension $\downarrow$ $\Rightarrow$ Accuracy $\downarrow$.

---

**Experiments II: PILLAR outperforms other Algorithms across datasets**

Comparison across datasets and pre-training for $\epsilon = 0.1$.

---

**Experiments III: Distribution Shift**

- Public and private data may come from different distributions.
- **PILLAR**’s performance is robust to using CIFAR-10v1 for public data and CIFAR10/100 for private data.