Antipodes of Label Differential Privacy: PATE and ALIBI

Anonymous Author(s)
Affiliation
Address
email

Abstract

We consider the privacy-preserving machine learning (ML) setting where the trained model must satisfy differential privacy (DP) with respect to the *labels* of the training examples. We propose two novel approaches based on, respectively, the Laplace mechanism and the PATE framework, and demonstrate their effectiveness on standard benchmarks.

While recent work by Ghazi et al. proposed Label DP schemes based on a randomized response mechanism, we argue that additive Laplace noise coupled with Bayesian inference (ALIBI) is a better fit for typical ML tasks. Moreover, we show how to achieve very strong privacy levels in some regimes, with our adaptation of the PATE framework that builds on recent advances in semi-supervised learning.

We complement theoretical analysis of our algorithms' privacy guarantees with empirical evaluation of their memorization properties. Our evaluation suggests that comparing different algorithms according to their *provable* DP guarantees can be misleading and favor a less private algorithm with a tighter analysis.

1 Introduction

Sophisticated machine learning models perform well on their target tasks despite of—or thanks to—their predilection for data memorization [37, 1, 16]. When such models are trained on non-public inputs, privacy concerns become paramount [29, 6, 5], which motivates the actively developing area of privacy-preserving machine learning.

With some notable exceptions, which we discuss in the related works section, existing research has focused on an "all or nothing" privacy definition, where all of the training data, i.e., both *features* and *labels*, is considered private information. While this goal is appropriate for many applications, there are several important scenarios where *label-only* privacy is the right solution concept.

A prominent example of label-only privacy is in online advertising, where the goal is to predict conversion probability (the label) given a user's profile and context (the features). The features are available to the advertising network, which trains the model, while the labels (data on past conversion events) are visible only to the advertiser. More generally, any two-party setting where data is vertically split between public inputs and (sensitive) outcomes is a candidate for training with label-only privacy.

In this work we adopt the definition of differential privacy as our primary notion of privacy. The definition, introduced in the seminal work by Dwork et al. [11], satisfies several important properties that make it well-suited for applications: composability, robustness to auxiliary information, preservation under post-processing, and graceful degradation in the presence of correlated inputs (group privacy). Following Ghazi et al. [17], we refer to the setting of label-only differential privacy as Label DP.

Submitted to 35th Conference on Neural Information Processing Systems (NeurIPS 2021). Do not distribute.

Our contributions. We explore two approaches—with very different characteristics—toward Label DP. These approaches and our methodology for estimating empirical privacy loss via label memorization are briefly reviewed below:

- *PATE*: We adapt the PATE framework (Private Aggregation of Teacher Ensembles) of Papernot et al. [27] to the Label DP setting by observing that PATE's central assumption—availability of a public unlabeled dataset—can be satisfied for free. Indeed, a public unlabeled dataset is simply the private dataset with the labels *removed*! By instantiating PATE with a state-of-the-art technique for semi-supervised learning, we demonstrate an excellent tradeoff between empirical privacy loss and accuracy.
- *ALIBI (Additive Laplace with Iterative Bayesian Inference)*: We propose applying additive Laplace noise to a one-hot encoding of the label. Since differential privacy is preserved under post-processing, we can de-noise the mechanism's output by performing Bayesian inference using the prior provided by the model itself, doing so continuously during the training process. ALIBI improves, particularly in a high-privacy regime, on a previously proposed approach based on randomized response [17].
- *Empirical privacy loss.* We describe a memorization attack targeted at the Label DP scenario that efficiently extracts lower bounds for the privacy parameter that, in some cases, come within a factor of 2.5 from the theoretical, worst-case upper bounds against practically relevant, large-scale models. For comparison, recent, most advanced black-box attacks on DP-SGD have approximately $10\times$ gap between the upper and lower bounds [19, 24].

Both algorithms, PATE and ALIBI, come with rigorous privacy analyses that, for any fixed setting of parameters, result in an (ε, δ)-DP bound. We emphasize that these bounds are just that—they are upper limits on an attacker's ability to breach privacy (in a precise sense) on worst-case inputs. Even though these bounds can be pessimistic, intuitively, a smaller ε for the same δ corresponds to a more private instantiation of a mechanism, and indeed this is likely the case within an algorithmic family.

Can the privacy upper bounds be used to compare diverse mechanisms with widely dissimilar analyses, such as ours? We argue that focusing on the upper bounds alone may be misleading to the point of making us prefer a less private algorithm with tighter analysis over a more private one whose analysis is more conservative. To level the playing field, we estimate the *empirical* privacy loss of all trained models by evaluating the performance of a black-box membership inference attack [29, 19, 24].

Our attack directly measures memorization of deliberately mislabeled examples, or *canaries* [6]. Following prior work [24, 19], we use the success rate of our attack to compute a lower bound on the level ε of label-DP achieved by the training algorithm. To avoid the prohibitive cost of retraining a model for each canary, we propose and analyze a heuristic that consists in inserting multiple canaries into one model, and measuring an attacker's success rate in guessing each canary's label. In some settings, we find that the empirical privacy of PATE (as measured by our attack) is significantly stronger than that of ALIBI, even though the provable DP bound for PATE is much weaker.

Finally, to characterize setups where label-only privacy may be applicable, it is helpful to distinguish between *inference* tasks, where the label is fully determined by the features, and *prediction*, where there is some uncertainty as to the eventual outcome, despite (hopefully) some predictive value of the feature set. We are mostly concerned with the latter scenario, where the outcome is not evident from the features, or protecting choices made by individuals may be mandated or desirable (for connection between privacy and self-determination see Schwartz [28]). While we do use public data sets (CIFAR-10 and CIFAR-100) in which it is possible to "infer" the label, we do so only to demonstrate our approaches on standard tasks. We completely remove the triviality of *inference* by adding mislabeled canaries in our attack, thereby introducing a measure of non-determinism.

2 Notation and Definitions

Throughout the paper we consider standard supervised learning problems. The inputs are (x, y) pairs where $x \in X$ are the *features* and $y \in Y$ are the *labels*. (If some labels are absent, the problem becomes semi-supervised learning.) The size of the set Y is the number of *classes* C. The task is to learn a model M parameterized with weights W that predicts y given x. To this end the training algorithm has access to a training set of n samples $\{(x_i, y_i)\}_n$.

Differential privacy due to Dwork et al. [11] is a rigorous, quantifiable notion of individual privacy for statistical algorithms. (See Dwork and Roth [10] and Vadhan [31] for book-length introductions.)

Definition 2.1 (Differential Privacy)**.** *We say that a randomized mechanism $\mathcal{M}\colon U \to R$ satisfies (ε, δ)-differential privacy (DP) if for all* adjacent *inputs $D, D' \in U$ that differ in contributions of a single sample, the following holds:*

$$\forall S \subset R \quad \Pr[\mathcal{M}(D) \in S] \leq e^{\varepsilon} \cdot \Pr[\mathcal{M}(D') \in S] + \delta.$$

If $\delta = 0$, we refer to it as ε-DP.

The notion of adjacency between databases D and D' is domain- and application- dependent. To instantiate the Label DP setting, we say that D and D' are adjacent if they consist of the same number of examples $\{(x_i, y_i)\}_n$ and are identical except for a difference in a single label at index i^*: $(x_{i^*}, y_{i^*}) \in D$ and $(x_{i^*}, y'_{i^*}) \in D'$.

3 Background and related work

DP and machine learning. Differential privacy aligns extremely well with the goal of machine learning, which is to produce valid models or hypotheses on the basis of observed data. In fact, the relationship can be made precise. An important metric in ML is *generalization error*, which measures the model's performance on previously unseen samples. Differentially private mechanisms provably generalize [13]. For an introduction to some important early results on connections between differential privacy and learning theory see Dwork and Roth [10, Chapter 11].

Randomized response (RR). As a disclosure avoidance methodology, randomized response (RR) [34] precedes the advent of differential privacy. In RR's basic form, with some probability the sensitive input is replaced by a sample drawn uniformly from its entire domain. RR can be implemented at the source, making it an essential building block in achieving Local DP [14].

More generally, RR is an instance of the *input perturbation* technique, which leaves the ML training algorithm intact and achieves differential privacy via input randomization. Input perturbations methods are particularly friendly to implementers as they require minimal changes to existing algorithms, treating them as black boxes.

Additive noise mechanisms. Another important class of differentially private mechanisms are *additive noise* methods. Two canonical examples are additive Laplace [11] and additive Gaussian [12] that can be applied to vector-valued functions. Their noise distributions are calibrated to the function's *sensitivity*—the maximal distance between the function's outputs on adjacent inputs (D and D' in Definition 2.1) under the ℓ_1 or ℓ_2 metrics for the Laplace and Gaussian mechanisms respectively.

PATE. Private Aggregation of Teacher Ensembles (PATE) [27, 26] is a framework based on private knowledge aggregation of an ensemble model and knowledge transfer. PATE trains an ensemble of "teachers" on disjoint subsets of the private dataset. The ensemble's knowledge is then transferred to a "student" model via differentially private aggregation of the teachers' votes on samples from an unlabeled public dataset. Only the student model is released as the output of the training, as it accesses sensitive data via a privacy-preserving interface.

Since PATE consumes the privacy budget each time the student queries the teachers, the training algorithm must be optimized to minimize the number of queries. To this end, Papernot et al. explore the use of semi-supervised learning techniques, most notably GANs. Recent advances in semi-supervised learning have been shown to boost the performance of PATE on standard benchmarks [4].

FixMatch. FixMatch [30] is a state-of-the-art semi-supervised learning algorithm, which achieves high accuracy on benchmark image datasets with very few labeled examples. It is based on the concepts of pseudo-labeling [22] and consistency regularization [2]: FixMatch uses a partially trained model to generate labels on weakly-augmented unlabeled data, and then, if the prediction is confident enough, uses the output as a label for the strongly-augmented version of the same data point.

Label-only privacy. The setting of label-only DP was formally introduced by Chaudhuri and Hsu [7], who proved lower bounds on sample complexity for private PAC-learners. Beimel et al. [3] demonstrated that the sample complexity of Label DP matches that of non-private PAC learning (ignoring constants, dependencies on the privacy parameters, and computational efficiency). Wang and Xu [32] considered the linear regression problem in the local, label-only privacy setting.

Most recently, Ghazi et al. [17] considered label-only privacy for deep learning. They propose a Label Privacy Multi-Stage Training (LP-MST) algorithm, which we revisit in Section 5. The algorithm advances in stages (Ghazi et al. evaluate it up to four), training the model on disjoint partitions of the dataset. In each stage, the private labels are protected using a randomized response scheme.

The most innovative part of LP-MST happens at the point of transition between stages. Labels of the training examples of the next partition are perturbed using randomized response. The (soft) output of the previous stage's model is interpreted as a prior, which is used to choose parameters for the randomized response algorithm *separately for each example*. For instance, if the current model assigns high probabilities to labels 1–10 and low probabilities to labels 11–100, the randomized response will be constrained to outputting a label within the set 1–10.

We build on the insights of Ghazi et al. by making two observations. First, training algorithms used for deep learning (such as SGD and its variants) can naturally handle soft labels (i.e., probability distributions over the label space); there is thus no need to force hard labels by sampling from the posterior. Second, by applying additive noise, we can repeatedly recompute the posterior distribution as better priors become available *without* consuming privacy budget. By following the "once and done" approach to label perturbation, we forego the need to split training into disjoint stages.

To summarize, Ghazi et al. fix the prior at the beginning of the stage, choose parameters of the randomized response algorithm on the basis of this prior, and update the model by feeding it the perturbed label. We flip the order of these operations by applying a DP mechanism (additive Laplace) first, and then repeatedly use Bayesian inference by combining the prior that changes with each model update and the observables that do not.

To our knowledge, we are the first to explore connections between PATE and Label DP.

4 PATE with Semi-Supervised Learning

The PATE framework [27] splits the learning procedure into two stages. First, T teachers are trained on disjoint partitions of the private dataset. Second, a student acquires labels for training its own model by querying the teacher ensemble on samples drawn from a public (non-sensitive) unlabeled dataset. Differential privacy is enforced at the interface between the student and the teachers, by means of a private aggregation of the teachers' votes.

The critical observation underlying the PATE privacy analysis is that a private sample taints at most one teacher due to disjointness of the teachers' training sets. The voting mechanism bounds the maximal impact of a single teacher's votes across all student queries by injecting noise in each voting procedure. (We use the Confident Gaussian aggregation mechanism and its analysis from [26].)

The Label DP setting allows for unrestricted use of the features. We leverage this capability for training both teachers and the student:

- The unlabeled examples on which the student queries the teacher ensemble are random samples from the dataset *without* labels.
- All models—the teachers and the student—are trained with the FixMatch algorithm that uses (few) labeled examples and has access to the entirety of the original dataset as the supplementary unlabeled data.

We present the following adaptation of PATE to the Label DP setting. To draw a distinction between the PATE framework, which is generic and black-box, and its instantiation with the FixMatch algorithm for semi-supervised learning, we refer to the latter as PATE-FM.

The PATE framework does not require the student and the teacher models to have identical architecture, or share hyperparameters. In our experience, however, the optimal privacy/accuracy trade-offs force very similar choices on these models.

The selection of the number of teachers, T, balances two competing objectives. On the one hand, each teacher has access to n/T labeled and n unlabeled examples, which means that a smaller T corresponds to higher-accuracy since individual teachers agree more frequently with one another. On the other hand, larger Ts allow for higher level of noise and lower privacy budget per query.

A similar dynamic controls K, the number of labels requested by the student. A higher number allows for more accurate training but inflates the privacy budget.

Algorithm 1: `PATE-FM.TrainTeacherEnsemble`

Input: Dataset $D \leftarrow \{(x_1, y_1), \ldots, (x_n, y_n)\}$, number of teachers T, training procedure `FixMatch`$(labeled_data, unlabeled_data)$

Define the unlabeled part of D: $D^- \leftarrow \{x_1, \ldots, x_n\}$
Partition D into T equal-sized disjoint subsets $D^{(1)}, \ldots, D^{(T)}$
for $i \leftarrow 1$ **to** T **do**
  $teacher_i \leftarrow$ `FixMatch`$(D^{(i)}, D^-)$
end
Output: Ensemble $\{teacher_1, \ldots, teacher_T\}$

Algorithm 2: `PATE-FM.TrainStudent`

Input: Dataset $D = \{(x_1, y_1), \ldots, (x_n, y_n)\}$, number of label classes C, number of teachers T, training procedure `FixMatch`$(labeled_data, unlabeled_data)$, number of student samples K, noise parameters σ_1, σ_2, voting threshold τ

Define the unlabeled part of D: $D^- \leftarrow \{x_1, \ldots, x_n\}$
Initialize student dataset $D_S \leftarrow \emptyset$
$\{teacher_1, \ldots, teacher_T\} \leftarrow$ `TrainTeacherEnsemble`(D, T)
while $|D_S| < K$ **do**
  $x \leftarrow$ random sample from D^-
  for $i \leftarrow 1$ **to** C **do** // tallying up the votes
    $v_i \leftarrow |\{j \colon teacher_j(x) = i\}|$
  end
  if $\max\{v_i + \mathcal{N}(0, \sigma_1^2)\} \geq \tau$ **then**
    $y \leftarrow \mathrm{argmax}_i\{v_i + \mathcal{N}(0, \sigma_2^2)\}$
    $D_S \leftarrow D_S \cup \{(x, y)\}$
  end
end
$student \leftarrow$ `FixMatch`(D_S, D^-)
Output: Student model $student$

Boosting teachers' accuracy for a given number of labels and minimizing the number of student queries and their privacy costs are key to producing high utility models with strong privacy guarantees. To this end, we use the state-of-the-art algorithm for semi-supervised learning FixMatch [30].

The FixMatch algorithm's primary domain is image classification: in addition to labelled and unlabelled examples, it assumes access to a pair of weak and strong data augmentation algorithms. The loss function of FixMatch is a weighted sum of two losses that enforce consistency of the model's prediction (i) between labeled examples and their weakly augmented versions, and (ii) between weakly and strongly augmented unlabeled images (restricted to high-confidence instances).

5 ALIBI: Additive Laplace with Iterative Bayesian Inference

We describe the general approach of Soft Randomized Response with post-processing and its concrete instantiation, ALIBI.

5.1 Soft Randomized Response

Consider the application of *Randomized Response (RR)* to the setting of Label DP. In its standard form, the random perturbation maps labels to labels, i.e., the label either retains its value with probability p or assumes a random value with probability $1 - p$.

We deviate from RR by replacing label randomization with a differentially private mechanism applied to a one-hot encoding of the training sample label; we refer to this mechanism as Soft Randomized Response (Soft-RR). By retaining more information (without significantly impacting privacy analysis), we support several possible post-processing algorithms (Section 5.2). Additionally, we argue that Soft-RR performs better than RR in practice since it does not force wrong hard labels.

Algorithm 3: Additive Laplace with Iterative Bayesian Inference, `ALIBI`

Input: Dataset $D = \{(x_1, y_1), \ldots, (x_n, y_n)\}$, noise parameter λ, Bayesian post-processing mechanism $\texttt{BPP}(\mathbf{o}, \lambda, prior)$ defined in Eqn. (3)

Initialize noised dataset $D^* \leftarrow \emptyset$
for $i \leftarrow 1$ **to** n **do** `// noise labels`
  $\mathbf{o}_i \leftarrow \text{OneHot}(y_i) + \text{Laplace}(\lambda)$
  $D^* \leftarrow D^* \cup \{(x_i, \mathbf{o}_i)\}$
end

Randomly initialize parameters (W) of model M
repeat
  for $i \leftarrow 1$ **to** n **do**
    $\mathbf{pred}_i \leftarrow M_W(x_i)$
    $\mathbf{post}_i \leftarrow \texttt{BPP}(\mathbf{o}_i, \lambda, \mathbf{pred}_i)$
    $loss \leftarrow \text{CrossEntropy}(\mathbf{post}_i, \mathbf{pred}_i)$
    $W \leftarrow \text{Update}(M, W, loss)$
  end
until *convergence*;

Output: weights W

Following standard analysis (Dwork and Roth [10, Chapter 3.3]), ε-DP can be achieved with additive Laplace noise with per-coordinate standard deviation $2\sqrt{2}/\varepsilon$. Analogously, Gaussian noise sampled from $\mathcal{N}(0, \sigma^2 \cdot \mathbb{I}_C)$ results in (ε, δ)-DP if $\sigma = \sqrt{2\ln(1.25/\delta)}/\varepsilon$ and $\varepsilon, \delta < 1$ ([10, Appendix A]).

5.2 Post-processing of Soft Randomized Response

The output of Soft-RR is no longer a valid soft label vector—values are not necessarily constrained to the [0,1] interval and do not sum up to 1. Thankfully, the fundamental property of DP allows privacy preservation under post-processing, which we use to obtain a probability mass function on noisy labels to reduce the amount of noise in the mechanism's output. With $\mathbf{o}$ the observable (noised) label, and λ as the noise parameter, we can calculate the posterior $p(y = c \mid \mathbf{o}, \lambda)$ by Bayes' rule as:

$$p(y = c \mid \mathbf{o}, \lambda) = \frac{p(\mathbf{o} \mid y = c, \lambda) \cdot p(y = c)}{\sum_k p(\mathbf{o} \mid y = k, \lambda) \cdot p(y = k)}. \tag{1}$$

In the context of SGD, the current model's output could be interpreted as a prior probability distribution over the classes ($p(y)$).

ALIBI, or Additive Laplace with Iterative Bayesian Inference, is an algorithm that applies Bayesian post-processing to the output of the Laplace mechanism, i.e., the noised Soft-RR labels. With Laplace noise, the output of the mechanism for a specific label k is distributed as:

$$p(\mathbf{o} \mid y = k, \lambda) \propto e^{-|\mathbf{o}_k - 1|/\lambda} \prod_{j \neq k} e^{-|\mathbf{o}_j|/\lambda}. \tag{2}$$

Plugging (2) into (1) we derive:

$$p(y = c \mid \mathbf{o}, \lambda) = \text{SoftMax}(f(o_c)/\lambda + \log p(y = c)), \tag{3}$$

where $f(o_c) = -\sum_k |\mathbf{o}_k - [c = k]|$ and $[\cdot]$ is the Iverson bracket.

We use the above insight in the ALIBI training algorithm (Algorithm 3). At a given privacy level, ALIBI empirically outperforms iterative Bayesian inference on additive Gaussian noise and naïve "uninformed" post-processing strategies, the details of which are deferred to Section C (Supplemental materials).

6 Evaluation

We evaluate both our algorithms on the CIFAR-10 and CIFAR-100 datasets [21] using the Wide-ResNet architecture [36]. We set the widen-factor to 4 and 8 for CIFAR-10 and CIFAR-100 respectively. To facilitate comparison of privacy assured by the two approaches, we train our models to

achieve similar accuracy levels and provide the computed theoretical (ε, δ) upper bound. We also provide the empirical privacy loss lower bound, ε_m, as estimated by the black-box attacks (Section 7).

6.1 PATE-FM

PATE-FM parameters are given in Table 3 (Supplemental materials). The student and the teacher models share the same architecture and are trained using FixMatch [30, 20] with hyperparameters from Sohn et al. [30] (we use the RandAugment variant [8]). The number of epochs is set so that the test accuracy reaches a plateau: for CIFAR-10, we train teachers for 40 epochs and the student for 200 epochs; for CIFAR-100, we train both the teachers and the student for 125 epochs. To report privacy, we set $\delta = 10^{-5}$. The student's accuracy is reported as the average of three runs (for a fixed teacher ensemble).

There are several hyperparameters affecting privacy/utility trade-off in PATE: number of teachers, level of noise, voting threshold, and number of labeled samples in the student dataset. Apart from the expected dependencies (increasing noise and the number of teachers benefits privacy at some accuracy cost), we observe the following:

- The number of labeled student samples beyond a certain level (10–25 samples per class) has little effect on the eventual model accuracy. This is in contrast with the standard (non-private) FixMatch where increasing the number of labeled samples usually improves accuracy.
- The voting threshold τ needs to be kept between 10% and 75% of the overall number of teachers. As pointed out in Papernot et al. [26], a lack of consensus between teachers hurts both privacy and utility, as the teacher ensemble errs more often on such inputs and a single vote can have more impact on the outcome. Setting the threshold too high leads to a selection bias in training samples, forcing the student model to train only on the most trivial samples. Even in the zero-noise regime, the threshold above 75% considerably hurts the accuracy.

6.2 ALIBI

We use mini-batch SGD with a batch size of 128 and a momentum of 0.9. We train all models for 200 epochs and pick the best checkpoint. We tune the learning rate, weight decay and noise multiplier to obtain the desired accuracy while minimizing privacy ε (see Table 4 in Supplemental materials). Since we use Laplace noise here, we implicitly set $\delta = 0$.

6.3 Results

Table 1 presents the privacy budget and the memorization metric at three levels of accuracy across our two approaches for the both datasets. Additionally, for ALIBI, we provide the results of a higher accuracy model on the CIFAR-100 task; this higher accuracy was not attainable with PATE-FM.

For correct comparison with LP-2ST on CIFAR-100, we factor out modelling differences by applying both mechanisms to training the same architecture—ResNet18 [18, 23] with appropriate modifications to suit the task. Results are presented in Table 2.

We note that there is a significant difference in computational resources required to train with PATE-FM and ALIBI. The reasons are twofold. First, in our experiments, models trained in a semi-supervised regime with few labeled examples take longer to converge. Second, PATE training involves training the teacher ensemble, in which computational costs scale linearly with the size of the ensemble. Overall this accounts for PATE-FM consuming 1,000–1,500× more computational resources (GPU·hr) compared to ALIBI.

7 Measuring Memorization

We complement our evaluation with an empirical study of the (label) memorization abilities of classifiers trained with PATE-FM and ALIBI. While we can derive *provable* upper-bounds on the level of ε-Label DP provided by both algorithms, a direct comparison between the (actual) privacy of both algorithms is challenging as they rely on very different privacy analyses. As we will see, for CIFAR-100, PATE-FM empirically appears to provide much stronger privacy guarantees than ALIBI, even though the privacy analysis suggests the opposite.

Table 1: Privacy of PATE-FM [27, 30] and ALIBI, on CIFAR-10 and CIFAR-100 using Wide-ResNet18, matched by test accuracy levels. Empirical privacy loss ε_m is reported as a 95% confidence interval (CI).

Dataset	Accuracy level	Approach	Accuracy	ε	95%-CI ε_m
CIFAR-10	High	PATE-FM	93.7%	1.6	0.0–0.9
		ALIBI	94.0%	8.0	2.7–4.0
	Medium	PATE-FM	86.9%	0.29	0.0–0.5
		ALIBI	84.2%	2.1	0.3–2.2
	Low	PATE-FM	73.4%	0.18	0.0–0.4
		ALIBI	71.0%	1.0	0.0–0.4
CIFAR-100	Very High	PATE-FM	–	–	–
		ALIBI	75.3%	8.1	3.2–5.8
	High	PATE-FM	69.9%	715	0.4–1.0
		ALIBI	71.4%	6.3	2.8–3.7
	Medium	PATE-FM	50.0%	16	0.2–0.7
		ALIBI	51.6%	3.0	1.4–2.4
	Low	PATE-FM	30.5%	7.9	0.2–0.6
		ALIBI	31.4%	2.0	0.5–1.0

Table 2: Test accuracy of ALIBI and LP-2ST [17, Table 4], on CIFAR-100 applied to ResNet18, matched by ε.

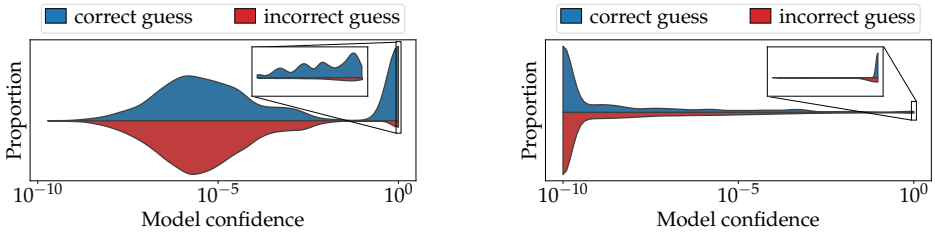
Algorithm	$\varepsilon = 3$	$\varepsilon = 4$	$\varepsilon = 5$	$\varepsilon = 6$	$\varepsilon = 8$
ALIBI	**55.0**	**65.0**	**69.0**	**71.5**	**74.4**
LP-2ST	28.7	50.2	63.5	70.6	74.1

To empirically measure privacy loss, we *instantiate* the implicit adversary in the DP definition [24, 19]. We construct two datasets D, D' that differ only in the label of one example, and train a model on one of these two datasets. We then build an attack that "guesses" which of the two datasets was used. The attacker's advantage over a random guess can be used to derive an empirical lower bound on the mechanism's differential privacy. A formal treatment of memorization attacks using the framework of security games appears in Section B (Supplemental materials).

We point out the following differences between our approach and prior work. When providing lower bounds on privacy leakage, it is appropriate to consider the most powerful attacker pursuing the least challenging goal. In the context of standard DP (privacy for labels and features), it means an attacker that can add or remove a sample and seeks to determine whether the sample was part of the training dataset (i.e., membership inference [29]). In contrast, we operate within the constraints of Label DP, where the attacker's power is limited to manipulating a single label and the goal is to infer which label was used during training. (The closest analogue is attribute inference [35]).

Prior work replicates a memorization experiment many times (e.g., $1{,}000$ times [24]) to lower bound ε with standard statistical tools [24, 19]. As this approach is prohibitively expensive in our setting (prior work computed DP lower bounds for simpler datasets such as MNIST), we introduce the following heuristic: we train a *single* model on a training set with $1{,}000$ labels randomly flipped to a different class. For each of these "canaries" [6] with (flipped) label y', the attacker has to guess whether the canary's assigned label is y' or y'', where $y'' \neq y'$ is a different random incorrect label. If the adversary has accuracy α in this guessing game, we can lower bound ε by $1 - \log(\frac{\alpha}{1-\alpha})$. As in prior work [24, 19], we compute a 95% confidence interval on the adversary's guessing accuracy α and thus on the level of privacy ε against our attack. We formally define our attacking game and analyze the relationship between the attacker's success and the privacy budget ε in Appendix B.

Our empirical estimates of the privacy loss ε_m are given in Table 1. The estimates for ALIBI are approximately within a factor of 2 of the theoretical upper bound on ε. This suggests that the theoretical privacy analysis of ALIBI is close to tight. On the other hand, for PATE-FM our empirical



(a) ALIBI (CIFAR-100, High)

(b) PATE-FM (CIFAR-100, High)

Figure 1: Comparison of the adversary's success rates in guessing the label of inserted canaries with ALIBI and PATE-FM (for CIFAR-100, with High accuracy level). We sort canaries by the model's maximal confidence on the two labels y', y'' that the adversary has to guess from. The violin plots show the proportion of correct guesses (the model is more confident in the canary label) and incorrect guesses. To maximize the adversary's distinguishing power, we limit the adversary to only issuing guesses for canaries where the model's confidence in either y' or y'' is above 99% (zoomed-in box). ALIBI is clearly more vulnerable to the attack (i.e., it is easier for the adversary to guess a canary's label), even though its theoretical privacy analysis yields a much lower bound on ϵ than for PATE-FM.

estimates of the privacy loss are up to three orders of magnitude smaller than the theoretical upper bound. While we have no guarantee that our attack is the strongest possible attack (and it likely is not), our experiment does suggest that for a fixed accuracy level, PATE-FM is much less likely to memorize labels compared to ALIBI (see Figure 1). Empirically, it thus appears that PATE-FM provides a much better privacy-utility tradeoff than ALIBI, even though the theoretical analysis suggests the opposite.

This being said, we encourage critical interpretation of privacy claims backed by memorization estimates. Among many confounding factors are the trained model's architecture and test accuracy (see discussion in Erlingsson et al. [15]). To isolate the impact that can be attributed to the difference between privacy-preserving training procedures, we apply ALIBI and PATE-FM to the same target model architecture and tune their privacy parameters to achieve similar accuracy levels. Furthermore, we deliberately limit memorization attacks to be trainer-agnostic, to avoid privileging, for instance, a more complex training procedure over a simpler one.

8 Conclusion

We have proposed and evaluated two approaches toward achieving Label DP in ML: ALIBI and PATE-FM (the PATE framework instantiated with FixMatch). We have demonstrated that both approaches can achieve state-of-the-art results on standard datasets. As the two approaches have different theoretical foundations and exhibit very different performance characteristics, they also present an interesting combination of trade-offs.

PATE-FM offers impressive empirical privacy despite a very conservative theoretical privacy analysis. That being said, its training setup is fairly complicated. The dependency on semi-supervised learning techniques further restricts the tasks this method can be used for at present.

In contrast, ALIBI's implementation and interpretation are quite simple. (1) It is a generic algorithm that is compatible with any iterative procedure for ML training, such as SGD or its variants. It is not a black-box however, and requires the ability to update training data labels as they are processed by the training algorithm. (2) It enjoys a tighter privacy analysis resulting in a more realistic upper-bound on the privacy budget, but appears to offer less privacy than PATE-FM empirically. (3) It can be used to train models to accuracy levels which PATE cannot achieve without significantly more data.

In addition to privacy and performance trade-offs, our two algorithms also differ significantly in their time and computational resource requirements (as discussed in the Section 6.3).

Beyond the concrete improvements offered by our new techniques, our work emphasizes the need for more research across multiple avenues: (1) bridging the gap between privacy lower bounds, backed by attacks, and upper bounds, based on privacy analyses (in particular for PATE); (2) making the privacy analysis of different approaches comparable; (3) designing stronger attack models to better communicate empirical privacy guarantees.

References

[1] Devansh Arpit et al. "A closer look at memorization in deep networks". In: *International Conference on Machine Learning*. PMLR. 2017, pp. 233–242.

[2] Philip Bachman, Ouais Alsharif, and Doina Precup. "Learning with pseudo-ensembles". In: *Advances in Neural Information Processing Systems*. Ed. by Z. Ghahramani et al. Vol. 27. 2014.

[3] Amos Beimel, Kobbi Nissim, and Uri Stemmer. "Private learning and sanitization: pure vs. approximate differential privacy". In: *Theory of Computing* 12.1 (2016), pp. 1–61.

[4] David Berthelot et al. "MixMatch: A holistic approach to semi-supervised learning". In: *Advances in Neural Information Processing Systems*. Ed. by H. Wallach et al. Vol. 32. 2019.

[5] Nicholas Carlini et al. "Extracting training data from large language models". In: *arXiv preprint arXiv:2012.07805* (2020).

[6] Nicholas Carlini et al. "The Secret Sharer: Evaluating and testing unintended memorization in neural networks". In: *28th USENIX Security Symposium*. 2019, pp. 267–284.

[7] Kamalika Chaudhuri and Daniel Hsu. "Sample complexity bounds for differentially private learning". In: *Proceedings of the 24th Annual Conference on Learning Theory*. 2011, pp. 155–186.

[8] Ekin D Cubuk et al. "RandAugment: Practical automated data augmentation with a reduced search space". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*. 2020, pp. 702–703.

[9] John Duchi et al. "Efficient Projections onto the ℓ_1-ball for learning in high dimensions". In: *Proceedings of the 25th International Conference on Machine Learning*. 2008, pp. 272–279.

[10] Cynthia Dwork and Aaron Roth. "The algorithmic foundations of differential privacy." In: *Foundations and Trends in Theoretical Computer Science* 9.3-4 (2014), pp. 211–407.

[11] Cynthia Dwork et al. "Calibrating noise to sensitivity in private data analysis". In: *Proceedings of the 3rd Conference on Theory of Cryptography*. TCC '06. Berlin, Heidelberg: Springer, 2006, pp. 265–284.

[12] Cynthia Dwork et al. "Our data, ourselves: Privacy via distributed noise generation". In: *Advances in Cryptology—EUROCRYPT 2006*. Ed. by Serge Vaudenay. 2006, pp. 486–503.

[13] Cynthia Dwork et al. "Preserving statistical validity in adaptive data analysis". In: *Proceedings of the forty-seventh annual ACM Symposium on Theory of Computing (STOC)*. 2015, pp. 117–126.

[14] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. "RAPPOR: Randomized aggregatable privacy-preserving ordinal response". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Nov. 2014).

[15] Úlfar Erlingsson et al. "That which we call private". In: *CoRR* abs/1908.03566 (2019). arXiv: `1908.03566`. URL: `http://arxiv.org/abs/1908.03566`.

[16] Vitaly Feldman. "Does learning require memorization? A short tale about a long tail". In: *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. 2020, pp. 954–959.

[17] Badih Ghazi et al. *On deep Learning with label differential privacy*. 2021. arXiv: `2102.06062 [cs.LG]`.

[18] Kaiming He et al. *Deep Residual Learning for Image Recognition*. 2015. arXiv: `1512.03385 [cs.CV]`.

[19] Matthew Jagielski, Jonathan Ullman, and Alina Oprea. "Auditing differentially private machine learning: How private is private SGD?" In: *Advances in Neural Information Processing Systems*. Ed. by H. Larochelle et al. Vol. 33. 2020, pp. 22205–22216.

[20] Jungdae Kim. *FixMatch-pytorch*. `https://github.com/kekmodel/FixMatch-pytorch`. Available under MIT License.

[21] Alex Krizhevsky. *Learning multiple layers of features from tiny images*. Tech. rep. 2009.

[22] Dong-Hyun Lee. "Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks". In: *Workshop on challenges in representation learning, ICML*. Vol. 3. 2. 2013.

[23] Kuang Liu. `https://github.com/kuangliu/pytorch-cifar/blob/master/models/resnet.py`. Available under MIT License.

[24] Milad Nasr et al. "Adversary instantiation: Lower bounds for differentially private machine learning". In: *2021 IEEE Symposium on Security and Privacy (S&P)*. May 2021, pp. 1183–1199.

[25] Aleksandar Nikolov, Kunal Talwar, and Li Zhang. "The geometry of differential privacy: The sparse and approximate cases". In: *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing (STOC)*. STOC '13. 2013, pp. 351–360.

[26] Nicolas Papernot et al. "Scalable private learning with PATE". In: *6th International Conference on Learning Representations (ICLR)*. Paper available from `https://openreview.net/forum?id=rkZB1XbRZ`. Code available from `https://github.com/tensorflow/privacy/tree/master/research/pate_2018` under Apache 2.0 license. 2018.

[27] Nicolas Papernot et al. "Semi-supervised knowledge transfer for deep learning from private training data". In: *5th International Conference on Learning Representations (ICLR)*. 2017. URL: `https://openreview.net/forum?id=HkwoSDPgg`.

[28] Paul M Schwartz. "Privacy and democracy in cyberspace". In: *Vanderbilt Law Review* 52 (1999), pp. 1607–1702.

[29] Reza Shokri et al. "Membership inference attacks against machine learning models". In: *2017 IEEE Symposium on Security and Privacy (S&P)*. IEEE. 2017, pp. 3–18.

[30] Kihyuk Sohn et al. "FixMatch: Simplifying semi-supervised learning with consistency and confidence". In: *Advances in Neural Information Processing Systems*. Ed. by H. Larochelle et al. Vol. 33. 2020, pp. 596–608. URL: `https://arxiv.org/abs/2001.07685`.

[31] Salil Vadhan. "The complexity of differential privacy". In: *Tutorials on the Foundations of Cryptography*. Springer, 2017, pp. 347–450.

[32] Di Wang and Jinhui Xu. "On sparse linear regression in the local differential privacy model". In: *Proceedings of the 36th International Conference on Machine Learning*. Ed. by Kamalika Chaudhuri and Ruslan Salakhutdinov. Vol. 97. Proceedings of Machine Learning Research. PMLR, June 2019, pp. 6628–6637.

[33] Weiran Wang and Miguel Á. Carreira-Perpiñán. *Projection onto the probability simplex: An efficient algorithm with a simple proof, and an application*. 2013. arXiv: `1309.1541 [cs.LG]`.

[34] Stanley L Warner. "Randomized response: A survey technique for eliminating evasive answer bias". In: *Journal of the American Statistical Association* 60.309 (1965), pp. 63–69.

[35] Samuel Yeom et al. "Privacy risk in machine learning: Analyzing the connection to overfitting". In: *31st IEEE Computer Security Foundations Symposium (CSF)*. 2018, pp. 268–282.

[36] Sergey Zagoruyko and Nikos Komodakis. "Wide residual networks". In: *Proceedings of the British Machine Vision Conference (BMVC)*. Ed. by Richard C. Wilson, Edwin R. Hancock, and William A. P. Smith. Sept. 2016, pp. 87.1–87.12.

[37] Chiyuan Zhang et al. "Understanding deep learning requires rethinking generalization". In: *5th International Conference on Learning Representations (ICLR)*. 2017. URL: `https://openreview.net/forum?id=Sy8gdB9xx`.

Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope? [Yes]
   (b) Did you describe the limitations of your work? [Yes]
   (c) Did you discuss any potential negative societal impacts of your work? [No]
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes]
2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [Yes]
   (b) Did you include complete proofs of all theoretical results? [Yes] *See Section B in Supplemental results.*
3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] *The code is included in the supplemental materials.*
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] *See Section 6.*
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [No] *All reported accuracies are stable* $\pm .5\%$*, empirical privacy estimates (Table 1) are reported as 95%-confidence intervals.*
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [No]
4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] *We cite Kim [20], Krizhevsky [21], Papernot et al. [26], Liu [23], and Zagoruyko and Komodakis [36].*
   (b) Did you mention the license of the assets? [Yes] *We list licenses for code where available.*
   (c) Did you include any new assets either in the supplemental material or as a URL? [Yes] *The supplemental materials include training code and implementation of memorization attacks.*
   (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? [N/A]
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [N/A]
5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]
   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]
   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]