Gradient Leakage Attack Resilient Deep Learning
Wenqi Wei, Student Member, IEEE, Ling Liu, Fellow, IEEE,

Abstract—Gradient leakage attacks are considered one of the wickedest privacy threats in deep learning as attackers covertly spy gradient updates during iterative training without compromising model training quality, and yet secretly reconstruct sensitive training data using leaked gradients with high attack success rate. Although deep learning with differential privacy is a defacto standard for publishing deep learning models with differential privacy guarantee, we show that differentially private algorithms with fixed privacy parameters are vulnerable against gradient leakage attacks. This paper investigates alternative approaches to gradient leakage resilient deep learning with differential privacy (DP). First, we analyze existing implementation of deep learning with differential privacy, which use fixed noise variance to inject constant noise to the gradients in all layers using fixed privacy parameters. Despite the DP guarantee provided, the method suffers from low accuracy and is vulnerable to gradient leakage attacks. Second, we present a gradient leakage resilient deep learning approach with differential privacy guarantee by using dynamic privacy parameters. Unlike fixed-parameter strategies that result in constant noise variance, different dynamic parameter strategies present alternative techniques to introduce adaptive noise variance and adaptive noise injection which are closely aligned to the trend of gradient updates during differentially private model training. Finally, we describe four complementary metrics to evaluate and compare alternative approaches. Extensive experiments on six benchmark datasets show that differentially private deep learning with dynamic privacy parameters outperforms the deep learning using fixed DP parameters, and existing adaptive clipping approaches in all aspects: compelling accuracy performance, strong differential privacy guarantee, and high attack resilience.

Index Terms—deep learning, gradient leakage attack, differential privacy

I. INTRODUCTION

D eep neural networks (DNNs) have demonstrated superior capability of learning complex tasks with high prediction accuracy. With the premium environment for model training using rich data that companies are collecting about their users, two questions remain an overwhelming challenge: (i) how can a model be trained on private collections of sensitive data so that it can be deployed safely, minimizing disclosure of sensitive training data? and (ii) can a DNN model trained with differential privacy be trusted for its outputs against privacy intrusion?

Privacy Risks in Deep Learning. Deep learning is vulnerable to many privacy attacks at both training phase and prediction phase, by exploiting its large capacity from the large number of model parameters sufficient for encoding the details of the individual data. Gradient leakage attacks are the dominating privacy threats during training phase [1]–[10], assuming training data is encrypted in storage and transportation. The attacker, without any prior knowledge about the learning model, can breach secrecy and confidentiality of the training data from the intermediate gradients. There are also privacy threats in prediction phase, e.g., model inversion [11], [12], attribute inference [13], [14], membership inference [15]–[20] and GAN-based reconstruction attack [21], [22]. These privacy concerns aggravate with the broad deployment of deep learning applications and deep learning as a service. Although recent studies on gradient leakage attacks were in the context of federated learning [3], [4], [5], the attacks are high-risk threats for both centralized cloud and edge clients because the same spying process and unauthorized read can be silently employed during model training without being noticed, and the same reconstruction algorithms can be utilized to disclose private training data from the leaked gradients. This paper presents risk assessment of gradient leakage attacks and presents a gradient leakage resilient deep learning approach by extending conventional deep learning with differential privacy algorithms with dynamic privacy parameter optimizations.

Deep Learning with Differential Privacy. Differentially private deep learning is the de facto standard for publishing DNN models with provable privacy guarantee [23]: It is extremely hard to characterize the difference in output between any two models trained using two neighboring inputs differing by at most one element. In other words, by simply observing the output of a DNN model trained using the differentially private learning algorithm, one cannot tell if a single example is used in the training. [24] is the first to implement differentially private deep learning with moments accountant method for a much tighter privacy accounting under random sampling. To regulate the maximum influence of the model under the two neighboring inputs, conventional approaches [24]–[28] implement differentially private deep learning by first clipping the gradients and then applying differential privacy-controlled noise to perturb the gradients before employing the stochastic gradient descent (SGD) algorithm, ensuring that each gradient descent step is differentially private. Based on composition properties of differential privacy algorithms [23], the final model produced upon completion of the total training steps provides a certain level of differential privacy.

Inherent Limitations of Baseline. Inspired by the pioneer work [24], many proposals in the literature [25], [27], [29] and open source community [30], [31] employ the fixed privacy parameter strategy to decide clipping method, define the sensitivity of gradient updates and noise scale, which results in constant noise injection throughout every step of the entire training process. Although such a rigid setting of privacy parameters has shown reasonable accuracy while providing a certain level of differential privacy guarantee, they suffer some inherent limitations. First, fixed privacy parameters induce constant differential privacy noise throughout the training,
which deems unnecessary especially at the later stage of training, and leads to low accuracy utility. Second, even with differential privacy guarantee, such algorithms require careful privacy parameter selection as otherwise remaining vulnerable against gradient leakage induced privacy violation, breaking the intended privacy protection. Although some development aim to improve the accuracy of differentially private deep learning by optimizing the noise [24], [26], [32]–[36], all these methods are not designated to defend against the gradient leakage attacks.

Scope and Contributions. In this paper, we investigate alternative approaches to differentially private deep learning, aiming for strong privacy, high accuracy performance as well as high resilience against gradient leakage attacks. This paper makes three original contributions. First, we analyze existing implementation of deep learning with differential privacy which injects differential privacy controlled noise to perturb the gradients in all layers using fixed privacy parameters. We show that despite the differential privacy guarantee provided, the deep learning model suffers from low accuracy utility and can be vulnerable to gradient leakage attacks. This motivates us to analyze the inherent limitations of using fixed-parameter strategies in deep learning with differential privacy. Second, we propose a differentially private deep learning approach with adaptive DP parameters to address the inherent limitations of conventional deep learning algorithms with fixed DP parameters. We propose three adaptive DP parameter optimizations to allow dynamic DP controlled noise variance such that more noise is injected in early rounds and smaller noise is used to perturb the gradients in the later rounds, including dynamic gradient clipping method, dynamic sensitivity and dynamic noise scale. We show that our approach with dynamic DP parameters can achieve high resilience against gradient leakage attacks, competitive accuracy performance, better differential privacy guarantee. Unlike fixed-parameter strategies that result in constant noise variance, differentially private deep learning with adaptive DP parameters can align noise injection to the trend of gradient updates during differentially private model training. Third, we present four complementary metrics for evaluation and comparative analysis of alternative approaches to differentially private deep learning: (i) comparing accuracy (utility) performance under the same privacy budget, (ii) comparing privacy cost and the level of privacy protection under the same target model accuracy, and (iii) comparing resilience against gradient leakage attacks. Extensive experiments are conducted on six benchmark datasets with five privacy accounting methods. The results show that deep learning with dynamic differential privacy optimization on sensitivity and noise scale outperforms both the baseline and other alternative approaches with dynamic parameter optimizations, offering compelling accuracy performance, strong differential privacy guarantee, and high attack resilience.

II. GRADIENT LEAKAGE THREAT MODEL

Gradient leakage attacks are most relevant privacy threats in the context of deep learning, in which a curious or malicious insider may conduct unauthorized read on the gradients and reconstruct private training data based on the gradients obtained through spying over the layer-wise gradients utilized by per-step SGD in each iteration of the training. Such insider threats do not directly compromise the accuracy of the trained model and thus are much harder to detect and mitigate through reactive defense methods. We argue that effective approaches to deep learning with differential privacy can build one of the best defense methods against such threats. Our threat model makes the following assumptions about the insider adversary: (1) the insider adversary cannot gain access to the encrypted training data prior to training; (2) the insider adversary has no intention of compromise the training procedure or the quality of the trained model; and (3) the insider adversary may gain access to the intermediate model training parameters that are often saved as checkpoint data to allow the resume of iterative training from a given step. Unlike white-box adversarial example attacks [37]–[40], gradient leakage attacks do not need any prior knowledge of the DNN training algorithm and simply use independent reconstruction algorithms on leaked gradients to infer and disclose the private training data [5] while keeping the integrity of the training.

With parallel processing of the data, the module is replicated on each device in the forward pass and each replica handles a portion of the input. During the backward pass, gradients from each replica are summed into the original module. Figure 1 gives a sketch of the gradient leakage attack algorithm under the multi-GPU setting, which configures and executes the reconstruction attack in five steps: (1) It configures the initialization seed $(x^0_{rec}(t))$, a dummy data of the same resolution (or attribute structure for text) as the training data. Fig. 2 shows some significant impact of different initialization seeds on
the attack success rate and attack cost (\# attack iterations to succeed). (2) The dummy attack seed is fed into the current copy of the model. (3) The gradient of the dummy attack seed is obtained by backpropagation. (4) The gradient loss is computed using a vector distance loss function, e.g., $L_2$, between the gradient of the attack seed and the actual gradient from the training. The choice of this reconstruction loss function is another tunable attack parameter. (5) The dummy attack seed is modified by the attack reconstruction learning algorithm. It aims to minimize the vector distance loss by a loss optimizer such that the gradients of the reconstructed seed $x_{\text{rec}}(t)$ at round $i$ will be closer to the actual gradient updates stolen upon the completion of computing the gradients of one input in the batch or of the entire batch. For batch gradient, $\{1\}$ and $[4]$ maliciously introduce separate weights for each batch example, making it possible for a recovery of a batch of data: $x_{\text{rec}}(t) \mod B \leftarrow x_{\text{rec}}(t) \mod B - \nabla x_{\text{rec}}(t) \mod B \cdot D$ where $B$ is the batch size and $i$ is index of data in the batch. This attack reconstruction learning iterates until it reaches the attack termination condition ($\mathbb{T}$), typically defined by the \# attack iterations, e.g., $\mathbb{T} = 300$ (also a configurable attack parameter). If the reconstruction loss is smaller than the specified distance threshold then the reconstruction attack is successful. Figure 2 provides a visualization by examples from four datasets at different attack iterations. The details of these datasets are given in Section [V]. All the experiments on gradient leakages in this paper use the patterned random seed initialization $\mathbb{P}$ with a $L_2$ based loss function and L-BFGS optimizer, for high attack success rate (ASR) and fast attack convergence.

III. BASELINE SOLUTION WITH DIFFERENTIAL PRIVACY

In this section, we first review the differential privacy concept. Then we present the baseline deep learning with differential privacy approach that utilizes fixed privacy parameters and point out the inherent problem of fixed privacy parameters in terms of accuracy utility loss and gradient leakage vulnerability.

A. Preliminary

Definition 1. Differential privacy [23]: Let $\mathcal{D}$ be the domain of possible input data and $\mathcal{R}$ be the range of all possible output. A randomized mechanism $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ satisfies $(\epsilon, \delta)$-differential privacy if for any two input sets $A \subseteq \mathcal{D}$ and $A' \subseteq \mathcal{D}$, differing with only one entry: $||A - A'||_0 = 1$, Equation 7 holds with $0 \leq \delta < 1$ and $\epsilon > 0$.

\[
\Pr(\mathcal{M}(A) \in \mathcal{R}) \leq e^\epsilon \Pr(\mathcal{M}(A') \in \mathcal{R}) + \delta.
\]  

(1)

This definition states that given $\delta$, a smaller $\epsilon$ would indicate a smaller difference between the output of $\mathcal{M}(A)$ and the output of $\mathcal{M}(A')$. By Lemma 3.17 of [23], $(\epsilon, \delta)$-differential privacy ensures that for any adjacent $A, A'$, the absolute value of the privacy loss will be bounded by $\epsilon$ with probability of at least $1 - \delta$. When $0 \leq \delta < 1$, this definition implies that it is most likely that the observed output for $A'$ will be similar to the output for its neighboring input $A$, whereas when $\delta = 0$, it indicates that the output observed under $A'$ is highly likely to be observed under $A$. Since $\delta$ is the upper bound probability of $\mathcal{M}(A)$ for breaking $\epsilon$-differential privacy, a smaller $\delta$ is desired. Following the literature [24, 26, 27, 36], $\delta$ is set to $1e-5$ in our experiments such that $\epsilon$-differential privacy would hold with probability of at least 0.9999.

Definition 2. Sensitivity [17]: Let $\mathcal{D}$ be the domain of possible input data and $\mathcal{R}$ be the domain of all possible output. The sensitivity of a function $f : \mathcal{D} \rightarrow \mathcal{R}$ is the maximum amount that the function value varies when a single entry of the input is changed.

\[
S = \max_{A, A' \subseteq \mathcal{D}} ||A - A'||_0 = 1 ||f(A) - f(A')||_p.
\]  

(2)

Definition 2 implies that to produce a randomized differentially private algorithm $\mathcal{M}(f)$ by injecting noise that follows some randomization distribution while preserving the utility of $f$, we need to bound the noise by the maximum change defined as the sensitivity of function $f$ with neighboring inputs. In this paper, we consider Gaussian mechanism as our randomization noise distribution, which adds Gaussian noise calibrated to the sensitivity of the function $f$ in $l_2$ norm. Hence, we define $S$ by $l_2$ sensitivity under Gaussian noise injection.

Theorem 1. Gaussian mechanism [23]: Let $\mathcal{D}$ be the domain of possible input data and $\mathcal{R}$ be the range of all possible output. With privacy parameter $\epsilon$, applying Gaussian noise $\mathcal{N}(0, \varsigma^2)$ calibrated to a real valued function: $f : \mathcal{D} \rightarrow \mathcal{R}$ with noise variance $\varsigma^2$ such that $\mathcal{M}(A) = f(A) + \mathcal{N}(0, \varsigma^2)$ is $(\epsilon, \delta)$-differentially private if $\varsigma^2 > \frac{2\log(1.25/\delta)}{\epsilon^2}$. This theorem indicates that for a constant $\epsilon$, when $\varsigma^2 > 2\log(1.25/\delta)$, we have Gaussian mechanism $\mathcal{M}(A) = f(A) + \mathcal{N}(0, \varsigma^2)$, and if $\varsigma \geq cS/\epsilon$, then $\log \frac{e^{c - 1/2c^2 x^2} + \exp(\varsigma)}{e^{c - 1/2c^2 x^2} + \exp(-\varsigma)} \leq \epsilon$ holds with probability at least $1 - \delta$, where $\varsigma$ is the random variable utilizing the Gaussian distribution noise with Gaussian density function $\frac{1}{\sqrt{2\pi}\varsigma} e^{-\frac{x^2}{2\varsigma^2}}$. Hence, it is straightforward to get the following lemma:

Lemma 1. Let noise variance $\varsigma^2$ in Gaussian mechanism be $\sigma^2 S^2$ where $\sigma$ is the noise scale and $S$ is the $l_2$ sensitivity. We have the noise scale $\sigma$ satisfying $\sigma^2 > \frac{2\log(1.25/\delta)}{\epsilon^2}$. According to this lemma, noise scale $\sigma$ and privacy loss $\epsilon$ have an inverse correlation given a fixed $\delta$, i.e., a large noise scale indicates a small $\epsilon$, and conversely, a small noise scale implies the spending of a large privacy budget $\epsilon$.

B. Privacy Accounting

Based on the DP composition theory [23], post processing theory [23], and privacy amplification [22], the privacy budget spending can be tracked throughout the iterations of DNN training. There are four representative privacy accounting methods: moments accountant (MA) [24], zCDP [27], advanced composition (AdvC) [43] and optimal composition (OptC) [44].

Theorem 2. Composition theorem [23]: Let $\mathcal{M}_i : \mathcal{D} \rightarrow \mathcal{R}_i$ be a randomized function that is $(\epsilon_i, \delta_i)$-differentially private.

https://github.com/git-disl/ESORICS20-CPL
If $M$ is a sequence of consecutive invocations (executions) of $(\epsilon_i, \delta_i)$-differentially private algorithm $M_i$, then $M$ is $(\sum_i \epsilon_i, \sum_i \delta_i)$-differentially private.

By Theorem 3, a randomized function $M$ that consists of a sequence of $n$ differentially private mechanisms is differentially private, and its privacy guarantee is determined by the sum of the $n$ individual privacy losses, defined by $\sum^n_i \epsilon_i$. In our experiments, we consider five privacy accounting rules: base composition, advanced composition, optimal composition, Moments Accountant, and zCDP.

**Advanced composition (AdvC [43]):** Let $\epsilon, \delta' \geq 0$. The class of $\epsilon, \delta'$-differentially private mechanisms satisfies $(\epsilon, \delta')$-differential privacy under $T$-fold composition for:

$$
\epsilon' = \sum_T \frac{(\epsilon - 1)\epsilon}{\epsilon + 1} + \sqrt{\sum_T 2\epsilon^2 \log(1/\delta)}
$$

(3)

**Optimal composition (OptC [44]):** Let $\epsilon, \delta' \geq 0$. The class of $\epsilon, \delta'$-differentially private mechanisms satisfies $(\epsilon, \delta')$-differential privacy under $T$-fold composition for:

$$
\epsilon' = \sum_T \frac{(\epsilon - 1)\epsilon}{\epsilon + 1} + \sqrt{\sum_T 2\epsilon^2 \log(e + \sqrt{T^2 \epsilon^2 / \delta})}
$$

(4)

**Moments accountant (MA [24]):** For a mechanism $M$ with Gaussian noise $\mathcal{N}(0, \sigma^2 S^2)$ added at each iteration where $S$ denotes the sensitivity and $\sigma$ is the noise scale, given dataset $D$ with a total of $N$ data points, the random sampling with replacement and the sampling rate $q = n/N$ where $n$ is the sample size, and the number of iterations $T$, if $q < \frac{\sigma}{N\epsilon}$, there exist constants $c1$ and $c2$ so that for any $\epsilon < c1\sqrt{T}, M$ is $(\epsilon, \delta)$-differentially private for $\delta > 0$ and

$$
\epsilon' \geq c2q\sqrt{T\log(1/\delta)}
$$

(5)

Note that Rényi differential privacy [45], [46] is proposed on top of moments accountant to keep track of the $\epsilon$ privacy spending of a sequence of randomized mechanisms with elegant composition rules. Rényi differential privacy can be transformed to the standard differential privacy definition. We will use Moments accountant for fair comparison with other privacy accounting methods.

**zCDP [27]:** For a mechanism $M$ with Gaussian noise $\mathcal{N}(0, \sigma^2 S^2)$ added at each iteration where $S$ denotes the sensitivity and $\sigma$ is the per-iteration noise scale, given dataset $D$ with a total of $N$ data points, the random sampling with replacement and the sampling rate $q = n/N$ where $n$ is the sample size, and the number of iterations $T$, if $q < \frac{\sigma}{N\epsilon}$, $M$ is $(\epsilon', \delta)$-differentially private for $\delta > 0$ and

$$
\epsilon' = \sum_T q^2/\sigma^2 + 2\sqrt{\sum_T q^2/\sigma^2 \log(1/\delta)}
$$

(6)

Due to the random sampling involved, both advanced composition and optimal composition $(\epsilon_i, \delta_i)$ consider an amplified per-iteration privacy spending and assume a fixed $\delta$ to track $\epsilon$ using the following privacy amplification theorem. Note that for Moments accountant, we follow the implementation provided by the Tensorflow Privacy module [47] as no closed-form expression in terms of the noise scale nor the heterogeneous per-step $\epsilon_i$ is given to compute the accumulated $\epsilon$.

**Theorem 3. Privacy amplification [22]:** Given dataset $D$ with $|D|$ data points, subsampling is defined as random sampling with replacement with $n$ as the sample size. If $M$ is $(\epsilon, \delta)$-differentially private, then the subsampled mechanism with sampling rate $q = n/|D|$ is $(\log(1 + q(\exp(\epsilon) - 1)), q\delta)$-differentially private.

**C. Baseline with Fixed Parameters**

The goal of deep learning with differential privacy is to train a $(\epsilon, \delta)$-differentially private model over $T$ iterations. By composition theorem, we need to ensure that the per-step SGD, denoted by $f_i$, is $(\epsilon_i, \delta_i)$-differentially private $(1 \leq t \leq T)$ with $\epsilon = \sum_T \epsilon_i$ and $\delta = \sum_T \delta_i$. Hence, for each iteration $t$, we inject differential privacy controlled noise to the gradients before performing per-step SGD. Given a DNN of $M$ layers, the baseline implementation for ensuring that $f_i$ is $(\epsilon_i, \delta_i)$-differentially private injects noise to all layers of the model during each training iteration.

**Fixed privacy parameters.** Most of existing approaches to deep learning with differential privacy [24], [27], [36], [48], including Tensorflow privacy module [30] and Pytorch Opacus privacy module [31], all employ fixed privacy parameter strategies, such as the constant clipping method with pre-defined clipping bound (e.g., $C = 4$), the fixed pre-defined noise scale (e.g., $\sigma = 6$), and the fixed sensitivity $S$ defined using the constant clipping bound $C$. As a result, in addition to distributing the privacy budget $\epsilon$ uniformly across the total $T$ training iterations, the noise variance is fixed during the training, resulting in injecting constant noise to the gradients in each training iteration.

**Constant clipping method with fixed clipping bound.**

Given a training example $i$, let $\nabla W(t)_{im}$ denote the layer-wise per-example gradient vector for the $m^{th}$ layer ($1 \leq m \leq M$). The clipping method is used prior to noise injection to address the problem of gradient explosion [49]. With a constant clipping method using a fixed clipping bound $C$, the layer-wise per-example gradient vector $\nabla W(t)_{im}$ is preserved if its $l_2$ norm satisfies $||\nabla W(t)_{im}||_2 \leq C$. Otherwise, $||\nabla W(t)_{im}||_2 \geq C$ holds, and the gradient vector $\nabla W(t)_{im}$ needs to be brought down so that its $l_2$ norm is capped by $C$. This is done by multiplying every coordinate of the gradients with a scaling factor: $C/||\nabla W(t)_{im}||_2$. Such per-example gradient clipping will be performed on all $M$ layers for each example $i$ in the batch $B$ of the given iteration. Let $\nabla W(t)_{im}$ denote the clipped per-example gradient for layer $m$ of training example $i$ at iteration $t$ ($m \in \{1, 2, ..., M\}$). The clipped per-example gradients are then gathered for batch averaging: $\nabla W(t) = \frac{1}{B} \sum_{B} \nabla W(t)_i$. Algorithm 1 presents pseudo code for baseline clipping function using the constant clipping method initialized with a preset clipping bound $C$ [24].

**Noise injection with fixed sensitivity $S$ and fixed $\sigma$.**

Next, the $(\epsilon_i, \delta_i)$-differentially private controlled Gaussian noise $\mathcal{N}(0, \sigma^2 S^2)$ is injected to each layer of the batch gradients: $\nabla W(t) = \nabla W(t) + \mathcal{N}(0, \sigma^2 S^2)$. The per-step SGD function $f_i$ performs the gradient descent at iteration $t$ using the Gaussian noise perturbed gradients $\nabla W(t)$, such that $W(t + 1) = W(t) - \eta \nabla W(t)$. This process of sampling,
Algorithm 1: CLIP (C, \nabla W_i)

Input: Per-example gradient \nabla W_i with M layers, clipping bound C.
1 for layer m in \{1, \ldots, M\} do
   // compute \ell_2 norm for layer m of sample i.
   \ell_2_{im} = \|\nabla W_{im}\|_2
   // clip per-example gradients by coordinate for layer m of sample i.
   \nabla W_{im} \leftarrow \nabla W_{im} \times \min\{1, \frac{C}{\ell_2_{im}}\}
end
5 Output: the clipped per-example gradients for sample i:
   \nabla W_i \leftarrow \{\nabla W_{im}\}, m = 1, \ldots, M.

Given that gradients at early training iterations tend to leak more information than gradients in the later stage of the training \cite{5}, an obvious approach is to design a differential privacy algorithm that can inject larger noise at the early stage of training and resort to smaller noise injection as the training is close to the end. Given that the noise variance \( \varsigma \) is the product of sensitivity \( S \) and noise scale \( \sigma \), several possible strategies can be promising, such as having the sensitivity calibrated to the \( \ell_2 \)-norm of the gradients, or having a smoothly decaying noise scale such that the noise variance follows the trend of gradient updates across the \( T \) training iterations.

IV. Dynamic Privacy Parameters

A detrimental limitation of using fixed privacy parameter strategies for deciding the clipping method and for defining sensitivity and noise scale is the result of constant noise variance and constant noise injection in each iteration of deep learning, which is a root cause for poor resilience against gradient leakage attacks. In this section, we address such inherent limitations by developing dynamic parameter strategies for determining and configuring these privacy parameters in a training progress-aware manner. This brings out a significant advantage: smaller noise variance will be used to inject noise at the later stage of the training, improving the convergence speed of training with high accuracy performance; and at the same time larger noise variance will be used to inject a larger amount of noise at the early stage of the training, leading to higher resilience against gradient leakage attacks. Given that the noise variance \( \varsigma \) is the product of sensitivity \( S \) and noise scale \( \sigma \) (recall Theorem 1), several possible dynamic strategies are promising, such as having the sensitivity calibrated to the \( \ell_2 \)-norm of the gradients or having a smoothly decaying noise scale such that the noise variance follows the trend of gradient updates across the \( T \) training iterations.

A. Dynamic Sensitivity

We describe three different strategies for implementing dynamic sensitivity, aiming to derive declining noise variance as the training progresses in iterations: \( \ell_2 \)-norm based sensitivity, denoted by DP-dynS[\( l_2 \)-max], dynamic decaying clipping method, denoted by DP-dynS[\( C_{\text{decay}} \)], and the combination of both, denoted by DP-dynS.

DP-dynS[\( l_2 \)-max]. Given that the clipping with a fixed bound \( C \) is performed on the \( \ell_2 \)-norm of the layer-wise gradients of per-example in a batch, one way to accommodate the noise variance calibrated to the \( \ell_2 \) norm of the gradient is to use the max \( \ell_2 \) norm measured on per-example gradients in a batch \( B \) as the sensitivity of the training function \( f_t \) for iteration \( t \) (recall Definition 2). Consider two scenarios: (1) When any of the per-example gradients in a batch is larger than the clipping bound \( C \), the sensitivity is set to \( C \), and however, (2) when \( \ell_2 \) norm of all per-example gradients in a batch is smaller than the pre-defined clipping bound \( C \), the clipping bound \( C \) is unfortunately a loose estimation of the true sensitivity of function \( f_t \) at iteration \( t \). If we instead define the sensitivity of \( f_t \) by the max \( \ell_2 \) norm among these per-example gradients in the batch, we will correct the problems.
in the above scenario (2). In summary, the $l_2$-max sensitivity will take the smallest of the max $l_2$ norm and the clipping bound $C$. Given that the $l_2$-norm of the gradients closely follows the trend of gradient changes as the training progresses in iterations, our dynamic $l_2$ sensitivity approach will have adaptive sensitivity $S$, and hence adaptive noise variance when a fixed $\sigma$ is used, and consequently inject larger noise at the early stage of training and smaller differential privacy noise at the later stage of training.

Note that unlike mean estimation [51], [52], knowing the $l_2$ norm-based sensitivity of the multi-dimension gradient vector on per-example gradients in deep learning training cannot help disclosing the gradient value at each coordinate. Meanwhile, the $l_2$-max norm actually tracks the sensitivity of the training function at each iteration. Yet composition theorem only requires the individual training function component to be differentially private, with each training function component taking care of its own sensitivity. This makes the $l_2$-max sensitivity a possible choice for sensitivity optimization.

**DP-dynS$[C_{\text{decay}}]$**. The second dynamic sensitivity strategy is to use dynamic decaying clipping. Given that clipping is used to regulate the largest change of gradients during the training, as the training progresses, the maximum changes of the gradients decrease, and gradually approach zero when training. However, with an accuracy target, the model with combined sensitivity optimizations may reach the accuracy and terminate the training earlier, resulting in smaller accumulated privacy spending.

```
Algorithm 2: DP-dynS$[S]$.
Input: input data $D$, batch size $B$, learning rate $r$, maximum iteration $T$, decaying trend $\gamma_C$ and $\gamma_r$, loss function $L$.

1. initialization: model $W(0)$, noise scale $\sigma_0$, clipping bound $C_0$.
2. for iteration $t$ in $\{0, 1, 2, ..., T - 1\}$ do
   3. // batch processing, sampled over $D$, start $f_t$.
   4. // determine the clipping bound for iteration $t$.
   5. $C_t = \text{DECAY}_C(C_{0}, \gamma_C, t)$
   6. $\sigma_t = \text{DECAY}_\sigma(\sigma_0, \gamma_r, t)$
   7. for instance $i$ in $\{1, ..., B\}$ do
      8. // obtain the per-example gradients for sample $i$ at iteration $t$.
      9. $\nabla W(t) \leftarrow \frac{1}{B} \nabla L(W(t), i)$
      10. // obtain the clipped per-example gradients for sample $i$ at iteration $t$.
      11. $\nabla W(t) \leftarrow \text{CLIP}(C_t, \nabla W(t), \phi)$
   12. // compute batch gradients on $M$ layers for iteration $t$.
   13. $\nabla W(t) \leftarrow \sum_{i=1}^{B} \nabla W(t)$
   14. // compute the max of $l_2$ norm over $M$ layers on the batch gradient for iteration $t$, assign the sensitivity $S$.
   15. $S \leftarrow \text{max}_i ||\nabla W(t)||_2$
   16. // compute sanitized batch gradients.
   17. $\nabla W(t) \leftarrow \nabla W(t) + N(0, \sigma_t S)$
   18. // gradient descent.
   19. $W(t + 1) \leftarrow W(t) - r \nabla W(t)$
   20. // end $f_t$, and start next iteration until reaching $T$.

15. Output: trained differential private model $W(T)$.
```

| baseline | dynS$[C_{\text{decay}}]$ | dynS$[\text{max}]$ | dynS$[\text{max}]$ | dyn$\sigma$ | dyn$[S, \sigma]$ |
|---------|--------------------------|------------------|------------------|-------------|------------------|
| $C_0$  | $C_0$  | $C_0$ | $C_0$ | $C_0$ | $C_0$ |
| $C_t$  | $C_{\text{decay}}$ | $C_{\text{decay}}$ | $C_{\text{decay}}$ | $C_{\text{decay}}$ | $C_{\text{decay}}$ |
| $\sigma_t$ | $\sigma_{\text{decay}}$ | $\sigma_{\text{decay}}$ | $\sigma_{\text{decay}}$ | $\sigma_{\text{decay}}$ | $\sigma_{\text{decay}}$ |

**TABLE I**: Comparison of privacy parameters in DP-baseline and the five dynamic privacy parameter approaches.

### B. Dynamic Sensitivity with Dynamic $\sigma$

Dynamic noise scale with a decaying policy is an alternative approach to supporting dynamic Gaussian noise variance over the number of $T$ training iterations, denoted by DP-dyn$\sigma$. Recall that the per-example gradients in early iterations are more informative and thus more vulnerable against gradient leakage attacks. With a dynamic decaying noise scale, we can ensure a larger noise scale and thus larger noise variance in the early stage of training and smoothly decay the scale $\sigma$ as training progresses, such that the per-example gradients are perturbed with larger noise in early iterations and relatively less exploitable by the attacker, even when a fixed sensitivity defined by the fixed clipping bound $C$ is used. In our prototype implementation, we implement the dynamic decaying noise scale policies with a starting noise scale $\sigma_0$, by employing the same set of three decay policies, denoted by $\text{DECAY}_\sigma(\sigma_0, \gamma, t)$, used in designing our decay-clipping dynamic sensitivity.

When combining dynamic $\sigma$ with dynamic sensitivity based on both $l_2$-max and decay clipping, denoted by DP-dyn$S[\cdot, \sigma]$, we expect the best dynamic parameter optimization for differentially private deep learning. Algorithm 2 provides a sketch of the pseudo-code of DP-dyn$S[\cdot, \sigma]$, which modifies DP-baseline by adding dynamic decay clipping (line 3), dynamic decay noise scale (line 4), and combining with dynamic $l_2$-max sensitivity (line 11) for each iteration of the training. Table I provides a summary of comparison for the five different dynamic parameter optimization.
dynamic privacy parameter optimizations and the DP-baseline with respect to the three privacy parameters: clipping $C$, sensitivity $S$ and noise scale $\sigma$. Figure 4 measures the noise variance $\varsigma = S\sigma$ on MNIST with three different settings: (i) fixed $S = C = 4$ and fixed $\sigma = 6$ (DP-baseline), (ii) $l_2$-max sensitivity and fixed $\sigma$ (DP-dynS) and (iii) DP-dyn$[S, \sigma]$ with $l_2$-max sensitivity and decaying noise scale starting from $\sigma_0 = 15$. Compared to the baseline approach with fixed privacy parameters and our methods with dynamic $l_2$-max or dynamic clipping, the method of DP-dyn$[S, \sigma]$ with both dynamic sensitivity $S$ and dynamic noise scale $\sigma$ offers more resilience and better accuracy because it can add larger noise in the early stage of training and small noise as the training progresses towards convergence.

V. PRIVACY ANALYSIS METRICS

For DP algorithms with fixed-parameter strategies, such as fixed clipping $C = 4$, fixed noise scale $\sigma = 6$ and fixed sensitivity $S = C$, no matter which one of the five privacy accounting methods outlined in Section III-A we choose to use, the total privacy spending $\epsilon$ will be the same, given the sampling rate and $\delta = 1e-5$. Hence, the evaluation will focus on measuring and comparing the accuracy performance of the model trained by using these DP-algorithms. However, for DP-algorithms with dynamic privacy parameter strategies, additional metrics should be considered. In this section, we describe four complementary metrics to evaluate and compare the effectiveness of alternative approaches to different differentially private deep learning; (1) model accuracy, (2) differential privacy, (3) resilience against gradient leakage attacks.

Accuracy with a target privacy budget. This metric is designed for performing utility analysis with respect to model accuracy under the same differential privacy spending (budget). When the privacy budget $\epsilon$ is given and fixed for comparing different algorithms, according to the privacy accounting methods outlined in Section III-A, the following parameters are fixed: the total iterations $(T)$, the sampling rate $q$, the privacy parameter $\delta$. By Lemma 1 the lower bound of noise scale $\sigma$ are also fixed. By Theorem 1 the definition of sensitivity $S$ will directly impact on how the noise variance $\varsigma$ is defined. This motivates us to advocate this metric as one of the four principled criteria to compare the baseline DP algorithm that use fixed privacy parameter strategies (see Section III-C) with the alternative DP algorithms that use different dynamic privacy parameter strategies (see Section IV). Following a similar setting, one may conduct privacy analysis to compare alternative DP algorithms under a fixed privacy budget $\epsilon$ and a pre-defined total training iteration $(T)$ on different datasets. This allows us to measure the level of differential privacy spending using all five representative privacy accounting methods (recall Section III-A), and to gain a deeper understanding of the difference among different accounting methods in tracking privacy spending over the same $T$ iterations of training on the same training set. The DP-algorithm with the highest accuracy performance will be the winner in this analysis.

Next, we introduce two additional privacy analysis metrics:

Privacy with a target accuracy and a fixed $\sigma$. By Lemma 1 noise scale $\sigma$ defines the lower bound of the accumulative privacy spending $\epsilon$ over the training iterations used to achieve the given target accuracy. Hence, those DP algorithms that can achieve the target model accuracy before reaching the pre-defined $T$ iterations will terminate the training earlier, which may result in smaller accumulated privacy spending. Based on Gaussian Mechanism, when a DP algorithm uses a dynamic sensitivity $S$ with a fixed noise scale $\sigma$, it will result in a dynamically changing noise variance $\varsigma$, following the trend of dynamic sensitivity. In this case, even the fixed $\sigma$ will lead to the same privacy spending $\epsilon$ under the same $T$ iterations, the dynamic sensitivity optimized DP training may achieve the target accuracy and terminate earlier. This will result in smaller accumulated privacy spending. However, for DP algorithms with fixed privacy parameters, e.g., a fixed noise scale $\sigma$ is combined with a fixed sensitivity $S$, then a constant noise variance will be used in each iteration of the training, which may result in excessive noise in the later stage of the training, degrading the utility without any gain on privacy.

Privacy with a target accuracy and a fixed $\varsigma$. This metric allows us to conduct privacy analysis from a very different perspective. Based on Theorem 1 andLemma 1, the Gaussian noise variance is defined as the multiplication of sensitivity $S$ and noise scale $\sigma$. With a fixed noise variance $\varsigma$, all DP-algorithms will inject the same amount of noise in each of the total $T$ training iterations, regardless of whether
TABLE II: Benchmark datasets and parameters

| Dataset      | # tran | # test | # features | # class | # iter | batch size | acc   |
|--------------|--------|--------|------------|---------|--------|------------|-------|
| MNIST        | 60000  | 10000  | 28×28      | 10      | 10000  | 600        | 0.875 |
| Fashion-MNIST| 60000  | 10000  | 28×28      | 10      | 10000  | 600        | 0.875 |
| CIFAR10      | 50000  | 10000  | 32×32×3    | 10      | 10000  | 500        | 0.887 |
| LFW          | 2267   | 756    | 32×32×3    | 62      | 60000  | 22         | 0.765 |
| Purchase-10  | 10000  | 2000   | 600        | 10      | 50000  | 100        | 0.825 |
| Purchase-50  | 10000  | 2000   | 600        | 50      | 5000   | 100        | 0.567 |

Resilience against Gradient Leakage Attacks. This metric is designed to measure and compare alternative DP-algorithms with respect to attack resilience, which can be defined using both (i) adverse effect of the attack, measured by the accuracy performance under attack, and (ii) attack cost in terms of the time spent to perform reconstruction inference on the leaked gradients and whether the inference results in a successful disclosure of a private training example. A DP-algorithm is considered highly resilient in the effectiveness evaluation, if under the same privacy spending, this algorithm outperforms other alternatives with the highest attack resilience.

VI. EXPERIMENTAL EVALUATION

We evaluate alternative approaches to deep learning with differential privacy using six benchmark datasets. Table II list the six datasets with training set, test set, #features, #classes, total training iterations T, batch size B, and non-private accuracy. MNIST is a grey-scale handwritten digit image dataset. Fashion-MNIST is an image dataset associated with a label from 10 clothing classes such as T-shirt, Trouser, and Pullover. CIFAR10 is a dataset of color images of objects. LFW is a dataset, originated from 13233 images of 5749 classes, by resizing the original image size of 250×250 to 32×32 and extracting the 'interesting' region. Since most of the classes have a very limited number of data points, we consider 3023 images from 62 classes that have more than 20 images per class. A 4:1 train-test ratio is applied. Purchase is a dataset adopted from Kaggle challenge of “acquire valued shopper”, with shopping histories for several thousand individuals. We consider a simplified version with 197,325 records, each with 600 binary features converted from the non-numerical raw data. Similar to [15], we cluster the data record into 10 and 50 classes for classification. A 4:1 ratio is used for training and test data split. For the four image datasets, a deep convolutional neural network with two convolutional layers and one fully connected layer is used. For

Fig. 5: Gradient leakage attack evaluation. Dynamic privacy parameters can help improving the robustness.

TABLE III: Comparing gradient leakage resilience of non-private training with DP-baseline and DP-dyn[S,σ]. The maximum attack iteration is set to 300.

| Dataset     | MNIST | Fashion-MNIST | cifar10 | LFW |
|-------------|-------|----------------|--------|-----|
| Attack iter | 11.5  | 12.4           | 28.3   | 25  |
| ASR         | 0.975 | 1.20E-05       | 2.20E-04 | 2.20E-04 |
| MSE         | 2.20E-04 | 2.20E-04       | 2.20E-04 | 2.20E-04 |

A. Resilience against Gradient Leakages

The first set of experiments measures and compares the resilience of alternative DP algorithms with fixed-parameter strategies, existing adaptive clipping approaches, and dynamic parameter strategies against gradient leakage attacks. The following three attack metrics are used to evaluate the adverse effect and cost of gradient leakage attacks, which in turn can be used to measure the resilience of different DP approaches in the presence of attacks. They are attack success rate (ASR), #attack iterations (attack iter) to succeed the inference with 300 as the default, and attack reconstruction distance in MSE (mean square error). The successful attack reconstruction is defined by MSE smaller than 0.70. We report the attack iterations and attack reconstruction distance only for

the two attribute datasets, a fully connected model with two hidden layers is applied.

Under attack No DP

Original data

MNIST Fashion-MNIST CIFAR10 LFW

Quantile clipping

Adaclip

DP-dyn[S,σ]
those successful attack examples. For attacks with complete failure, we record their reconstruction distance at the pre-defined maximum reconstruction/inference iterations of 300.

**Table III** reports the attack results under non-private models, the DP-baseline, DP-dyn\([S,\sigma]\), and two representative adaptive clipping methods: quantile-based clipping \([55]\), Adaclip \([56]\) and for the four image datasets. AdaClip performs the clipping bound estimation based on the coordinates and adaptively add different noise levels to different dimensions of the gradients, whereas the quantile clipping estimates the clipping bound using the quantile of the unclipped gradient norm. The default setting of \(C = 4, \sigma = 6\) is used for DP-baseline algorithms (fixed parameters) and also used as the initial value for quantile-based clipping \([55]\) and DP-dyn\([S,\sigma]\). The attack is performed on the gradients from the first training iteration as gradients at early training iterations tend to leak more information than gradients in the later stage of the training \([5]\). Figure 5 illustrates the reconstruction results. We make three observations: (1) For all four datasets, the gradients in non-private models are vulnerable to the gradient leakage attack. (2) The quantile-based clipping \([55]\) and AdaClip \([56]\) method can slightly improve the resilience against the gradient leakage attack compared to non-private training. The two adaptive clipping approaches focus mainly on reducing the noise variance rather than gradient attack resilience. Therefore, the DP-baseline, with large and constant noise, is more effective with high resilience against the gradient leakage threats. (3) Compared to both DP-baseline and existing adaptive clipping approaches, DP-dyn\([S,\sigma]\) offers the highest resilience against gradient leakage attacks. This is because DP-dyn\([S,\sigma]\) adds larger noise at the early iterations of the training thanks to the combined effect of dynamic sensitivity and dynamic noise scale, which effectively creates difficulty for the gradient leakage attack to succeed. The high attack reconstruction distance in Table III shows strong attack resilience against gradient leakage threats. The visualization in Figure 5 also provides an intuitive illustration of this effect. For the two existing approaches, the adaptive clipping brings down the differential privacy noise compared to DP-baseline and thus shows less improvement on the resilience of DP training against gradient leakage attacks, compared to DP-baseline. However, differential privacy noise injection combined with dynamic sensitivity and dynamic noise scale will offer the best defense against gradient leakage threats.

In the rest of the experiments, we provide empirical results and analysis to further illustrate the benefits of the proposed gradient leakage resilient deep learning with dynamic differential privacy parameter optimizations. We first demonstrate how the proposed DP-dyn\([S,\sigma]\) achieves higher accuracy compared to the DP-baseline at the same \((\epsilon, \delta)\) differential privacy level. Then we show how DP-dyn\([S,\sigma]\) obtains a stronger differential privacy guarantee in terms of smaller \(\epsilon\) spending at a target accuracy. Finally, we show that in addition to high resilience against gradient leakage, the proposed dynamic privacy parameter optimizations have an acceptable time cost compared to the conventional DP deep learning baseline. Furthermore, our approach consistently offers high test accuracy on all benchmark datasets, compared to both the conventional DP deep learning baseline and existing adaptive clipping proposals.

**B. Dynamic Sensitivity: Accuracy Analysis**

This set of experiments compares the DP-baseline with three dynamic sensitivity methods on six datasets: DP-dyn\([l_2\text{-max}\)]\), DP-dyn\([C_{\text{decay}}]\), and DP-dyn\(S\), which denotes the dynamic sensitivity defined by combining \(l_2\)-max sensitivity with dynamic clipping. Given that both DP-baseline and DP-dyn\([l_2\text{-max}\)] use a constant clipping method with fixed pre-defined clipping bound, for a fair comparison, we vary the setting of clipping bound from 1 to 32 by the interval of the power of 2 and set \(\sigma = 6\). **Table IV** reports the results. We make three observations. First, DP-dyn\([l_2\text{-max}\)] consistently outperforms DP-baseline under all settings of clipping bounds on all six datasets. This is because by Lemma 1, DP-baseline uses constant noise variance, and injects constant noise in each iteration of the training, regardless of the decreasing trend of gradients in the later stage of the training. Also, DP-baseline is highly sensitive to the settings of clipping bound for all six datasets. It results in lower accuracy when the clipping bound is set too large (e.g. \(C=16, 32\)) or too small bound (e.g. \(C=1\)). In contrast, DP-dyn\([l_2\text{-max}\)] uses dynamic \(l_2\)-max sensitivity, which changes from iteration to iteration and closely aligns with the declining trend of gradients throughout the training. Second, DP-dyn\([l_2\text{-max}\)] consistently outperforms DP-dyn\([C_{\text{decay}}]\), showing that noise variance \(\varsigma\) defined by \(l_2\)-max sensitivity and noise scale \(\sigma\) offers tighter alignment than dynamic sensitivity defined by decaying clipping bound \(C_{\text{decay}}\). A simple policy of linearly decaying from the initial clipping bound \(C\) to \(C/2\) is used in this experiment. Third, DP-dyn\(S\) takes the best from both \(l_2\)-max sensitivity and dynamic clipping and consistently outperforms all other alternative approaches on all six datasets. Based on our empirical observations, it is hard to provide a scalable

| Method         | C=1    | C=2    | C=4    | C=8    | C=16   | C=32   |
|----------------|--------|--------|--------|--------|--------|--------|
| DP-baseline    | 0.905  | 0.958  | 0.980  | 0.995  | 0.919  | 0.881  |
| DP-dyn\([C_{\text{decay}}]\) | 0.948  | 0.956  | 0.960  | 0.945  | 0.915  | 0.865  |
| DP-dyn\([l_2\text{-max}\)] | 0.959  | 0.979  | 0.977  | 0.983  | 0.975  | 0.976  |
| DP-dyn\(S\)    | 0.955  | 0.955  | 0.970  | 0.980  | 0.970  | 0.977  |

**Table IV**: Effectiveness of dynamic sensitivity optimizations in model accuracy improvement. \(\sigma = 6\) and \(T\) is given in Table I.
C. Dynamic Sensitivity: Privacy Analysis

Privacy under five accounting methods. The first set of experiments for privacy analysis is designed to measure privacy spending using five privacy accounting methods for DP-baseline and three alternative optimizations of dynamic sensitivity: DP-dynS[\(l_2\)-max], DP-dynS[C\(_{decay}\)] and DP-dynS, with clipping bound \(C = 4\), noise scale \(\sigma = 6\), and \(\delta = 1 - 5\).

Table V reports the results. We make two observations. First, all five accounting methods show consistent performance for all four DP algorithms on the six benchmark datasets, with Moment Accountant as the most efficient tracking of privacy spending followed by zCDP. Second, DP-dynS consistently outperforms both DP-baseline and the other two dynamic sensitivity algorithms with high accuracy performance, showing that the combination of \(l_2\) sensitivity with decay clipping method \(C_{decay}\) is more effective in enabling the sensitivity \(S\) to be aligned with the trend of gradient updates during the training.

Privacy under a target accuracy and a fixed \(\sigma\). In this second set of experiments, we analyze and compare DP-baseline with three alternative dynamic sensitivity optimizations in terms of their privacy spending under a target accuracy and a fixed noise scale \(\sigma\). We use the accuracy achieved by DP-baseline at \(T\) iterations as the target accuracy for each of the six datasets (recall Table 2). Table VI reports the results. DP-dynS is the winner consistently across all six datasets because it is the first to achieve the target accuracy with the smallest privacy spending. In the third and fourth experiments, the target accuracy is set to the accuracy of DP-baseline for both MNIST and CIFAR10 in the first four scenarios. For the last scenario, the target accuracy is set to the accuracy of DP-dynS[\(l_2\)-max] (0.9733) for MNIST with \(C = 4\).

Privacy under a target accuracy and a fixed \(\delta\). The third set of experiments for privacy analysis measures the privacy spending under a target accuracy and a fixed noise variance \(\delta\). We compare DP-baseline and the three alternative DP algorithms with three different dynamic sensitivity strategies DP-dynS[\(l_2\)], DP-dynS[C\(_{decay}\)], and DP-dynS on MNIST and CIFAR10. The accuracy of DP-baseline is used as the target accuracy for both MNIST and CIFAR10. We set \(\sigma = 6\), \(C = 4\)
and $C = 8$ and conduct the experiments with two fixed noise variance settings: $\varsigma = 24$ with $C = 4$ and $\varsigma = 48$ with $C = 8$. Based on Theorem 2 and Lemma 1, when the noise variance $\varsigma$ is fixed, with dynamic sensitivity $S$, the noise scale $\sigma$ will follow the trend of $S$ in a reverse trend: as $S$ continues to decline with the training progresses in #iterations, the noise scale $\sigma$ will increase to keep the noise scale $\sigma$ constant. As a result, larger sensitivity $S$ in the early stage of the training will lead to a smaller noise scale and larger privacy spending to protect informative gradients. As the training is approaching the end, the sensitivity $S$ will become smaller, resulting in larger $\sigma$ and smaller privacy spending. Table VII shows the results. Consider the first four scenarios, in which the target accuracy is set to the accuracy of DP-baseline for each dataset. We make three observations: (1) DP-dynS consistently outperforms the other three alternatives for the two noise variance settings on both datasets when given a target accuracy and a fixed noise variance $\varsigma$. (2) DP-dynS[$l_2$-max] consistently ranked as the second winner with significantly smaller privacy spending than DP-dynS[$C_{decay}$] for all four scenarios under all five privacy accounting methods. This further demonstrates that using adaptive clipping with decay function is still a loose estimation compared to using the $l_2$-max sensitivity for differentially private deep learning. Hence, DP-dynS[$C_{decay}$] consumes more privacy budget under both fixed noise variances for both datasets, compared to DP-dynS[$l_2$-max] and DP-dynS. (3) When comparing the privacy spending on the same dataset with two different fixed noise variances, or when comparing two different datasets on the same fixed noise variance, it is interesting to note that DP-baseline has the same privacy spending under both variance settings on both MNIST and CIFAR10. This is because the privacy spending $\epsilon$ is anti-correlated to noise scale $\sigma$ (recall Lemma 1) and not sensitive to the different settings of clipping bound for the constant clipping method. However, for DP algorithms with dynamic sensitivity, the privacy spending is also training data dependent. For each of the two fixed noise variances, both with $\sigma = 6$, all three dynamic sensitivity algorithms on CIFAR10 will incur higher privacy spending while their respective privacy spending on MNIST will be smaller. This confirms the common knowledge that the gradient update trend during training is model-dependent and dataset-dependent.

The last scenario is included for privacy analysis under two different target accuracy. For MNIST with $C = 4$, we set the target accuracy to the accuracy of DP-dynS[$l_2$-max] (0.9773) instead of 0.9596 from DP-baseline. We make two interesting observations. (1) DP-dynS remains the winner with strong privacy guarantee at the smallest privacy spending $\epsilon$, followed by DP-dynS[$C_{decay}$]. (2) To achieve the target accuracy of 0.9773, DP-baseline has to enforce a smaller $\sigma$ to maintain the fixed $\varsigma$, resulting in much higher spending of privacy budget according to all five privacy accounting methods. For MA, DP-baseline results in $\epsilon = 21.174$ for target accuracy of 0.9773 compared to $\epsilon = 0.823$ for the target accuracy of 0.9596 obtained at $T = 10000$. For zCDP and base composition, DP-baseline spent $4\times$ of the privacy budget for achieving the target accuracy of 0.9773, compared to the privacy spent for achieving the target accuracy of 0.9596 at $T = 10000$.

### TABLE VIII: Accuracy analysis for eight alternative DP algorithms on MNIST under three different dynamic noise scale policies ($C = 4$, $\delta = 1e-5$). The target $\epsilon$ is from Table VIII $\sigma = 6$ for DP algorithms with fixed $\sigma$ and $\sigma = 6$ is also used as the initial $\sigma$ value for dynamic $\sigma$ algorithms under each of the three decaying policies.

| $\sigma$ | BaseC | AdvC | OptC | zCDP | MA |
|----------|-------|------|------|------|----|
| DP-baseline | 0.9596 | 0.9596 | 0.9596 | 0.9596 | 0.9596 |
| DP-dynS[$C_{decay}$] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |
| DP-dynS[$l_2$-max] | 0.9773 | 0.9773 | 0.9773 | 0.9773 | 0.9773 |

#### D. Dynamic Noise Scale Optimization

In this section, we evaluate the effectiveness of incorporating dynamic noise scale into DP-baseline and the three alternative dynamic sensitivity optimized DP algorithms.

**Accuracy analysis under a target privacy budget $\epsilon$.** The first set of experiments evaluate and compare these eight alternative DP algorithms on MNIST under a given target privacy budget $\epsilon$ such that each algorithm will terminate when its target privacy budget is exhausted. Unless otherwise stated, $\delta = 1e-5$, $C = 4$ and $T = 10000$ for MNIST. Table VIII reports the results. We make three observations. (1) For DP-baseline and the three dynamic sensitivity algorithms under fixed $\sigma = 6$, we measure and compare their accuracy since they have the same privacy spending as shown in Table VIII when reaching $T$ iterations. DP-dynS and DP-dynS[$l_2$-max] are clear winners with DP-dynS slightly higher in accuracy. (2) By Lemma 1, the decaying noise scale will lead to increased per-iteration $\epsilon$ spending for early iterations in the training. As a result, the training is terminated early when the accumulated privacy loss reaches the target privacy budget under each accounting method. Different privacy composition methods accumulate heterogeneous privacy spending differently and result in different ending iterations. (3) By integrating dynamic noise scale optimization, one can further improve accuracy performance under all three noise scale decay policies compared to their corresponding algorithms under the fixed $\sigma$. DP-dynS[$S, \sigma$] is consistently the best performing algorithm under all three $\sigma$ decaying policies. Although DP-dynS with only dynamic noise scale slightly outperforms DP-baseline under the three decaying $\sigma$ policies, dynamic sensitivity approaches consistently outperform DP-dynS in accuracy performance, showing the critical role of sensitivity in achieving high training utility of DP algorithms. (4) Empirically, noise scale decay with the exponential trend has the best accuracy performance.

**Privacy analysis under a target accuracy.** In the next set of experiments, we measure and compare the accumulated privacy spending under a given target accuracy to evaluate the effectiveness of the best dynamic parameter optimization.
DP-dyn[S,σ] by comparing it with DP-baseline and three alternative dynamic sensitivity algorithms with fixed σ for MNIST: DP-dyn[S(l2-max)], DP-dyn[S(Cdecay)], DP-dynS and DP-dyn[S,σ]. The target accuracy is set to 0.9596, the accuracy of DP-baseline on MNIST with C = 4, σ = 6, δ = 1ε − 5.

We make two observations: (1) DP-dyn[S,σ] with exponential σ decay provides the best differential privacy guarantee at the smallest privacy spending ε under all five privacy accounting methods. (2) Both DP-dynS and DP-dynS[l2-max] terminate slightly earlier than DP-dyn[S,σ] under the same target accuracy. This is likely because the large early noise in the dynamic noise scale algorithm may have some marginal effect on the convergence, leading to take a fewer iterations more than the DP-dynS in reaching the target accuracy. However, DP-dyn[S,σ] spent the smallest privacy budget to achieve the target accuracy even with a slightly longer training time. This also shows that early termination does not always guarantee smaller privacy spending. The dynamic sensitivity and dynamic noise scale ultimately control the right amount of noise to be added for achieving the best privacy under a target accuracy.

### E. Time Cost Evaluation

This set of experiments compare the time cost for the non-private algorithm and five alternative approaches to differentially private deep learning using all six benchmark datasets. Table IX reports the per-iteration time cost measurement in seconds. We make three observations: (1) Incorporating dynamic parameters of sensitivity and noise scale incurs negligible additional cost. This is because all differentially private deep learning algorithms will always need to compute the l2 norm of the gradients in order to perform clipping. The difference between DP algorithms and non-private model indicates the cost of computing l2 norm of the gradients per iteration. (2) The relative cost is smaller when the model is simpler with a smaller number of parameters. For example, the two attribute datasets have a lower time cost than the four image datasets. (3) In addition to model complexity, batch size may also impact this additional time cost. The relative cost is smaller when the batch size is smaller. For example, LFW has a much smaller batch size than the other three image datasets and is relatively faster to run one iteration.

### F. Comparison with Existing Dynamic Clipping

We have shown in Section VI-A that our proposed approach for gradient leakage resilient deep learning with dynamic parameter optimizations offers the strongest resilience against gradient leakage attacks to training data privacy by comparing with both the state of the art DP baseline for deep learning and the two representative adaptive clipping enhancements [55], [56]. In this set of experiments, we provide the accuracy performance comparison to show that our dynamic parameter optimization on both noise scale and sensitivity outperforms both the baseline DP approach [24] and the two adaptive clipping proposals. Table XI compares DP-dyn[S,σ] with the two approaches in terms of accuracy performance and time cost. We consider the accuracy for the four image datasets and measure the time cost by sec/iteration. We make two observations: (1) The proposed dynamic optimization on both sensitivity S and noise-scale σ consistently outperforms both baseline DP and the two existing proposals to improve the baseline DP with AdaClip or Quantile clipping with larger accuracy performance enhancements. (2) Comparing to the baseline DP [24], the proposed dynamic parameter optimization approach incurs the smallest time cost compared to AdaClip and Quantile clipping while offering the highest accuracy improvement in comparison.

### VII. RELATED WORK

We have given an overview of related work in privacy threats and deep learning with differential privacy in Section I. In this section, we focus on the most relevant literature. The first proposal for deep learning with DP [24] has been deployed in google TensorFlow [30]. However, one known problem for deep learning with DP is the degradation of model accuracy compared to the non-DP trained model. Several recent efforts have been put forward for improving the accuracy of the approach proposed in [24]. The most relevant efforts to this paper include the recent zCDP proposal with dynamic privacy budget allocation [27] instead of uniformed privacy budget allocation in [24], and the adaptive clipping proposals represented by AdaClip [56] and Quantile Clipping [55]. The main contribution of Yu et al. [27] is the new privacy accounting method zCDP that can compute the privacy spending when the DP training is using an approximate differential privacy under CDP with parameter ρ to control dynamic privacy budget instead of ε privacy budget as in [24]. In addition, [27] also proposed a dynamic privacy budget allocation solution to improve [24] which uses fixed privacy vulnerabilities.
budget in every iteration of the DNN training, aiming to improving the accuracy of trained DNN model with DP. [27] did not consider gradient leakage attack and resilience, and also uses the fixed clipping as the approximation to sensitivity in the same way as [24]. AdaClip performs the clipping bound estimation based on the coordinates of the gradient norm and adaptively add different noise levels to different dimensions of the gradients. Quantile clipping is an alternative approach to AdaClip. It estimates the clipping bound during the training iterations using the quantile of the unclipped gradient norm instead of estimation of clipping bound based on the coordinates of the gradient norm in AdaClip. Both approaches are costly to compute dynamic clipping bounds since both needs to compute the clipping estimation on all M layers of a DNN for every example. Also both use the dynamic clipping bound to approximate the sensitivity while maintaining the fixed noise scale throughout the iterations of training to ensure that a sufficient amount of DP-noise is added according to the DP theory. Both are designed to improve accuracy of DNN training with DP but fail to be resilient against gradient leakages. In comparison, our approach is by design both gradient leakage resilient and improving model accuracy thanks to injecting dynamic controlled DP noise. Our dynamic DP parameter optimization approach DP-dyn[l2-max] incorporates dynamic sensitivity and dynamic noise scale to support decaying noise variance, such that as learning progresses in iterations, we inject less amount of DP controlled noises to the gradients instead of constant noise amount as done in [24]. As a result, our dynamic l2-max sensitivity provide a tighter DP controlled noise bound than the fixed Gaussian noise variance in used in conventional approaches.

VIII. CONCLUSIONS

We have presented a suite of algorithms with dynamic privacy parameters for gradient leakage resilient deep learning with differential privacy. We first analyze some limitations of existing algorithms using fixed-parameter strategies that inject constant differential privacy noise to all layers during each training iteration. We then presented a suite of DP algorithms with dynamic parameter optimizations, including dynamic sensitivity mechanisms, dynamic noise scale mechanisms, and different combinations of dynamic parameter strategies. Extensive experiments on six benchmark datasets demonstrate that the proposed differentially private deep learning with dynamic hybrid sensitivity and dynamic decaying noise scale can outperform existing state-of-the-art approaches and other dynamic parameter alternatives with competitive accuracy performance, strong differential privacy guarantee, high resilience against gradient privacy leakage.

Acknowledgement. The authors would like to first thank the associate editor Dr. Grigoris Loukides and the reviewers for their constructive and helpful comments. The authors acknowledge partial support by the National Science Foundation under Grants NSF 2038029, NSF 1564097, and an IBM faculty award.

References

[1] L. Zhu, Z. Liu, and S. Han, “Deep leakage from gradients,” in NeurIPS, 2019, pp. 14747–14756.
[2] B. Zhao, K. R. Mopuri, and H. Bilen, “idlg: Improved deep leakage from gradients,” arXiv preprint arXiv:2001.02610, 2020.
[3] Y. Aono, T. Hayashi, L. Wang, and S. Moriai, “Privacy-preserving deep learning via additively homomorphic encryption,” TIFS, vol. 13, no. 5, pp. 1333–1345, 2017.
[4] J. Geiping, H. Bauernheister, H. Dröge, and M. Moeller, “Inverting gradients - how easy is it to break privacy in federated learning?” in NeurIPS, 2020, pp. 16937–16947.
[5] W. Wei, L. Liu, M. Loper, K.-H. Chow, M. E. Gursoy, S. Truex, and Y. Wu, “A framework for evaluating client privacy leakages in federated learning," in ESORICS. Springer, 2020, pp. 545–566.
[6] J. Zhu and M. Blaschko, “R-gap: Recursive gradient attack on privacy,” arXiv preprint arXiv:2010.07733, 2020.
[7] H. Wang, J. Zhang, F. Xue, T. Wei, S. Ji, and Z. Zong, “Privacy leakage of real-world vertical federated learning,” arXiv preprint arXiv:2011.09290, 2020.
[8] Y. Liu, X. Zhu, J. Wang, and J. Xiao, “A quantitative metric for privacy leakage in federated learning,” in ICASSP. IEEE, 2021.
[9] H. Yin, A. Malliya, A. Vadhat, J. M. Alvarez, J. Kautz, and P. Molchanov, “See through gradients: Image batch recovery via gradinversion,” in CVPR. IEEE, 2021.
[10] J. Qian, H. Nassar, and L. K. Hansen, “Minimal conditions analysis of gradient-based reconstruction in federated learning,” arXiv preprint arXiv:2010.15718, 2020.
[11] M. Fredrikson, S. Jha, and T. Ristenpart, “Model inversion attacks that exploit confidence information and basic countermeasures,” in CCS. ACM, 2015, pp. 1322–1333.
[12] C. Song, T. Ristenpart, and V. Shmatikov, “Machine learning models that remember too much,” in CCS. ACM, 2017, pp. 587–601.
[13] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, “Exploiting unintended feature leakage in collaborative learning,” in S&P. IEEE, 2019, pp. 691–706.
[14] K. Ganju, Q. Wang, W. Yang, C. A. Gunter, and N. Borisov, “Property inference attacks on fully connected neural networks using permutation invariant representations,” in CCS. ACM, 2018, pp. 619–633.
[15] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, “Membership inference attacks against machine learning models,” in S&P. IEEE, 2017, pp. 3–18.
[16] M. Nasr, R. Shokri, and A. Houmansadr, “ Comprehensive privacy analysis of deep learning: Stand-alone and federated learning under passive and active white-box inference attacks,” in S&P. IEEE, 2019, pp. 739–753.
[17] B. Hui, Y. Yang, H. Yuan, P. Burlina, N. Z. Gong, and Y. Cao, “Practical blind membership inference attack via differential comparisons,” in NDSS, 2021.
[18] A. Salem, Y. Zhang, M. Humbert, P. Berrang, M. Fritz, and M. Backes, “MI-leaks: Model and data independent membership inference attacks and defenses on machine learning models,” in NDSS, 2018.
[19] L. Song and P. Mittal, “Systematic evaluation of privacy risks of machine learning models,” in USENIX Security, 2021.
[20] G. Liu, J. Zhao, R. Zhang, C. Wang, and L. Liu, “Gradient-leaks: Enabling black-box membership inference attacks against machine learning models,” TIFS, 2021.
[21] B. Hitaj, G. Ateniese, and F. Perez-Cruz, “Deep models under the gan: information leakage from collaborative deep learning,” in CCS. ACM, 2017, pp. 603–618.
[22] Z. Wang, M. Song, Z. Zhang, Y. Song, Q. Wang, and H. Qi, “Beyond inferring class representatives: User-level privacy leakage from federated learning,” in INFOCOM. IEEE, 2019, pp. 2512–2520.
[23] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy,” Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.
[24] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, “Deep learning with differential privacy,” in CCS. ACM, 2016, pp. 308–318.
[25] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, “Learning differentially private recurrent language models,” in ICLR, 2018.
[26] N. Papernot, S. Song, I. Mironov, A. Raghunanathan, K. Talwar, and U. Erlingsson, “Scalable private learning with pate,” in ICLR, 2018.
[27] L. Yu, L. Liu, C. Pu, M. E. Gursoy, and S. Truex, “Differentially private model publishing for deep learning,” in S&P. IEEE, 2019, pp. 332–349.
[28] K. Chaudhuri, C. Monteleoni, and A. D. Sarwate, “Differentially private empirical risk minimization,” JMLR, vol. 12, no. 3, 2011.
[29] R. C. Geyer, T. Klein, and M. Nabi, “Differentially private federated learning: A client level perspective,” arXiv preprint arXiv:1712.07557, 2017.

[30] “Tensorflow privacy module,” https://github.com/tensorflow/privacy/blob/master/tensorflow_privacy/privacy/keras_models/dp_keras_model.py (accessed Nov 2, 2020).

[31] “Pytorch privacy module,” https://github.com/pytorch/opacus/blob/master/opacus/privacy_engine.py, (accessed Nov 2, 2020).

[32] R. Bassily, A. Smith, and A. Thakurta, “Private empirical risk minimization: Efficient algorithms and tight error bounds,” in FCS. IEEE, 2014, pp. 464–473.

[33] N. Phan, X. Wu, H. Hu, and D. Dou, “Adaptive laplace mechanism: Differential privacy preservation in deep learning,” in ICDM. IEEE, 2017, pp. 385–394.

[34] Z. Xu, S. Shi, A. X. Liu, J. Zhao, and L. Chen, “An adaptive and fast convergent approach to differentially private deep learning,” in INFOCOM. IEEE, 2020, pp. 1867–1876.

[35] K. L. van der Veen, R. Seggers, P. Bloem, and G. Patrini, “Three tools for practical differential privacy,” arXiv preprint arXiv:1812.02890, 2018.

[36] L. Xiang, J. Yang, and B. Li, “Differentially-private deep learning from an optimization perspective,” in INFOCOM. IEEE, 2019, pp. 559–567.

[37] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, “Intriguing properties of neural networks,” arXiv preprint arXiv:1312.6199, 2013.

[38] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, “The limitations of deep learning in adversarial settings,” in EuroS&P. IEEE, 2016, pp. 372–387.

[39] N. Carlini and D. Wagner, “Towards evaluating the robustness of neural networks,” in S&P. IEEE, 2017, pp. 39–57.

[40] W. Wei and L. Liu, “Robust deep learning ensemble against deception,” TDSC, 2020.

[41] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in TCC. Springer, 2006, pp. 265–284.

[42] B. Balle, G. Barthe, and M. Gaboardi, “Privacy amplification by subsampling: Tight analyses via couplings and divergences,” in NeurIPS, 2018, pp. 6277–6287.

[43] C. Dwork, G. N. Rothblum, and S. Vadhan, “Boosting and differential privacy,” in FOCS. IEEE, 2010, pp. 51–60.

[44] P. Kairouz, S. Oh, and P. Viswanath, “The composition theorem for differential privacy,” in ICML, 2015, pp. 1376–1385.

[45] I. Mironov, “Rényi differential privacy,” in CSF. IEEE, 2017, pp. 263–275.

[46] Y.-X. Wang, B. Balle, and S. P. Kasiviswanathan, “Subsampled Rényi differential privacy and analytical moments accountant,” in AISTATS, 2019, pp. 1226–1235.

[47] “Moments accountant implementation,” https://github.com/tensorflow/privacy/blob/master/tensorflow_privacy/privacy/analysis/compute_dp_sgd_privacy.py (accessed Nov 2, 2020).

[48] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, “A hybrid approach to privacy-preserving federated learning,” in AISec, 2019, pp. 1–11.

[49] R. Pascanu, T. Mikolov, and Y. Bengio, “On the difficulty of training recurrent neural networks,” in ICML, 2013, pp. 1310–1318.

[50] M. Nasr, R. Shokri et al., “Improving deep learning with differential privacy using gradient encoding and denoising,” arXiv preprint arXiv:2007.11524, 2020.

[51] K. Nissim, S. Raskhodnikova, and A. Smith, “Smooth sensitivity and sampling in private data analysis,” in STOC. ACM, 2007, pp. 75–84.

[52] M. Bun and T. Steinke, “Average-case averages: Private algorithms for smooth sensitivity and mean estimation,” in NeurIPS, 2019, pp. 181–191.

[53] C. Darken and J. E. Moody, “Note on learning rate schedules for stochastic optimization,” in NeurIPS, 1990, pp. 832–838.

[54] L. N. Smith, “Cyclical learning rates for training neural networks,” in WACV. IEEE, 2017, pp. 464–472.

[55] O. Thakkar, G. Andrew, and H. B. McMahan, “Differentially private learning with adaptive clipping,” arXiv preprint arXiv:1905.03871, 2019.

[56] V. Pichapati, A. T. Suresh, F. X. Yu, S. J. Reddi, and S. Kumar, “Adaclip: Adaptive clipping for private sgd,” arXiv preprint arXiv:1908.07643, 2019.