OPTIMAL MEMBERSHIP INFERENCE BOUNDS FOR ADAPTIVE COMPOSITION OF SAMPLED GAUSSIAN MECHANISMS

Anonymous authors
Paper under double-blind review

ABSTRACT

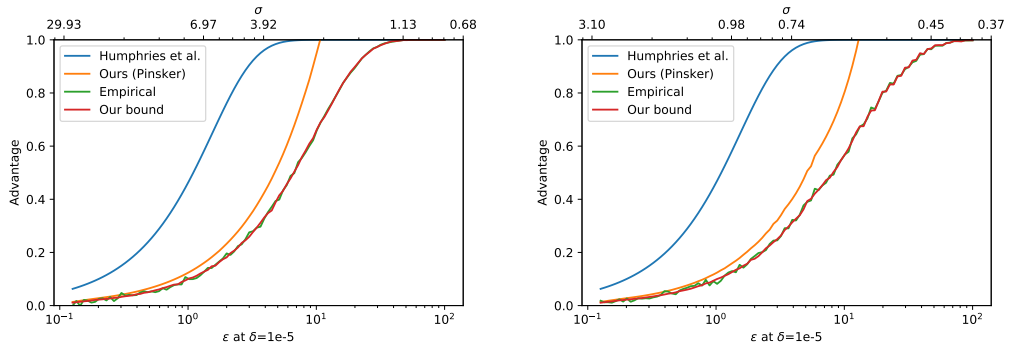
Given a trained model and a data sample, membership-inference (MI) attacks predict whether the sample was in the model's training set. A common countermeasure against MI attacks is to utilize differential privacy (DP) during model training to mask the presence of individual examples. While this use of DP is a principled approach to limit the efficacy of MI attacks, there is a gap between the bounds provided by DP and the empirical performance of MI attacks. In this paper, we derive bounds for the *advantage* of an adversary mounting a MI attack, and demonstrate tightness for the widely-used Gaussian mechanism. Our analysis answers an open problem in the field of differential privacy, namely the fact that membership inference is not 100% successful even for relatively high budgets ($\epsilon > 10$). Finally, using our analysis, we provide MI metrics for models trained on CIFAR10 dataset. To the best of our knowledge, our analysis provides the state-of-the-art membership inference bounds.

1 INTRODUCTION

The recent success of machine learning models makes them the go-to approach to solve a variety of problems, ranging from computer vision (Krizhevsky et al., 2012) to NLP (Sutskever et al., 2014), including applications to sensitive data such as health records or chatbots. Access to a trained machine learning model, be it a white-box published model or through a black-box API, can leak traces of information (Dwork et al., 2015) from the training data. Researchers have tried to measure this information leakage through metrics such as membership inference (Shokri et al., 2017). Membership inference is the task of guessing, from a trained model, whether it includes a given sample or not. This task is interesting in its own right, as the participation of an individual in a data collection can be sensitive information. Furthermore, it also serves as the "most significant bit" of information: if membership inference fails, attacks revealing more information such as reconstruction attacks (Fredrikson et al., 2014; Carlini et al., 2020) will also fail. In other words, defending against membership inference attacks also defends against more advanced attacks.

The standard approach to provably defeat these membership privacy attacks is differential privacy (Dwork et al., 2006). The traditional variant of differential privacy defines a class of algorithms that apply on a database D and respect a privacy budget ϵ and a probability of failure δ. These parameters control the divergence between the distribution of outcome of the algorithm when applied on two "neighboring" databases that only differ in one location. In particular, our mechanism of interest, the Sampled Gaussian Mechanism (SGM), makes an arbitrary function $f : X^* \to R^d$ differentially private by first sub-sampling a database of smaller size from the original database, using Poisson sampling, and then calculating f on the sub-sampled database, and finally adding Gaussian noise to the outcome. Increasing the amount of injected noise provides stronger privacy guarantees, and enables to trade off between privacy and utility of the trained model. To measure the privacy of a given algorithm, researchers have developed advanced mathematical tools and notions such as Renyi differential privacy (Mironov, 2017; Abadi et al., 2016) and advanced composition theorems (Dwork et al., 2010; Kairouz et al., 2015). These tools allow us to calculate (ϵ, δ) values for carefully designed algorithms.

Previous work has shown that any differentially private algorithm will provably bound the accuracy of any membership inference adversary. Specifically, Yeom et al. (2018), Humphries et al. (2020), and



(a) Without subsampling ($q = 1$)

(b) With subsampling ($q = 0.01$)

Figure 1: Comparison of advantage bounds in a Gaussian setup. We run the sampled Gaussian Mechanism in one dimension with 50 epochs, and either no subsampling (**left**) or subsampling with $q = 0.01$ (**right**). Our attack compares likelihood of the observations under both hypothesis, and chooses the most likely (see Appendix E.1 for details). We compute the empirical advantage by measuring the percentage of time p the adversary guesses membership correctly, and report $2p - 1$.

Thudi et al. (2022) prove that any model trained with (ϵ, δ) differential privacy will induce an upper bound on the accuracy of membership inference. These upper bounds help practitioners calibrate the privacy budget ϵ to defeat the adversary. As can be seen in Figure 1, there is a large gap between the best existing upper bound and the performance of empirical attacks. In this work, we use a new proof technique to bypass DP analysis and directly bound the advantage of MI attacks, and close the gap between theoretical guarantees and empirical performance.

The most widely-used DP algorithm in machine learning applications is DP-SGD: it is a small change of the classical stochastic gradient descent algorithm that only requires to clip per-sample gradients, average them and add Gaussian noise. Each iteration of DP-SGD is an instance of the sampled Gaussian mechanism, which chooses a fraction q of a dataset and outputs a noisy sum of the desired quantity. DP-SGD has been shown to be more accurate than other differentially private training algorithms in the case of linear and convex models (van der Maaten and Hannun, 2020). Our analysis mirrors the recent shift in the field of empirical membership inference, from advantage (or accuracy) metrics (Shokri et al., 2017; Yeom et al., 2018; Sablayrolles et al., 2019) to precision/recall measures (Watson et al., 2022; Carlini et al., 2020). Differential privacy guarantees are known to yield tight true positive and false positive rates (Nasr et al., 2021). Our paper is the first to show equivalent results in the case of advantage. Our analysis explains, from a theoretical point of view, why the precision and recall of membership inference attacks is stronger than the accuracy.

Our contributions in this work are as follows:

- Our main theorem in Section 4 bounds the membership inference advantage of any adversary for the composition of an arbitrary set of sampled Gaussian mechanisms that could adaptively depend on each other. This bound is optimal as it reflects the membership inference advantage for a real adversary on a particular series of Gaussian mechanisms.
- We propose a numerical way to calculate the total variation distance between mixtures of Gaussians (Section 4.3). Our algorithm is computationally tractable, works in linear time with respect to the number of mechanisms and is independent from the dimension. We use our numerical approach to obtain concrete bounds for Gaussian mechanisms and compare our bounds to that of Humphries et al. (2020).
- Finally, to understand the practical implication of our bound for mainstream datasets, we use DP-SGD to train models on CIFAR10 and MNIST and calculate the membership inference bounds using our techniques. Our approach allows us to achieve state-of-the-art provable membership inference privacy for any given accuracy.

2 BACKGROUND

In this section, we briefly recall the main properties of KL divergence and total variation (TV), as well as differential privacy and membership inference.

2.1 TOTAL VARIATION, KL DIVERGENCE, AND PINSKER INEQUALITY

We consider a random variable X (resp. Y) with probability distribution μ (resp. ν) over a measurable space Ω. With a slight abuse of notation, we consider quantities as function of either the random variables X, Y or their probability distributions μ, ν. Here we recall the definition of total variation (TV) distance and Kullback-Leibler (KL) divergence:

$$\mathbf{TV}(X, Y) = \sup_{\mathcal{A}} \Pr[X \in \mathcal{A}] - \Pr[Y \in \mathcal{A}], \qquad \mathrm{KL}(X \parallel Y) = \int_{\Omega} \log\left(\frac{d\mu}{d\nu}\right) d\mu. \tag{1}$$

Post-processing. Given a function $g : E \to F$, applying g to X and Y can only decrease $\mathbf{TV}$,

$$\mathbf{TV}(g(X), g(Y)) \leq \mathbf{TV}(X, Y).$$

In particular, if g is a bijective transform, we have $\mathbf{TV}(g(X), g(Y)) = \mathbf{TV}(X, Y)$.

Pinsker's Inequality. For any two random variables X and Y, Pinsker (1964)'s inequality states

$$\mathbf{TV}(X, Y) \leq \sqrt{\frac{\mathrm{KL}(X \parallel Y)}{2}}. \tag{2}$$

2.2 DIFFERENTIAL PRIVACY AND THE GAUSSIAN MECHANISM

Differential privacy. A randomized algorithm $\mathcal{M}$ satisfies (ϵ, δ)-differential privacy if, for any two datasets D and D' that differ in at most one sample, and any subset R of the output space, we have:

$$\Pr(\mathcal{M}(D) \in R) \leq \exp(\epsilon) \Pr(\mathcal{M}(D') \in R) + \delta. \tag{3}$$

While the probability of failure δ is often chosen to be inversely proportional to the number of samples, there is no consensus in the literature over desirable values of ϵ.

DP-SGD with the subsampled Gaussian mechanism. DP-SGD (Abadi et al., 2016) is a modification of Stochastic Gradient Descent that makes it differentially private. The core mechanism behind it is the subsampled Gaussian mechanism. Given a function ϕ that operates on sets S with sensitivity 1 (i.e. $\|\phi(S) - \phi(S')\|_2 \leq 1$), the subsampled Gaussian mechanism selects sets S at random and adds noise to the output of ϕ. Note that the mechanism is differentially private *even* if all intermediate steps of the training process are revealed.

2.3 MEMBERSHIP INFERENCE ATTACKS

Membership Inference is the task of predicting whether a given sample was in the training set of a given model. Homer et al. (2008) showed the first proof of concept, and Shokri et al. (2017) showed that a wide variety of machine learning models are vulnerable to such attacks. Shokri et al. (2017) train neural networks to attack machine learning models, and measure the success of the attack by the percentage of correctly predicted (train/test) samples, or equivalently the advantage (Yeom et al., 2018). Later work showed that simple heuristics such as the loss (Yeom et al., 2018; Sablayrolles et al., 2019; Choquette-Choo et al., 2021) provide a more accurate and robust measure of membership inference. Membership inference attacks have also been used as an evaluation mechanism for differentially private mechanisms (Jayaraman et al., 2020; Jayaraman and Evans, 2019).

Recent works (Watson et al., 2022; Carlini et al., 2021; Rezaei and Liu, 2021) have proposed to evaluate membership inference by the precision/recall trade-off (Watson et al., 2022) or the precision at low levels of recall (Carlini et al., 2021). In particular, such works show that some setups which were thought to be private because the membership accuracy is significantly less than 100% can actually reveal membership of a small group of samples with very high precision. There is also a

line of work developed to design algorithms to specifically defend against membership inference attacks (Nasr et al., 2018; Jia et al., 2019; Tang et al., 2021). While these works offer no theoretical guarantees against attackers, the empirical defenses achieve better utility at the same membership advantage than their differentially private equivalents. Finally, membership inference has been studied in the context of differential identifiability Bernau et al. (2021); Lee and Clifton (2012) (see Appendix E.1 for Gaussian experiments that correspond to differential identifiability techniques).

3 MEMBERSHIP INFERENCE AND TOTAL VARIATION

In this section, we define our security game for membership inference and show its connection to the notion of total variation distance (or statistical distance) between probability distributions.

3.1 SECURITY GAME

We adopt the classical assumptions of membership inference (Yeom et al., 2018; Sablayrolles et al., 2019; Humphries et al., 2020). In particular, we assume that the datasets differ by adding/removing one element. We define a security game between an Adversary (who wants to guess training set membership) and a Challenger (who wants to hide training set membership).

1. Adversary picks a datasets $D = \{z_1, \ldots, z_n\}$ and a data point z'
2. Challenger samples a bit b uniformly at random and creates

$$D' = \begin{cases} D \cup \{z'\} & \text{if } b = 1 \\ D & \text{if } b = 0 \end{cases}$$

3. Challenger runs the learning algorithm L on D' to train a model and sends a transcript of training θ to the adversary [1]
4. Adversary observes θ and guesses a bit b'. Adversary wins if $b' = b$.

We define the advantage of adversary A on learning algorithm L as $\mathbf{Adv}(L, A) = 2 \cdot \Pr[b = b'] - 1$. We also use $\mathbf{Adv}(L) = \sup_A \mathbf{Adv}(A, L)$ to denote the advantage of any adversary against L.

Remark 1 (Comparing with security game of Yeom et al. (2018))**.** *The security game of Yeom et al. (2018) for membership inference attacks (See Appendix G) is slightly weaker than ours. This means that the upper bounds we prove in this work also apply to the security game of Yeom et al. (2018). A curious reader might question if our security game is too strong; the worst-case advantage of adversary might be lower in the security game of Yeom et al. (2018). In Appendix G we answer this question negatively. Through experiments, we show that we cannot prove better upper bounds in the alternative security game of Yeom et al. (2018), even if we assume the adversary does not control the neighboring datasets and only sees the final model (and not the intermediate steps). This shows that our bounds in Section 4 are tight even in the weaker security games.*

Remark 2 (Non-uniform prior)**.** *One can define a similar security game where the selection of the bit b is non-uniform. This security game captures settings that the adversary has some prior knowledge about the inclusion of the example in the training set. This setting was studied in Thudi et al. (2022), they provide some upper bounds for the advantage of adversary in such a security game. In Appendix I, we show that we can extend our analysis to this setting and provide optimal bounds.*

Comparison to existing bounds. In the reminder of the paper we bound the membership inference advantage for DP-SGD. We first recall the best existing upper bound that is proved and improved in prior work (Jayaraman et al., 2020; Jayaraman and Evans, 2019; Humphries et al., 2020; Yeom et al., 2018; Thudi et al., 2022).

Theorem 3 (Humphries et al. (2020))**.** *For any (ϵ, δ)-DP algorithm L we have $\mathbf{Adv}(L) \leq \frac{e^\epsilon - 1 + 2\delta}{e^\epsilon + 1}$.*

Note that Theorem 3 applies to any DP algorithm and hence covers DP-SGD as well. Because of its generality, the bound is loose for DP-SGD (see Figure 4(a)). To improve on this bound, we perform a direct analysis of the advantage instead of using the DP tools and then converting to advantage.

[1] The transcript can only include the final model or more information like the intermediate steps of training.

Advantage. Let us first mathematically characterize the notion of advantage for a general learning algorithm. For a fixed learning algorithm L and fixed neighboring datasets, let us define $X := \theta \mid (b = 0)$ and $Y := \theta \mid (b = 1)$ to be the distributions of the output of the learning algorithm for two cases of the security game. A deterministic adversary A defines a region $\mathcal{A}$ and predicts that θ is sampled from μ if $\theta \in \mathcal{A}$ and from ν if $\theta \notin \mathcal{A}$. We use $\mu(\mathcal{A})$ and $\nu(\mathcal{A})$ to denote $\Pr[X \in \mathcal{A}]$ and $\Pr[Y \in \mathcal{A}]$. For such an adversary we have

$$\mathbf{Adv}(L, A) = \Pr[X \in \mathcal{A}] - \Pr[Y \in \mathcal{A}] = \mu(\mathcal{A}) - \nu(\mathcal{A}).$$

Note that with a simple averaging argument we can show that the best adversarial strategy in membership security game is a deterministic strategy. Therefore, the advantage for the learning algorithm L is then defined as

$$\mathbf{Adv}(L) = \sup_{\mathcal{A}} \mu(\mathcal{A}) - \nu(\mathcal{A}) = \mathbf{TV}(X, Y), \tag{4}$$

where $\mathbf{TV}$ is the total variation distance. Total variation distance thus gives us an upper bound on the advantage of any adversary. Since we do not know the exact density function for X and Y it is not clear how to calculate or approximate the total variation distance in general. In the next subsection we discuss how Pinsker's inequality upper bounds total variation distance.

3.2 Bounding membership inference using Pinsker's inequality

Using Equation (4) and directly applying Pinsker's inequality (2), we have:

$$\mathbf{Adv}(L) \leq \mathbf{TV}(X, Y) \leq \sqrt{\frac{\mathrm{KL}(X \parallel Y)}{2}} = \lim_{\alpha \to 1} \sqrt{\frac{D_\alpha(X \parallel Y)}{2}} \tag{5}$$

where D_α is the Rényi divergence at α. This bound enables us to use Rényi divergence, which is routinely calculated in DP-SGD (Mironov, 2017) to obtain numerical upper bounds on the membership inference advantage of any adversary against adaptive composition of sampled Gaussian mechanisms.

To this end, we use RDP accounting to calculate the D_α for an $\alpha > 1$. We know that for any $\alpha > 1$, $D_\alpha(X, Y)$ is greater than $\mathrm{KL}(X \parallel Y)$ because D_α is increasing in α. This means that for any $\alpha > 1$ D_α will be a valid upper bound on the membership inference advantage and the bound becomes better as we decrease α.

In our evaluation (see Figures 4(a) and 6) we use this formulation to calculate numerical upper bounds for membership inference for DP-SGD using typical parameters. We refer to this bound as the Pinsker bound. The figure shows that it obtains better numerical values compared to the bound of Humphries et al. (2020). However, there are two main limitations with Pinsker's bound: 1) The bound is not tight. 2) It is vacuous in cases where $\mathrm{KL}(X \parallel Y) > 2$. In next section, we will optimally bound the membership inference for composition of adaptive and sampled Gaussian mechanisms.

4 Optimal bounds for composition of sampled Gaussian mechanisms

In this section, we show a tighter upper-bound for the adversary's advantage. In particular, we will upper-bound the total variation between the *transcripts* of the (subsampled) Gaussian mechanism, specifically the noisy gradients produced by the DP-SGD algorithm (Theorem 6 and Theorem 18).

As the first step of calculating our optimal bounds, we show that the adaptivity of Gaussian mechanisms does not increase the membership advantage. In other words, the entire process of DP-SGD can be replaced by a process where each step is replaced by either $\mathcal{N}(0, \sigma^2)$ or $\mathcal{N}(r, \sigma^2)$ for the basic Gaussian mechanism, and replaced by either $\mathcal{N}(0, \sigma^2)$ or $(1 - q)\mathcal{N}(0, \sigma^2) + q\mathcal{N}(r, \sigma^2)$ for the sampled Gaussian mechanism, without decreasing the total variation distance. Our analysis relies on a modified version of $\mathbf{TV}$, that we denote by $\mathbf{TV}_a$.

Definition 4. *For $a > 0$ define $\mathbf{TV}_a(X, Y) = \frac{1}{2} \int_\Omega |\mu(x) - a \cdot \nu(x)| dx$ where μ and ν are the probability density functions for X and Y respectively.*

While we do not know an explicit form of the $\mathbf{TV}_a$ divergence between Gaussians, we can still prove that it increases with $\|u_1 - u_2\|_2$, as formalized in the following lemma.

Lemma 5. *Let $X \equiv \mathcal{N}(u_1, \sigma^2 \cdot I_d)$ and $Y \equiv \mathcal{N}(u_2, \sigma^2 \cdot I_d)$. Then, for any $a \in \mathbb{R}^+$, $\mathbf{TV}_a(X, Y)$ is only a function of $\|u_1 - u_2\|_2$ and σ^2. Moreover this function is monotonically increasing with respect to $\|u_1 - u_2\|_2$. That is,*

$$\mathbf{TV}_a(X, Y) \leq \mathbf{TV}_a(\mathcal{N}(0, \sigma^2), \mathcal{N}(\|u_1 - u_2\|_2, \sigma^2)).$$

The proof involves some careful gradient calculations and is deferred to Appendix A.

4.1 Warm up: Without sampling

We first focus on the case of adaptive Gaussian mechanisms without sub-sampling. But before that we state several useful notations.

Notation. We use $\theta = (s_1, \ldots, s_T)$ to denote the transcript of the learning algorithm L that consists of T adaptive steps. We use $s_{\leq t}$ to denote the first t steps of the transcript of the random process. We use S_i to denote the union of the support set of the ith step of the mechanism M on all possible datasets. That is $S_i = \{s_i; \exists D, s_i \in \mathsf{Supp}(M(D)_i)\}$. We also define $S_{\leq i} = S_1 \times \ldots, S_i$.

Theorem 6 (Gaussian Composition without sub-sampling)**.** *Let $M_1, \ldots, M_T$ be a series of adaptive Gaussian Mechanisms with L_2 sensitivity r and Gaussian noise with standard deviation σ. The membership inference risk of the composition of M_i's is bounded by*

$$\mathbf{TV}(X, Y) \leq \mathbf{TV}(\mathcal{N}(0, \sigma^2 I_T), \mathcal{N}(r1_T, \sigma^2 I_T)) \tag{6}$$

Proof. Let $M^i(D)$ be the mechanism that works on D (resp. D') and consists of i Gaussians $\mathcal{N}(0, \sigma^2)$ (resp. $\mathcal{N}(r, \sigma^2)$) steps followed by $T - i$ steps of SGM applied to D (resp. D').

Specifically, the mechanism M^0 corresponds to SGM, and M^T to pure Gaussians. We will show in this proof that

$$\mathbf{TV}(M^i(D), M^i(D')) \leq \mathbf{TV}(M^{i+1}(D), M^{i+1}(D')) \tag{7}$$

and hence

$$\mathbf{TV}(X, Y) = \mathbf{TV}(M^0(D), M^0(D')) \leq \mathbf{TV}(M^T(D), M^T(D')) = \mathbf{TV}(\mathcal{N}(0, \sigma^2 I_T), \mathcal{N}(r1_T, \sigma^2 I_T).$$

To this end, we will first argue that the very final step of the mechanism M^i can be replaced with a Gaussian step without increasing the total variation distance. Then we can move this noise to the start of the process without affecting the result, obtaining M^{i+1}. Figure 2 illustrates this procedure.

Let us fix a step i and let $s = (s_1, \ldots, s_T)$ be a transcript. Denoting $X \sim M^i(D)$ and $Y \sim M^i(D')$, we have

$$\begin{aligned}
2\mathbf{TV}(M^i(D), M^i(D')) &= \sum_{s_{\leq T} \in S_{\leq T}} |\Pr[X = s_{\leq T}] - \Pr[Y = s_{\leq T}]| \\
&= \sum_{s_{\leq T-1} \in S_{\leq T-1}} \sum_{s_T \in S_T} |\Pr[X = s_{\leq T}] - \Pr[Y = s_{\leq T}]| \\
&= \sum_{s_{\leq T-1} \in S_{\leq T-1}} \sum_{s_T \in S_T} |\Pr[X_T = s_T \mid s_{\leq T-1}] \cdot \Pr[X_{\leq T-1} = s_{\leq T-1}] \\
&\qquad - \Pr[Y_T = s_T \mid s_{\leq T-1}] \Pr[Y_{\leq T-1} = s_{\leq T-1}]| \,. \\
&= \sum_{s_{\leq T-1} \in S_{\leq T-1}} \Pr[X_{\leq T-1} = s_{\leq T-1}] \sum_{s_T \in S_T} \Bigg| \Pr[X_T = s_T \mid s_{\leq T-1}] \\
&\qquad - \Pr[Y_T = s_T \mid s_{\leq T-1}] \frac{\Pr[Y_{\leq T-1} = s_{\leq T-1}]}{\Pr[X_{\leq T-1} = s_{\leq T-1}]} \Bigg| .
\end{aligned} \tag{8}$$

We know that the last (T'th) step of $M^i(D)$ (resp. $M^i(D')$) has two isotropic Gaussian distributions centered around two points u_1 and u_2 such that $\|u_1 - u_2\|_2 \leq r$ and with standard deviation σ. These centers could be chosen adaptively according to the history of the mechanism. We use $a(s_{\leq T-1})$ to denote $\frac{\Pr[Y_{\leq T-1} = s_{\leq T-1}]}{\Pr[X_{\leq T-1} = s_{\leq T-1}]}$. By Lemma 5 we have

$$\sum_{s_T \in S_T} \Big| \Pr[X_T = s_T \mid s_{\leq T-1}] - \Pr[Y_T = s_T \mid s_{\leq T-1}] a(s_{\leq T-1}) \Big|$$

$$\leq 2\mathbf{TV}_{a(s_{\leq T-1})}(\mathcal{N}(0,\sigma^2),\mathcal{N}(r,\sigma^2)).$$

Denoting by N^i the mechanism that coincides with M^i for the first $T-1$ steps and is replaced by a Gaussian at the last (T'th) step, we thus have, by following Equation (8) in the reverse direction

$$2\mathbf{TV}(M^i(D), M^i(D')) \leq 2\mathbf{TV}(N^i(D), N^i(D')). \tag{9}$$

Given that the last step of N^i does not depend on the first $T-1$ steps, we can permute to put it in first position (see Figure 2), which shows that $\mathbf{TV}(N^i(D), N^i(D')) = \mathbf{TV}(M^{i+1}(D), M^{i+1}(D'))$. □

4.2 WITH SAMPLING

Notation. We use $B(q)$ to denote a Bernoulli random variable that is equal to 1 with probability q and 0 with probability $1-q$. We use $B(q)^n$ to denote an n dimensional random variable where each coordinate is independent and distributed as $B(q)$. For $r \in \mathbb{R}$, we use $r \cdot B(q)^n$ to denote the random variable that is sampled by the following process: first sample from $B(q)^n$ and then multiply by r. We also use $\mathcal{N}(r \cdot B(q)^n, \sigma^2)$ to denote an n dimensional random variable that is distributed according to a mixture of Gaussians which all have standard deviation σ and centers are chosen at random from $r \cdot B(q)^n$.

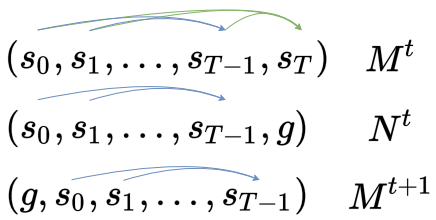


Figure 2: Main component of the proof of Theorem 6. The last step of SGM is replaced by Gaussian noise (independent of previous steps). This step is then put at the start of the transcript.

Theorem 7 (Gaussian Composition with sub-sampling)**.** *Let $M_1, \ldots, M_T$ be a series of adaptive Gaussian Mechanisms with L_2 sensitivity r and Gaussian noise with standard deviation σ and sub-sampling rate q. The membership inference risk of the composition of M_i's is at most*

$$\mathbf{TV}\big(\mathcal{N}(0^T,\sigma^2), \mathcal{N}(r \cdot B(q)^T, \sigma^2)\big)$$

Proof sketch. We defer the full proof of Theorem 18 to the Appendix D. However, we provide a high level idea behind the proof based on the proof of Theorem 18. The first step is to characterize the $\mathbf{TV}_a$ for sub-sampled mechanisms and relate it to the $\mathbf{TV}_a$ for the case without sub-sampling.

Lemma 8. *Let $X' \equiv (1-q) \cdot Y + q \cdot X$. Then we have*

$$\mathbf{TV}_a(X', Y) = q\mathbf{TV}_{\frac{a+q-1}{q}}(X, Y)$$

The proof of this lemma is provided in Appendix D. Now we use Lemma 8 to convert $\mathbf{TV}_a$ of the sub-sampled Gaussians to $\mathbf{TV}_a$ of Gaussians and use Lemma 5 to upper bound them with $\mathbf{TV}_a$ of independent Gaussians. Then we use Lemma 8 again to convert the independent Gaussians to independent sub-sampled Gaussians. □

Optimality of our bound We note that the bound of Theorem 18 is optimal. This is because the bound is equal to the advantage of an adversary defined on sequence of independent Gaussian mechanisms. In Appendix G we empirically show this tightness. We also note that the optimality of our bounds only hold for the notion of addition/removal in neighnoring dataset. For the notion of advantage defined based on replacement, if we double the bounds, only the bound without sampling remains tight. We leave the question of obtaining tight bounds on the advantage based on replacement for the sub-sampled Gaussian as an open question.

Varying noise levels Theorem 6 could be simply extended to composition of Gaussian mechanisms with varying noise levels, assuming the noise levels are not selected adaptively. We leave the composition of Gaussians with adaptive noise selection as an open question.

Extending to other monotonous mechanisms Although Theorem 6 is stated only for Gaussian mechanism, the theorem extends to any mechanism that satisfies monotonicity under $\mathbf{TV}_a$ according to some notion of sensitivity. For example, if one can show that $\mathbf{TV}_a(\mathcal{L}(0,\sigma), \mathcal{L}(u,\sigma))$ is monotonically increasing with respect to some norm of u, then Theorem 6 extends to composition of Laplace mechanisms with bounded sensitivity according to that norm.

4.3 MONTE CARLO COMPUTATION

In order to numerically approximate the upper-bound, we write the total variation as

$$\mathbf{TV}(X,Y) = \int_{\Omega} (d\mu(t) - d\nu(t))\, \mathbb{1}\left(d\nu(t) \leq d\mu(t)\right) \tag{10}$$

$$= \int_{\Omega} \left(1 - \frac{d\nu(t)}{d\mu(t)}\right) \mathbb{1}\left(d\nu(t) \leq d\mu(t)\right) d\mu(t) \tag{11}$$

$$= \mathbb{E}_{t\sim\mu}\left(\left(1 - \frac{d\nu(t)}{d\mu(t)}\right) \mathbb{1}\left(d\nu(t) \leq d\mu(t)\right)\right). \tag{12}$$

The expectation is over the distribution μ, so we can sample a dataset from μ and approximate this expectation using empirical averaging (or Monte-Carlo sampling):

$$\mathbf{TV}(X,Y) \approx \frac{1}{m}\sum_{i=1}^{m}\left(1 - \frac{d\nu(t_i)}{d\mu(t_i)}\right) \mathbb{1}\left(d\nu(t_i) \leq d\mu(t_i)\right), \tag{13}$$

where $t_i \sim_{\text{i.i.d.}} \mu$. The Monte-Carlo estimation of this quantity is very accurate, as it is bounded between 0 and 1. Figures 4(a) and 6 show the upper bound using this Monte-Carlo simulation for typical settings in DP-SGD. We also provide a detailed algorithm on how we this in Appendix C. Following we provide a proposition on the accuracy of our Monte Carlo approximation which directly follows by Applying Chernoff-Hoefding bound.

Proposition 9. *Our Monte Carlo simulation (Algorithm 1 in Appendix C) returns a value η that with high probability is close to the optimal membership inference bound η^* of Theorem 6, namely* $\Pr[|\eta - \eta^*| \geq \delta] \leq e^{-m\cdot\delta^2/3}$.

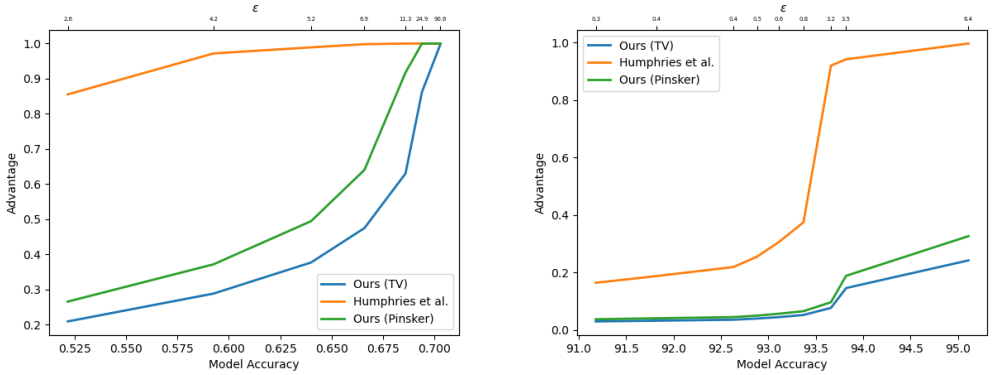
5 EVALUATION

In this section we perform experiments to calculate the concrete trade-off between accuracy and membership inference on mainstream datasets. For our experiments, we use DP-SGD (Algorithm 2) to train models and use Algorithm 1 to calculate the corresponding membership inference bounds.

Experiments on the MNIST and CIFAR datasets. We use the MNIST (LeCun) and CIFAR (Krizhevsky et al., 2009) datasets to perform experiments with DP-SGD. Figures 3(a) and 3(b) shows the result of our experiments. For MNIST, we used 3-layer convolutional neural networks (CNN) and train it for 10 epochs with sampling rate $q = 0.001$ and learning rate $.1$ using the cross-entropy loss function. We also choose the gradient clipping threshold to be 1.0 and change the noise scale between $[0.5, 1.5]$. For the CIFAR-10 experiments, we use 5-layer CNNs and trained them for 50 epochs with sampling rate 0.02 and learning rate 0.5 using the cross-entropy loss. We set the gradient clipping threshold to 10.0 and the noise scale changed between $[0.5, 2]$. Our experiments show that differentially private training using DP-SGD can obtain a significantly better trade-off between accuracy and membership inference advantage than was previously thought. For instance, on the MNIST dataset we obtain membership inference bounds that are close to 0.01 while maintaining accuracy at around 93%.

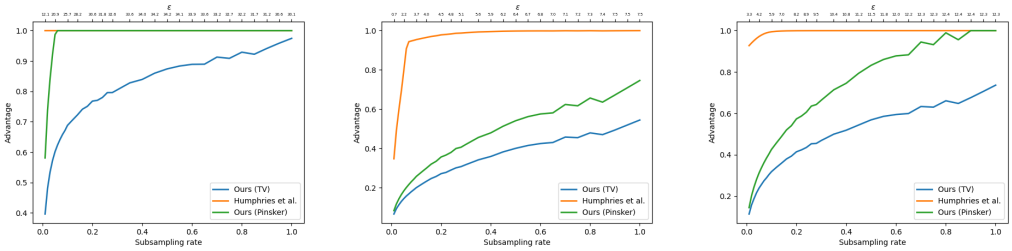
Study of the role of noise scale and sampling rate. To understand the role of sub-sampling on membership inference advantage we perform experiments with varying sub-sampling rates. In Figure 5 we show the results of our experiments where we change the sampling rate between $[0, 1]$ at three different values of noise scale. Our experiments are done for 5 epochs of training. Note that although the number of epochs are fixed, the number of iterations are different for different sampling rates. One interesting observation is that our optimal bound is less dependent on very small sampling rate. For instance at noise scale $\sigma = 0.5$, both the Pinsker and Humphries et al. (2020) bounds become vacuous abruptly as the sampling rate grows but our optimal membership inference bound remains meaningful. Another interesting phenomenon is the oscillations that happens at certain locations for the optimal and Pinsker bounds. These oscillations happen independently for both the Pinsker and optimal bound. As these two bounds are calculated using completely different techniques, we believe this phenomenon is not due to numerical issues.

Monte Carlo error for the experiments. In our experiments for optimal membership bounds we use Monte Carlo simulation (see Section 4.3 and in Algorithm 1), with $m = 5e5$ samples. Via Proposition 9, we guarantee that with probability at least 99.999% that the bound has error less than 0.01.



(a) Membership Inference v.s. Accuracy on CIFAR10. (b) Membership inference v.s. Accuracy on MNIST.

Figure 3: Empirical results on membership advantage



(a) $\sigma = 0.5$ (b) $\sigma = 1.0$ (c) $\sigma = 1.5$

Figure 4: Effect of sub-sampling rate at various noise scales with 5 epochs.

6 Conclusion

In this paper, we directly analyzed membership inference bounds for adaptive composition of sampled Gaussian mechanisms. Our analysis enables us to obtain bounds that are better than bounds from prior analyses of differential privacy. Our analysis shows that although differential privacy guarantees might sometimes lead to large/vacuous membership inference guarantees, the mechanisms that obtain differential privacy can be in fact much more secure against membership inference attacks. Previously, this phenomenon was observed for DP-SGD and here, for the first time, we prove it.

Our analysis is the first to directly analyze membership inference bounds. We limited our study to membership inference attacks against sampled Gaussian mechanisms as DP-SGD, the most widely used differentially private learning algorithm. Direct study of membership inference could be potentially done for other mechanisms and algorithms as well. We leave this for future work.

We also note that the hyper-parameters for DP-SGD that achieve optimal membership privacy versus utility might be different than that of differential privacy. Our new analysis opens up the possibility of a systematic search for the hyper-parameters and architectures (using recent advancements in privacy-preserving hyperparameter tuning and architecture search (Papernot et al., 2020; Papernot and Steinke, 2021; Chaudhuri and Vinterbo, 2013)) that obtain optimal utility for a given upper bound on membership inference.

Last, while our paper closes the gap between theoretical and empirical measures of an adversary's advantage, the bounds apply to the subsampled Gaussian mechanism. We leave the tightness of advantage measure on other mechanisms for future work.

REFERENCES

Martin Abadi, Andy Chu, Ian Goodfellow, Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *CCS*, 2016.

Daniel Bernau, Günther Eibl, Philip W Grassal, Hannah Keller, and Florian Kerschbaum. Quantifying identifiability to choose and audit ϵ in differentially private deep learning. *arXiv preprint arXiv:2103.02913*, 2021.

Nicholas Carlini, Florian Tramer, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Ulfar Erlingsson, et al. Extracting training data from large language models. *arXiv preprint arXiv:2012.07805*, 2020.

Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramer. Membership inference attacks from first principles. *arXiv preprint arXiv:2112.03570*, 2021.

Kamalika Chaudhuri and Staal A Vinterbo. A stability-based validation procedure for differentially private machine learning. *Advances in Neural Information Processing Systems*, 26, 2013.

Christopher A Choquette-Choo, Florian Tramer, Nicholas Carlini, and Nicolas Papernot. Label-only membership inference attacks. In *International Conference on Machine Learning*, pages 1964–1974. PMLR, 2021.

Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

Cynthia Dwork, Guy N Rothblum, and Salil Vadhan. Boosting and differential privacy. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 51–60. IEEE, 2010.

Cynthia Dwork, Adam Smith, Thomas Steinke, Jonathan Ullman, and Salil Vadhan. Robust traceability from trace amounts. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 650–669. IEEE, 2015.

Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In *23rd USENIX Security Symposium*, pages 17–32, 2014.

Nils Homer, Szabolcs Szelinger, Margot Redman, David Duggan, Waibhav Tembe, Jill Muehling, John V Pearson, Dietrich A Stephan, Stanley F Nelson, and David W Craig. Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. *PLoS genetics*, 4(8):e1000167, 2008.

Thomas Humphries, Matthew Rafuse, Lindsey Tulloch, Simon Oya, Ian Goldberg, Urs Hengartner, and Florian Kerschbaum. Differentially private learning does not bound membership inference. *arXiv preprint arXiv:2010.12112*, 2020.

Bargav Jayaraman and David Evans. Evaluating differentially private machine learning in practice. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1895–1912, 2019.

Bargav Jayaraman, Lingxiao Wang, David Evans, and Quanquan Gu. Revisiting membership inference under realistic assumptions. *arXiv:2005.10881*, 2020.

Jinyuan Jia, Ahmed Salem, Michael Backes, Yang Zhang, and Neil Zhenqiang Gong. Memguard: Defending against black-box membership inference attacks via adversarial examples. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 259–274, 2019.

Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The composition theorem for differential privacy. In *International conference on machine learning*, pages 1376–1385. PMLR, 2015.

Alex Krizhevsky, Geoffrey Hinton, et al. Learning multiple layers of features from tiny images. 2009.

Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, 25, 2012.

Yann LeCun. The mnist database of handwritten digits. *http://yann. lecun. com/exdb/mnist/*.

Jaewoo Lee and Chris Clifton. Differential identifiability. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1041–1049, 2012.

Ilya Mironov. Rényi differential privacy. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 263–275. IEEE, 2017.

Milad Nasr, Reza Shokri, and Amir Houmansadr. Machine learning with membership privacy using adversarial regularization. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 634–646, 2018.

Milad Nasr, Shuang Songi, Abhradeep Thakurta, Nicolas Papemoti, and Nicholas Carlin. Adversary instantiation: Lower bounds for differentially private machine learning. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 866–882. IEEE, 2021.

Opacus. Opacus PyTorch library. Available from opacus.ai.

Nicolas Papernot and Thomas Steinke. Hyperparameter tuning with renyi differential privacy. *arXiv preprint arXiv:2110.03620*, 2021.

Nicolas Papernot, Abhradeep Thakurta, Shuang Song, Steve Chien, and Ulfar Erlingsson. Tempered sigmoid activations for deep learning with differential privacy. *arXiv preprint arXiv:2007.14191*, page 10, 2020.

Mark S Pinsker. *Information and information stability of random variables and processes*. Holden-Day, 1964.

Shahbaz Rezaei and Xin Liu. On the difficulty of membership inference attacks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 7892–7900, 2021.

Alexandre Sablayrolles, Matthijs Douze, Cordelia Schmid, Yann Ollivier, and Hervé Jégou. White-box vs black-box: Bayes optimal strategies for membership inference. In *International Conference on Machine Learning*, pages 5558–5567. PMLR, 2019.

Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 3–18. IEEE, 2017.

Ilya Sutskever, Oriol Vinyals, and Quoc V Le. Sequence to sequence learning with neural networks. *Advances in neural information processing systems*, 27, 2014.

Xinyu Tang, Saeed Mahloujifar, Liwei Song, Virat Shejwalkar, Milad Nasr, Amir Houmansadr, and Prateek Mittal. Mitigating membership inference attacks by self-distillation through a novel ensemble architecture. *arXiv preprint arXiv:2110.08324*, 2021.

Anvith Thudi, Ilia Shumailov, Franziska Boenisch, and Nicolas Papernot. Bounding membership inference. *arXiv preprint arXiv:2202.12232*, 2022.

Laurens van der Maaten and Awni Hannun. The trade-offs of private prediction. *arXiv preprint arXiv:2007.05089*, 2020.

Lauren Watson, Chuan Guo, Graham Cormode, and Alexandre Sablayrolles. On the importance of difficulty calibration in membership inference attacks. In *International Conference on Learning Representations*, 2022.

Samuel Yeom, Irene Giacomelli, Matt Fredrikson, and Somesh Jha. Privacy risk in machine learning: Analyzing the connection to overfitting. In *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, pages 268–282. IEEE, 2018.