Privately Estimating Monotone Statistics in Polynomial Time

Gavin Brown
University of Wisconsin–Madison
gavin.brown@wisc.edu

Ephraim Linder
Boston University
ejlinder@bu.edu

Mahbod Majid
MIT Mathematics
mahbod@mit.edu

Vikrant Singhal
University of Copenhagen
vikrant.singhal@di.ku.dk

Abstract

We study efficient differentially private algorithms for estimating monotone statistics, i.e., statistics that are monotone under the addition of new observations. The starting point for our investigation is *subsample-and-aggregate*: a classical paradigm that partitions the dataset into blocks, estimates the statistic on each block, and then privately aggregates the estimates. While practical and generically applicable, this approach is quite data-hungry. We improve upon this framework for the class of monotone statistics—compared to subsample-and-aggregate, our algorithms save a factor of t in sample complexity and pay a factor of e^t in running time, where $t > 0$ is a tunable parameter. We complement our results with a query-complexity lower bound, showing that our algorithms are essentially optimal for this task. As an application, we obtain improved results for private eigenvalue estimation, private loss estimation, and privately estimating a single parameter of a high-dimensional model, e.g., in linear regression.

1 Introduction

In this work, we consider the task of generically producing differentially private (DP) [DMNS06] algorithms from non-private estimators. The literature on differentially private statistics supplies a toolkit for a variety of fundamental tasks such as mean estimation, linear regression, and principal component analysis. For all of these tasks and more, the literature provides efficient algorithms that achieve near-optimal accuracy. These algorithms, however, require a bespoke design and considerable care in their analysis. Even the general-purpose statistical tools built on the inverse sensitivity mechanism seem to require considerable technical effort in their application [AD20, HKMN23, AUZ23]. Building on prior work with the same goal, we develop differentially private algorithms that treat the base estimator as a black box.

Specifically, we start with any function f that takes in a dataset and returns a (univariate) quantity. As a motivating example, consider estimating the first parameter of a larger regression problem. We seek to produce differentially private algorithms that, given a dataset Z and query access[1] to f, return an output with accuracy comparable to the non-private estimator. Since f is an arbitrary function, the measure of accuracy is context dependent. To begin our informal discussion, we suppose there is a benchmark number of samples N under which we expect an "adequate" non-private estimator.

[1]The algorithm can specify a query in the form of a dataset X and receives response $f(X)$. The *query complexity* of an algorithm is the maximum number of queries it makes when given query access to any function f.

40th Conference on Neural Information Processing Systems (NeurIPS 2026).

For example, for least squares in d dimensions we require $N \approx d$ for non-trivial estimation. We will evaluate the private estimator in terms of the number of samples n it needs in order to compete with the non-private estimator on N samples.

One classic approach to this problem is *subsample-and-aggregate* (S&A) [NRS07]. Algorithms in this framework proceed as follows: split the data into τ disjoint buckets $B_1, \ldots, B_\tau$, and use a private aggregation method to release an approximation to some center (such as the average or median) of the $f(B_i)$'s. This approach is computationally efficient, as we make τ queries to f, but suffers a blowup in sample complexity—in order for any one $f(B_i)$ to be meaningful, we must have $|B_i| \gtrsim N$. Many standard settings require $\tau \gtrsim \frac{1}{\varepsilon} \log \frac{1}{\delta}$ buckets, and thus the private sample complexity is at least $N \cdot \frac{\log 1/\delta}{\varepsilon}$, a multiplicative factor larger than the non-private counterpart.

Recent work of [LRSS25] shows that one can do considerably better: They construct an (ε, δ)-differentially private mechanism requiring only $n \approx N + \frac{1}{\varepsilon} \log \frac{1}{\delta}$ samples—that is, an additive overhead in sample complexity. Unfortunately, their mechanism requires exponential time—it makes $n^{\Theta\left(\frac{1}{\varepsilon} \log \frac{1}{\delta}\right)}$ queries to f. Shortly thereafter, [SS25] demonstrated a tradeoff between sample complexity and query complexity: compared to subsample-and-aggregate, one can save a factor of t in sample complexity at the cost of a blowup of $e^{O(t)}$ in query complexity[2]. However, despite making fewer queries to f, the mechanism of [SS25] nevertheless has runtime $n^{O\left(\frac{1}{\varepsilon} \log \frac{1}{\delta}\right)}$.

In this work, we provide an efficient algorithm that improves on the sample complexity of subsample-and-aggregate for the class of *monotone* functions, i.e., functions whose output does not decrease when a new observation is added to the input. In the context of privacy, monotone functions were first studied by [FDY22] who design an algorithm to privately evaluate a monotone function f with finite range κ. In the language above, their algorithm outputs an accurate estimate with probability at least $1 - \beta$ and achieves sample complexity $n \approx N + \frac{1}{\varepsilon} \log \frac{\kappa}{\beta}$ and runtime $n^{\Theta\left(\frac{1}{\varepsilon} \log \frac{\kappa}{\beta}\right)}$. Moreover, the tools they develop for the monotone function setting play a key role in the development of algorithms for general (i.e., non-monotonic) functions in [LRSS25, SS25]. We revisit the setting of monotone functions with an eye towards computational efficiency. In particular, we show that for all $t \leq \frac{\log 1/\delta}{2\varepsilon}$ one can achieve sample complexity $\frac{N}{t} \cdot \frac{\log 1/\delta}{\varepsilon}$ while only incurring a blowup of $e^{O(t)}$ in *both* query complexity and runtime. In Table 1, we highlight several settings of t that demonstrate our improvement over the aforementioned baselines.

Table 1: Comparison of our approach for monotone functions with black-box (ε, δ)-DP estimators. Here $k_{\varepsilon,\delta} := \frac{1}{\varepsilon} \log \frac{1}{\delta}$ and N denotes the non-private sample benchmark. We suppress absolute constants and assume that evaluating the underlying function takes unit time, and we compare with [FDY22, SS25] in the text.

Approach	**Setting**	**Samples** n	**Time**
S&A [NRS07]	-	$N \cdot k_{\varepsilon,\delta}$	$k_{\varepsilon,\delta}$
[LRSS25]	-	$N + k_{\varepsilon,\delta}$	$n^{k_{\varepsilon,\delta}}$
This work (monotone functions)	any $t \leq k_{\varepsilon,\delta}$	$N \cdot \frac{k_{\varepsilon,\delta}}{t}$	$e^t \cdot \mathrm{poly}(k_{\varepsilon,\delta})$
	$t = k_{\varepsilon,\delta}$	$N + k_{\varepsilon,\delta}$	$(1/\delta)^{1/\varepsilon} \cdot \mathrm{poly}(k_{\varepsilon,\delta})$
	$t = \log(k_{\varepsilon,\delta})$	$N \cdot \frac{k_{\varepsilon,\delta}}{\log(k_{\varepsilon,\delta})}$	$\mathrm{poly}(k_{\varepsilon,\delta})$

Organization We next informally present our main results: new algorithms for monotone functions, a lower bound on query complexity, and applications to learning problems. We then discuss additional related work. In Section 2.2, we present and analyzes our median-of-quantiles mechanism, which illustrates our central algorithmic advancements. The rest of our contributions, including the average-of-quantiles mechanism—our sister mechanism of median-of-quantiles, which obtains a different flavor of guarantee—are deferred to the appendix.

[2]The main result of [SS25] provides a general tradeoff in terms of the size of a certain combinatorial object, which, upon close inspection, yields the bound $e^{O(t)}$ (ignoring log factors). For further discussion see Appendix F.2

1.1 Our results

We consider functions and distributions that satisfy the following assumption, which allows us to meaningfully compare our results to S&A, and briefly defer our more general results.

Assumption 1.1. *For function f and distribution $\mathcal{D}$ there exist $N : \mathbb{R} \to \mathbb{R}$ and $\nu \in \mathbb{R}$ such that for all $n \geq N(\alpha) + \frac{\log 1/\beta}{\alpha^2}$, we have*

$$\Pr_{Z \sim \mathcal{D}^n}\left[\left|\frac{f(Z)}{n} - \nu\right| \geq \alpha\right] \leq \beta,$$

where $\mathcal{D}^n$ denotes the distribution over n i.i.d. samples from $\mathcal{D}$.

As an example, if $f(Z) = \sum z_i$ and $\mathcal{D}$ is subgaussian, then we can take $\nu = \mathbb{E}_{z \sim \mathcal{D}}[z]$. While the exact dependence on lower order terms varies depending on the private aggregation method used, for functions f and distributions $\mathcal{D}$ that satisfy Assumption 1.1, S&A requires at least

$$n = \Omega\left(\frac{N(\alpha)\log 1/\delta}{\varepsilon}\right)$$

samples to estimate ν up error α. We note that if the function has finite range $[\kappa]$ for some $\kappa \in \mathbb{N}$, then $1/\delta$ can be replaced with κ/β. Our results focus on improving the dependence on the privacy parameters in this leading term of the sample complexity bound.

1.1.1 Privately evaluating monotone statistics

Our general results apply to functions that do not decrease when new data is added to input. While our main results provide accuracy guarantees in terms of the value of f on random subsets of the input dataset, we now state a simplified version that applies to functions that satisfy Assumption 1.1. We assume a computational model where queries to f take unit time. For a function f, a dataset Z, and an algorithm $\mathcal{A}$, we let $\mathcal{A}^f$ denote algorithm $\mathcal{A}$ with query access to f, and we let random variable $\mathcal{A}^f(Z)$ denote the output of algorithm $\mathcal{A}^f$ on input Z.

In this setting, our algorithm *average-of-quantiles* gives the following guarantees.

Theorem 1.2 (Informal Corollary of Theorem 2.4)**.** *Fix privacy parameters $\varepsilon, \delta > 0$ and $t \leq \frac{1}{\varepsilon}\log\frac{1}{\delta}$. There exists a mechanism $\mathcal{M}$ such that for all monotone, real-valued functions f mechanism $\mathcal{M}^f$ is (ε, δ)-DP and has query complexity and runtime $e^{O(t)}\operatorname{poly}\left(\frac{\log 1/\delta}{\varepsilon}\right)$. Additionally, if f and $\mathcal{D}$ satisfy Assumption 1.1, then for all $\alpha, \beta > 0$ and*

$$n = \Omega\left(\frac{N(\alpha)\log 1/\delta}{t\varepsilon} + \frac{\log 1/\delta \log 1/\beta}{t\alpha^2\varepsilon} + \frac{\log 1/\delta}{\alpha^2\varepsilon}\right)$$

we have

$$\Pr_{Z \sim \mathcal{D}^n}\left[\left|\mathcal{M}^f(Z, \alpha) - \nu\right| \geq \alpha\right] \leq \beta.$$

Average-of-quantiles requires some prior information about the concentration of the non-private estimator (in the above setting, it requires knowledge of α). We analyze a second algorithm, *median-of-quantiles*, which does not use such information but requires functions that have a bounded range. We state its slightly different guarantees in Theorem 2.3.

We also prove a query complexity lower bound, which implies that our results are essentially tight for privately estimating black-box monotone statistics. The version we state below applies to functions with unbounded range, however the full version (Theorem E.2) also applies to the setting where f has finite range, and it shows that our results are essentially tight for that setting as well. In fact, our lower bound holds for mechanisms that satisfy a much weaker accuracy guarantee: informally, if for all $n \geq N$, we have $f(Z) = \nu$ with probability 1 when $Z \sim \mathcal{D}^n$, then the mechanism should output $y \approx \nu$ with probability at least $2/3$ when given $n = \Omega\left(\frac{N\log 1/\delta}{t\varepsilon}\right)$ samples from $\mathcal{D}$. We define this weaker guarantee more formally in Appendix E, and present an informal version of the lower bound below.

Theorem 1.3 (Informal Corollary of Theorem E.2)**.** *Fix $\varepsilon, \delta \in (0,1)$ and $t \le \frac{1}{\varepsilon}\log\frac{1}{\delta}$. Suppose $\mathcal{M}^f$ is (ε,δ)-DP for all monotone functions f. Additionally, suppose that for all monotone f and distributions $\mathcal{D}$ that are "eventually constant", mechanism $\mathcal{M}$ has the following accuracy guarantee:*

$$\text{If } n = \Omega\left(\frac{N(1)\log 1/\delta}{t\varepsilon}\right) \text{ then } \Pr_{Z\sim\mathcal{D}^n}\left[\mathcal{M}^f(Z) \approx \nu\right] \ge \frac{2}{3}.$$

Then $\mathcal{M}$ has query complexity $e^{\Omega(t)}$.

1.1.2 Application to eigenvalue estimation

We apply our tools towards the problem of privately estimating the ith eigenvalue $\lambda_i(\Sigma)$ of the covariance Σ of a subgaussian distribution $\mathcal{D}$. Our mechanism witnesses a tradeoff between sample and time complexity in line with Theorem 1.2, providing a multiplicative approximation to λ_i.

Theorem 1.4 (Informal version of Theorem C.1)**.** *Fix $\varepsilon, \delta, \beta, \alpha \in (0,1)$ and $t \le \frac{1}{\varepsilon}\log\frac{1}{\delta}$. There exists an (ε,δ)-DP mechanism $\mathcal{M}$ that gets as input $Z \sim \mathcal{D}^n$ and for each $i \in [d]$ satisfies the following guarantee: if $\mathcal{D}$ is subgaussian and*

$$n = \Omega\left(\frac{d\log 1/\delta}{\alpha^2 t\varepsilon} + \frac{\log 1/\delta \log 1/\beta}{\alpha^2 t\varepsilon} + \frac{\log 1/\delta}{\alpha^2\varepsilon}\right)$$

then

$$\Pr_{Z\sim\mathcal{D}^n}\left[1-\alpha \le \frac{\mathcal{M}(Z,i)}{\lambda_i(\Sigma)} \le 1+\alpha\right] \ge 1-\beta.$$

Moreover, $\mathcal{M}$ has runs in time $e^{O(t)}\operatorname{poly}(n,d)$.

1.1.3 Applications around linear regression

Taking as inspiration the work of [ADT25], we consider the problem of privately estimating a single parameter in a larger parametric task. As a highlight, in the introduction, we will focus on the setting of linear regression in d dimensions with least squares loss. In Appendix D, we discuss applications to more general M-estimation tasks.

Our results apply to estimating a single coordinate of the population minimizer. This problem arises naturally in scientific analyses when attempting to infer the effect of some variable x_1 on an outcome y, while controlling for $d-1$ additional variables $x_2, \dots, x_d$.

In the following theorem, we assume the data $Z = ((x_1,y_1),\dots,(x_n,y_n))$ satisfy $y_i = x_i^\top\theta + e_i$ for some $\theta \in \mathbb{R}^d$, noise $e_i \sim \mathcal{N}(0,\sigma^2)$ and $x_i \sim \mathcal{N}(0,\Sigma)$. Let $\mathcal{D}$ denote this distribution over (x_i,y_i). Our first result gives a private mechanism for testing if θ_1 is positive or negative.

Theorem 1.5 (Informal Corollary of Theorem D.7)**.** *Fix $\varepsilon, \delta \in (0,1)$, and $t \le \frac{1}{\varepsilon}\log\frac{1}{\delta}$. There exists an (ε,δ)-DP mechanism $\mathcal{M}$ that gets as input $Z \sim \mathcal{D}^n$, runs in time $e^{O(t)}\operatorname{poly}(n,d)$, and for all $\alpha > 0$ and*

$$n = \Omega\left(\frac{d\log 1/\delta}{t\varepsilon} + \operatorname{poly}\left(\frac{1}{\alpha\varepsilon}\log\frac{n}{\delta}\right)\right),$$

satisfies the following guarantees:

- *If $|\theta_1| > 2\alpha\sqrt{\Sigma_{11}^{-1}}$ then $\mathcal{M}(Z)$ outputs $\operatorname{sign}(\theta_1)$ with probability at least $1-\delta$.*
- *If $|\theta_1| < \alpha\sqrt{\Sigma_{11}^{-1}}$ then $\mathcal{M}(Z)$ outputs 0 with probability at least $1-\delta$.*

Our second result states that we can obtain a similar tradeoff for the problem of estimating θ_1. For simplicity, we state our result in the regime where α and σ^2 are constant.

Theorem 1.6 (Informal Corollary of Theorem D.8)**.** *Assume $\theta_1 \in [\pm 1]$. Fix $\varepsilon, \delta, \beta \in (0,1)$, and $t \le \frac{1}{\varepsilon}\log\frac{1}{\beta}$. There exists an (ε,δ)-DP mechanism $\mathcal{M}$ that gets as input $Z \sim \mathcal{D}^n$, runs in time $e^{O(t)}\operatorname{poly}(n,d)$, and if*

$$n = \Omega\left(\frac{d\log 1/\beta}{t\varepsilon} + \operatorname{poly}\left(\frac{1}{\varepsilon}\log\frac{n}{\beta}\log\log\frac{1}{\delta}\right)\right),$$

outputs an estimate $\widehat{\theta}_1$ *such that* $\left|\widehat{\theta}_1 - \theta_1\right| \leq 0.01\left(1 + \sqrt{\Sigma_{11}^{-1}}\right)$ *with probability at least* $1 - \beta$.

In addition to our application to estimating a single parameter, we obtain similar results for estimating σ^2, and more generally, for estimating the population loss of a class of hypotheses.

1.2 Our techniques

Subsampling quantiles for privately evaluating monotone functions. In order to privately evaluate a monotone function f at a dataset Z, we develop a novel analysis of the distribution of $f(S)$ where $S \sim \mathcal{S}_p(Z)$ is the distribution given by subsampling each $z_i \in Z$ with probability p. In a slight abuse of notation, we let $f(\mathcal{S}_p(Z))$ denote the distribution of $f(S)$ where $S \sim \mathcal{S}_p(Z)$, and let $Q_Z(\alpha)$ denote the α quantile of the distribution $f(\mathcal{S}_p(Z))$. Our privacy analysis shows that, on adjacent datasets Z and Z', the subsampling quantiles Q_Z and $Q_{Z'}$ are *interleaved* in the following sense:

$$Q_Z(\alpha(1-p)) \leq Q_{Z'}(\alpha) \leq Q_Z\left(\frac{\alpha}{1-p}\right).$$

As in [FDY22, LRSS25], the interleaving relationship allows us to transform the problem of evaluating f into the problem of releasing an interior point from a sequence of increasing quantiles of $f(\mathcal{S}_p(Z))$. While [FDY22, LRSS25] construct two interleaved sequences by performing a brute force search over all "large" subsets of the dataset, our approach can be implemented efficiently via subsampling. Crucially, we show that one can efficiently compute an appropriate sequence of empirical quantiles via subsampling, and that with high probability over the subsampling, the empirical quantiles that are computed on neighbors Z and Z' will satisfy the interleaving relationship. Since each subsample has size approximately pn, this approach gives an approximation to the value of f on subsets S with $|S| \approx pn$. The bottleneck in the running time of our algorithms is the number of subsamples required to accurately estimate very small quantiles, which we show is approximately $\exp\left(O\left(\frac{p}{\varepsilon}\log\frac{1}{\delta}\right)\right)$. Notice that smaller p translates into a faster runtime but a worse accuracy guarantee—the estimation is on smaller subsets. Thus, our mechanism witnesses a tradeoff between sample complexity and runtime for privately estimating monotone statistics.

Estimating a single parameter via private loss comparison. Our algorithm for estimating the ith coordinate of a high dimensional model works by privately computing estimates of the empirical loss of the minimizer when the ith coordinate is fixed to different candidates $w \in \mathcal{C}$ for some set of candidates $\mathcal{C} \subseteq \mathbb{R}$, and outputting the candidate w that achieves the smallest empirical loss. We leverage the tools we develop for privately evaluating monotone functions to estimate the loss for each candidate. In order to argue that our mechanism is accurate, we analyze the distribution of the minimum empirical loss on subsampled data. Specifically, we show that for a typical dataset the empirical loss of subsampled data concentrates around its mean at a dimension independent rate. The fast rate of concentration under subsampling allows us to argue that the private loss comparisons are accurate without paying a dimension dependent accuracy term (e.g., d/α^2) in the sample complexity.

Query complexity lower bound. We build on the approaches of [LRSS25, SS25] and prove a query complexity lower bound for privately estimating monotone statistics. We combine the central ideas behind the constructions of [LRSS25, SS25] with a technique from [LLRV25] used to prove a lower bound in the context of property testing. At a high level, the proof of our lower bound proceeds as follows: we construct two families distributions $\{\mathcal{D}_0\}$ and $\{\mathcal{D}_1\}$ and a family of monotone functions $\{f\}$, such that for each f, there is a corresponding $\mathcal{D}_0$ and $\mathcal{D}_1$ such that for all $n \geq N$, the following holds with probability 1: If $Z' \sim \mathcal{D}_0^N$ then $f(Z') = y_0$, and if $Z \sim \mathcal{D}_1^N$ then $f(Z) = y_1$, where y_0 and y_1 are chosen uniformly from $[\kappa]$. Thus, any algorithm that satisfies a weak accuracy guarantee should output y_0 when the data comes from $\mathcal{D}_0$, and y_1 when the data comes from $\mathcal{D}_1$. We then construct a distribution over pairs of datasets (X, X') at distance $\tau \approx \frac{1}{\varepsilon}\log\min\left(\frac{\kappa}{\beta}, \frac{1}{\delta}\right)$, and show that any algorithm, which has sample complexity $n = N/p$ and query complexity less than $e^{p\tau}$, cannot distinguish Z from X or Z' from X'. Thus, if an algorithm outputs y_1 on input Z and y_0 on input Z', it will also output y_1 on input X and y_0 on input X'. However, since X and X' are at distance τ, this contradicts group privacy, and we obtain that any private and accurate mechanism must make at least $e^{p\tau}$ queries.

1.3 Related work

Local sensitivity and subsample-and-aggregate. The *local sensitivity* of a function f at a dataset Z is the maximum over all X in some neighborhood around Z of $|f(X) - f(Z)|$. In order to privately evaluate a function with error proportional to the local sensitivity, [NRS07] develop a smoothed version of local sensitivity, called *smooth sensitivity*, and introduce subsample-and-aggregate as a framework for constructing estimators with bounded smooth-sensitivity. Given the generality of subsample-and-aggregate it is no surprise that is has found application in many statistical estimation tasks: see [Smi11, KSGB23, CDK24, SS21, Tsf24] for examples and further discussion.

Privately evaluating black-box functions. A long line of work explicitly considers the problem of privately evaluating a black-box function f. The *inverse sensitivity mechanism* is the most prominent example: it adds noise proportional to the local sensitivity of the function. [AD20] introduced the study of its instance optimality; see [McS09, CPS+12] for early applications. In black-box settings, the mechanism apparently requires a brute-force search over the space of all possible datasets (and thus it is not clear how to even compute it when data domain is infinite). Work of [JR13, LLRV25] study the connections between privately release of black-box functions and sublinear-time algorithms. A related line of work [CD20, FDY22, KL23, LRSS25, SS25] focuses on *down-local* algorithms—that is, algorithms that only query f on subsets of the dataset. These algorithms are computable even when the data domain is infinite.

We refer the reader to [LRSS25, SS25] for a more extensive discussion of the benefits of down-local algorithms, and we note that all of our algorithms satisfy this constraint. While the algorithms in this line of work suffer minimal blowup in sample complexity for the setting of Assumption 1.1, they are unfortunately all inefficient—they run in time at least $n^{\Omega(\log n)}$ in general. Additionally, an important building block in both [LRSS25] and [SS25], who focus on privately evaluating arbitrary functions, is a technique developed in [FDY22] for privately evaluating monotone functions. Cast in this light, we hope our results will lead toward the development of efficient algorithms for arbitrary functions.

Single-parameter release for GLMs. A central motivation of our work aligns with the recent work of [ADT25], who provide algorithms for privately estimating a single parameter from a larger model. Operating on a large subset of generalized linear models (GLMs), they show how to privately certify the stability of the empirical estimate and, when that certification passes, adds Gaussian noise at a scale they show is instance-optimal. However, it appears that their techniques only show that this certification succeeds with high probability once the sample size is quite large; larger than the number of samples needed for adequate non-private estimation.

Privacy and Robustness. A recurring theme in differentially private algorithm design is to use robust estimation as a starting point. Early work such as propose–test–release [DL09] formalized how to privatize estimators that are stable on typical datasets by first privately certifying a sensitivity bound and then releasing a suitably noised estimate. Most recently, multiple results give general-purpose blueprints for converting robust (or stable) algorithms into private ones [LKO22, KMV22, HKM22, HKMN23, AUZ23].

Going in this direction, efficient algorithms for estimating mean and covariance in the presence of arbitrary outliers have been used to obtain sample-optimal private algorithms for estimating a Gaussian distribution in total variation distance [HKMN23]. More broadly, these results and other reductions between robustness and privacy [AUZ23] suggest that privacy and robustness can often be viewed as complementary stability guarantees, and that robust estimators can serve as useful primitives for obtaining private ones.

1.4 Notation

In the interest of space, we defer the rest of the preliminaries to Appendix A, but for clarity define our notation here.

Let $\mathcal{Z}$ denote the set of all data points (or data universe). A dataset $Z \in \mathcal{Z}^n$ is a tuple of n elements where $z_i \in \mathcal{Z}$ for each $i \in [n]$. Let $\mathcal{Z}^* = \bigcup_{n\in\mathbb{N}} \mathcal{Z}^n$. We say two datasets Z and Z' are *neighbors* if there exists exactly one $i \in [n]$ such that $z_i \neq z'_i$. Our results leverage subsampling from a dataset Z, which we define as follows: Let $\mathcal{Z}_\perp = \mathcal{Z} \cup \{\perp\}$ and let $\mathcal{Z}_\perp^* = \bigcup_{n\in\mathbb{N}} \mathcal{Z}_\perp^n$. Suppose $Z \in \mathcal{Z}_\perp^n$,

then a subsample $S \subseteq Z$ is a tuple of n elements $(s_1, \ldots, s_n)$ such that $z_i = \perp \implies s_i = \perp$, and $s_i \in \{z_i, \perp\}$ otherwise. We let $|S| = |\{i \in [n] \mid s_i \neq \perp\}|$, and for all $z \in \mathcal{Z}_\perp$ we let $S^{j \leftarrow z}$ denote S with $s_j \leftarrow z$ and we let S_{-j} denote $S^{j \leftarrow \perp}$.

With this notation, we can now formally define our notion of monotonicity.[3]

Definition 1.7 (Monotone functions)**.** *A function $f : \mathcal{Z}_\perp^* \to \mathbb{R}$ is* monotone *if $f(S) \leq f(Z)$ for all $Z \in \mathcal{Z}_\perp^*$ and $S \subseteq Z$.*

2 Framework for privately evaluating monotone functions

In this section, we develop our main tools for privately approximating monotone functions. We first present and analyze Algorithm 1, our "quantile finder." This algorithm is not itself differentially private but provides a strong interleaving guarantee when run on monotone functions, as discussed in the introduction. We then show how to use the output of this algorithm to produce an approximate median (in Section 2.2) or approximate mean (in Section 2.3).

2.1 Subsampling quantiles

Recall that we write $\mathcal{S}_p(Z)$ to denote the distribution over $S \subseteq Z$ given by $s_i \leftarrow z_i$ with probability p and $s_i \leftarrow \perp$ with probability $1 - p$. For any function f over $\mathcal{Z}_\perp^n$ let $f(\mathcal{S}_p(Z))$ denote the distribution given by sampling $S \sim \mathcal{S}_p(Z)$ and evaluating $f(S)$. For a distribution $\mathcal{D}$ over a totally ordered domain, let $Q_{\mathcal{D}}(v) = \inf_\ell \{\ell \mid \Pr_{y \sim \mathcal{D}}[y \leq \ell] \geq v\}$ be the v-quantile of $\mathcal{D}$.

Lemma 2.1 (Quantile-finder)**.** *Fix $p \in (0, 1/4)$, $\delta \in (0, 1)$, and $\tau \in \mathbb{N}$ and let $T = O\big(e^{4p\tau} p^{-2} \log \frac{1}{\delta}\big)$. There exists an algorithm $\mathcal{A}$ that gets query access to a monotone function f on $\mathcal{Z}_\perp^n$, and on input Z, samples $S_1, \ldots, S_T \sim \mathcal{S}_p(Z)$ and outputs a list $q(1), \ldots, q(\tau)$ such that*

- ***Accuracy:*** $\min_{t \in [T]} f(S_t) \leq q(1) \leq q(2) \leq \ldots \leq q(\tau) \leq \max_{t \in [T]} f(S_t)$.
- ***Interleaving:*** *Fix a neighbor Z' of Z, and let q and q' denote the output of $\mathcal{A}$ on input Z and Z' respectively. Then with probability at least $1 - \delta$ for all $t \in [\tau - 2]$ we have*
$$q'(t) \leq q(t+1) \leq q'(t+2).$$

Moreover $\mathcal{A}$ has query complexity and runtime $O(T)$.

Proof. Let $c > 0$ be sufficiently large and let γ be a parameter to be determined later.

Algorithm 1 quantile-finder $\mathcal{A}^f(Z)$

Input: Dataset $Z \in \mathcal{Z}^n$, query access to monotone f, and parameters p, τ and δ.
Output: Empirical quantiles $(q(1), \ldots, q(\tau))$ of $f(\mathcal{S}_p(Z))$.

1: Set $\eta \leftarrow \left(\frac{1-p}{1+\gamma}\right)^\tau$, and $m \leftarrow \frac{c \log(1/\delta)}{(\eta\gamma(1-\gamma^2)(1-p))^2}$.
2: Draw m samples from $f(\mathcal{S}_p(Z))$ and let $\widehat{\mathcal{D}}$ denote the resulting empirical distribution.
3: For each $t \in [\tau]$ compute
$$q(t) = Q_{\widehat{\mathcal{D}}}\left(\left(\frac{1+\gamma}{1-p}\right)^t \eta\right).$$
4: Return $q(1), \ldots, q(\tau)$.

Let Z and Z' be neighboring datasets, and let q and q' denote the output of $\mathcal{A}$ on input Z and Z' respectively.

Claim 2.2 (Quantile interleaving)**.** *For all $t \in [\tau - 2]$ we have*
$$q'(t) \leq q(t+1) \leq q'(t+2)$$
with probability at least $1 - \delta$.

[3] We remark that the literature supplies several distinct notions with the name "monotonicity." The definition we consider here is, in particular, distinct from the notion of *sample-monotone functions* used in [AD20].

We defer the proof of Claim 2.2 to Appendix B and complete the proof of Lemma 2.1 below.

The first guarantee of the lemma follows by inspection of the algorithm, and the second guarantee follows from Claim 2.2. The query complexity and runtime of $\mathcal{A}$ are easily seen to be $O(m)$, where m is the number of subsamples drawn by $\mathcal{A}$. Note that if $\gamma = p/2$ and $p \leq 1/4$, then $\frac{1+\gamma}{1-p} \leq 1 + 2p$ and thus $m = O\big(e^{4p\tau} p^{-2} \log \frac{1}{\delta}\big)$. □

2.2 Median-of-quantiles

In this section, we use Lemma 2.1 to construct a mechanism for privately evaluating a monotone function $f : \mathcal{Z}_\perp^n \to [\kappa]$. We use the exponential mechanism to release the median of the quantiles returned by the algorithm of Lemma 2.1. Accuracy follows immediately, but privacy requires a new argument that relies on the interleaving property.

Theorem 2.3 (Median-of-quantiles)**.** *Fix $\varepsilon, \delta, \beta \in (0,1)$ and $p \in (0, 1/4)$. There exists an (ε, δ)-DP mechanism $\mathcal{M}$ that for all monotone functions $f : \mathcal{Z}_\perp^n \to [\kappa]$ and datasets Z runs in time at most $T = \exp\Big(O\Big(\frac{p \log \kappa/\beta}{\varepsilon}\Big)\Big) p^{-2} \log \frac{1}{\delta}$, samples $S_1, \ldots, S_T \sim \mathcal{S}_p(Z)$, and with probability at least $1 - \beta$ satisfies*

$$\min f(S_i) \leq \mathcal{M}^f(Z) \leq \max f(S_i).$$

Proof. We construct the median-of-quantiles mechanism below (Algorithm 2). The mechanism first uses the quantile-finder algorithm given by Lemma 2.1, and subsequently outputs an approximate median of the resulting quantiles using the exponential mechanism.

Algorithm 2 median-of-quantiles mechanism $\mathcal{M}^f(Z)$

Input: Dataset $Z \in \mathcal{Z}^n$, query access to monotone f, and parameters $\varepsilon, \delta, \beta, p$.
Output: $y \in [\kappa]$.

1: Set $\tau \leftarrow \frac{4}{\varepsilon} \log \frac{\kappa}{\beta}$ and let $\bar{q} = (q(1), \ldots, q(\tau)) \leftarrow \mathcal{A}^f(Z)$.
▷ $\mathcal{A}$ is the mechanism given by Lemma 2.1 with parameters τ, p and δ.
2: For each $y \in [\kappa]$ let $\mathsf{score}(y; Z) = |\mathsf{rank}(y : \bar{q}) - \tau/2|$.
3: Release $y \in [\kappa]$ via the exponential-mechanism with score as the score.

First, we argue that Algorithm 2 is (ε, δ)-DP. Let EM denote the exponential mechanism as in Algorithm 2, which receives a vector of quantiles and returns some $y \in [\kappa]$. When we have two vectors of quantiles $\bar{q} = (q(1), \ldots, q(\tau))$ and $\bar{q}' = (q'(1), \ldots, q'(\tau))$ that are interleaved—that is, $q'(i) \leq q(i+1) \leq q'(i+2)$ for all $i \in [\tau - 2]$, the random variables $EM(\bar{q})$ and $EM(\bar{q}')$ are ε-indistinguishable. To see this, observe that for any $y \in [\kappa]$ we must have $|\mathsf{score}(y; Z) - \mathsf{score}(y; Z')| \leq 1$, and so the standard privacy argument for the exponential mechanism applies. By Lemma 2.1, the quantiles $\bar{q}$ and $\bar{q}'$ are interleaved with probability at least $1 - \delta$, and thus by Fact A.8 mechanism $\mathcal{M}$ is (ε, δ)-DP.

To see why accuracy holds, observe that by the accuracy guarantee of the exponential mechanism we have $\mathcal{M}^f(Z) \in [q(\tau/4), q(3\tau/4)]$ with probability at least $1 - \beta$, which, by the guarantee of Lemma 2.1 is contained in $[\min_i f(S_i), \max_i f(S_i)]$. Last, the final runtime follows from the runtime of $\mathcal{A}$ and our setting of τ. □

2.3 Average-of-quantiles

In this section, we use Lemma 2.1 to construct a mechanism for privately evaluating a monotone function $f : \mathcal{Z}_\perp^n \to \mathbb{R}$. Unlike Theorem 2.3, the mechanism in this section requires an input parameter α which controls the maximum allowed diameter of the list of quantiles returned by the algorithm of Lemma 2.1; however, the mechanism in this section works for functions with unbounded range. The mechanism first tests that the diameter of the list of quantiles is not too large, and then releases a noisy average of the list of quantiles.

Theorem 2.4 (Average-of-quantiles)**.** *Fix $\alpha > 0$, $\varepsilon, \delta \in (0,1)$ and $p \in (0, 1/4)$. There exists an (ε, δ)-DP mechanism $\mathcal{M}$ that for all monotone functions $f : \mathcal{Z}_\perp^n \to \mathbb{R}$ and, on input Z, runs in*

time $T = \exp\left(O\left(\frac{p \log 1/\delta}{\varepsilon}\right)\right) p^{-2} \log \frac{1}{\delta}$, *samples* $S_1, \dots S_T \sim \mathcal{S}_p(Z)$, *and satisfies the following: If* $\max f(S_i) - \min f(S_i) \le \alpha$ *then*

$$\min f(S_i) - \alpha \le \mathcal{M}^f(Z) \le \max f(S_i) + \alpha.$$

Proof. The proof is similar to that of Theorem 2.3, except instead of running the exponential mechanism, the mechanism first tests if there is a large "core" of quantiles within an interval of width α, and if there is, the mechanism releases the average of these quantiles plus truncated Laplace noise.

Algorithm 3 average-of-quantiles mechanism $\mathcal{M}^f(Z)$

Input: Dataset $Z \in \mathcal{Z}^n$, query access to monotone f, and parameters $\varepsilon, \delta, \alpha, p$.
Output: $y \in \mathbb{R} \cup \{\perp\}$

1: Set $c = 16$, $\varepsilon \leftarrow \varepsilon/2$, $\delta \leftarrow \delta/3$ and $\tau \leftarrow \frac{c}{\varepsilon} \log \frac{1}{\delta}$.
2: Let $(q(1), \dots, q(\tau)) \leftarrow \mathcal{A}^f(Z)$.
▷ $\mathcal{A}$ is the mechanism given by Lemma 2.1 with parameters τ, p, and δ.
3: Let $t^* = \min\{t \in [\tau/2] \mid q(\tau - t) - q(t) \le \alpha\}$
4: If $t^* + \mathsf{TruncLap}\left(\frac{1}{\varepsilon}, \frac{\tau}{8}\right) \le \frac{\tau}{4} - 1$ then set

$$y \leftarrow \frac{4}{\tau} \sum_{i \in [\tau/4]} q(t^* + i)$$

and release $\widehat{y} \sim y + \mathsf{TruncLap}\left(\frac{16\alpha}{\tau\varepsilon}, \frac{16\alpha \log(1/\delta)}{\tau\varepsilon}\right)$.
5: Else release $\perp$.

First, we argue that $\mathcal{M}$ is (ε, δ)-DP. Recall that Lemma 2.1 states that for any two neighboring datasets Z and Z' and all $t \in [\tau - 2]$ we have

$$q'(t) \le q(t+1) \le q'(t+2)$$

with probability at least $1 - \delta$. Let E denote the event that the above interleaving holds. Let $\bar{q}$ and $\bar{q}'$ denote a fixed list quantiles output by $\mathcal{A}^f(Z)$ and $\mathcal{A}^f(Z')$ respectively. We first prove that for fixed $\bar{q}$ and $\bar{q}'$, Algorithm 3 is DP conditioned on the event E, and then we apply Fact A.8 and the fact that $\Pr[\bar{q}, \bar{q}' \in E] \ge 1 - \delta$ to complete the proof. In the remaining parts of the proof, fix $\bar{q}$ and $\bar{q}'$, and let $t^*(Z), y(Z)$ and $t^*(Z'), y(Z')$ denote the values of t^* and y when the inputs are Z and Z' and the quantiles are fixed to $\bar{q}$ and $\bar{q}'$, respectively.

The crux of the proof of privacy is the following sensitivity bound.

Claim 2.5 (Stability of the average of quantiles)**.** *Assume that for all* $t \in [\tau - 2]$ *we have* $q'(t) \le q(t+1) \le q'(t+2)$, *and* $t^*(Z), t^*(Z') \le \frac{3\tau}{8}$. *Then* $|y(Z) - y(Z')| \le \frac{16\alpha}{\tau}$.

Proof. First, for all $i \in [\tau/4]$ let $g(i) = q(t^*(Z) + i))$, and define g' analogously for Z'. Since the interleaving holds we have $|t^*(Z) - t^*(Z')| \in \{0, 1\}$, and thus for all $i \in [\tau/4]$

$$g'(i) = q'(t^*(Z') + i) \le q'(t^*(Z) + i + 1) \le q(t^*(Z) + i + 2) = g(i + 2),$$

where the second inequality follows by the hypothesis on the quantiles. By the same argument, we also have that $g(i) \le g'(i+2)$. By definition of g, and because $t^*(Z) \le 3\tau/8$, we have $g(i) \in [q(t^*(Z)+1), q(t^*(Z)+\tau/4)]$ for all $i \in [\tau/4]$ (the same holds for g'), and by our assumption on t^*, the width of this interval is at most α. Taken together, this implies that $g'(1) \le g(3) \le g'(5) \le g(\tau/4)$, and thus, that $g(\tau/4) - g'(1) \le 2\alpha$ (since $g'(5) - g'(1) \le \alpha$ and $g(\tau/4) - g(3) \le \alpha$). By the same argument, $g'(\tau/4) - g(1) \le 2\alpha$.

Next, we express $y(Z)$ and $y(Z')$ in terms of g and g', and using the above inequalities argue that the difference is small.

$$\begin{aligned} y(Z) - y(Z') &= \frac{4}{\tau}\left(\sum_{i\in[\tau/4]} g(i) - g'(i)\right) \\ &= \frac{4}{\tau}\left(\sum_{i\in[\tau/4-2]} g(i) - g'(i+2)\right) + \frac{4}{\tau}(g(\tau/4-1) + g(\tau/4) - g'(1) - g'(2)). \end{aligned}$$

Since $g(i) \le g'(i+2)$, the first term on the right-hand side is at most zero. Continuing, we have

$$\begin{aligned} y(Z) - y(Z') &\le \frac{4}{\tau}(g(\tau/4-1) + g(\tau/4) - g'(1) - g'(2)) \\ &\le \frac{8}{\tau}(g(\tau/4) - g'(1)) \\ &\le \frac{16\alpha}{\tau}. \end{aligned}$$

A symmetrical argument establishes an upper bound on $y(Z') - y(Z)$, so we are done. □

To complete the proof of privacy, let $G = \left\{(Z, Z') \mid |y(Z) - y(Z')| \le \frac{16\alpha}{\tau}\right\}$ and condition on the event E. We consider two cases: First, suppose $(Z, Z') \notin G$, then by Claim 2.5, at least one of $t^*(Z)$ or $t^*(Z')$ is at least $\frac{3\tau}{8}$. Since we are conditioned on E, we have that both are at least $\frac{3\tau}{8} - 1$, and thus $\mathcal{M}^f(Z)$ and $\mathcal{M}^f(Z')$ both output $\perp$. Next, suppose $(Z, Z') \in G$. Observe that by Claim 2.5 we have $|y(Z) - y(Z')| \le \frac{16\alpha}{\tau}$ and thus

$$y(Z) + \mathsf{TruncLap}\left(\frac{16\alpha}{\varepsilon\tau}, \frac{16\alpha\log(1/\delta)}{\varepsilon\tau}\right) \approx_{\varepsilon,\delta} y(Z') + \mathsf{TruncLap}\left(\frac{16\alpha}{\varepsilon\tau}, \frac{16\alpha\log(1/\delta)}{\varepsilon\tau}\right).$$

Similarly, since we are conditioned on E, we have $|t^*(Z) - t^*(Z')| \le 1$. Therefore,

$$t^*(Z) + \mathsf{TruncLap}\left(\frac{1}{\varepsilon}, \frac{\tau}{8}\right) \approx_{\varepsilon,\delta} t^*(Z') + \mathsf{TruncLap}\left(\frac{1}{\varepsilon}, \frac{\tau}{8}\right).$$

By composition (Fact A.3), we have that $\mathcal{M}^f(Z)|_E \approx_{2\varepsilon,2\delta} \mathcal{M}^f(Z')|_E$. Since E occurs with probability at least $1-\delta$ we can apply Fact A.8 to see that $\mathcal{M}^f(Z) \approx_{2\varepsilon,3\delta} \mathcal{M}^f(Z')$. This completes the proof of privacy since we rescaled ε and δ at the start of Algorithm 3.

Runtime follows by Lemma 2.1 and our setting of τ. To see why the accuracy guarantee holds, observe that if $\max f(S_i) - \min f(S_i) \le \alpha$ then $\mathcal{M}^f(Z)$ releases

$$\widehat{y} \sim y(Z) + \mathsf{TruncLap}\left(\frac{16\alpha}{\varepsilon\tau}, \frac{16\alpha\log(1/\delta)}{\varepsilon\tau}\right).$$

Since $\tau = \frac{c\log(1/\delta)}{\varepsilon}$ and $c = 16$, the noise is at most α, and hence $|\widehat{y} - y(Z)| \le \alpha$. By the definition of $y(Z)$, this implies that $\min f(S_i) - \alpha \le \widehat{y} \le \max f(S_i) + \alpha$. □

Acknowledgments and Disclosure of Funding

Ephraim Linder was supported in part by NSF grant BCS-2218803 and a grant from the Sloan Foundation. Vikrant Singhal was supported in part by NSF grant BCS-2218803, the Digital Data Design Trustworthy AI Lab at Harvard, a grant from the Sloan Foundation, and the Novo Nordisk Foundation grant NNF24OC0087820.

References

[ABMT25] Prashanti Anderson, Ainesh Bakshi, Mahbod Majid, and Stefan Tiegel. Sample-optimal private regression in polynomial time. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 2341–2349, New York, NY, USA, 2025. Association for Computing Machinery.

[AD20] Hilal Asi and John C Duchi. Instance-optimality in differential privacy via approximate inverse sensitivity mechanisms. In *Advances in Neural Information Processing Systems 33*, NeurIPS '20, pages 14106–14117. Curran Associates, Inc., 2020.

[ADH+24] Hilal Asi, John C Duchi, Saminul Haque, Zewei Li, and Feng Ruan. Universally instance-optimal mechanisms for private statistical estimation. In *The Thirty Seventh Annual Conference on Learning Theory*, pages 221–259. PMLR, 2024.

[ADT25] Hilal Asi, John C. Duchi, and Kunal Talwar. On privately estimating a single parameter, 2025.

[AUZ23] Hilal Asi, Jonathan Ullman, and Lydia Zakynthinou. From robustness to privacy and back. In *International Conference on Machine Learning*, pages 1121–1146. PMLR, 2023.

[AV23] Daniel G Alabi and Salil P Vadhan. Differentially private hypothesis testing for linear regression. *Journal of Machine Learning Research*, 24(361):1–50, 2023.

[BDE+24] Gavin Brown, Krishnamurthy Dj Dvijotham, Georgina Evans, Daogao Liu, Adam Smith, and Abhradeep Guha Thakurta. Private gradient descent for linear regression: Tighter error bounds and instance-specific uncertainty estimation. In *International Conference on Machine Learning*, pages 4561–4584. PMLR, 2024.

[BGS+21] Gavin Brown, Marco Gaboardi, Adam Smith, Jonathan Ullman, and Lydia Zakynthinou. Covariance-aware private mean estimation without private covariance estimation. In *Advances in Neural Information Processing Systems 34*, NeurIPS '21. Curran Associates, Inc., 2021.

[BHH+24] Gavin Brown, Jonathan Hayase, Samuel Hopkins, Weihao Kong, Xiyang Liu, Sewoong Oh, Juan C Perdomo, and Adam Smith. Insufficient statistics perturbation: Stable estimators for private least squares extended abstract. In Shipra Agrawal and Aaron Roth, editors, *Proceedings of Thirty Seventh Conference on Learning Theory*, volume 247 of *Proceedings of Machine Learning Research*, pages 750–751. PMLR, 30 Jun–03 Jul 2024.

[BHS23] Gavin Brown, Samuel Hopkins, and Adam Smith. Fast, sample-efficient, affine-invariant private mean and covariance estimation for subgaussian distributions. In Gergely Neu and Lorenzo Rosasco, editors, *Proceedings of Thirty Sixth Conference on Learning Theory*, volume 195 of *Proceedings of Machine Learning Research*, pages 5578–5579. PMLR, 12–15 Jul 2023.

[BKSW19] Mark Bun, Gautam Kamath, Thomas Steinke, and Zhiwei Steven Wu. Private hypothesis selection. In *Advances in Neural Information Processing Systems 32*, NeurIPS '19, pages 156–167. Curran Associates, Inc., 2019.

[BLSM26] Simone Bombari, Jialei Luo, Inbar Seroussi, and Marco Mondelli. High-dimensional private linear regression with optimal rates. *arXiv preprint arXiv:2505.16329*, 2026.

[CD20] Rachel Cummings and David Durfee. Individual sensitivity preprocessing for data privacy. In *Proceedings of the 31st Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '20, Philadelphia, PA, USA, 2020. SIAM.

[CDK24] Karan Chadha, John Duchi, and Rohith Kuditipudi. Resampling methods for private statistical inference. *arXiv preprint arXiv:2402.07131*, 2024.

[CKM+19] Clément L. Canonne, Gautam Kamath, Audra McMillan, Adam Smith, and Jonathan Ullman. The structure of optimal private tests for simple hypotheses. In *Proceedings of the 51st Annual ACM Symposium on the Theory of Computing*, STOC '19, pages 310–321, New York, NY, USA, 2019. ACM.

[CPS+12] Graham Cormode, Cecilia Procopiuc, Divesh Srivastava, Entong Shen, and Ting Yu. Differentially private spatial decompositions. In *2012 IEEE 28th International Conference on Data Engineering*, pages 20–31. IEEE, 2012.

[DF18] Cynthia Dwork and Vitaly Feldman. Privacy-preserving prediction. In *Conference On Learning Theory*, pages 1693–1702. PMLR, 2018.

[DF20] Yuval Dagan and Vitaly Feldman. Pac learning with stable and private predictions. In *Conference on Learning Theory*, pages 1389–1410. PMLR, 2020.

[DKW56] A. Dvoretzky, J. Kiefer, and J. Wolfowitz. Asymptotic Minimax Character of the Sample Distribution Function and of the Classical Multinomial Estimator. *The Annals of Mathematical Statistics*, 27(3):642 – 669, 1956.

[DL09] Cynthia Dwork and Jing Lei. Differential privacy and robust statistics. In *Proceedings of the 41st ACM Symposium on Theory of Computing*, STOC '09, pages 371–380. ACM, 2009.

[DLY22] Wei Dong, Yuting Liang, and Ke Yi. Differentially private covariance revisited. *Advances in Neural Information Processing Systems*, 35:850–861, 2022.

[DMNS06] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam D. Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, volume 3876 of *Lecture Notes in Computer Science*, pages 265–284. Springer, 2006.

[DTTZ14] Cynthia Dwork, Kunal Talwar, Abhradeep Thakurta, and Li Zhang. Analyze Gauss: Optimal bounds for privacy-preserving principal component analysis. In *Proceedings of the 46th Annual ACM Symposium on the Theory of Computing*, STOC '14, pages 11–20, New York, NY, USA, 2014. ACM.

[ENP22] Alexander Edmonds, Aleksandar Nikolov, and Toniann Pitassi. On learning and refutation in noninteractive local differential privacy. *Advances in Neural Information Processing Systems*, 35:18256–18266, 2022.

[FDY22] Juanru Fang, Wei Dong, and Ke Yi. Shifted inverse: A general mechanism for monotonic functions under user differential privacy. In *Proceedings of the SIGSAC Conference on Computer and Communications Security, CCS*, pages 1009–1022. ACM, 2022.

[FVH25] Ferdinando Fioretto and Pascal Van Hentenryck. *Differential Privacy in Artificial Intelligence: From, Theory to Practice*. Emerald Group Publishing, 2025.

[FWS22] Cecilia Ferrando, Shufan Wang, and Daniel Sheldon. Parametric bootstrap for differentially private confidence intervals. In *Proceedings of the 25th International Conference on Artificial Intelligence and Statistics*, AISTATS '22, pages 1598–1618. JMLR, Inc., 2022.

[HKM22] Samuel B Hopkins, Gautam Kamath, and Mahbod Majid. Efficient mean estimation with pure differential privacy via a sum-of-squares exponential mechanism. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1406–1417, 2022.

[HKMN23] Samuel B. Hopkins, Gautam Kamath, Mahbod Majid, and Shyam Narayanan. Robustness implies privacy in statistical estimation. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 497–506, New York, NY, USA, 2023. Association for Computing Machinery.

[JR13] Madhav Jha and Sofya Raskhodnikova. Testing and reconstruction of Lipschitz functions with applications to data privacy. *SIAM Journal on Computing*, 42(2):700–731, 2013.

[KL23] Nitin Kohli and Paul Laskowski. Differential privacy for black-box statistical analyses. *Proc. Priv. Enhancing Technol.*, 2023(3):418–431, 2023.

[KMV22] Pravesh Kothari, Pasin Manurangsi, and Ameya Velingker. Private robust estimation by stabilizing convex relaxations. In *Conference on Learning Theory*, pages 723–777. PMLR, 2022.

[KSGB23] Zeki Kazan, Kaiyan Shi, Adam Groce, and Andrew P Bray. The test of tests: A framework for differentially private hypothesis testing. In *International Conference on Machine Learning*, pages 16131–16151. PMLR, 2023.

[KV18] Vishesh Karwa and Salil Vadhan. Finite sample differentially private confidence intervals. In *Proceedings of the 9th Conference on Innovations in Theoretical Computer Science*, ITCS '18, pages 44:1–44:9, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[LJK+23] Xiyang Liu, Prateek Jain, Weihao Kong, Sewoong Oh, and Arun Suggala. Label robust and differentially private linear regression: Computational and statistical efficiency. *Advances in Neural Information Processing Systems*, 36:23019–23033, 2023.

[LKO22] Xiyang Liu, Weihao Kong, and Sewoong Oh. Differential privacy and robust statistics in high dimensions. In *Conference on Learning Theory*, pages 1167–1246. PMLR, 2022.

[LLRV25] Jane Lange, Ephraim Linder, Sofya Raskhodnikova, and Arsen Vasilyan. Local lipschitz filters for bounded-range functions with applications to arbitrary real-valued functions. In Yossi Azar and Debmalya Panigrahi, editors, *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2025, New Orleans, LA, USA, January 12-15, 2025*, pages 2881–2907. SIAM, 2025.

[LRSS25] Ephraim Linder, Sofya Raskhodnikova, Adam Smith, and Thomas Steinke. Privately evaluating untrusted black-box functions. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 2350–2361, New York, NY, USA, 2025. Association for Computing Machinery.

[LT19] Jingcheng Liu and Kunal Talwar. Private selection from private candidates. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 298–309, New York, NY, USA, 2019. Association for Computing Machinery.

[Mas90] P. Massart. The Tight Constant in the Dvoretzky-Kiefer-Wolfowitz Inequality. *The Annals of Probability*, 18(3):1269 – 1283, 1990.

[McS09] Frank McSherry. Privacy integrated queries: An extensible platform for privacy-preserving data analysis. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data*, SIGMOD '09, pages 19–30, New York, NY, USA, 2009. ACM.

[MT07] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 94–103, Washington, DC, USA, 2007. IEEE Computer Society.

[MWK+22] Oren Mangoubi, Yikai Wu, Satyen Kale, Abhradeep Thakurta, and Nisheeth K Vishnoi. Private matrix approximation and geometry of unitary orbits. In *Conference on Learning Theory*, pages 3547–3588. PMLR, 2022.

[Nar24] Shyam Narayanan. Better and simpler lower bounds for differentially private statistical estimation, 2024.

[NB20] Anupama Nandi and Raef Bassily. Privately answering classification queries in the agnostic pac model. In *Algorithmic Learning Theory*, pages 687–703. PMLR, 2020.

[NRS07] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 75–84. ACM, 2007.

[PB22] Víctor Peña and Andrés F Barrientos. Differentially private hypothesis testing with the subsampled and aggregated randomized response mechanism. *arXiv preprint arXiv:2208.06803*, 2022.

[PH25] Victor S Portella and Nicholas JA Harvey. Lower bounds for private estimation of gaussian covariance matrices under all reasonable parameter regimes. In *The Thirty Eighth Annual Conference on Learning Theory*, pages 4640–4667. PMLR, 2025.

[She17] Or Sheffet. Differentially private ordinary least squares. In *Proceedings of the 34th International Conference on Machine Learning*, ICML '17, pages 3105–3114. JMLR, Inc., 2017.

[She19] Or Sheffet. Old techniques in differentially private linear regression. In *Algorithmic Learning Theory*, ALT '19, pages 789–827. PMLR, 2019.

[Smi11] Adam Smith. Privacy-preserving statistical estimation with optimal convergence rates. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 813–822, 2011.

[SS21] Vikrant Singhal and Thomas Steinke. Privately learning subspaces. In *Advances in Neural Information Processing Systems 34*, NeurIPS '21. Curran Associates, Inc., 2021.

[SS25] Günter F. Steinke and Thomas Steinke. Privately estimating black-box statistics, 2025.

[TAK+24] Shuai Tang, Sergul Aydore, Michael Kearns, Saeyoung Rho, Aaron Roth, Yichen Wang, Yu-Xiang Wang, and Zhiwei Steven Wu. Improved differentially private regression via gradient boosting. In *2024 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, pages 33–56. IEEE, 2024.

[Tsf24] Eliad Tsfadia. On differentially private subspace estimation in a distribution-free setting. *Advances in Neural Information Processing Systems*, 37:39923–39962, 2024.

[Ver18] Roman Vershynin. *High-dimensional probability: An introduction with applications in data science*, volume 47. Cambridge university press, 2018.

[VTJ22] Prateek Varshney, Abhradeep Thakurta, and Prateek Jain. (nearly) optimal private linear regression for sub-gaussian data via adaptive clipping. In *Conference on Learning Theory*, pages 1126–1166. PMLR, 2022.

[Wan18] Yu-Xiang Wang. Revisiting differentially private linear regression: optimal and adaptive prediction & estimation in unbounded domain. In *Conference on Uncertainty in Artificial Intelligence*, 2018.

[War15] Lutz Warnke. On the method of typical bounded differences. *Combinatorics, Probability and Computing*, 25(2):269–299, August 2015.

Contents

1 Introduction **1**

1.1 Our results . . . 3

1.1.1 Privately evaluating monotone statistics . . . 3

1.1.2 Application to eigenvalue estimation . . . 4

1.1.3 Applications around linear regression . . . 4

1.2 Our techniques . . . 5

1.3 Related work . . . 6

1.4 Notation . . . 6

2 Framework for privately evaluating monotone functions **7**

2.1 Subsampling quantiles . . . 7

2.2 Median-of-quantiles . . . 8

2.3 Average-of-quantiles . . . 8

A Preliminaries **15**

B Proof of Claim 2.2 **16**

C Application to eigenvalue estimation **18**

D Applications to M-estimation **19**

D.1 Setup: Exponential Families and Concentration 19

D.2 Estimating the population loss 21

D.3 Estimating a single parameter 23

D.4 When an exact oracle for the loss is unavailable 30

E Query complexity lower bound for monotone statistics **31**

F Technical discussion of existing guarantees **36**

F.1 Extension of [LRSS25] 37

F.2 Translating [SS25] to our setting 38

G Related work for applications **39**

G.1 Subsample-and-aggregate baseline 39

G.2 Eigenvalue estimation 40

G.3 Testing problems 41

G.4 Loss estimation 41

G.5 Single-parameter estimation 42

H Analysis of random-design linear regression **42**

A Preliminaries

Let $\mathcal{Z}$ denote the set of all data points (or data universe). A dataset $Z \in \mathcal{Z}^n$ is a tuple of n elements where $z_i \in \mathcal{Z}$ for each $i \in [n]$. Let $\mathcal{Z}^* = \bigcup_{n\in\mathbb{N}} \mathcal{Z}^n$. We say two datasets Z and Z' are *neighbors* if there exists exactly one $i \in [n]$ such that $z_i \neq z'_i$. We define subsampling from a dataset Z as follows: let $\mathcal{Z}_\perp = \mathcal{Z} \cup \{\perp\}$ and let $\mathcal{Z}_\perp^* = \bigcup_{n\in\mathbb{N}} \mathcal{Z}_\perp^n$. Suppose $Z \in \mathcal{Z}_\perp^n$, then a subsample $S \subseteq Z$ is a tuple of n elements $(s_1, \ldots, s_n)$ such that $z_i = \perp \implies s_i = \perp$, and $s_i \in \{z_i, \perp\}$ otherwise. We let $|S| = |\{i \in [n] \mid s_i \neq \perp\}|$, and for all $z \in \mathcal{Z}_\perp$ we let $S^{j\leftarrow z}$ denote S with $s_j \leftarrow z$ and we let S_{-j} denote $S^{j\leftarrow\perp}$.

With this notation, we can now formally define our notion of monotonicity.[4]

Definition A.1 (Monotone functions)**.** *A function $f : \mathcal{Z}_\perp^* \to \mathbb{R}$ is* monotone *if $f(S) \leq f(Z)$ for all $Z \in \mathcal{Z}_\perp^*$ and $S \subseteq Z$.*

Next, we present the definition of differential privacy as well as a few standard results that will be useful throughout the paper.

Definition A.2 (Differential privacy [DMNS06])**.** *For random variables X and Y we say $X \approx_{\varepsilon,\delta} Y$ if for all measurable sets $E \subseteq \operatorname{supp}(X) \cup \operatorname{supp}(Y)$*

$$\Pr[X \in E] \leq e^\varepsilon \Pr[Y \in E] + \delta,$$

[4] We remark that the literature supplies several distinct notions with the name "monotonicity." The definition we consider here is, in particular, distinct from the notion of *sample-monotone functions* used in [AD20].

and the same inequality holds with X and Y swapped. If $\delta = 0$ we write $X \approx_\varepsilon Y$. A randomized algorithm $\mathcal{M}$ is (ε, δ)-differentially private *(DP) if $\mathcal{M}(Z) \approx_{\varepsilon,\delta} \mathcal{M}(Z')$ for all neighboring datasets $Z, Z' \in \mathcal{Z}^n$.*

Fact A.3 (Composition)**.** *Fix $\varepsilon_1, \varepsilon_2 > 0$ and $\delta_1, \delta_2 \in (0,1)$. Suppose $\mathcal{M}_1$ and $\mathcal{M}_2$ are (respectively) $(\varepsilon_1, \delta_1)$-DP and $(\varepsilon_2, \delta_2)$-DP. Then, the mechanism that, on input x, outputs $(\mathcal{M}_1(x), \mathcal{M}_2(x))$ is $(\varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2)$-DP.*

Fact A.4 (Group privacy)**.** *Fix $\varepsilon, \delta > 0$, and $n \in \mathbb{N}$. Suppose $\mathcal{M}$ is (ε, δ)-DP and $E \subsetneq \mathcal{Y}$ is measurable. For any pair of datasets $Z, Z' \in \mathcal{Z}^n$ that differ in exactly k elements,*

$$\Pr_{\mathcal{M}}[\mathcal{M}(Z) \in E] \leq e^{\varepsilon \cdot k}\left(\Pr_{\mathcal{M}}[\mathcal{M}(Z') \in E] + \frac{\delta}{\varepsilon}\right).$$

Definition A.5 (Lap and TruncLap)**.** *The* Laplace *distribution, denoted* $\mathsf{Lap}(b)$*, is defined over $\mathbb{R}$ by the probability density function $f(x) = \frac{1}{2b}e^{-|x|/b}$. The* truncated Laplace *distribution, denoted* $\mathsf{TruncLap}(b, \tau)$*, is given by the probability density function $f(x) = a_{b,\tau} \cdot \frac{1}{2b}e^{-|x|/b}$ when $|x| \leq \tau$ and 0 otherwise, where $a_{b,\tau}$ is a normalizing constant.*

Fact A.6 (Laplace mechanism [DMNS06])**.** *Fix $\varepsilon > 0$ and a function $f : \mathcal{Z}_\perp^n \to \mathbb{R}$. For all neighboring datasets $Z, Z' \in \mathcal{Z}^n$ with $|f(Z) - f(Z')| \leq \Delta$ we have $f(Z) + \mathsf{Lap}\left(\frac{\Delta}{\varepsilon}\right) \approx_\varepsilon f(Z') + \mathsf{Lap}\left(\frac{\Delta}{\varepsilon}\right)$. Additionally, for all $\delta > 0$ we have $f(Z) + \mathsf{TruncLap}\left(\frac{\Delta}{\varepsilon}, \frac{\Delta}{\varepsilon}\ln\frac{1}{\delta}\right) \approx_{\varepsilon,\delta} f(Z') + \mathsf{TruncLap}\left(\frac{\Delta}{\varepsilon}, \frac{\Delta}{\varepsilon}\ln\frac{1}{\delta}\right)$.*

Fact A.7 (Exponential Mechanism [MT07])**.** *The* exponential mechanism *takes a dataset $Z \in \mathcal{Z}^n$, computes a score ($\mathsf{score} : \mathcal{Z}^n \times \mathcal{Y} \to \mathbb{R}$) for each $y \in \mathcal{Y}$ with respect to Z, and outputs $y \in \mathcal{Y}$ with probability proportional to $\exp\left(\frac{\varepsilon \cdot \mathsf{score}(Z,y)}{2 \cdot \Delta}\right)$, where*

$$\Delta = \max_{y \in \mathcal{Y}} \max_{Z \sim Z' \in \mathcal{Z}^n} |\mathsf{score}(Z, y) - \mathsf{score}(Z', y)|.$$

The mechanism is ε-DP and outputs $\widetilde{y}$ that satisfies the following guarantee:

$$\Pr\left(\mathsf{score}(Z, \widetilde{y}) \leq \max_{y \in \mathcal{Y}}\{\mathsf{score}(Z, y)\} - \frac{2\Delta}{\varepsilon}(\ln|\mathcal{Y}| + t)\right) \leq e^{-t}.$$

Fact A.8 (DP with high probability)**.** *Fix $\varepsilon, \delta, \delta' \in (0,1)$, algorithm $\mathcal{A}$ and neighbors Z, Z'. Suppose there exists an event G over the coins of both $\mathcal{A}(Z)$ and $\mathcal{A}(Z')$ such that $\mathcal{A}(Z)|_G \approx_{\varepsilon,\delta} \mathcal{A}(Z')|_G$. If $\Pr[G] \geq 1 - \delta'$ then $\mathcal{A}(Z) \approx_{\varepsilon, \delta+\delta'} \mathcal{A}(Z')$.*

Proof. Fix a set E. Then

$$\begin{aligned}\Pr[\mathcal{A}(Z) \in E] &\leq \Pr[\mathcal{A}(Z) \in E \mid G]\Pr[G] + \delta' \\ &\leq e^\varepsilon \Pr[\mathcal{A}(Z') \in E \mid G]\Pr[G] + \delta + \delta' \\ &\leq e^\varepsilon \Pr[\mathcal{A}(Z') \in E] + \delta + \delta'.\end{aligned}$$

□

Definition A.9 (TV distance)**.** *For distributions $\mathcal{D}$ and $\mathcal{D}'$ over a set S define*

$$d_{\mathrm{TV}}(\mathcal{D}, \mathcal{D}') = \max_{T \subseteq S}\left(\left|\Pr_{x \sim \mathcal{D}}[x \in T] - \Pr_{x \sim \mathcal{D}'}[x \in T]\right|\right).$$

Lemma A.10 (Coupling lemma)**.** *Let $\mathcal{D}$ and $\mathcal{D}'$ be distributions over Ω. For any coupling of $\mathcal{V}$ of $\mathcal{D}$ and $\mathcal{D}'$ we have $d_{\mathrm{TV}}(\mathcal{D}, \mathcal{D}') \leq \Pr_{(X,Y)\sim\mathcal{V}}[X \neq Y]$.*

Lemma A.11 (Weyl's Inequality)**.** *Let $A, B \in \mathbb{R}^{d \times d}$ be symmetric matrices with ordered eigenvalues $\lambda_1(\cdot) \leq \lambda_2(\cdot) \leq \cdots \leq \lambda_d(\cdot)$. For any $i \in [d]$ we have $|\lambda_i(A) - \lambda_i(B)| \leq \|A - B\|_{\mathrm{op}}$.*

B Proof of Claim 2.2

In this section, we complete the proof of the quantile interleaving claim.

Proof. Let F and F' denote the CDF of $f(\mathcal{S}_p(Z))$ and $f(\mathcal{S}_p(Z'))$ respectively. Additionally, let $\widehat{F}$ and $\widehat{F}'$ denote the empirical CDF of m samples from $f(\mathcal{S}_p(Z))$ and $f(\mathcal{S}_p(Z'))$. To prove Claim 2.2,

we will prove that $\widehat{F}$ and $\widehat{F}'$ satisfy the following with probability at least $1-\delta$: For all $\ell \in \mathbb{R}$ the following holds:

$$\widehat{F}'(\ell) \geq \eta(1-\gamma^2) \implies \widehat{F}(\ell) \in \left[(1-\gamma)(1-p), \frac{1+\gamma}{1-p}\right] \cdot \widehat{F}'(\ell) \tag{1}$$

$$\widehat{F}(\ell) \geq \eta(1-\gamma^2) \implies \widehat{F}'(\ell) \in \left[(1-\gamma)(1-p), \frac{1+\gamma}{1-p}\right] \cdot \widehat{F}(\ell) \tag{2}$$

To see that (1) and (2) suffice to prove Claim 2.2, let $\ell = q(t+1)$ for some $t \in [\tau - 1]$. Then by definition of $q(t+1)$ and $\widehat{F}$ we have $\eta(1-\gamma^2) \leq \left(\frac{1+\gamma}{1-p}\right)^{t+1} \eta \leq \widehat{F}(\ell)$, which by (2) implies that $\widehat{F}'(\ell) \geq \eta(1-\gamma^2)$. But by (1), this implies that

$$\left(\frac{1+\gamma}{1-p}\right)^{t+1} \eta \leq \widehat{F}(\ell) \leq \frac{1+\gamma}{1-p} \cdot \widehat{F}'(\ell).$$

Rearranging terms yields $\widehat{F}'(\ell) \geq \left(\frac{1+\gamma}{1-p}\right)^{t} \eta$, and thus $q'(t) \leq \ell = q(t+1)$. An analogous argument suffices to show that $q(t+1) \leq q'(t+2)$. Since (1) and (2) hold for all $\ell \in \mathbb{R}$ with probability at least $1-\delta$ we have $q'(t) \leq q(t+1) \leq q'(t+2)$ for all $t \in [\tau - 2]$ with probability at least $1-\delta$ as well.

To complete the proof of Claim 2.2, it remains to prove (1) and (2). First, we show that the following stronger relationship between F and F' holds for all $\ell \in \mathbb{R}$:

$$(1-p) \cdot F'(\ell) \leq F(\ell) \leq \frac{1}{1-p} \cdot F'(\ell). \tag{3}$$

To see why (3) holds, suppose Z and Z' differ on z_j, and let $G = \{S \subseteq Z \mid s_j = \perp \wedge f(S) \leq \ell\}$ and let $B = \{S \subseteq Z \mid s_j = z_j \wedge f(S) \leq \ell\}$. Define G' and B' analogously for dataset Z'. Observe that $F(\ell) = \Pr_{S \sim \mathcal{S}_p(Z)}[S \in G] + \Pr_{S \sim \mathcal{S}_p(Z)}[S \in B]$. We bound $F(\ell)$ by F' using the following two observations: First, since $Z_{-j} = Z'_{-j}$ we have $\Pr_{S \sim \mathcal{S}_p(Z)}[S \in G] = \Pr_{S' \sim \mathcal{S}_p(Z')}[S' \in G']$. And second, since f is monotone, each $S \in B$ can be mapped to a unique $S \in G$ by setting $z_j \leftarrow \perp$, and thus $\Pr_{S \sim \mathcal{S}_p(Z)}[S \in B] \leq \frac{p}{1-p} \Pr_{S \sim \mathcal{S}_p(Z)}[S \in G]$. Combining these observations yields

$$\begin{aligned} F(\ell) \leq \left(1 + \frac{p}{1-p}\right) \Pr_{S' \sim \mathcal{S}_p(Z')}[S' \in G'] &\leq \frac{1}{1-p}\left(\Pr_{S' \sim \mathcal{S}_p(Z')}[S' \in G'] + \Pr_{S' \sim \mathcal{S}_p(Z')}[S' \in B']\right) \\ &= \frac{1}{1-p} \cdot F'(\ell). \end{aligned}$$

An analogous argument with the roles of Z and Z' swapped suffices to complete the proof of (3).

Next, we complete the proof of (1) by combining (3) with the well-known DKW inequality.

Fact B.1 (DKW inequality [DKW56, Mas90])**.** *Fix $\varepsilon > 0$ and $m \in \mathbb{N}$. Let $Y_1, \ldots, Y_m$ be independent samples from a distribution $\mathcal{D}$ over $\mathbb{R}$ with CDF F, and for all $t \in \mathbb{R}$ let $\widehat{F}(t) = \frac{1}{m}\sum_{i=1}^{m} \mathbb{1}[Y_i \leq t]$ be the empirical CDF. Then,*

$$\Pr_{Y_1, \ldots, Y_m}\left[\sup_{t \in \mathbb{R}} \left|\widehat{F}(t) - F(t)\right| \geq \varepsilon\right] \leq 2e^{-2m\varepsilon^2}.$$

Let $\zeta = \sup_{\ell \in \mathbb{R}} \left|\widehat{F}(\ell) - F(\ell)\right|$ and define ζ' analogously for $\widehat{F}'$ and F'. By Fact B.1 and our setting of m we see that $\zeta^* := \max(\zeta, \zeta') \leq \gamma(1-\gamma^2)(1-p)\eta/2$ with probability at least $1-\delta$. Conditioned on this event, we see that (3) implies

$$(1-p) \cdot \widehat{F}'(\ell) - 2\zeta^* \leq \widehat{F}(\ell) \leq \frac{1}{1-p}\left(\widehat{F}'(\ell) + 2\zeta^*\right).$$

Now, fix $\ell \in \mathbb{R}$ and suppose that $\widehat{F}'(\ell) \geq \eta(1-\gamma^2)$. Since we assumed $\zeta^* \leq \gamma(1-p)(1-\gamma^2)\eta/2$, we have $2\zeta^* \leq \gamma(1-p) \cdot \widehat{F}'(\ell)$ and hence

$$(1-p)(1-\gamma) \cdot \widehat{F}'(\ell) \leq \widehat{F}(\ell) \leq \frac{1+\gamma}{1-p}\widehat{F}'(\ell).$$

An analogous argument with the roles of $\widehat{F}$ and $\widehat{F}'$ swapped suffices to prove (2), and completes the proof of Claim 2.2. □

C Application to eigenvalue estimation

In this section, we explain how to apply our techniques to estimating the ith largest eigenvalue $\lambda_i(\Sigma)$ of the covariance Σ of a subgaussian distribution for any $i \in [d]$. Our main result provides a tradeoff between sample and time complexity for estimating a single eigenvalue.

Theorem C.1 (Private eigenvalue estimation)**.** *There exists a mechanism $\mathcal{M}$ that, for all privacy parameters $\varepsilon, \delta \in (0,1)$, failure probability $\beta > 0$, accuracy parameter $\alpha \in (0, 1/4)$, and subsampling probability $p \in (0, \frac{1}{4})$, satisfies (ε, δ)-DP. Moreover, for all subgaussian distributions $\mathcal{D}$ over $\mathbb{R}^d$ with covariance $\Sigma \succ 0$, there exists a constant $K_{\mathcal{D}}$, such that for all $i \in [d]$, the following holds:*

If

$$n = \Omega\left(\frac{K_{\mathcal{D}}}{\alpha^2}\left(\frac{d + \log(1/\beta)}{p} + \frac{\log(1/\delta)}{\varepsilon} + \frac{\log(p^{-1}\log 1/\delta)}{p}\right)\right),$$

then

$$\Pr_{Z\sim\mathcal{D}^n}\left[1 - \alpha \le \frac{\mathcal{M}(Z,i)}{\lambda_i(\Sigma)} \le 1 + \alpha\right] \ge 1 - \beta.$$

Moreover, $\mathcal{M}$ has runs in time $\exp\left(O\left(\frac{p\log 1/\delta}{\varepsilon}\right)\right)\operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$.

The proof of Theorem C.1 leverages the following standard concentration result regarding the convergence of the empirical covariance for subgaussian distributions. For a dataset Z of size n let $\widehat{\Sigma}(Z) = \frac{1}{n}\sum_{i\in[n]} Z_i Z_i^T$.

Theorem C.2 ([Ver18])**.** *Let $\mathcal{D}$ be a subgaussian distribution over $\mathbb{R}^d$ with covariance matrix $\Sigma \succ 0$. Then there exists a constant $K_{\mathcal{D}}$ such that for all $n \in \mathbb{N}$, $\beta > 0$, and $Z \sim \mathcal{D}^n$*

$$\left\|\Sigma^{-1/2}\widehat{\Sigma}(Z)\Sigma^{-1/2} - \mathbb{I}\right\|_{op} \le K_{\mathcal{D}}\left(\sqrt{\frac{d + \log(2/\beta)}{n}} + \frac{d + \log(2/\beta)}{n}\right)$$

with probability at least $1 - \beta$.

Remark C.3. By Weyl's inequality (Lemma A.11), Theorem C.2 implies that the eigenvalues of the empirical covariance and the true covariance are close on a multiplicative scale—that is,

$$\left|\frac{\lambda_i(\widehat{\Sigma}(Z))}{\lambda_i(\Sigma)} - 1\right| \le \left\|\Sigma^{-1/2}\widehat{\Sigma}(Z)\Sigma^{-1/2} - \mathbb{I}\right\|_{op}$$

for all $i \in [d]$.

Proof of Theorem C.1. The proof proceeds by applying the average-of-quantiles mechanism (Theorem 2.4) to estimate λ_i on a log scale. The additive error guarantee of Theorem 2.4, combined with the concentration guarantee of Theorem C.2, provides a multiplicative estimate of λ_i. Note that for all $m \in \mathbb{N}$, the function $h_m(Z, i) = \frac{1}{m}\cdot\lambda_i\left(\sum_{j\in[n]} Z_j Z_j^T\right)$, the ith largest eigenvalue, is monotone (this follows from the min-max characterization of the eigenvalues). First, we argue that with high probability over Z and $S \sim \mathcal{S}_p(Z)$ we have $h_{np}(S,i)/\lambda_i(\Sigma) \approx 1$. Second, we apply the average-of-quantiles mechanism from Theorem 2.4 to privately estimate $\log(h_{np}(S))$ to within some appropriate additive error, which translates to a multiplicative estimate of $\lambda_i(\Sigma)$.

Claim C.4. *For all $\alpha \in (0,1)$ and*

$$n = \Omega\left(K_{\mathcal{D}}\left(\frac{d + \log(1/\beta)}{\alpha^2 p}\right)\right),$$

if $Z \sim \mathcal{D}^n$ and $S \sim \mathcal{S}_p(Z)$, then with probability at least $1 - \beta$

$$1 - \alpha \le \frac{h_{np}(S,i)}{\lambda_i(\Sigma)} \le 1 \pm \alpha.$$

Proof. We prove this in two steps. First, we show that the empirical estimate $h_m(S,i)$ (with m random) is close to the true quantity $\lambda_i(\Sigma)$. Then, we show that m concentrates around its expectation, so $h_m(S,i)$ is close to $h_{np}(S,i)$.

Let $m = |S|$. Then $m \sim \mathsf{Bin}(n,p)$ and thus, by a Chernoff bound we have $|m - pn| \le \sqrt{cpn \log 1/\beta}$ with probability at least $1 - \beta/2$. It follows that $|h_{np}(S,i) - h_m(S,i)| = h_m(S,i)\left|\frac{m-np}{np}\right|$ and that

$$|h_{np}(S,i) - h_m(S,i)| \le h_m(S,i)\sqrt{\frac{c \log 1/\beta}{np}}$$

with probability at least $1-\beta/2$. Additionally, since $\sqrt{cpn \log 1/\beta} \le pn/2$, we have that $m \ge pn/2$ with probability at least $1 - \beta/2$, and conditioned on this event, Theorem C.2, Remark C.3, and our setting of n imply that $\frac{h_m(S,i)}{\lambda_i(\Sigma)} \in [1 \pm \frac{\alpha}{4}]$ with probability at least $1 - \beta/2$. By the union bound, we obtain that $\frac{h_{np}(S,i)}{\lambda_i(\Sigma)} \in [1 \pm \alpha]$ with probability at least $1 - \beta$. □

Let $\mathcal{A}$ denote the average-of-quantiles mechanism (Theorem 2.4) with accuracy parameter α, privacy parameters ε and δ, subsampling probability p, and query access to $\log(h_{np})$. We argue that $\mathcal{A}(Z)$ outputs a y such that $|y - \log h_{np}(S)| \le \alpha$ for some subsample S drawn by $\mathcal{A}$, and thus, by Claim C.4 that $|y - \log \lambda_i(\Sigma)| \le 2\alpha$, and by extension, that $e^{-\alpha} \le \frac{e^y}{\lambda_i(\Sigma)} \le e^{\alpha}$. By the accuracy guarantee of $\mathcal{A}$, it suffices to argue that $|\log(h_{np}(S,i)) - \log(\lambda_i(\Sigma))| \le \alpha/2$ for every subsample S drawn by the algorithm. Let $S_1, \dots, S_T$ denote the $T = \exp\left(O\left(\frac{p \log 1/\delta}{\varepsilon}\right)\right) \mathrm{poly}\left(\frac{\log 1/\delta}{p}\right)$ subsamples drawn by $\mathcal{A}$, and let B_j denote the event that $\left|\log \frac{h_{np}(S_j,i)}{\lambda_i(\Sigma)}\right| > \alpha/2$. By Claim C.4 and our setting of n, we have $\Pr\left[\bigcup_{j \in [T]} B_j\right] \le \beta$. Now, conditioned on $\bigcap \overline{B_j}$, by the accuracy guarantee of $\mathcal{A}$, we see that $\mathcal{A}(Z)$ outputs y such that $|y - \log \lambda_i(\Sigma)| \le 2\alpha$. By our bound on $\Pr[\bigcap \overline{B}_j]$, we have $e^{-\alpha} \le \frac{e^y}{\lambda_i(\Sigma)} \le e^{\alpha}$ with probability at least $1 - \beta$. Letting $\mathcal{M}$ be the mechanism that sets $y \leftarrow \mathcal{A}(Z)$ and returns e^y, completes the proof. □

D Applications to M-estimation

In this section, we will turn the tools we have developed to *M-estimation*, that is, solving problems of the form

$$\min_{\theta} \frac{1}{n} \sum_{i=1}^{n} \ell_\theta(z_i) \tag{4}$$

for some loss function ℓ. We will present applications to univariate estimation and testing problems based on (4), including estimating a single coordinate of the minimizer and estimating the minimum achievable loss.

Appendix D.1 will further develop the learning setting we address and present the assumptions we use. We then state our results: Appendix D.2 contains results for approximating the best-possible population loss and Appendix D.3 contains results for parameter estimation.

D.1 Setup: Exponential Families and Concentration

In the context of M-estimation, we associate a *learning task* with a triple $(\Theta, \ell, \mathcal{D})$. Here Θ is a set of parameters, $\ell = \{\ell_\theta : \theta \in \Theta\}$ a set of loss functions, and $\mathcal{D}$ a data-generating distribution over a data space $\mathcal{Z}$, which we leave implicit. We assume that $\ell_\theta : \mathcal{Z}_\perp \to \mathbb{R}_{\ge 0}$ satisfies $\ell_\theta(\perp) = 0$ for all θ (recall our convention that $\mathcal{Z}_\perp = Z \cup \{\perp\}$). Ideally, we would minimize over Θ with respect to the underlying distribution $\mathcal{D}$ itself:

$$\theta(\mathcal{D}) = \arg\min_{\theta \in \Theta} \mathop{\mathbb{E}}_{z \sim \mathcal{D}}[\ell_\theta(z)] = \arg\min_{\theta \in \Theta} L_\theta(\mathcal{D}),$$

where we have defined $L_\theta(\mathcal{D})$ to denote the expected population loss. We will use $L(\mathcal{D})$ to denote $\min_\theta L_\theta(\mathcal{D})$, the smallest possible population loss.

As we can only approximate $\mathcal{D}$ through a finite set of samples $Z = (z_1, \ldots, z_n)$ drawn i.i.d., we will extend our notation and define

$$\theta(Z) = \arg\min_{\theta \in \Theta} \frac{1}{n} \sum_{i=1}^{n} \ell_\theta(z_i) = \arg\min_{\theta \in \Theta} L_\theta(Z).$$

Similarly, we define $L_\theta(Z)$ as the empirical loss and $L(Z)$ as the smallest possible empirical loss.

Exponential Families One important example of M-estimation arises from the problem of modeling exponential families. An *exponential family model* is a set of distributions over an underlying space $\mathcal{Z}$ of the form

$$p_\theta(z) = h(z) \cdot \exp\left(\langle \theta, \phi(z) \rangle - A(\theta)\right).$$

The distribution is defined by the parameter vector θ, the *sufficient statistic* ϕ, and the *carrier* h. The function $A(\theta)$ is the *log partition function*. When fitting such a model to a set of observations $Z = (z_1, \ldots, z_n)$, we take as our loss function the negative log likelihood:

$$\min_\theta \sum_i \ell_\theta(z_i) = \min_\theta \sum_i -\log p_\theta(z_i) = \min_\theta \sum_i A(\theta) - \langle \theta, \phi(z_i) \rangle. \tag{5}$$

This maximum likelihood problem has several advantageous features. Since $A(\theta)$ is convex, the overall problem is also convex and can be solved efficiently. Additionally, the solution to (5) admits a clean asymptotic description: as $n \to \infty$, we have

$$\theta(Z) - \theta(\mathcal{D}) \sim \mathcal{N}(0, n^{-1} \nabla^2 A(\theta(\mathcal{D}))^{-1}).$$

If the distribution satisfies some mild regularity conditions and the sufficient statistic ϕ is *minimal*, informally meaning that the family is not overparameterized, we furthermore have that $\nabla^2 A(\theta(\mathcal{D})) \succ 0$, i.e., in a neighborhood around the true minimizer the loss function behaves as if it is strongly convex. Crucially for some of our downstream applications, we do not require strong convexity to hold for the whole loss function. For our purposes, it will suffice to show that any parameter sufficiently far from the empirical minimizer will have appreciably larger loss.

For more discussion on this topic and as a point of comparison, we refer the reader to [ADT25]. Their methods rely not versions of the above conditions which are themselves privately certifiable; that is, their algorithms check whether these local conditions hold and this check must itself be privatizable. In contrast, our approach allows us to write down the conditions we desire and establish accuracy whenever these conditions are met, a simpler argument.

Learning Task Assumptions We now operationalize the above discussion and state the assumptions we will use going forward to establish accuracy. In both Assumptions D.1 and D.3, we attempt to write down an interpretable set of general conditions under which our algorithm delivers improvements over existing results. We emphasize that our privacy guarantees do not rely on assumptions about the distribution.

Our results in Appendix D.2 provide accurate loss estimation for learning tasks $(\Theta, \ell, \mathcal{D})$ that satisfy the following assumption.

Assumption D.1 (Concentration of the empirical loss)**.** *For task $(\Theta, \ell, \mathcal{D})$, there exists a function $N_{D.1} : \mathbb{R} \to \mathbb{R}$ and a value $K_{D.1} > 0$ such that for all $\alpha, \beta > 0$ and $n \geq N_{D.1}(\alpha) + \frac{K_{D.1} \log 1/\beta}{\alpha^2}$*

$$\Pr_{Z \sim \mathcal{D}^n}\left[|L(Z) - L(\mathcal{D})| \geq \alpha\right] \leq \beta.$$

Informally, this captures a type of subgaussian concentration. In our applications, $N_{D.1}$ will correspond to a dimension-dependent term or a measure of the complexity of Θ.

Remark D.2. Once we have an algorithm for loss estimation, we can easily construct an algorithm for estimating a single parameter it is "influential" in the following sense: If $|\hat{\theta}_1 - \theta_1| \geq \alpha$ then $L_{\hat{\theta}_1}(\mathcal{D}) \geq L_{\theta_1}(\mathcal{D}) + h(\alpha)$—that is, the if the first coordinate differs from the population minimizer by at least α then the population loss increases by at least $h(\alpha)$ for some function $h(\cdot)$. To estimate an influential parameter, it suffices to estimate the loss of finitely many candidates up to error $h(\alpha)$. In many natural estimation problems, estimating the loss up to error $h(\alpha)$ requires $d/h(\alpha)^2$ samples; however, for estimation problems with additional structure, the first coordinate of the empirical minimizer will typically be within α of the population minimizer after $d + 1/\alpha^2$ samples. We introduce Assumption D.3 in order to take advantage of this faster rate of convergence.

Our results in Appendix D.3, which focus estimating a single coordinate of the larger minimizer $\theta(Z)$, require more care to set up. Recall that $L^{(w)}(Z)$ denotes the minimum empirical loss achievable among parameters θ with $\theta_1 = w$ and Z_{-i} denotes the dataset Z with the i-th element removed.

Assumption D.3 (Identifiability, Concentration, Stability)**.** *For task $(\Theta, \ell, \mathcal{D})$, there exists a function $N_{D.3} : \mathbb{R} \to \mathbb{R}$ and values $M_{D.3}, K_{D.3}, \lambda, \mu, \sigma > 0$ such that the following holds for all $\alpha, \beta > 0$:*

1 *For all $n \geq N_{D.3}(\alpha) + \frac{K_{D.3} \log 1/\beta}{\alpha^2}$ we have*

$$\Pr_{Z \sim \mathcal{D}^n}\left[|\theta(Z)_1 - \theta(\mathcal{D})_1| \geq \alpha\mu^{-1/2}\right] \leq \beta.$$

2 *For all $n \geq M_{D.3} + K_{D.3} \log 1/\beta$ we have*

$$\Pr_{Z \sim \mathcal{D}^n}\left[\forall w \in \mathbb{R} \colon \frac{\mu(w - \theta(Z)_1)^2}{2} \leq L^{(w)}(Z) - L(Z) \leq 2\mu(w - \theta(Z)_1)^2\right] \geq 1 - \beta.$$

3 *For all $n \geq M_{D.3} + K_{D.3} \log 1/\beta$ and all $i \in [n]$ we have*

$$\Pr_{Z \sim \mathcal{D}^n}\left[|L(Z) - L(Z_{-i})| \geq \frac{\lambda \log 2/\beta}{n}\right] \leq \beta.$$

4 *For all $n \in \mathbb{N}$ we have*

$$\Pr_{Z \sim \mathcal{D}^n}\left[L(Z) \geq \sigma^2\left(1 + \frac{\log 1/\beta}{n}\right)\right] \leq \beta.$$

We now discuss each part of the assumption informally. In Appendix H we prove that this assumption is satisfied for random design linear regression: Assumption D.3.1 is straightforward: we ask that the first coordinate of the empirical minimizer is usually close to the first coordinate of the true minimizer. Assumption D.3.4 is similarly transparent: the minimum empirical loss should have subexponential behavior on its upper tail. As a key example, this will be satisfied when we have subexponential concentration of $\ell_{\theta(\mathcal{D})}(z)$, the loss of a single observation with respect to the true minimizer. Under such conditions we also expect Assumption D.3.3 to hold, as any single observation is unlikely to strongly influence the empirical minimizer.

Informally, Assumption D.3.2 enforces an approximate notion of *identifiability*: any θ' with close-to-optimal loss must have $\theta'_1 \approx \theta(Z)_1$. Technically, we read it as a "typical smoothness and strong convexity" condition, yielding quantitative control over this tradeoff. The steps needed to establish this tradeoff are significantly more delicate than those for the other three, as we have to reason about loss minimization with the first parameter fixed. Weaker conditions would also suffice: the core of the argument requires us to show that poor choices for the first parameter lead to large losses.

D.2 Estimating the population loss

Our first result witnesses a sample and time complexity tradeoff for the problem of estimating the population loss. The subsampling hyperparameter p controls this tradeoff.

Theorem D.4 (Private loss estimation via subsampling)**.** *There exists a mechanism $\mathcal{M}$ that, for any task $(\Theta, \ell, \mathcal{D})$ satisfying Assumption D.1, privacy parameters $\varepsilon, \delta \in (0, 1)$, accuracy parameter $\alpha > 0$, and subsampling probability $p \in (0, \frac{1}{4})$, satisfies (ε, δ)-DP and the following accuracy guarantee:*

If

$$n = \Omega\left(\frac{N_{D.1}(\alpha/8)}{p} + \frac{K_{D.1} + L(\mathcal{D})^2}{\alpha^2}\left(\frac{\log 1/\delta}{\varepsilon} + \frac{\log 1/\delta}{p} + \frac{\log(p^{-1} \log 1/\delta)}{p}\right)\right)$$

then

$$\Pr_{Z \sim \mathcal{D}^n}\left[\left|\mathcal{M}^L(Z) - L(\mathcal{D})\right| \leq \alpha\right] \geq 1 - \delta.$$

Moreover, $\mathcal{M}$ has query complexity and runtime $\exp\left(O\left(\frac{p \log 1/\delta}{\varepsilon}\right)\right) \operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$.

Our next result provides an improved sample and time complexity tradeoff for the problem of testing whether the loss is large. Essentially, the result states that we can achieve the same tradeoff as in Theorem D.4, but with the privacy parameter δ replaced with a failure probability β.

Theorem D.5 (Private loss testing via subsampling)**.** *There exists a mechanism $\mathcal{M}$ that, for all tasks $(\Theta, \ell, \mathcal{D})$ satisfying Assumption D.1, privacy parameters $\varepsilon, \delta \in (0,1)$, failure probability $\beta > 0$, accuracy parameter $\alpha > 0$, and subsampling probability $p \in (0, \frac{1}{4})$, satisfies the following:*

If

$$n = \Omega\left(\frac{N_{D.1}(\alpha/2)}{p} + \frac{K_{D.1} + L(\mathcal{D})^2}{\alpha^2}\left(\frac{\log 1/\beta}{\varepsilon} + \frac{\log 1/\beta}{p} + \frac{\log(p^{-1}\log 1/\delta)}{p}\right)\right)$$

then the following holds:

- *If $L(\mathcal{D}) \geq 2\alpha$ then $\Pr_{Z\sim\mathcal{D}^n}\left[\mathcal{M}^L(Z) \text{ outputs reject}\right] \geq 1-\beta$.*
- *If $L(\mathcal{D}) \leq \alpha$ then $\Pr_{Z\sim\mathcal{D}^n}\left[\mathcal{M}^L(Z) \text{ outputs accept}\right] \geq 1-\beta$.*

Moreover, $\mathcal{M}$ has query complexity and runtime $\exp\left(O\left(\frac{p\log 1/\beta}{\varepsilon}\right)\right)\operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$.

Proof of Theorem D.4

Proof. The proof is a direct application of Theorem 2.4: since ℓ_θ is non-negative for all z and θ, we have that $L(Z)$ is monotone, and thus we can safely apply the average-of-quantiles mechanism (Theorem 2.4) with query access to L. Let $\mathcal{A}$ denote the average-of-quantiles mechanism with accuracy parameter $\alpha' \leftarrow \alpha/2$, privacy parameters ε and δ, and subsampling probability p. Let $\mathcal{M}$ be the mechanism which, given query access to L and input Z, simulates $\mathcal{A}$ with query access to $\frac{L}{p}$ and input Z.

We first prove a claim which states that if $Z \sim \mathcal{D}^n$ and $S \sim \mathcal{S}_p(Z)$ then with high probability $\left|\frac{L(S)}{p} - L(\mathcal{D})\right| \lesssim \alpha + o(1)$. This is not immediate from Assumption D.1 since $|S| \sim \mathsf{Bin}(n,p)$ and is not always equal to np. However, the proof follows from a straightforward application of Chernoff bounds for Bernoulli random variables.

Claim D.6. *There exists a constant $c > 0$ such that for all*

$$n = \Omega\left(\frac{N_{D.1}(\alpha)}{p} + \frac{K_{D.1}\log 1/\beta}{\alpha^2 p}\right),$$

if $Z \sim \mathcal{D}^n$ and $S \sim \mathcal{S}_p(Z)$ then

$$\left|\frac{L(S)}{p} - L(\mathcal{D})\right| \leq \alpha\left(1 + \sqrt{\frac{c\log 1/\beta}{n}}\right) + L(\mathcal{D})\sqrt{\frac{c\log 1/\beta}{n}}$$

with probability at least $1-\beta$.

Proof. Let $m = |S|$. Then $m \sim \mathsf{Bin}(n,p)$ and thus, by a Chernoff bound we have $|m - pn| \leq \sqrt{cpn\log 1/\beta}$ with probability at least $1 - \beta/2$. It follows that $|L(S)/p - L(S)n/m| = \frac{L(S)}{mp}|m - np|$. Applying the bound on $|m-pn|$ and multiplying by n/n yields

$$\left|\frac{L(S)}{p} - \frac{nL(S)}{m}\right| \leq \frac{nL(S)}{m}\sqrt{\frac{c\log 1/\beta}{np}}$$

with probability at least $1-\beta/2$. Now, applying Assumption D.1 to S and $\frac{nL(S)}{m}$, we see that $\left|\frac{nL(S)}{m} - L(\mathcal{D})\right| \leq \alpha$ with probability at least $1-\beta/2$. Combining the two bounds completes the proof. □

Let $T = \exp\left(O\left(\frac{p\log 1/\delta}{\varepsilon}\right)\right)\operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$ and let $S_1, \dots S_T \sim \mathcal{S}_p(Z)$ denote the subsamples drawn by $\mathcal{A}$. If B is the event that $\max_{i\in[T]}|L(\mathcal{D}) - L(S_i)/p| \geq \alpha'/2$, then conditioned on $\overline{B}$, we

have $\max L(S_i)/p - \min L(S_i)/p \le \alpha'$, and thus, by the accuracy guarantee of Theorem 2.4, that $\left|\mathcal{A}^{L/p}(Z) - L(\mathcal{D})\right| \le 2\alpha' = \alpha$. Hence, it suffices to show that

$$\Pr_{\substack{Z\sim\mathcal{D}^n \\ S_1,\dots S_T\sim\mathcal{S}_p(Z)}}\left[\max_{i\in[T]}|L(\mathcal{D}) - L(S_i)/p| \ge \alpha'/2\right] \le \delta.$$

To see why this holds, observe that if $n \ge \Omega\left(\frac{N_{D.1}(\alpha'/4)}{p} + \frac{(K_{D.1}+L(\mathcal{D})^2)\log 1/\beta}{\alpha^2 p}\right)$ then by Claim D.6 and Assumption D.1

$$\Pr_{\substack{Z\sim\mathcal{D}^n \\ S\sim\mathcal{S}_p(Z)}}\left[|L(\mathcal{D}) - L(S)/p| \ge \alpha'/2\right] \le \beta,$$

and thus, setting $\beta \leftarrow \delta/T$ and applying a union bound over all T subsamples completes the proof. □

Proof of Theorem D.5

Proof. Let $\mathcal{A}$ denote the median-of-quantiles mechanism (Theorem 2.3) with subsampling probability p, privacy parameters ε, δ, and failure probability $\beta/2$. Let $\mathcal{M}$ be the mechanism which, given query access to L and input Z, simulates $\mathcal{A}$ with query access to h and input Z, where $h(Z) = \mathbb{1}\left[\frac{L(Z)}{p} \ge 3\alpha/2\right]$. If $\mathcal{A}^h(Z) = 1$ then $\mathcal{M}$ outputs "reject" and otherwise $\mathcal{M}$ outputs "accept".

We argue that $\mathcal{A}$ outputs 1 with probability at least $1-\beta$ when $L(\mathcal{D}) \ge 2\alpha$, and outputs 0 with probability at least $1-\beta$ when $L(\mathcal{D}) \le \alpha$. Let $T = \exp\left(O\left(\frac{p\log 1/\beta}{\varepsilon}\right)\right)\text{poly}\left(\frac{\log 1/\delta}{p}\right)$. By our setting of n, and the same argument as in the proof of Theorem D.4 (except now with $\beta \leftarrow \beta/2T$ instead of $\beta \leftarrow \delta/T$), we have that

$$\Pr_{\substack{Z\sim\mathcal{D}^n \\ S_1,\dots S_T\sim\mathcal{S}_p(Z)}}\left[\max_{i\in[T]}|L(\mathcal{D}) - L(S_i)/p| \ge \alpha/2\right] \le \beta/2.$$

Thus, if $L(\mathcal{D}) \ge 2\alpha$, then $h(S_i) = 1$ for all $i \in [T]$ with probability at least $1-\beta/2$, and therefore $\mathcal{A}$ outputs 1 with probability at least $1-\beta$. By the same argument, if $L(\mathcal{D}) \le \alpha$ then $\mathcal{A}$ outputs 0 with probability at least $1-\beta$. The accuracy guarantee now follows from the definition of $\mathcal{M}$. The runtime and privacy guarantees follow from Theorem 2.3 and the fact that h is monotone (since L is monotone). □

D.3 Estimating a single parameter

The first result of this section states that one can achieve a sample and time complexity tradeoff for the problem of testing if $|\theta(\mathcal{D})_1|$ is large or small.

Theorem D.7 (Testing a single parameter via loss comparisons)**.** *There exists a mechanism $\mathcal{M}$ such that for all learning tasks $(\Theta, \ell, \mathcal{D})$ satisfying Assumption D.3, privacy parameters $\varepsilon, \delta > 0$, accuracy parameter $\alpha > 0$, and subsampling probability $p \in (0, 1/4)$, satisfies (ε,δ)-DP and the following accuracy guarantee: Fix $\rho \ge 2\sigma^2 + \alpha^2$ and $t > 20\alpha\mu^{-1/2}$. If*

$$n = \Omega\left(\frac{N_{D.3}(\alpha/2) + M_{D.3}}{p} + \left(\frac{K_{D.3}(1+\alpha^2)}{\alpha^2 p} + \frac{\rho^2+\lambda^2}{\alpha^4 p}\right)\left(1 + \frac{p^3}{\varepsilon^3}\right)\text{poly}\log\frac{n\rho}{\alpha\delta\varepsilon}\right),$$

then

1. *If $|\theta(\mathcal{D})_1| > 2t$ then $\Pr[\mathcal{M}^L(Z,\rho,t,\alpha,p) = \text{sign}(\theta(\mathcal{D})_1)] \ge 1-\delta$.*
2. *If $|\theta(\mathcal{D})_1| < t/2$ then $\Pr[\mathcal{M}^L(Z,\rho,t,\alpha,p) = 0] \ge 1-\delta$.*

Moreover $\mathcal{M}$ runs in time $\exp\left(O\left(\frac{p}{\varepsilon}\log\frac{1}{\delta}\right)\right)\cdot\text{poly}\left(\frac{\log 1/\delta}{p}\right)$.

Our next result provides a similar tradeoff for the problem of estimating $\theta(\mathcal{D})_1$. We first introduce some additional notation: Let $\Theta|_1$ denote the set $\{w \in \mathbb{R} \mid \exists\theta \in \Theta : \theta_1 = w\}$ and let $\Pi = \{\pi_i\}_{i\in[\kappa]}$ be an interval partition of $\Theta|_1$. For an interval π and value $w \in \mathbb{R}$, let $\Delta(w,\pi) = \min_{w'\in\pi}|w - w'|$.

Theorem D.8 (Estimating a single parameter via loss comparisons)**.** *There exists a mechanism $\mathcal{M}$ such that for all learning tasks $(\Theta, \ell, \mathcal{D})$ satisfying Assumption D.3, interval partition $\Pi = \{\pi_i\}_{i\in[\kappa]}$ of $\Theta|_1$, privacy parameters $\varepsilon, \delta > 0$, failure probability $\beta \in (0,1)$, accuracy parameter $\alpha > 0$, and subsampling probability $p \in (0, 1/4)$, is (ε, δ)-DP and satisfies the following: Fix clipping parameter $\rho \geq 2\sigma^2 + \alpha^2$. If*

$$n = \Omega\left(\frac{N_{D.3}(\alpha/2) + M_{D.3}}{p} + \left(\frac{K_{D.3}(1+\alpha^2)}{\alpha^2 p} + \frac{\rho^2+\lambda^2}{\alpha^4 p}\right)\left(1 + \frac{p^3}{\varepsilon^3}\right)\operatorname{poly}\log\frac{n\rho\kappa\log 1/\delta}{\alpha\beta\varepsilon}\right),$$

then

$$\Pr_{\substack{Z\sim\mathcal{D}^n \\ \pi\sim\mathcal{M}^L(Z,\rho,\alpha)}}\left[\Delta(\theta(\mathcal{D})_1, \pi) < 10\alpha\mu^{-1/2}\right] \geq 1-\beta.$$

Moreover $\mathcal{M}$ runs in expected time $\exp\left(O\left(\frac{p}{\varepsilon}\log\frac{1}{\beta}\log\frac{\kappa\rho}{\alpha}\right)\right)\cdot\kappa\operatorname{poly}\left(\frac{\log\kappa/\delta\log 1/\beta}{p}\right)$.

One can construct a mechanism $\mathcal{M}'$ that has the same sample complexity, accuracy, and privacy guarantees as in Theorem D.8, but with expected runtime $\exp\left(O\left(\frac{p}{\varepsilon}\log\frac{\kappa\rho}{\alpha\beta}\right)\right)\operatorname{poly}\left(\frac{\kappa\log\kappa/\delta\log 1/\beta}{p\beta}\right)$. These running times are incomparable in general; the main difference is that the mechanism in Theorem D.8 allows us to set p such that we avoid a $\operatorname{poly}(1/\beta)$ dependence. See Remark D.11 for more details.

In order to state the key technical lemma we will use to prove Theorems D.7 and D.8, we introduce the following additional notation: For each interval π let $L^{(\pi)} = \min_{w\in\pi} L^{(w)}$ and let $\widetilde{L}$ and $\widetilde{L}^{(\pi)}$ denote the functions $\frac{1}{p}\cdot\mathsf{clip}_\rho[L]$ and $\frac{1}{p}\cdot\mathsf{clip}_\rho[L^{(\pi)}]$ respectively, where $\mathsf{clip}_\rho[L]$ denotes the function L with range clipped to $[0,\rho]$. Informally, Lemma D.9 states that if $\theta(\mathcal{D})_1$ is in π and far from π', then we can distinguish π and π' by comparing the losses on different subsamples of Z. Somewhat more formally, if $S, S' \sim \mathcal{S}_p(Z)$ then $L^{(\pi)}(S) < L^{(\pi')}(S')$ with high probability.

Lemma D.9. *Fix a learning task $(\Theta, \ell, \mathcal{D})$ satisfying Assumption D.3. Fix $p \in (0, \frac{1}{4}), \alpha, \beta > 0$, and set $\rho \geq 2\sigma^2 + \alpha^2$, and let Π be an interval partition of size κ. There exists a function $h : \mathcal{Z}^* \to \mathbb{R}$ such that if*

$$n = \Omega\left(\frac{N_{D.3}(\alpha/2) + M_{D.3}}{p} + \left(\frac{K_{D.3}(1+\alpha^2)}{\alpha^2 p} + \frac{\rho^2+\lambda^2}{\alpha^4 p}\right)\log\left(\frac{n\rho\kappa}{\beta}\right)^3\right)$$

then with probability at least $1-\beta$ over $Z\sim\mathcal{D}^n$ and $S\sim\mathcal{S}_p(Z)$ the following holds for all $\pi\in\Pi$:

1. *If $\Delta(\pi, \theta(\mathcal{D})_1) \geq 10\alpha\mu^{-1/2}$ then $\widetilde{L}^{(\pi)}(S) > h(Z) + 3\alpha^2$.*
2. *If $\theta(\mathcal{D})_1 \in \pi$ then $h(Z) < \widetilde{L}^{(\pi)}(S) < h(Z) + \alpha^2$.*

In the remainder of the section we prove Theorems D.7 and D.8, and then prove Lemma D.9.

Proof of Theorem D.7

Proof. Our testing mechanism uses Theorem 2.4 to estimate the loss when the first coordinate is close to zero, and when the first coordinate is far from zero. It then compares the two outcomes and outputs the result.

Algorithm 4 Parameter tester $\mathcal{M}^L$

Input: Dataset $Z\in\mathcal{Z}^n$, query access to loss L, parameters $\varepsilon, \delta, \rho, \alpha, p$, and threshold $t\in\Theta|_1$.
Output: Bit $b\in\{0,1\}$.

1: Set $\varepsilon' \leftarrow \frac{\varepsilon}{3}$, and $\delta' \leftarrow \frac{\delta}{6}$.
2: Let $\mathcal{A}$ denote Algorithm 3 with privacy parameters ε', δ', and accuracy parameter α^2.
3: Set $\pi_0 \leftarrow (-t, t)$ and $\pi_1 \leftarrow [t, \infty)$ and $\pi_{-1} \leftarrow (-\infty, -t]$.
4: For each $j\in\{-1,0,1\}$, let $y_j \leftarrow \mathcal{A}^{\widetilde{L}^{(\pi_j)}}(Z)$. ▷ We treat the output $\perp$ as ∞.
5: Return $\arg\min_{j\in\{-1,0,1\}}\{y_j\}$.

Privacy and runtime. Fix neighboring datasets Z and Z'. Our proof proceeds by arguing that there exists an event E of probability at least $1 - 3\delta/6$ such that conditioned on E the mechanism $\mathcal{M}$ is $(\varepsilon, 3\delta/6)$-DP. We then apply Fact A.8 to see that $\mathcal{M}$ is (ε, δ)-DP. Let E be the event that the interleaving relationship in Lemma 2.1 fails to hold for some $\widetilde{L}^{(\pi_j)}$. By Lemma 2.1 and our setting of δ' we have $\Pr[E] \leq 3\delta/6$. Since each call to $\mathcal{A}$ is (ε', δ')-DP conditioned on E, Fact A.8 implies that $\mathcal{M}$ is (ε, δ)-DP. By Theorem 2.3, each call to $\mathcal{A}$ has runtime $\exp\left(O(\frac{p}{\varepsilon}\log\frac{1}{\delta})\right)\operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$.

Accuracy. The proof of accuracy proceeds by analyzing the following bad event: Let E denote the event that the conclusion of Lemma D.9 fails to hold for some π_j and some subsample drawn by $\mathcal{A}$. Assume without loss of generality that $\theta(\mathcal{D})_1 > 2t$ (the cases where $|\theta(\mathcal{D})_1| < t/2$ and $\theta(\mathcal{D})_1 < -2t$ are symmetric). Then, conditioned on $\overline{E}$, we have that $\left|\widetilde{L}^{(\pi_1)}(S) - \widetilde{L}^{(\pi_1)}(S')\right| \leq \alpha^2$, and that $\widetilde{L}^{(\pi_1)}(S) + \alpha^2 < \widetilde{L}^{(\pi_b)}(S') - \alpha^2$ for each $b \in \{-1, 0\}$ and every S and S' drawn by $\mathcal{A}$. By the guarantee of Theorem 2.4, we have that $\mathcal{A}^{\widetilde{L}^{(\pi_1)}}(Z) < \mathcal{A}^{\widetilde{L}^{(\pi_b)}}(Z)$ and hence the mechanism correctly outputs 1. To complete the accuracy argument, it suffices to bound the probability of the event E. Recall that by Theorem 2.4 each $\mathcal{A}$ draws $T = \exp\left(O(\frac{p}{\varepsilon}\log\frac{1}{\delta})\right)\operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$ subsamples. By Lemma D.9, our setting of n, and the union bound over the T subsamples drawn in each call to $\mathcal{A}$ we have $\Pr[E] \leq \delta$. □

Proof of Theorem D.8

Proof. Below, we define a mechanism for estimating a single parameter. Our algorithm uses median-of-quantiles to privately evaluate the loss when the first coordinate is restricted to a candidate interval π_i, and then uses private selection from private candidates [LT19] to select the candidate that achieved the best loss.[5]

Theorem D.10 (Private selection from private candidates [LT19])**.** *Fix $\varepsilon, \beta \in (0, 1)$, and $\kappa \in \mathbb{N}$, and let $T_{pspc}(\kappa, \beta) = O(\frac{\kappa}{\beta}\log\frac{\kappa}{\beta}\log\frac{1}{\beta})$. Suppose $\{\mathcal{M}_i\}_{i\in[\kappa]}$ is a collection of ε-DP mechanisms with real-valued outputs. There exists a 3ε-DP mechanism $\mathcal{M}_{pspc}$ that on input D calls mechanisms $\{\mathcal{M}_i(D)\}_{i\in[\kappa]}$, and outputs $\arg\min_i \min_j \left\{y_i^j\right\}$ where y_i^j is the output of the jth call to $\mathcal{M}_i$. Moreover, $\mathcal{M}_{pspc}$ makes $O(\frac{\kappa}{\beta}\log\frac{\kappa}{\beta})$ calls in expectation, and with probability at least $1 - \beta$ makes at least one and at most $T_{pspc}(\kappa, \beta)$ calls to each $\mathcal{M}_i$.*

Because our mechanism uses median-of-quantiles, it will be convenient to introduce a notation for the loss with discretized range. Let $f^{(\pi)}$ denote $\widetilde{L}^{(\pi)}$ with range rounded to $\alpha^2 \cdot \mathbb{Z}$.

Algorithm 5 θ_1 estimation mechanism $\mathcal{M}^L(Z, \rho, \alpha)$

Input: Dataset $Z \in \mathcal{Z}^n$, query access to loss L, interval partition Π, and parameters $\varepsilon, \delta, \beta, \rho, \alpha, p$.
Output: Interval $\pi \in \Pi$

1: Let $c \leftarrow \frac{1}{10}$, $t \leftarrow \frac{5}{c}\log\frac{1}{\beta}$, $\varepsilon' \leftarrow \frac{\varepsilon}{3t}$, and $\delta' \leftarrow \frac{\delta}{\kappa}$.
2: Sample the random seed r used by Algorithm 1 run with failure probability δ'.
3: For all $i \in [\kappa]$ let $\mathcal{A}_i(Z, r)$ denote the median-of-quantiles mechanism (Algorithm 2) with input Z, and random seed r given as input to Algorithm 1, privacy parameters ε' and δ', failure probability $\operatorname{poly}(c/\kappa)$, subsampling parameter p, and query access to $f^{(\pi_i)}$.
4: For each $j \in [t]$ let i_j denote the output of the jth run of $\mathcal{M}_{pspc}$ run with privacy parameter ε', failure probability $c/2$, and mechanisms $\{\mathcal{A}_i(Z, r)\}_{i\in[\kappa]}$.
5: Output the median interval from $\left\{\pi_{i_j} \mid j \in [t]\right\}$.

We describe Algorithm 5 at a high level below: The algorithm first samples a random seed r to give to the quantile-finder (Algorithm 1), which will be used to fix the subsamples drawn across all calls

[5] Theorem D.10 does not appear explicitly in [LT19]; however, it is a straightforward corollary of their Algorithm 2 and an analysis of geometric random variables.

to the $\mathcal{A}_i$'s since Algorithm 1 uses the same random seed each time; however, we do not fix the randomness used for the exponential mechanism in each call to $\mathcal{A}_i$, as this is essential for privacy to hold. For each random seed r, the algorithm defines the mechanism $\mathcal{A}_i(Z;r)$ as the median-of-quantiles mechanism run with the fixed random seed r given to the quantile-finder, and query access to the function $f^{(\pi_i)}$—that is, the clipped and appropriately normalized loss corresponding to the ith candidate π_i. Then, the algorithm runs t iterations of $\mathcal{M}_{pspsc}$, the selection mechanism in Theorem D.10, with a small constant failure probability. The basic idea is that most of the runs of $\mathcal{M}_{pspsc}$ will succeed and output a candidate π_{i_j} such that $\Delta(\pi_{i_j}, \theta(\mathcal{D})_1)$ is small, and thus this will hold for the median interval in $\{\pi_{i_j}\}$ as well.

Privacy. Fix neighboring datasets Z and Z'. Our proof proceeds by arguing that there exists an event E of probability at least $1-\delta$ over the choice of random seed, such that conditioned on E each of the t calls to $\mathcal{M}_{pspc}$ is $3\varepsilon'$-DP. We then apply Fact A.8 (DP with high probability) to complete the proof.

By Lemma 2.1 and Theorem 2.3, for each $i \in [\kappa]$, there exists an event E_i (the interleaving in Claim 2.2) that occurs with probability at least $1-\delta'$ over the choice of random seeds r and r' (the random seeds chosen on input Z and Z') such that conditioned on E_i we have $\mathcal{A}_i(Z,r) \approx_{\varepsilon'} \mathcal{A}_i(Z',r')$. Let $E = \bigcap_{i\in[\kappa]} E_i$. By the union bound $\Pr[E] \geq 1-\delta$, and moreover, conditioned on E we have $\mathcal{A}_i(Z,r) \approx_{\varepsilon'} \mathcal{A}_i(Z',r')$ for all $i \in [\kappa]$. Thus, by Theorem D.10 we have that $\mathcal{M}_{pspc}(Z) \approx_{3\varepsilon'} \mathcal{M}_{pspc}(Z')$ conditioned on E. Basic composition and our setting of ε' implies that conditioned on E we have $\mathcal{M}(Z) \approx_{\varepsilon} \mathcal{M}(Z')$. Since E occurs with probability at least $1-\delta$ we can apply Fact A.8 to see that $\mathcal{M}$ is (ε,δ)-DP.

Runtime. Since the range of $f^{(\pi)}$ has size ρ/α^2 for each $\pi \in \Pi$, Theorem 2.3 implies that each call to $\mathcal{A}_i$ has runtime $\exp\left(O(\frac{p}{\varepsilon}\log\frac{1}{\beta}\log\frac{\kappa\rho}{\alpha})\right)\operatorname{poly}\left(\frac{\log\kappa/\delta}{p}\right)$. Since $\mathcal{M}_{pspc}$ makes $O(\kappa\log\kappa)$ calls in expectation, mechanism $\mathcal{M}$ runs in expected time $\exp\left(O(\frac{p}{\varepsilon}\log\frac{1}{\beta}\log\frac{\kappa\rho}{\alpha})\right)\cdot\kappa\operatorname{poly}\left(\frac{\log\kappa/\delta\log 1/\beta}{p}\right)$.

Accuracy. We leverage Theorem 2.3 and Lemmas 2.1 and D.9 in order to analyze the following bad events: For each $j \in [t]$, let E_j denote the event that in the jth iteration of $\mathcal{M}_{pspc}$, there exists $i \in [\kappa]$ such that some execution of $\mathcal{A}_i$ fails to satisfy the accuracy guarantee of Theorem 2.3. Assume $\theta(\mathcal{D})_1 \in \pi_{i^*}$ and let E'_j denote the event that the jth iteration of $\mathcal{M}_{pspc}$ does not call $\mathcal{A}_{i^*}$ or makes more than $T_{pspc}(\kappa,c)$ calls to the $\mathcal{A}_i$'s. Let E denote the event that $\frac{1}{t}\sum \mathbb{1}\left[E_j \cup E'_j\right] \geq 3c$. Additionally, let B denote the event that there exists some $i \in [\kappa]$ and some subsample S drawn by Algorithm 1 such that $\widetilde{L}^{(\pi_i)}(S)$ fails to satisfy the conclusion of Lemma D.9.

Observe that if B, E_j and E'_j, do not occur, then for every i with $\Delta(\pi_i,\theta(\mathcal{D})_1) \geq \alpha\mu^{-1/2}$ we have $f^{(\pi_i)}(S) > h(Z) + 2\alpha^2$ (since $f^{(\pi)}$ and $\widetilde{L}^{\pi}$ differ by at most α^2) for every subsample S drawn by Algorithm 1, and thus $\mathcal{A}_i(Z;r) > h(Z)+2\alpha^2$. On the other hand, we have $f^{(\pi_{i^*})}(S) < h(Z)+2\alpha^2$ and thus $\mathcal{A}_{i^*}(Z;r) < h(Z)+2\alpha^2$. It follows that the index i_j returned by the jth iteration of $\mathcal{M}_{pspc}$ satisfies $\Delta(\pi_{i_j},\theta(\mathcal{D})_1) < \alpha\mu^{-1/2}$. Moreover, if the neither B nor E occur, then at least a $1-3c$ fraction of the π_{i_j} satisfy the above guarantee, and hence the median π_{i_j} does as well. Thus, it suffices to bound the probability of B and E.

First, we bound the probability of B. By Lemma 2.1, the total number of subsamples drawn by Algorithm 1 is $T = \exp\left(O(\frac{p}{\varepsilon}\log\frac{1}{\beta}\log\frac{\kappa\rho}{\alpha})\right)\operatorname{poly}\left(\frac{\log\kappa/\delta}{p}\right)$. By Lemma D.9 and the union bound over the $S_1,\ldots,S_T$ subsamples, if

$$n = \Omega\left(\frac{N_{D.3}(\alpha/2)+M_{D.3}}{p} + \left(\frac{K_{D.3}}{\alpha^2 p} + \frac{K_{D.3}}{p} + \frac{\rho^2+\lambda^2}{\alpha^4 p}\right)\log\left(\frac{n\rho\kappa\cdot T}{\beta}\right)^3\right)$$

then $\Pr[B] \leq \beta/2$.

Next, we bound the probability of E. By Theorem D.10 and our setting of parameters in Algorithm 5 we have that $\Pr[E'_j] \leq c$. Next, by the law of total probability we have $\Pr[E_j] \leq \Pr[E_j \mid \overline{E'_j}] + \Pr[E'_j]$. If E'_j does not occur, then $\mathcal{M}_{pcpc}$ makes at most $T_{pspc}(\kappa,c)$ calls to any $\mathcal{A}_i$. Since $\mathcal{A}_i$ is

executed with failure probability $\mathrm{poly}(c/\kappa)$, the $T_{pspc}(\kappa, c)$ calls implies that $\Pr[E_j \mid \overline{E'_j}] \le c$. Since $\Pr[E_j \cup E'_j] \le 2c$ for each $j \in [t]$, a Chernoff bound implies that $\Pr[E] \le e^{-O(ct)}$ which is at most $\beta/2$ by our setting of t.

Thus $\Pr[B \cup E] \le \beta$, which completes the proof of accuracy. □

Remark D.11. We briefly explain how to construct a mechanism matching the guarantees in Theorem 2.3 but with expected runtime $\exp\left(O\left(\frac{p}{\varepsilon}\log\frac{\kappa\rho}{\alpha\beta}\right)\right)\mathrm{poly}\left(\frac{\kappa\log\kappa/\delta\log 1/\beta}{p\beta}\right)$. Let $\mathcal{M}'$ be defined as Algorithm 5, but set $c = \beta$ and $t = 1$. Essentially, $\mathcal{M}'$ executes $\mathcal{M}_{pspc}$ (see Theorem D.10) once with failure probability $\beta/2$ and outputs the result. The privacy analysis is the same as that of Algorithm 5. The runtime follows from Theorems 2.3 and D.10, and our setting of $c = \beta$ and $t = 1$. The accuracy argument is identical to that of Algorithm 5, except that we no longer need to consider multiple runs of $\mathcal{M}_{pspc}$.

Proof of Lemma D.9

Proof. We argue that there exists some $h(Z)$, such that with high probability over $S \sim \mathcal{S}_p(Z)$, if $\Delta(\pi, \theta(\mathcal{D})_1) > 10\alpha\mu^{-1/2}$, then $\widetilde{L}^{(\pi)}(S) > h(Z) + 3\alpha^2$; while if $\theta(\mathcal{D})_1 \in \pi$, then $h(Z) < \widetilde{L}^{(\pi)}(S) < h(Z) + \alpha^2$.

Claim D.12. *If* $\rho \ge 2\sigma^2 + \alpha^2$ *and*

$$n = \Omega\left(\frac{N_{D.3}(\alpha/2) + M_{D.3}}{p} + \frac{K_{D.3}\log 1/\beta}{\alpha^2 p} + \frac{K_{D.3}\log 1/\beta}{p} + \frac{\rho^2\log 1/\beta}{\alpha^4 p}\right),$$

then for all intervals π*, the following holds:*

1. *If* $\Delta(\theta(\mathcal{D})_1, \pi) \ge 10\alpha\mu^{-1/2}$*, then*
$$\Pr_{Z,S}\left[\widetilde{L}^{(\pi)}(S) \ge \widetilde{L}(S) + 5\alpha^2\right] \ge 1 - \beta.$$
2. *If* $\theta(\mathcal{D})_1 \in \pi$*, then*
$$\Pr_{Z,S}\left[\widetilde{L}^{(\pi)}(S) \le \widetilde{L}(S) + \alpha^2\right] \ge 1 - \beta.$$

While Claim D.12 provides a guarantee in terms of S, our goal is to provide a bound in terms of Z. To obtain the desired bound, we will use Claim D.13, which states that $\widetilde{L}(S)$ concentrates around its mean—this allows us to set $h(Z) \approx \mathbb{E}_{S\sim\mathcal{S}_p(Z)}[L(S)]$ and apply a union bound over the subsamples.

Claim D.13. *For all* $n = \Omega\left(\frac{M_{D.3} + K_{D.3}\log(n\rho/\beta)}{p}\right)$*, we have*

$$\Pr_{\substack{Z\sim\mathcal{D}^n \\ S\sim\mathcal{S}_p(Z)}}\left[\left|\widetilde{L}(S) - \mathop{\mathbb{E}}_{S'\sim\mathcal{S}_p(Z)}[\widetilde{L}(S')]\right| \gtrsim \frac{\lambda(\log(n\rho/\beta))^{3/2}}{\sqrt{np}}\right] \le \beta.$$

We defer the proofs of Claims D.12 and D.13 for later, and complete the proof of Lemma D.9. Let $\Pi^- \subseteq \Pi$ denote the set of intervals π such that $\Delta(\theta(\mathcal{D})_1, \pi) \ge 10\alpha\mu^{-1/2}$ and let $\pi^* \in \Pi$ be the interval containing $\theta(\mathcal{D})_1$. Define E_1 as the event that $\widetilde{L}^{(\pi)}(S) < \widetilde{L}(S) + 5\alpha^2$ for some $\pi \in \Pi^-$, or $\widetilde{L}^{(\pi^*)}(S) > \widetilde{L}(S) + \alpha^2$. Define E_2 as the event that $\left|\widetilde{L}(S) - \mathbb{E}_{S'\sim\mathcal{S}_p(Z)}[\widetilde{L}(S')]\right| > \frac{c\lambda(\log(n\rho\kappa/\beta))^{3/2}}{\sqrt{np}}$. Observe that conditioned on $\overline{E_1 \cup E_2}$ we have

$$\widetilde{L}^{(\pi)}(S) \ge \mathbb{E}[\widetilde{L}(S)] + 5\alpha^2 - \frac{c\lambda(\log(n\rho\kappa/\beta))^{3/2}}{\sqrt{np}}$$

for all $\pi \in \Pi^-$, and

$$\mathbb{E}[\widetilde{L}(S)] - \frac{c\lambda(\log(n\rho\kappa/\beta))^{3/2}}{\sqrt{np}} \le \widetilde{L}^{(\pi^*)}(S) \le \mathbb{E}[\widetilde{L}(S)] + \alpha^2 + \frac{c\lambda(\log(n\rho\kappa/\beta))^{3/2}}{\sqrt{np}}.$$

Let $h(Z) = \mathbb{E}[\widetilde{L}(S)] - \frac{c\lambda(\log(n\rho\kappa/\beta))^{3/2}}{\sqrt{np}}$. By our setting of n, we have that for all $\pi \in \Pi^-$, we have $\widetilde{L}^{(\pi)}(S) > h(Z) + 5\alpha^2$ and $\widetilde{L}^{(\pi^*)}(S) \in [h(Z), h(Z) + 3\alpha^2/2]$.

Rescaling $\alpha \leftarrow \alpha/\sqrt{1.5}$ and repeating the proof gives

$$\widetilde{L}^{(\pi)}(S) > h(Z) + 3\alpha^2 \;\text{ and }\; h(Z) < \widetilde{L}^{(\pi^*)}(S) < h(Z) + \alpha^2.$$

By Claims D.12 and D.13 and the union bound we have $\Pr[E_1 \cup E_2] \le \beta$, which yields the result.

□

In the remainder of the section we prove Claims D.12 and D.13.

Proof of Claim D.12. First set $\alpha_0 \leftarrow \alpha\mu^{-1/2}$. Let E_1 be the event that $m = |S| \notin \left[pn \pm \sqrt{cpn\log 1/\beta}\right]$, let E_2 be the event that $|\theta(S)_1 - \theta(\mathcal{D})_1| \ge \alpha_0/2$, let E_3 be the event that $nL(S)/m > 2\sigma^2$, and let E_4 be the event that some $w \in \mathbb{R}$ violates the inequality in Assumption D.3.2. First, we show that the conclusion holds conditioned on $\overline{\bigcup_{i\in[4]} E_i}$, and then we show that $\Pr[\bigcup_{i\in[4]} E_i] \le \beta$.

Let $\alpha_1 = 10\alpha_0$ and consider the case where $\Delta(\theta(\mathcal{D})_1, \pi) \ge \alpha_1$. By the triangle inequality and the fact that $|\theta(S)_1 - \theta(\mathcal{D})_1| \ge \alpha_0/2$, we have $\inf_{w\in\pi}|w - \theta(S)_1| \ge \alpha_1/2$. Now, if $m = |S|$ then,

$$\frac{n}{m}\cdot L^{(\pi)}(S) \ge \frac{n}{m}\cdot L(S) + \frac{\mu\alpha_1^2}{8} \ge \frac{1}{p}\,\mathsf{clip}_\rho[L(S)] - \frac{\rho}{p}\sqrt{\frac{c\log 1/\beta}{np}} + \frac{\mu\alpha_1^2}{8},$$

where the first inequality follows from Assumption D.3.2, and the second inequality follows from a similar analysis as Claim D.6. Next, we show that the same holds for $\widetilde{L}$—that is, when L is clipped and normalized by $\frac{1}{p}$ (instead of $\frac{n}{m}$). First, observe that if $L^{(\pi)}(S) \le \rho$ then $\mathsf{clip}_\rho L^{(\pi)}(S) = L^{(\pi)}(S)$, and thus,

$$\widetilde{L}^{(\pi)}(S) \ge \widetilde{L}(S) - \frac{\rho}{p}\sqrt{\frac{c\log 1/\beta}{np}} + \frac{\mu\alpha_1^2}{8} \ge \widetilde{L}(S) + 5\mu\alpha_0^2.$$

To see why the same holds when $L^{(\pi)}(S) \ge \rho$ (and thus, $\widetilde{L}^{(\pi)}(S) \ge \rho/p$), recall that $nL(S)/m \le 2\sigma^2$, and thus, by our assumption that $\rho \ge 2\sigma^2 + \alpha_0^2\mu$, and conditioned on event $\overline{E}_1$, we have

$$\widetilde{L}(S) \le \frac{nL(S)}{m}\left(1 + \sqrt{\frac{c\log 1/\beta}{np}}\right) \le \rho - \frac{\mu\alpha_1^2}{8} + \sigma^2\sqrt{\frac{c\log 1/\beta}{np}}.$$

Multiplying the right hand side by $\frac{1}{p}$ yields

$$\widetilde{L}^{(\pi)}(S) \ge \frac{\rho}{p} \ge \widetilde{L}(S) - \frac{\rho}{p}\sqrt{\frac{c\log 1/\beta}{np}} + \frac{\mu\alpha_1^2}{8} \ge \widetilde{L}(S) + 5\mu\alpha_0^2.$$

Next, we consider the case where $\Delta(\theta(\mathcal{D})_1, \pi) = 0$. Let $w = \theta(\mathcal{D})_1$. Then conditioned on $\overline{E_4}$, we can apply Assumption D.3.2 to obtain

$$\widetilde{L}^{(\pi)}(S) \le \frac{n}{m}L^{(w)}(S) + \frac{\rho}{p}\sqrt{\frac{c\log 1/\beta}{np}} \le \frac{n}{m}L(S) + \frac{\mu\alpha_0^2}{2} + \frac{\rho}{p}\sqrt{\frac{c\log 1/\beta}{np}}.$$

Since $L(S) < \rho$ we have $L(S) = \mathsf{clip}_\rho[L(S)]$, and thus,

$$\widetilde{L}^{(\pi)}(S) \le \widetilde{L}(S) + \frac{\mu\alpha_0^2}{2} + \frac{2\rho}{p}\sqrt{\frac{c\log 1/\beta}{np}} \le \widetilde{L}(S) + \mu\alpha_0^2.$$

We complete the proof of Claim D.12 by bounding the probability of $\bigcup_{i\in[4]} E_i$. By the argument in Claim D.6, we have $\Pr[E_1] \le \beta/4$. Since $n = \Omega\left(\frac{N_{D.3}(\alpha/2)}{p} + \frac{K_{D.3}\log 1/\beta}{\alpha^2 p}\right)$, Assumption D.3.1

implies that $\Pr[E_2] \le \beta/4$. Similarly, by our setting of $n = \Omega\left(\frac{M_{D.3}}{p} + \frac{K_{D.3}\log 1/\beta}{p}\right)$ and Assumptions D.3.2 and D.3.4, we have $\Pr[E_3] \le \beta/4$ and $\Pr[E_4] \le \beta/4$. By the union bound, $\Pr\left[\bigcup_{i\in[4]} E_i\right] \le \beta$ holds, which completes the proof. □

Proof of Claim D.13. A key tool in our proof is a type of bounded-differences inequality that applies when the difference between function values on neighboring points is bounded with high probability. While the most general version of the statement appears in [War15], we use a simplified form for binary random variables and where the differences are bounded by the same constant in every coordinate. At a high level, we use the inequality to argue that the function $\widetilde{L}$ concentrates around its expectation at a fast rate when $S \sim \mathcal{S}_p(Z)$. In particular, this rate is independent of the rate at which the empirical loss concentrates around the population loss (e.g., as in Assumption D.1, which we do not use here) and only depends on Assumption D.3.3.

Theorem D.14 (Typical bounded differences inequality [War15])**.** *Let $X = (X_1, \ldots, X_N)$ be a family of independent random variables taking values in $\{0,1\}$, where $\Pr[X_i = 1] = p$ for all $i \in [N]$. Let $\Gamma \subseteq \{0,1\}^N$ be an event and assume that the function $f : \{0,1\}^N \to \mathbb{R}$ satisfies the following* typical Lipschitz condition*:*

(TL) There are numbers a and b with $a \le b$ such that whenever $x, \tilde{x} \in \{0,1\}^N$ differ in exactly one coordinate, we have

$$|f(x) - f(\tilde{x})| \le \begin{cases} a & \text{if } x \in \Gamma, \\ b & \text{otherwise.} \end{cases}$$

For any $\gamma \in (0,1]$ there is an event $\mathcal{B} = \mathcal{B}(\Gamma, \gamma)$ satisfying

$$\Pr(\mathcal{B}) \le N\gamma^{-1} \cdot \Pr(X \notin \Gamma) \quad \text{and} \quad \neg\mathcal{B} \subseteq \Gamma,$$

such that for $\mu = \mathbb{E} f(X)$, $c = \gamma(b-a)$ and any $t \ge 0$ we have

$$\Pr\left[|f(X) - \mu| \ge t \text{ and } \overline{\mathcal{B}}\right] \le 2\exp\left(-\frac{t^2}{2Np(1-p)(a+c)^2 + 2(a+c)t/3}\right).$$

At a high level, we show that for a typical Z, one can apply Theorem D.14 to $\widetilde{L}$ with the domain $\{S \subseteq Z\}$. We use the λ-leave-one-out property (Assumption D.3.3) to argue that $\widetilde{L}$ has bounded differences with high probability under $\mathcal{S}_p(Z)$—that is, it satisfies the typical Lipschitz condition, and we use the definition of $\widetilde{L}$ to argue that the differences are always at most ρ/p.

In order to leverage Theorem D.14, we argue that for most Z, there exists a set Γ of subsets $S \subseteq Z$ with probability mass at least $1-\beta$ over $\mathcal{S}_p(Z)$ such that for all $S \in \Gamma$ the quantity $\sup_{i\in[n]} \frac{1}{p} \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right|$ is small. Let $c > 0$ be a sufficiently large constant, and for all Z and $\beta \in (0,1)$ define the set

$$\Gamma(Z,\beta) = \left\{ S \subseteq Z \mid \sup_{i\in[n]} \frac{1}{p} \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right| \le \frac{c\lambda\log(n/\beta)}{np} \right\}.$$

Next, we argue that for most Z, the set $\Gamma(Z,\beta)$ has probability mass at least $1-\beta$ under $\mathcal{S}_p(Z)$. We say a dataset Z is *β-typical* if $\Pr_{S\sim\mathcal{S}_p(Z)}[S \in \Gamma(Z,\beta)] \ge 1-\beta$. To apply Assumption D.3.3, we first relate the difference $\frac{1}{p} \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right|$ for a random subset $S \sim \mathcal{S}_p(Z)$ to the difference $\frac{n}{|S^{i\leftarrow z_i}|} \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right|$—that is, where the losses are normalized appropriately for samples of size $|S^{i\leftarrow z_i}|$. For all $S \subseteq Z$, where $S^{i\leftarrow z_i}$ has size $m = pn - r$ for some $r \in \mathbb{Z}$, we have

$$\begin{aligned} \frac{1}{p} \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right| &= \frac{n}{m+r}\left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right| \\ &= n\left(\frac{1}{m} - \frac{r}{m(m+r)}\right) \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right| \\ &= \frac{n}{m} \cdot \left|L(S^{i\leftarrow z_i}) - L(S_{-i})\right|\left(1 - \frac{r}{m+r}\right) \end{aligned}$$

By the arguments in Claim D.6, we have $r \in [\pm\sqrt{cpn \log 1/\beta}]$ with probability at least $1 - \beta^2/2$. Conditioned on this event, we have

$$\frac{1}{p} \cdot \left|L(S^{i \leftarrow z_i}) - L(S_{-i})\right| \le \frac{2n}{m} \cdot \left|L(S^{i \leftarrow z_i}) - L(S_{-i})\right|.$$

And thus, applying Assumption D.3.3 and our setting of n in the statement of Claim D.13 yields

$$\Pr_{Z,S}\left[\frac{1}{p} \cdot \left|L(S^{i \leftarrow z_i}) - L(S_{-i})\right| \ge \frac{2c\lambda \log 1/\beta}{m}\right] \le \Pr_{Z,S}\left[\frac{n}{m} \cdot \left|L(S^{i \leftarrow z_i}) - L(S_{-i})\right| \ge \frac{c\lambda \log 1/\beta}{m}\right] \le \beta^2/2.$$

By the union bound over all $i \in [n]$ and the event that $r \notin [\pm\sqrt{cpn \log 1/\beta}]$, we obtain that $\Pr_{Z,S}\left[S \in \Gamma(Z, \beta)\right] \ge 1 - \beta^2$. Now, let E be the event that Z is β-typical. Then by the law of total probability,

$$1 - \beta^2 \le \Pr[E] + (1 - \beta)(1 - \Pr[E]),$$

and thus Z is β-typical with probability at least $1 - \beta$.

We complete the proof of Claim D.13 by applying Theorem D.14 to $\widetilde{L}$ and β-typical Z. Let $a = \frac{c\lambda \log(n/\beta)}{np}$ and let $b = \rho/p$ and $\gamma = a/(b-a)$. Then by Theorem D.14, there is an event $\mathcal{B}$ such that $\Pr[\mathcal{B}] \le n\gamma^{-1}\beta$ and

$$\Pr_{S \sim \mathcal{S}_p(Z)}\left[\left|\widetilde{L}(S) - \mathop{\mathbb{E}}_{S \sim \mathcal{S}_p(Z)}[\widetilde{L}(S)]\right| \ge t \wedge \overline{\mathcal{B}}\right] \le 2\exp\left(-\frac{t^2}{8np(1-p)a^2 + 4at/3}\right).$$

Since $p \le \frac{1}{4}$, $\frac{\log(1/\beta)}{np} \le 1$, and $\Pr[\mathcal{B}] \le n\gamma^{-1}\beta$, there exists an absolute constant $c > 0$, such that if $t = a\sqrt{cpn \log \frac{1}{\beta}}$, then

$$\Pr_{S \sim \mathcal{S}_p(Z)}\left[\left|\widetilde{L}(S) - \mathop{\mathbb{E}}_{S \sim \mathcal{S}_p(Z)}[\widetilde{L}(S)]\right| \ge t\right] \le 2\exp\left(-\log\frac{1}{\beta}\right) + n\gamma^{-1}\beta.$$

Since Z is β-typical with probability at least $1 - \beta$, the union bound gives

$$\Pr_{\substack{Z \sim \mathcal{D}^n \\ S \sim \mathcal{S}_p(Z)}}\left[\left|\widetilde{L}(S) - \mathop{\mathbb{E}}_{S \sim \mathcal{S}_p(Z)}[\widetilde{L}(S)]\right| \ge t\right] \le 2n\gamma^{-1}\beta.$$

Since $\frac{n}{\gamma} \le n^2\rho$, setting $\beta' \leftarrow \frac{\beta}{2n^2\rho}$ and repeating the proof with β' yields the result. □

D.4 When an exact oracle for the loss is unavailable

In this section, we explain how the mechanisms in Appendices D.2 and D.3 can be realized with an oracle L_{approx} that satisfies $L_{\mathrm{approx}}(Z) \le L(Z) + \gamma$ for some sufficiently small $\gamma > 0$. In this case, one cannot directly apply our theorems since L_{approx} need not be monotone. In the two paragraphs below, we discuss a simple method for enforcing monotonicity while maintaining the accuracy guarantees.

Enforcing monotonicity. Instead of applying our mechanisms directly to L_{approx}, we instead use a slightly modified function f defined by $f(Z) = L_{\mathrm{approx}}(Z) + \gamma|Z|$. It is not hard to see that if $S \subsetneq Z$, then $f(Z) - f(S) = L_{\mathrm{approx}}(Z) - L_{\mathrm{approx}}(S) + \gamma(|Z| - |S|)$. Since $L_{\mathrm{approx}}(Z) \ge L(Z)$ and $L_{\mathrm{approx}}(S) \le L(S) + \gamma$, we have $f(Z) - f(S) \ge L(Z) - L(S) - \gamma + \gamma(|Z| - |S|)$. Since L is monotone and $|Z| > |S|$, we have $f(Z) - f(S) \ge 0$, and thus f is monotone.

Maintaining accuracy. While the above transformation enforces monotonicity, it is not immediately obvious how it affects the accuracy guarantees of our mechanisms. Fortunately, an additional simple transformation to L_{approx} suffices to ensure that the accuracy guarantees are preserved up to a constant factor. Consider the following transformation: set $\gamma \approx \alpha/\sqrt{np}$ and define $f(Z) = L_{\mathrm{approx}}(Z) + \gamma|Z| - \gamma np$. By the same argument as above, f is monotone. To see how this affects our accuracy guarantees, observe that the mechanisms of Theorems 2.3 and 2.4 only query f on datasets of size $np \pm \sqrt{np}$ with high probability. Moreover, for a dataset $S \in \mathcal{Z}_{\perp}^n$ of size $|S| = np \pm \sqrt{np}$, we have $f(S) \approx L_{\mathrm{approx}}(S) \pm \gamma\sqrt{np} \approx L(S) \pm \alpha$. Thus, for a sufficiently small setting of α, the accuracy arguments in Appendices D.2 and D.3 will not be affected.

E Query complexity lower bound for monotone statistics

In this section we prove a lower bound on the query complexity of any algorithm that is private for monotone functions and satisfies a weak accuracy guarantee. It will be convenient for the analysis of our lower bound to switch from treating datasets as n-tuples to treating datasets as sets of n distinct elements. For a set $\mathcal{Z}$, let $\mathcal{Z}^*$ denote the set of finite subsets of $\mathcal{Z}$. We say two datasets are neighbors if they have the same size and differ in exactly one element. Note that this is without loss of generality since we can always define the functions in our hard instances to treat n-tuples as sets, however, in the interest of simplifying the notation, we assume that the datasets are sets instead. We assume the dataset size is public, and we say two datasets Z and Z' are neighbors if they are the same size and differ in exactly one element: formally, $|Z| = |Z'|$ and $|Z \cap Z'| = |Z| - 1$.

Before presenting our result, we define a weak accuracy guarantee that the mechanism should satisfy in order for our lower bound to apply.

Definition E.1 ((ν, N)-constant, (p, β)-weakly accurate)**.** *A function $f : \mathcal{Z}^* \to \mathbb{R}$ is (ν, N)-*constant under a distribution $\mathcal{D}$ *if for all $n \geq N$, we have*

$$\Pr_{Z \sim \mathcal{D}^n}[f(Z) = \nu \mid |Z| \geq N] = 1.$$

*An algorithm $\mathcal{A}$ is (p, β)-*weakly accurate for a function f *if for all distributions $\mathcal{D}$ such that f is (ν, N)-constant under $\mathcal{D}$, algorithm $\mathcal{A}$ satisfies*

$$\Pr_{Z \sim \mathcal{D}^{N/p}}\left[\left|\mathcal{A}^f(Z) - \nu\right| \geq 1/2 \mid |Z| = \frac{N}{p}\right] \leq \beta.$$

In other words, the condition "(ν, N)-constant under $\mathcal{D}$" means that once the sample size reaches N, the value of $f(Z)$ is no longer random: for every $n \geq N$, a draw $Z \sim \mathcal{D}^n$ satisfies $f(Z) = \nu$ with probability 1 (so long as Z has enough unique elements). An algorithm $\mathcal{A}$ is "(p, β)-weakly accurate for f" if, for every distribution $\mathcal{D}$ where f becomes such an eventual constant ν, the algorithm can recover ν from only N/p fresh samples—with probability at least $1 - \beta$ over $Z \sim \mathcal{D}^{N/p}$, its output is within additive error $1/2$ of ν, as long as all elements of Z are distinct.

Theorem E.2 (Query complexity lower bound)**.** *Fix a sufficiently small constant $c > 0$. Let $\mathcal{Z} = \mathbb{N}$, and fix range size $\kappa \in \mathbb{N}$, failure probability $\beta \in (0, \frac{1}{4})$, privacy parameters $\varepsilon \in (0, 1)$ and $\delta \in (0, \varepsilon\beta^2)$, and sampling parameter $p \in (0, 1)$. Let*

$$\mathcal{F} = \{f : \mathcal{Z}^* \to [\kappa] \mid f \text{ is monotone}\}.$$

Suppose mechanism $\mathcal{M}^f$ is (ε, δ)-DP and (p, β)-weakly accurate for all $f \in \mathcal{F}$. Let

$$\tau = \frac{c}{\varepsilon} \log \min\left(\frac{\kappa}{\beta}, \frac{\varepsilon}{\delta}\right).$$

If $\tau \leq n$, then $\mathcal{M}^f$ has expected query complexity $\exp(\Omega(p\tau))$ for some $f \in \mathcal{F}$ and $Z \in \mathcal{Z}^n$.

As we will see in the proof, the parameter τ controls the distance between the "bad" datasets we use to show a privacy violation.

Proof. The proof proceeds by constructing a family of monotone functions $\mathcal{F}$, and two families of distributions $\{\mathcal{D}_0\}$ and $\{\mathcal{D}_1\}$ such that every $f \in \mathcal{F}$ is (y_0, N)-constant under some $\mathcal{D}_0$ and (y_1, N)-constant under some $\mathcal{D}_1$. We then argue that for every mechanism $\mathcal{M}$ with query complexity $\exp(o(p\tau))$ that is (p, β)-weakly accurate for $\mathcal{F}$, there exist neighboring inputs X, X' and a function $f \in \mathcal{F}$, such that $\mathcal{M}^f(X) \not\approx_{\varepsilon,\delta} \mathcal{M}^f(X')$, i.e., privacy is violated.

Let $G = [M]$ for some sufficiently large M, and fix t such that $n^2 \ll t \ll M$ (we will set M and t later in the proof). To sample distributions $\mathcal{D}_0$ and $\mathcal{D}_1$, sample $B_0 = \{b_1^0, \ldots, b_t^0\}$ uniformly without replacement from G, and $B_1 = \{b_1^1, \ldots, b_t^1\}$ uniformly without replacement from $G \setminus B_0$. Let $\mathcal{D}_0$ and $\mathcal{D}_1$ be the uniform distributions over B_0 and B_1 respectively. To sample a function $f \in \mathcal{F}$, sample B_0 and B_1, along with integers $y_0 \in [\kappa/2]$ and $y_1 \in [\kappa] \setminus [\kappa/2]$. Let $n = N/p$ and

$\tau = \frac{1}{2\varepsilon} \ln \gamma \min\left(\frac{\kappa}{\beta}, \frac{\varepsilon}{\delta}\right)$ for a sufficiently small absolute constant $\gamma \in (0,1)$. Define

$$f(Z) = \begin{cases} 0 & \text{if } |Z| < N \\ y_0 & \text{else if } Z \subseteq B_0 \\ y_1 & \text{else if } Z \subseteq B_0 \cup B_1 \\ \kappa & \text{otherwise} \end{cases}$$

It is not hard to see that f is monotone, and that it is (y_0, N)-constant and (y_1, N)-constant under the corresponding $\mathcal{D}_0$ and $\mathcal{D}_1$.

To prove the privacy violation, we will sample sets X and X' as follows: Let $X = \{x_1, \ldots, x_n\}$ where $x_1, \ldots, x_\tau$ are sampled uniformly from B_1 without replacement, and $x_{\tau+1}, \ldots, x_n$ are sampled uniformly from B_0 without replacement. Let $X' = \{x'_1, \ldots, x'_\tau, x_{\tau+1}, \ldots, x_n\}$ where $x'_1, \ldots, x'_\tau$ are sampled uniformly from $B_0 \setminus X$ without replacement. Note that $X' \subseteq B_0$ and that X and X' are at distance τ.

Lemmas E.3 and E.4 state that if $\mathcal{M}$ is (ε, δ)-DP and (p, β)-weakly accurate, and if f, X, and X' are sampled as above, then with high probability $\mathcal{M}^f(X')$ will be far from y_1, while $\mathcal{M}^f(X)$ will be close to y_1. Since the bounds we obtain are in terms of the query complexity of $\mathcal{M}$, we can combine them with group privacy to obtain a lower bound on the query complexity of any mechanism satisfying the aforementioned guarantees.

Let parameters $\varepsilon, \delta, \beta, \kappa$, p, and $\mathcal{M}$ be as in Theorem E.2, and let τ, y_1, f, X, and X' be as defined above. Additionally, for all $q \in \mathbb{N}$, an algorithm $\mathcal{A}$ is a *q-query algorithm* if $\mathcal{A}^f$ has expected query complexity at most q for all inputs Z and functions f. Then we can show the following lemmas:

Lemma E.3. *For all $q \in \mathbb{N}$, if $\mathcal{M}$ is a q-query algorithm, then*

$$\Pr\left[\left|\mathcal{M}^f(X') - y_1\right| < \frac{1}{2}\right] \leq \min\left(\beta, \frac{2}{\kappa}\right) + O\left(\frac{tq}{M} + \frac{n^2}{t}\right).$$

Lemma E.4. *For all $q \in \mathbb{N}$, if $\mathcal{M}$ is a q-query algorithm, then*

$$\Pr\left[\left|\mathcal{M}^f(X) - y_1\right| \geq 1/2\right] \leq \beta + qe^{-\Omega(p\tau)} + O\left(\frac{n^2}{t}\right).$$

To prove Lemmas E.3 and E.4, we show that the view of the mechanism on input X' and X is close in TV distance to the view of the mechanism on input $Z' \sim \mathcal{D}_0^n$ and $Z \sim \mathcal{D}_1^n$. We then apply the accuracy guarantee of $\mathcal{M}$ and the fact that y_1 is uniformly random in $[\kappa] \setminus [\kappa/2]$ to deduce each bound. We defer the proofs of Lemmas E.3 and E.4 to the end of the section, and complete the proof of Theorem E.2 below.

Since the lower bound holds trivially for $p = o(1/\tau)$ we assume $p = \Omega(1/\tau)$. Set $q = e^{O(p\tau)}$, set and M and t such that $\frac{qt}{M} + \frac{n^2}{t} = e^{-\omega(\tau)}$ (essentially, this term is small enough that we can ignore it). Suppose $\mathcal{M}$ has query complexity q. Combining Lemmas E.3 and E.4 with group privacy (Fact A.4) yields the desired privacy violation since

$$\begin{aligned} 1 - \beta - e^{-\Omega(\min(p\tau, pn))} &\leq \Pr\left[\left|\mathcal{M}^f(X) - y_1\right| < 1/2\right] \\ &\leq e^{\varepsilon\tau}\left(\Pr\left[\left|\mathcal{M}^f(X') - y_1\right| < 1/2\right] + \delta/\varepsilon\right) \\ &\leq e^{\varepsilon\tau}\left(\min\left(\beta, \frac{2}{\kappa}\right) + \delta/\varepsilon\right). \end{aligned}$$

The first inequality follows from Lemma E.4, the second follows from group privacy and the fact that X and X' are at distance τ, and the third follows from Lemma E.3. If $\tau = \frac{1}{2\varepsilon} \ln \gamma \min\left(\frac{\kappa}{\beta}, \frac{\varepsilon}{\delta}\right)$, $\delta < \varepsilon\beta^2$, and γ is sufficiently small, the right hand side is at most $\frac{1}{2}$. Additionally, since $p = \Omega(1/\tau)$ and $\beta < \frac{1}{4}$, the left hand side is at least $\frac{1}{2}$, which yields the desired contradiction. □

In the remainder of the section we prove Lemmas E.3 and E.4. We first introduce a standard definition for reasoning about the distribution of the view of an algorithm.

Definition E.5 (The view of an algorithm $\mathcal{A}[\mathcal{D}]$)**.** *For all algorithms $\mathcal{A}$, and all distributions $\mathcal{D}$ over tuples $\{(f, I)\}$, let $\mathcal{A}[\mathcal{D}]$ be the distribution over query answer histories $\{(f(J_i), J_i)\}$ when $(f, I) \sim \mathcal{D}$ and $\mathcal{A}^f$ is run on input I.*

One of the main challenges in proving query complexity lower bounds is handling algorithms that make "adaptive" queries to the function. An algorithm $\mathcal{A}$ is *nonadaptive* if given an input Z and query access to f, it specifies all queries $J_1, \ldots, J_q$ after reading Z—that is, its queries to f do not depend on previous query answers. An algorithm $\mathcal{A}$ is *adaptive* if it is not nonadaptive.

In order to argue that the statements hold for algorithms that make adaptive queries to f, we leverage the following idea, which was introduced in [LLRV25] who used it to prove a query complexity lower bound in the context of property testing. While the exact statement of Proposition E.6 does not appear in [LLRV25], it follows readily from their techniques. Informally, Proposition E.6 states that if a q-query nonadaptive algorithm cannot distinguish two distributions $\mathcal{D}_0$ over $\{(f_0, I)\}$ and $\mathcal{D}_1$ over $\{(f_1, I)\}$ when a description of f_0 is always included with its input I, then no q-query adaptive algorithm can distinguish between $\mathcal{D}_0$ and $\mathcal{D}_1$ when the description of f_0 is not included in the input.

Proposition E.6. *Let $\mathcal{D}$ be a distribution over tuples (f_0, f_1, Z) where f_0 and f_1 are functions with domain $\mathcal{Z}^*$ and $Z \in \mathcal{Z}^*$. Define the following distributions:*

- *Let $\mathcal{D}_0$ and $\mathcal{D}_1$ be distributions over tuples (f_0, Z) and (f_1, Z) respectively.*
- *Let $\widetilde{\mathcal{D}}_0$ and $\widetilde{\mathcal{D}}_1$ denote the distributions given by sampling $(f_0, f_1, Z) \sim \mathcal{D}$, and returning $(f_0, (f_0, Z))$ and $(f_1, (f_0, Z))$ respectively.*

Then, for every q-query adaptive algorithm $\mathcal{A}$, there exists a q-query nonadaptive algorithm $\mathcal{A}_{na}$ such that

$$d_{\mathrm{TV}}(\mathcal{A}[\mathcal{D}_0], \mathcal{A}[\mathcal{D}_1]) \le d_{\mathrm{TV}}\Big(\mathcal{A}_{na}[\widetilde{\mathcal{D}}_0], \mathcal{A}_{na}[\widetilde{\mathcal{D}}_1]\Big).$$

Proof. The proof proceeds by a simulation argument. Let $\mathcal{A}$ be a q-query adaptive algorithm that gets input Z and query access to h, and consider the following nonadaptive algorithm $\mathcal{A}_{na}$ that gets input (g, Z) and query access to h:

1. Simulate $\mathcal{A}$ and answer its queries $J_1, \ldots, J_Q \in \mathcal{Z}^*$ using g (i.e., return $g(J_i)$).
2. Nonadaptively query h on $J_1, \ldots, J_Q$. If $h(J_i) = g(J_i)$ for all $i \in [Q]$ then return 0, otherwise return 1.

Let $\mathcal{V}$ be a coupling over views $(v_0, v_1) \sim (\mathcal{A}[\mathcal{D}'_0], \mathcal{A}[\mathcal{D}'_1])$, where both runs of $\mathcal{A}$ are executed using the same random coins and the inputs are sampled jointly as $(f_0, f_1, Z) \sim \mathcal{D}$. By the coupling lemma

$$d_{\mathrm{TV}}(\mathcal{A}[\mathcal{D}_0], \mathcal{A}[\mathcal{D}_1]) \le \Pr[v_0 \neq v_1].$$

Next, we show that $\Pr[v_0 \neq v_1] \le d_{\mathrm{TV}}\Big(\mathcal{A}_{na}[\widetilde{\mathcal{D}}_0], \mathcal{A}_{na}[\widetilde{\mathcal{D}}_1]\Big)$. Let E be the set of query answer histories $\{(h(J_i), J_i)\}$ such that $h(J_i) \neq g(J_i)$ for some i. Observe that $\Pr_{\widetilde{v}_0 \sim \mathcal{A}_{na}[\widetilde{\mathcal{D}}_0]}[\widetilde{v}_0 \in E] = 0$ since $h = g$ when the input is sampled from $\widetilde{\mathcal{D}}_0$. On the other hand, when the input is sampled from $\widetilde{\mathcal{D}}_1$, event E occurs if and only if $v_0 \neq v_1$ (since otherwise $h(J_i) = g(J_i)$ for all queries). Thus,

$$\begin{aligned}
\Pr[v_0 \neq v_1] &\le \Pr_{\widetilde{v}_1 \sim \mathcal{A}_{na}[\widetilde{\mathcal{D}}_1]}[\widetilde{v}_1 \in E] \\
&= \left| \Pr_{\widetilde{v}_1 \sim \mathcal{A}_{na}[\widetilde{\mathcal{D}}_1]}[\widetilde{v}_1 \in E] - \Pr_{\widetilde{v}_0 \sim \mathcal{A}_{na}[\widetilde{\mathcal{D}}_1]}[\widetilde{v}_0 \in E] \right| \\
&\le d_{\mathrm{TV}}\Big(\mathcal{A}_{na}[\widetilde{\mathcal{D}}_0], \mathcal{A}_{na}[\widetilde{\mathcal{D}}_1]\Big),
\end{aligned}$$

which completes the proof. □

We now complete the proofs of Lemmas E.3 and E.4. We will abuse notation and treat f as both a function and a random variable whose distribution is given by the procedure for sampling B_0 and B_1 described in the proof of Theorem E.2. We will also define two additional functions h and g in the

proofs of Lemmas E.3 and E.4 respectively. As with f, we abuse notation and treat g and h as both functions and random variables whose distributions are given by the procedure for sampling B_0, B_1, y_0, and y_1, in the proof of Theorem E.2.

Proof of Lemma E.3. Let $\mathcal{D}'$ denote the distribution over pairs (f, X') sampled as in the proof of Theorem E.2. Define the function

$$h(Z) = \begin{cases} 0 & \text{if } |Z| < N \\ y_0 & \text{else if } Z \subseteq B_0 \\ \kappa & \text{otherwise.} \end{cases}$$

Let $\mathcal{D}''$ denote the distribution over pairs of the form (h, Z) where h is sampled by sampling B_0, and y_0 as in the proof of Theorem E.2, and $Z \sim \mathcal{D}_0^n$. We will first show that the bound holds when the input is sampled from $\mathcal{D}''$. Then, we will complete the argument by bounding the TV distance between $\mathcal{M}[\mathcal{D}']$ and $\mathcal{M}[\mathcal{D}'']$.

Since $Z \sim \mathcal{D}_0^n$ is a subset of B_0 with probability 1, the function h is (y_0, N)-constant under $\mathcal{D}_0$. To prove the first part of the bound, observe that since $|y_0 - y_1| \geq 1$, and a sample of n i.i.d. elements from $\mathcal{D}_0^n$ contains a collision with probability $O(n^2/t)$, the accuracy guarantee of $\mathcal{M}$ implies that $\Pr_{Z \sim \mathcal{D}_0^n}\left[\left|\mathcal{M}^h(Z) - y_1\right| < 1/2\right] \leq \beta + O\big(n^2/t\big)$. The $2/\kappa$ part of the bound holds since the distribution of y_1 is uniformly random over $[\kappa] \setminus [\kappa/2]$ even when conditioned on the input Z and a complete description of the function h.

To complete the argument, we bound the TV distance between $\mathcal{A}[\mathcal{D}']$ and $\mathcal{A}[\mathcal{D}'']$ for any q-query algorithm $\mathcal{A}$. Let $\mathcal{D}^*$ denote the distribution over pairs (h, X') where h and X' are sampled as above.

Claim E.7. *Let $\mathcal{A}$ be a q-query algorithm. Then,*

$$d_{\mathrm{TV}}(\mathcal{A}[\mathcal{D}'], \mathcal{A}[\mathcal{D}^*]) \leq O\left(\frac{qt}{M}\right).$$

Proof. For a fixed B_0 and B_1 and a query J, if $f(J) \neq h(J)$, then $|J| \geq N$ and $J \subseteq B_0 \cup B_1$ and $J \cap B_1 \neq \emptyset$.

We first consider nonadaptive algorithms $\mathcal{A}_{na}$ that are given additional input (B_0, y_0). Since B_0 and y_0 uniquely determine h, we can leverage Proposition E.6 to lift the argument to adaptive algorithms.

To bound the probability that the algorithm makes a query J such that $f(J) \neq h(J)$, it will be convenient to view the distribution over h, f and X' as follows: Instead of sampling B_0 and B_1 and then sampling X', we can equivalently first sample an X', then sample the remaining $t - n$ elements of B_0, and finally sample the t elements of B_1 from $G \setminus B_0$. Now, fix some query J made by $\mathcal{A}_{na}$ on input X' and (B_0, y_0). Over the randomness of B_1, the probability that $J \subseteq B_0 \cup B_1$ and $J \cap B_1 \neq \emptyset$ is at most the probability that the elements in $J \setminus B_0$ are in B_1. Since $|B_1| = t$ and $|G| = M$, the probability is at most $O\big(\frac{t}{M}\big)$. Let Q be a random variable denoting the number of queries made by $\mathcal{A}_{na}$ and denote the random queries $J_1, \ldots J_Q$. Since $\mathcal{A}_{na}$ has expected query complexity q, we can apply the union bound to see that

$$\Pr\left[\bigcup_{i=1}^{Q} \{f(J_i) \neq h(J_i)\}\right] \leq \mathop{\mathbb{E}}_{Q}\left[\sum_{i=1}^{Q} \Pr[f(J_i) \neq h(J_i) \mid Q]\right] \leq O\left(\frac{qt}{M}\right).$$

Since $\mathcal{A}_{na}$ is provided with a complete description of h as input, we can apply Proposition E.6 to complete the proof. □

Claim E.8. *For all algorithms $\mathcal{A}$ we have*

$$d_{\mathrm{TV}}(\mathcal{A}[\mathcal{D}^*], \mathcal{A}[\mathcal{D}'']) \leq O\left(\frac{n^2}{t}\right).$$

Proof. Since $\mathcal{D}^*$ and $\mathcal{D}''$ both have the same distribution over the function and only differ in distribution on the dataset, it suffices to bound the TV distance between the distributions of X' and Z. Notice that X' is defined by sampling n points from B_0 uniformly without replacement, while Z

is given by sampling n points uniformly and independently from B_0. Conditioned on the event that Z does not contain a collision, these distributions are the same. Since Z is uniform over B_1, a set of size t, it contains a collision with probability $O(n^2/t)$, and thus the TV distance between X' and Z is $O(n^2/t)$. □

By the triangle inequality and Claims E.7 and E.8, we have $d_{\mathrm{TV}}(\mathcal{A}[\mathcal{D}'], \mathcal{A}[\mathcal{D}'']) \le O\left(\frac{qt}{M} + \frac{n^2}{t}\right)$. It follows that

$$\Pr\left[\left|\mathcal{M}^f(X') - y_1\right| < 1/2\right] \le \min\left(\beta, \frac{2}{\kappa}\right) + O\left(\frac{qt}{M} + \frac{n^2}{t}\right),$$

which completes the proof of the lemma. □

Proof of Lemma E.4. The proof is similar to that of Lemma E.3. Let $\mathcal{D}'$ denote the distribution over (f, X) in the proof of Theorem E.2 and let $\mathcal{D}''$ denote the distribution over (f, Z) where $Z \sim \mathcal{D}_1^n$. We aim to bound $d_{\mathrm{TV}}(\mathcal{M}[\mathcal{D}'], \mathcal{M}[\mathcal{D}''])$. Since f is (y_1, N)-constant under $\mathcal{D}_1$, the accuracy guarantee of $\mathcal{M}$ and the TV distance bound together imply the result.

In order to facilitate the argument, we introduce an intermediate function g defined as

$$g(Z) = \begin{cases} 0 & \text{if } |Z| < N \\ y_1 & \text{else if } Z \subseteq B_0 \cup B_1 \\ \kappa & \text{otherwise.} \end{cases}$$

Let $\widetilde{\mathcal{D}}'$ and $\widetilde{\mathcal{D}}''$ denote the distributions over pairs (g, X) and (g, Z) respectively.

Claim E.9. *For any q-query algorithm $\mathcal{A}$ we have*

$$d_{\mathrm{TV}}\left(\mathcal{A}[\mathcal{D}'], \mathcal{A}[\widetilde{\mathcal{D}}']\right) \le q e^{-\Omega(p\tau)}.$$

Proof. Observe that for any query J, if $f(J) \neq g(Z)$ then $J \subseteq B_0$ and $|J| \ge N$. Thus, in order to bound the TV distance between $\mathcal{A}[\mathcal{D}']$ and $\mathcal{A}[\widetilde{\mathcal{D}}']$ it suffices to bound the probability that any query J of size at least N is a subset of B_0.

Let $B = B_0 \cup B_1$. We first prove the claim for nonadaptive algorithms $\mathcal{A}_{na}$ that are given additional input (B, y_1), and then use Proposition E.6 to prove the bound for adaptive algorithms. We note that $\mathcal{A}_{na}$ is given B for free, but is not provided with the partition of B into B_0 and B_1. Since B_0 and B_1 are chosen uniformly at random without replacement from G, we can equivalently sample them by first sampling the set B, and then sampling B_0 by choosing t elements uniformly without replacement from B, and letting B_1 be the remaining t elements. Additionally, since X consists of a uniform set of τ distinct elements from B_1 and $n - \tau$ distinct elements from B_0, the distribution of B_0 and B_1 conditioned on B and X is equivalent to the following distribution: First sample τ elements at random from X and place them in B_1 and place the remaining $n - \tau$ elements in B_0. Second, partition the remaining $2t - n$ elements from B by choosing $t - \tau$ elements uniformly and placing them in B_1 and placing the remaining $t - n + \tau$ elements in B_0.

Below, we leverage this alternative view of the sampling process to prove the bound for nonadaptive algorithms.

Fix a query J, and let J_X and $J_{\overline{X}}$ denote $J \cap X$ and $J \setminus X$. Recall that X is composed of τ distinct elements from B_1, and thus, over the randomness of B_1, the probability that J_X is a subset of B_0 is the probability that no element in J_X is placed in B_1. Since the τ elements from B_1 are chosen uniformly at random without replacement from X, a set with n elements, we have

$$\Pr\left[J_X \subseteq B_0\right] \le \left(1 - \frac{|J_X|}{n}\right)^{\tau} \le \exp\left(-|J_X| \cdot \frac{\tau}{n}\right).$$

Similarly, over the randomness of the partition of the elements in $B \setminus X$ into B_0 and B_1, the probability that $J_{\overline{X}} \subseteq B_0$ is at most $\exp\left(\Omega(-|J_{\overline{X}}|)\right)$.

Since the partition of the elements in X and $B \setminus X$ is chosen independently, the events $J_X \subseteq B_0$ and $J_{\overline{X}} \subseteq B_0$ are independent. Hence, for all $\tau \leq n$ we have

$$\Pr[J \subseteq B_0] = \Pr[J_X \subseteq B_0] \Pr[J_{\overline{X}} \subseteq B_0] \leq \exp\left(-\Omega\left(\frac{\tau}{n}(|J_X| + |J_{\overline{X}}|)\right)\right).$$

Since $|J| \geq N = pn$, we obtain $\Pr[J \subseteq B_0] \leq e^{-\Omega(p\tau)}$. A union bound as in the proof of Claim E.7 implies the bound for nonadaptive algorithms. Since B and y_1 uniquely determine the function g, we can apply Proposition E.6 and lift the bound to adaptive algorithms. □

Claim E.10. *For any q-query algorithm $\mathcal{A}$ we have*

$$d_{\mathrm{TV}}\left(\mathcal{A}[\mathcal{D}''], \mathcal{A}[\widetilde{\mathcal{D}}'']\right) \leq q \cdot e^{-\Omega(pn)}.$$

Proof. Fix a query J made by $\mathcal{A}$, and observe that if $J \subseteq Z$ then $f(J) = g(J)$. Thus, we can assume without loss of generality that $J \not\subseteq Z$. If $f(J) \neq g(J)$ then $|J| \geq N$ and $J \subseteq B_0$. We first prove the bound for a nonadaptive algorithm $\mathcal{A}_{na}$ that is given additional input (B, y_1) where $B = B_0 \cup B_1$. Note that this uniquely determines the function h, but conditioned on B and Z, the distribution over B_0 is equivalent to sampling t distinct elements uniformly from $B \setminus Z$, and thus, each element is included with probability $\frac{t}{2t-n} \leq \frac{2}{3}$.

Since $Z \sim \mathcal{D}_1^n$ we have that $Z \subseteq B_1$ and thus, if $f(J) \neq g(J)$ then J must contain at least N elements from B_0 and no elements from $G \setminus B_0$. But over the random sampling of B_0 conditioned on Z and B we have $\Pr[J \subseteq B_0] \leq e^{-\Omega(N)}$. A union bound argument as in the proof of Claim E.7 suffices to prove the bound for nonadaptive algorithms. Applying Proposition E.6 completes the proof. □

Claim E.11. *For any q-query algorithm $\mathcal{A}$ we have*

$$d_{\mathrm{TV}}\left(\mathcal{A}[\widetilde{\mathcal{D}}'], \mathcal{A}[\widetilde{\mathcal{D}}'']\right) \leq O\left(\frac{n^2}{t}\right).$$

Proof. Since B_0 and B_1 are sampled uniformly without replacement from G, the set $B_0 \cup B_1$ is sampled uniformly without replacement from G, as well. Let $B = B_0 \cup B_1$. Then since g only depends on the elements in B, and not on the partition of B into B_0 and B_1, the distribution $\widetilde{\mathcal{D}}'$ is the same whether X is sampled by choosing τ elements from B_0 and $n - \tau$ elements from B_1, or instead by choosing n uniformly random elements from B (without replacement). Similarly, conditioned on the event that there are no collisions in the sampling of Z from B_1, the distribution of $\widetilde{\mathcal{D}}''$ is the same whether Z is sampled from $\mathcal{D}_1^n$, or instead sampled uniformly without replacement from B. Thus, conditioned on the event that Z does not contain any collisions, the distributions $\widetilde{\mathcal{D}}'$ and $\widetilde{\mathcal{D}}''$ are equivalent, and hence, the TV distance between $\mathcal{A}[\widetilde{\mathcal{D}}']$ and $\mathcal{A}[\widetilde{\mathcal{D}}'']$ is at most the probability that Z contains a collision. Since Z consists of n independent and uniform samples from B_1, a set of size t, the probability of a collisions is at most $O(n^2/t)$. □

To complete the proof of Lemma E.4, it suffices to apply the triangle inequality and the above claims to obtain,

$$d_{\mathrm{TV}}(\mathcal{M}[\mathcal{D}'], \mathcal{M}[\mathcal{D}'']) \leq q e^{-\Omega(\min\{p\tau, pn\})} + O\left(\frac{n^2}{t}\right).$$

Since $Z \sim \mathcal{D}_1^n$ contains a collision with probability at most $O\big(n^2/t\big)$, the (p, β) accuracy guarantee of $\mathcal{M}$ and the TV distance bound yields the result. □

F Technical discussion of existing guarantees

In this section we present some minor extensions to the guarantees provided in prior work. The arguments are standard; we present them to give a more complete comparison with our results.

F.1 Extension of [LRSS25]

The work of [LRSS25] gives algorithms for privately evaluating arbitrary functions. They achieve nearly optimal error and sample complexity but require exponentially many queries (and thus exponential time). In this section, we discuss how amplification by subsampling allows one to reduce the time complexity at the cost of increased error. The same techniques would apply identically to the algorithms of [FDY22].

In the setting of Section 1.1, amplification by subsampling achieves the following tradeoff: sample complexity $\frac{N \log \kappa/\beta}{t\varepsilon}$ at a cost of runtime N^t. In contrast, our work achieves the same sample complexity at a cost of runtime e^t, but is restricted to monotone functions. This difference is significant for all settings of t, however it is most striking when $t = \Theta(\log N)$, in which case our mechanisms run in time $\operatorname{poly} N$, whereas the application of [LRSS25] runs in time $N^{\Theta(\log N)}$.

Recall Assumption 1.1: there exists some $\nu \in \mathbb{R}$ and $N : \mathbb{R} \to \mathbb{R}$ such that if $n \geq N(\alpha) + \frac{\log 1/\beta}{\alpha^2}$ and $Z \sim \mathcal{D}^n$, then $|f(Z) - \nu| \leq \alpha$ with probability at least $1 - \beta$. In this setting, amplification by subsampling and [LRSS25] achieve the following tradeoff.

Theorem F.1. *Fix range size $\kappa > 0$, privacy parameter $\varepsilon \in (0, 1]$, failure probability $\beta > 0$, and tradeoff parameter $t \leq \frac{1}{\varepsilon} \log \frac{\kappa}{\beta}$. There exists a mechanism $\mathcal{M}$ such that for all functions $f : \mathcal{Z}^* \to [\kappa]$ mechanism $\mathcal{M}^f$ is ε-DP, and on datasets of size n has query complexity and runtime $n^{O(t \log \frac{\kappa}{\beta})}$. Additionally, if f and $\mathcal{D}$ satisfy Assumption 1.1, then for all $\alpha > 0$ and*

$$n = \Omega\left(\frac{N(\alpha) \log \kappa/\beta}{t\varepsilon} + \frac{\log \kappa/\beta \log 1/\beta}{t\alpha^2\varepsilon} + \frac{\log \kappa/\beta \log n}{\alpha^2\varepsilon}\right)$$

we have

$$\Pr_{Z \sim \mathcal{D}^n}\left[\left|\mathcal{M}^f(Z) - \nu\right| \geq \alpha\right] \leq \beta.$$

While Theorem F.1 applies to bounded range functions, analogous to Theorem 2.3, a similar result can be shown for the setting of functions with range $\mathbb{R}$, analogous to Theorem 2.4. Additionally, for simplicity we only compare to the pure DP version of "sens-o-matic" (Theorem 3.1 in [LRSS25]); however, we can obtain a similar guarantee to their approximate DP version by substituting a generalized interior point mechanism for the exponential mechanism used to compute the median in Algorithm 2. Indeed, this is exactly the approach taken by [LRSS25] to obtain their approximate DP result. We apply standard amplification by subsampling for pure DP.

Proposition F.2 (Privacy Amplification by Subsampling, [FVH25], Theorem 3.28)**.** *Let $\mathcal{M} : \mathcal{Z}_\perp^* \to \mathcal{Y}$ satisfy ε-DP. For $p \in (0, 1)$, define $\mathcal{M}_p(Z) = \mathcal{M}(S)$ where $S \sim \mathcal{S}_p(Z)$, i.e., we set each element of Z to $\perp$ independently with probability p and then run $\mathcal{M}$. Then $\mathcal{M}_p$ is ε'-DP for $\varepsilon' = \log(1 + p(e^\varepsilon - 1))$. In particular, if $\varepsilon \leq 1$ then $\varepsilon' \leq 2p\varepsilon$.*

In order to state the guarantee of the sens-o-matic mechanism, we define the following notation: For a parameter $\lambda \in \mathbb{N}$ and a dataset $Z \in \mathcal{Z}^*$, let $N_\lambda(Z) = \{S \subseteq Z \mid |S| \geq |Z| - \lambda\}$, that is $N_\lambda(Z)$ is the set of subsets of Z given by removing up to λ points from Z. Additionally, for a function f, we let $f(N_\lambda(Z))$ denote the set $\{f(S) \mid S \in N_\lambda(Z)\}$.

Theorem F.3 ([LRSS25], Theorem 3.1, pure DP)**.** *Fix privacy parameter $\varepsilon > 0$, error probability, $\beta > 0$, and range size $\kappa \in \mathbb{N}$, there exist a mechanism $\mathcal{M}$ such that for every function $f : \mathcal{Z}^* \to [\kappa]$ and dataset $Z \in \mathcal{Z}^n$, with probability at least $1 - \beta$,*

$$\mathcal{M}^f(Z) \in \left[\min f\big(N_\lambda(Z)\big), \max f\big(N_\lambda(Z)\big)\right],$$

where $\lambda = O\big(\frac{1}{\varepsilon} \log \frac{\kappa}{\beta}\big)$.

With these in hand, the proof of Theorem F.1 is almost immediate.

Proof sketch. We subsample $S \subseteq Z$ by including each element with probability $p \geq \varepsilon$ and then run the sens-o-matic mechanism with privacy parameter ε/p and failure probability β. This mechanism is 2ε-DP and runs in time $(pn)^{O\left(\frac{p}{\varepsilon} \log \frac{\kappa}{\beta}\right)}$.

To see why accuracy holds, observe that sens-o-matic queries the function f on all subsets of the input dataset S given by removing at most $\frac{p}{\varepsilon} \log \frac{\kappa}{\beta}$. Since there are at most $n^{O\left(\frac{p}{\varepsilon} \log \frac{\kappa}{\beta}\right)}$ such subsets,

the applying Assumption 1.1 and the union bound implies that all subsets are within α of ν, and thus the mechanism outputs a y such that $|y - \nu| \le \alpha$. Reparameterizing $p = \varepsilon t$ yields the result. □

F.2 Translating [SS25] to our setting

In this section, we translate the guarantees provided by [SS25] to our setting. Specifically, we explain how their result yields a similar tradeoff between sample and *query* complexity for general functions—that is, one can save a factor of t over the sample complexity of subsample-and-aggregate, while paying a factor of e^t in query complexity. However, as discussed in the introduction, the mechanism in Theorem F.5 nevertheless has runtime $n^{O\left(\frac{1}{\varepsilon}\log\frac{1}{\delta}\right)}$.

Below, we state an informal corollary of [SS25] in the style of Theorem 1.2. Recall, that we are interested in functions f and distributions $\mathcal{D}$ that satisfy Assumption 1.1—that is, there exists $\nu \in \mathbb{R}$ and $N = N(\alpha)$ such that if $n \ge N + \frac{\log 1/\beta}{\alpha^2}$ and $Z \sim \mathcal{D}^n$ then $|f(Z)/n - \nu| \le \alpha$ with probability at least $1 - \beta$. Since the mechanism of [SS25] is for functions $f : \mathcal{Z}^* \to [\kappa]$ that need not be monotone, we modify this assumption to remove the normalization by n—that is, we make the slightly more general assumption that

$$\text{if } \; n \ge N + \frac{\log 1/\beta}{\alpha^2} \; \text{ then } \; \Pr_{Z\sim\mathcal{D}^n}\left[|f(Z) - \nu| \ge \alpha\right] \le \beta. \tag{6}$$

For functions and distributions that satisfy (6), the mechanism of [SS25] yields the following result:

Corollary F.4 (Corollary of [SS25])**.** *Fix privacy parameters $\varepsilon, \delta > 0$, and $t \le \widetilde{O}\left(\frac{1}{\varepsilon}\log\frac{1}{\delta}\right)$. There exists a mechanism $\mathcal{M}$ such that for all functions $f : \mathcal{Z}^* \to [\kappa]$ mechanism $\mathcal{M}^f$ is (ε, δ)-DP, has query complexity $\widetilde{O}\left(e^t \cdot \frac{\log(1/\delta)\log(n)}{\varepsilon}\right)$, and has runtime $n^{\widetilde{O}\left(\frac{1}{\varepsilon}\log\frac{1}{\delta}\right)}$. Additionally, if f and $\mathcal{D}$ satisfy (6), then for all $\alpha, \beta > 0$ and*

$$n = \widetilde{\Omega}\left(\frac{N(\alpha)\log 1/\delta}{t\varepsilon} + \frac{\log 1/\delta \log 1/\beta}{t\alpha^2\varepsilon} + \frac{\log 1/\delta}{\alpha^2\varepsilon} + \frac{\log(1/\delta)^2}{\varepsilon^2 t}\right)$$

we have

$$\Pr_{Z\sim\mathcal{D}^n}\left[\left|\mathcal{M}^f(Z,\alpha) - \nu\right| \ge \alpha\right] \le \beta.$$

Here $\widetilde{O}$ and $\widetilde{\Omega}$ hide an additional factor of $\exp(O(\log^* \kappa))$.

Proof sketch. The proof is a special case of the main result of [SS25] which we state below.

Theorem F.5 (Theorem 1.1 [SS25])**.** *Let $\mathcal{Y} \subseteq \mathbb{R}$ be finite and let $\mathcal{X}$ be arbitrary; denote $\mathcal{X}^* = \bigcup_{n\in\mathbb{N}} \mathcal{X}^n$. Let $\varepsilon, \delta > 0$ and $n, m, \tau \in \mathbb{N}$ satisfy*

$$n \ge m \ge \tau = \frac{1}{\varepsilon}\log(1/\delta)\exp(O(\log^* |\mathcal{Y}|)).$$

Let

$$k = \frac{\binom{n}{\tau}}{\binom{m}{\tau}}\left(1 + \log\binom{m}{\tau}\right) + 1$$

Then, for all $f : \mathcal{X}^* \to \mathcal{Y}$, there exists an algorithm $\mathcal{M}^f : \mathcal{X}^n \to \mathcal{Y}$ with the following properties.

- ***Privacy:*** *$\mathcal{M}^f$ is (ε, δ)-differentially private.*
- ***Statistical Accuracy:*** *Let $\mathcal{D}$ be an arbitrary probability distribution on $\mathcal{X}$. Suppose*

  $$\Pr_{X\leftarrow\mathcal{D}^{n-m}}\left[|f(X) - \nu| \le \alpha\right] \ge 1 - \beta$$

  for some $\alpha, \beta, \nu \in \mathbb{R}$. Then

  $$\Pr_{X\leftarrow\mathcal{D}^n}\left[|\mathcal{M}^f(X) - \nu| \le \alpha\right] \ge 1 - k\beta$$

- ***Oracle Efficiency:*** *On input $x \in \mathcal{X}^n$, mechanism $\mathcal{M}^f(x)$ selects $O(k)$ subsets of x, each of size $n - m$, and evaluates f on those subsets; other than these k evaluations, $\mathcal{M}^f(x)$ does not depend on either f or x.*

Recall that in our setting, we trade off between sample and time complexity by changing the subsampling probability p used in Theorems 2.3 and 2.4. Since our mechanisms query f on subsets at depth approximately pn, the relevant point of comparison is when $m = (1-p)n$. The following proposition allows us to bound the query complexity of $\mathcal{M}$, the mechanism in Theorem F.5, when $m = (1-p)n$.

Proposition F.6. *Fix $n, \tau \in \mathbb{N}$ and $p \in (0,1)$. If $\tau < (1-p)n$ and $p \geq 2\tau/n$ then*

$$\frac{\binom{n}{\tau}}{\binom{(1-p)n}{\tau}} \leq e^{p\tau}.$$

Proof. Expanding the binomial coefficients we obtain

$$\frac{\binom{n}{\tau}}{\binom{(1-p)n}{\tau}} = \prod_{i=0}^{\tau-1} \frac{n-i}{(1-p)n-i}.$$

Since $\frac{n-i}{(1-p)n-i} \leq \frac{n}{(1-p)n-(\tau-1)}$, we see that

$$\frac{\binom{n}{\tau}}{\binom{(1-p)n}{\tau}} \leq \left(\frac{n}{(1-p)n-(\tau-1)}\right)^{\tau} \leq \left(\frac{1}{(1-p)-\tau/n}\right)^{\tau}.$$

Since $p > 2\tau/n$ we have $1 - p - \tau/n \geq 1 - p/2$ the above is at most $e^{p\tau}$. □

Now, since all subsets are of size pn, we can apply (6) to see that if $n \geq \frac{N(\alpha)}{p} + \frac{\log 1/\beta}{\alpha^2 p}$ then the statistical accuracy assumption in Theorem F.5 will hold. Scaling $\beta \leftarrow \beta \cdot e^{-p\tau}$, we see that $\left|\mathcal{M}^f(X) - \nu\right| \leq \alpha$ with probability at least $1 - \beta$.

To obtain the desired tradeoff and complete the proof sketch we can simply set $p = \frac{t}{\tau}$. □

G Related work for applications

G.1 Subsample-and-aggregate baseline

In this section we formalize the baseline provided by the subsample-and-aggregate framework explained in the introduction. Recall that we are interested in providing accuracy guarantees for functions f and distributions $\mathcal{D}$ satisfying Assumption 1.1, which states that there exists N and ν such that for all $n \geq N(\alpha) + \frac{\log 1/\beta}{\alpha^2}$ we have $\left|\frac{f(Z)}{n} - \nu\right| \leq \alpha$ with probability at least $1 - \beta$ over the sampling of $Z \sim \mathcal{D}^n$.

Proposition G.1 (Subsample-and-aggregate baseline)**.** *For all $\varepsilon, \delta > 0$ there exists an (ε, δ)-DP mechanism $\mathcal{M}$ such that for all f and $\mathcal{D}$ that satisfy Assumption 1.1, and all $\alpha, \beta > 0$ the following holds: If*

$$n = \Omega\left(\frac{N(\alpha)\log(1/\beta\delta)}{\varepsilon} + \frac{\log(1/\beta\delta)}{\alpha^2\varepsilon}\right)$$

then

$$\Pr_{Z\sim\mathcal{D}^n}\left[\left|\mathcal{M}^f(Z) - \nu\right| \geq 3\alpha\right] \leq \beta.$$

Moreover, $\mathcal{M}$ runs in time $O\left(\frac{1}{\varepsilon}\log\frac{1}{\beta\delta}\right)$

Remark G.2. While we only include a formal result for the $\delta > 0$ case, for functions with finite range of size κ the standard exponential mechanism for median is $(\varepsilon, 0)$-DP and has the same sample complexity with $1/\delta$ replaced by κ/β.

Proof. We use the Stable Histograms approach as in [KV18]. The exact guarantees we cite appear in Appendix C of [BGS+21].

Lemma G.3 (Stable Histogram guarantees)**.** *There exists a constant $C > 0$ and an (ε, δ)-differentially private mechanism $\mathcal{A}_{\varepsilon,\delta}$ that gets as input a set of bins $\{B_b\}_{b\in\mathbb{Z}}$ and a dataset $Z = z_1, \ldots, z_n$ drawn i.i.d. from distribution P, and satisfies the following guarantees: Suppose that there exists $b \in \mathbb{Z}$ and a constant $\beta' < \frac{1}{4}$, such that $\Pr[z_i \notin B_{b-1} \cup B_b \cup B_{b+1}] \le \beta'$ for any fixed $i \in [n]$. Then for all $\varepsilon, \beta, \delta \in (0, 1)$, if*

$$n \ge \frac{C}{\varepsilon} \log \frac{1}{\beta\delta},$$

then $\mathcal{A}_{\varepsilon,\delta}(z_1, \ldots, z_k) \in \{b-1, b, b+1\}$ with probability at least $1 - \beta$.

Let C and $\mathcal{A}_{\varepsilon,\delta}$ be as in Lemma G.3. We define $\mathcal{M}^f(Z)$ as follows: *Partition Z into $k = \frac{C}{\varepsilon} \log \frac{1}{\beta\delta}$ datasets $\widetilde{Z}_1, \ldots, \widetilde{Z}_k$ of equal size. Let $y_i \leftarrow f(\widetilde{Z}_i)/n$ for each $i \in [k]$ and let $b^* \leftarrow \mathcal{A}_{\varepsilon,\delta}(y_1, \ldots, y_k)$ run with buckets B_i defined by a partition of $\mathbb{R}$ into intervals of size α. Release the midpoint of B_{b^*}*

Privacy of $\mathcal{M}$ follows immediately from the privacy guarantees of $\mathcal{A}_{\varepsilon,\delta}$. To see why accuracy holds, observe that by our setting of n, each bucket B_i consists of at least $N(\alpha) + \frac{\log 5}{\alpha^2}$ i.i.d. samples from $\mathcal{D}$. Hence, by our assumption on f and $\mathcal{D}$, there exists a $b \in \mathbb{N}$ such that $\nu \in B^* = B_{b-1} \cup B_b \cup B_{b+1}$ and $\Pr[y_i \notin B^*] \le 1/5$ for each $i \in [k]$, and therefore, $\mathcal{A}_{\varepsilon,\delta}(y_1, \ldots, y_k)$ returns a $b^* \in \{b-1, b, b+1\}$ with probability at least $1 - \beta$. Since $\nu \in B^*$, the midpoint of B_{b^*} is at distance at most 3α from ν, and $\left|\mathcal{M}^f(Z) - \nu\right| \le 3\alpha$ with probability at least $1 - \beta$. Runtime follows by inspection of $\mathcal{M}$ and algorithm 3 in Appendix C of [BGS+21]. □

G.2 Eigenvalue estimation

We compare with Theorem C.1, which with probability $1 - \beta$ gives a $1 \pm \alpha$ approximation to the i-th eigenvalue of the covariance given

$$n = \Omega\left(\frac{1}{\alpha^2}\left(\frac{d + \log(1/\beta)}{p} + \frac{\log(1/\delta)}{\varepsilon} + \frac{\log(p^{-1}\log 1/\delta)}{p}\right)\right)$$

samples from a d-dimensional subgaussian distribution. Here $p \in (0, 1/4)$ is the subsampling hyperparameter (Throughout this section, we suppress the subgaussian constant $K_{\mathcal{D}}$.) The algorithm runs in time $\exp\left(O\left(\frac{p \log 1/\delta}{\varepsilon}\right)\right) \operatorname{poly}\left(\frac{\log 1/\delta}{p}\right)$.

Subsample-and-aggregate yields the same guarantee with

$$n \gtrsim \Omega\left(\frac{d \log(1/\delta\beta)}{\alpha^2 \varepsilon}\right).$$

Off-the-shelf, any spectral approximation $\hat{\Sigma}$ of the true covariance Σ immediately leads to multiplicative eigenvalue approximations. if $(1-\alpha)\Sigma \preceq \hat{\Sigma} \preceq (1+\alpha)\Sigma$ then for all $i \in [d]$

$$(1-\alpha)\lambda_i(\Sigma) \le \lambda_i(\hat{\Sigma}) \le (1+\alpha)\lambda_i(\Sigma).$$

This is because the Löwner order "$\preceq$" is monotone under λ_i. It is beyond the scope of this work to survey the landscape of differentially private covariance estimation. In the setting we consider, producing such a private approximation to the entire covariance requires $n \gtrsim d^{3/2}$ samples, a polynomial-in-d overhead. See [DTTZ14, Nar24, PH25] for lower bounds and some discussion of existing algorithms.

The StableCovariance estimator of [BHS23] gives a direct way to estimate a single eigenvalue. Once $n \gtrsim \frac{\log(1/\delta)}{\varepsilon}$, on adjacent datasets Z and Z' the algorithm returns[6] non-private covariance estimates Σ_1 and Σ_2 such that $(1-\gamma)\Sigma_1 \preceq \Sigma_2 \preceq (1+\gamma)\Sigma_1$ for $\gamma = O(d/n)$. Once n is large enough to make γ a small constant, this leads to

$$|\log \lambda_i(\Sigma_1) - \log \lambda_i(\Sigma_2)| \le O(d/n).$$

[6] Formally, the algorithm either fails or returns covariance estimates which satisfy this guarantee. On data from a subgaussian distribution, with high probability it does not fail.

Therefore, we can add Laplace noise to $\log(\lambda_i(\Sigma_1))$ and obtain a multiplicative $1 \pm \alpha$ approximation to the underlying i-th eigenvalue as long as

$$n \gtrsim \frac{d}{\alpha^2} + \frac{d}{\alpha\varepsilon} + \frac{d\log(1/\delta)}{\varepsilon}.$$

Finally, we note that under additional assumptions on the data one can directly bound the global sensitivity of an individual eigenvalue. For example, if all data points are clipped to enforce $\|Z_i\|_2 \leq R$ then for datasets Z and Z' differing in index 1 we can relate their covariance matrices as

$$\left\| \frac{1}{n}\sum_i Z_i Z_i^T - \frac{1}{n}\sum_i Z_i' Z_i'^T \right\|_{\text{op}} = \frac{1}{n}\left\| Z_1 Z_1^T - Z_1' Z_1'^T \right\|_{\text{op}} \leq \frac{2R^2}{n}$$

(using the triangle inequality and the fact that $\|Z_i Z_i\|_{\text{op}} = \|Z_i\|_2^2 \leq R^2$). Thus, Weyl's inequality (Lemma A.11) gives

$$|\lambda_i(\Sigma_Z) - \lambda_i(\Sigma_{Z'})| \leq \|\Sigma_Z - \Sigma_{Z'}\|_{\text{op}} \leq \frac{2R^2}{n}.$$

Thus, we can add Laplace noise with scale $2R^2/\varepsilon n$ for a pure-DP additive approximation to the eigenvalue. This is an important step in multiple algorithms for private covariance estimation: see [MWK+22, DLY22] and references therein.

G.3 Testing problems

Theorems D.5 and D.7 concern deciding between two or three alternate hypotheses. In this setting, subsample-and-aggregate takes a simple form as one can aggregate with a DP histogram, where each "bin" is a hypothesis. Adding Laplace noise to each bin with scale $1/\varepsilon$ yields pure DP and, for a constant number of hypotheses, every noisy count will be within $O(\log(1/\beta)/\varepsilon)$ with probability at least $1-\beta$. One can use any variation (such as Stable Histogram as above) with subsample-and-aggregate, but all approaches yield at least a $1/\varepsilon$ factor blowup in sample complexity beyond the non-private cost.

There is substantial work on hypothesis testing and selection under differential privacy [see, e.g., CKM+19, BKSW19, KSGB23, ADH+24]. There are several approaches among these which bypass the $1/\varepsilon$ blowup for specific testing problems, but (to the best of our knowledge) these all rely on detailed distributional information that is not available in the settings we consider.

Several approaches consider hypothesis testing specifically for linear regression [She17, FWS22, AV23, PB22]. These are analyzed in various settings but, to the best of our knowledge, when applied to the problems we consider all would incur at least a $\sqrt{d}$ or $1/\varepsilon$ factor increase above the non-private sample complexity.

G.4 Loss estimation

Theorem D.4 gives our result for estimating the minimum achievable loss on a learning task under assumption D.1, a loss-concentration assumption. Under this assumption, Proposition G.1 gives us the sample complexity for subsample-and-aggregate.

The other off-the-shelf approach, for any loss estimation task, is to privately learn a near-optimal parameter vector; this is a central topic in differentially private learning and for many learning tasks there are efficient algorithms that avoid the $\frac{\log 1/\delta}{\varepsilon}$ penalty of subsample-and-aggregate. For any fixed parameter vector, one can expect to estimate the loss using very few additional samples.

One alternate approach comes from the observation that, to estimate the loss of a near-optimal model, we only need its predictions on fresh data. The paradigm of *private prediction* [DF18] enables exactly that, giving predictions which are close to those of the best-possible predictor. Work in this area shows how to accomplish this with significantly fewer samples than required for learning. For applications in the style we consider, one would need results for agnostic PAC learning [NB20, DF20], as in the realizable setting the optimal loss is zero by assumption.

Beyond this, we are aware of few techniques that permit estimating the minimum loss of a learning task with a sample complexity that beats subsample-and-aggregate, under any assumptions on the

learning task. [ENP22] considers the problem of *refutation* under local differential privacy. In the context of binary classification, refutation consists of determining if the loss is $1/2$ or $1/2 - \Omega(1)$. [VTJ22] provides a private gradient descent method for well-specified linear regression and the algorithm tracks σ^2, the variance of the label noise, implicitly.

G.5 Single-parameter estimation

We compare with the single-parameter estimation result of Theorem D.8, which relies on Assumption D.3. To provide comparable guarantees, subsample-and-aggregate requires only the first part of that assumption, which is itself a reformulation of Assumption 1.1. Proposition G.1 tells us that, under that assumption, subsample-and-aggregate can return an estimate $\tilde{\theta}_1$ such that, if

$$n = \Omega\left(\frac{N(\alpha)\log(1/\beta\delta)}{\varepsilon} + \frac{\log(1/\beta\delta)}{\alpha^2\varepsilon}\right)$$

then with probability at least $1-\beta$ we have $|\tilde{\theta}_1 - \theta(\mathcal{D})_1| \leq 3\alpha$.

We are not aware of any algorithms that rely on (any subset of) Assumption D.3 for this task. The closest work, from which our work draws an example, is that of [ADT25]. They provide a sophisticated algorithm for privately estimating a single parameter within a large parametric model. It is not immediately clear the exact sample complexity their algorithm would obtain in our setting (their work focuses on achieving the optimal error rate as $n \to \infty$ under different, but related, assumptions), but it appears unable to provide accurate estimates at a sample size smaller than that of subsample-and-aggregate.

Our primary motivation is estimating a single parameter in a least squares model. As with covariance estimation, any private estimator for the full least-squares model can be used for single-parameter estimation. And, as with covariance estimation, the landscape of DP least squares is too broad to survey here. We mention a few key themes with pointers to recent work. Many techniques perturb the sufficient statistics X^TX, X^Ty; accurate estimation here requires as many samples as private covariance estimation, incurring a $d^{3/2}$ in the sample complexity [Wan18, She19, TAK+24]. Work building on robust statistics requires either exponential time [LKO22] or d^2 samples [ABMT25], and this is believed to be inherent. A line of work analyzes gradient descent under distributional assumptions [VTJ22, LJK+23, BLSM26], and some of these arguments characterize output noise in a way that may be amenable to direct calculation about per-coordinate error [BDE+24]. However, all are first-order methods and have an dependence on the condition number of the covariance that Theorem D.8 does not. The approach of [BHH+24] admits clean reasoning about single parameters (see Claim 3), but requires $n \geq \frac{d}{\varepsilon^2}\log^2(1/\delta)$ samples to produce a non-trivial estimate, a larger requirement than subsample-and-aggregate.

H Analysis of random-design linear regression

In this section, we provide the formal claims necessary to show that Assumption D.3 applies to the task of well-specified random-design linear regression with Gaussian covariates and Gaussian noise.

Definition H.1 (Random-design linear regression task)**.** *Fix dimension $d \in \mathbb{N}$. Examples are $z = (x, y) \in \mathcal{Z} = \mathbb{R}^d \times \mathbb{R}$. We define $\Theta = \mathbb{R}^d$ and let $\ell_\theta(z) = (\langle x, \theta\rangle - y)^2$ be the standard squared loss. The distribution $\mathcal{D}$ over $\mathcal{Z}$ is defined by the symmetric positive definite matrix $\Sigma \in \mathbb{R}^{d\times d}$, noise variance $s^2 > 0$, and true parameter $\theta \in \mathbb{R}^d$. To sample $(x, y) \sim \mathcal{D}$ we draw $x_i \sim \mathcal{N}(0, \Sigma)$, $\eta_i \sim \mathcal{N}(0, s^2)$, and set $y_i = \langle x_i, \theta^*\rangle + \eta_i$.*

Proposition H.2. *Let $(\Theta, \ell, \mathcal{D})$ be a learning task as above, with $\mathcal{D}$ defined by $\Sigma \succ 0, s^2 > 0$, and $\theta \in \mathbb{R}^d$. Then $(\Theta, \ell, \mathcal{D})$ satisfies Assumption D.3 with*

- $N_{D.3} = M_{D.3} = 4d$ *(independent of α).*
- $K_{D.3} = 144\max\{1, s^2\}$
- $\lambda = 2s^2$
- $\mu = \frac{1}{(\Sigma^{-1})_{11}}$

- $\sigma = 2s$.

Assumption D.3 has four conditions; we establish them in order in Lemmas H.6 to H.9. To begin, we state a few standard concentration inequalities.

Claim H.3 (Gaussian tail)**.** *If $G \sim \mathcal{N}(0,1)$ then for all $\beta \in (0,1)$, $\Pr\Big(G^2 \geq 2\log\frac{2}{\beta}\Big) \leq \beta$.*

We use a slightly weaker (and simpler) version of the standard Laurent–Massart tail bounds for chi-squared random variables.

Claim H.4 (Laurent–Massart)**.** *If $U \sim \chi^2_k$ then for all $t \geq 0$, $\Pr(U \geq k + 2\sqrt{kt} + 2t)$ and $\Pr\left(U \leq k - 2\sqrt{kt}\right) \leq e^{-t}$.*

Claim H.5 (Inverse-Wishart scalar identity)**.** *Let $G \in \mathbb{R}^{n\times d}$ have i.i.d. $\mathcal{N}(0,1)$ entries and let $W = G^\top G$ (so $W \sim \mathrm{Wishart}(I_d, n)$). For any fixed nonzero $v \in \mathbb{R}^d$,*

$$\frac{\|v\|_2^2}{v^\top W^{-1} v} \sim \chi^2_{n-d+1}.$$

This identity is standard; it can be proved by rotating v to e_1 and using the Bartlett decomposition for Wishart distributions.

Lemma H.6 (Concentration of $\hat\theta_1$)**.** *Let $\hat\theta$ be the OLS estimator. In the setting of Definition H.1, for all $\alpha, \beta \in (0,1)$, if*

$$n \;\geq\; d + \frac{24\max\{1, s^2\}}{\alpha^2}\log(4/\beta)$$

we have

$$\Pr\Big(\big|\hat\theta_1 - \theta_1\big| \geq \alpha\,\mu^{-1/2}\Big) \leq \beta, \qquad \textit{where} \quad \mu = \frac{1}{(\Sigma^{-1})_{11}}.$$

Proof. Conditioned on X, the OLS estimator satisfies

$$\hat\theta - \theta = (X^\top X)^{-1} X^\top \eta, \qquad \eta \sim \mathcal{N}(0, s^2 I_n),$$

hence

$$(\hat\theta_1 - \theta_1) \mid X \sim \mathcal{N}\Big(0,\; s^2\,((X^\top X)^{-1})_{11}\Big).$$

Whiten and write $X = G\Sigma^{1/2}$ with i.i.d. standard normal G, so

$$(X^\top X)^{-1} = \Sigma^{-1/2}(G^\top G)^{-1}\Sigma^{-1/2}.$$

For the first standard unit vector e_1, let $v = \Sigma^{-1/2}e_1$, so $\|v\|_2^2 = e_1^\top \Sigma^{-1} e_1 = (\Sigma^{-1})_{11}$ and

$$((X^\top X)^{-1})_{11} = v^\top (G^\top G)^{-1} v.$$

By Claim H.5, with $k \coloneqq n - d + 1$,

$$\frac{\|v\|_2^2}{v^\top (G^\top G)^{-1} v} \sim \chi^2_k.$$

Let $U \sim \chi^2_k$ denote this variable; then

$$v^\top (G^\top G)^{-1} v = \frac{\|v\|_2^2}{U} = \frac{(\Sigma^{-1})_{11}}{U}.$$

Using Claim H.4 (lower tail) with $t = \log(2/\beta)$,

$$\Pr\left(U \leq k - 2\sqrt{k\log\frac{2}{\beta}}\right) \leq \frac{\beta}{2}.$$

If $k \geq 16\log(2/\beta)$, then $2\sqrt{k\log(2/\beta)} \leq k/2$ and thus

$$\Pr\left(U \geq \frac{k}{2}\right) \geq 1 - \frac{\beta}{2}.$$

On this event,

$$((X^\top X)^{-1})_{11} = \frac{(\Sigma^{-1})_{11}}{U} \le \frac{2(\Sigma^{-1})_{11}}{k} \le \frac{4(\Sigma^{-1})_{11}}{n}.$$

Therefore, on this event,

$$\mathrm{Var}(\hat{\theta}_1 - \theta_1 \mid X) \le s^2 \cdot \frac{4(\Sigma^{-1})_{11}}{n}.$$

Conditioning on X and applying a Gaussian tail bound gives, for any $t > 0$,

$$\Pr\Big(|\hat{\theta}_1 - \theta_1| \ge t \mid X\Big) \le 2\exp\left(-\frac{t^2 n}{8s^2(\Sigma^{-1})_{11}}\right).$$

Unconditioning and adding the $\beta/2$ failure probability of the event yields

$$\Pr\Big(|\hat{\theta}_1 - \theta_1| \ge t\Big) \le 2\exp\left(-\frac{t^2 n}{8s^2(\Sigma^{-1})_{11}}\right) + \frac{\beta}{2}.$$

Now $\mu = \big((\Sigma^{-1})_{11}\big)^{-1}$ and choose $t = \alpha\mu^{-1/2}$, so the exponential term becomes $2\exp\left(-\frac{\alpha^2 n}{8s^2}\right)$. If $n \ge \frac{8s^2\log(4/\beta)}{\alpha^2}$ then this is at most $\beta/2$.

Our other restriction on n (via $k = n - d + 1$) is that $n \ge d - 1 + 16\log(2/\beta)$. Taking $n \ge d + \frac{24\max\{1,s^2\}\log(4/\beta)}{\alpha^2}$ ensures both of these conditions are satisfied. □

Lemma H.7 (Typical Smoothness and Strong Convexity)**.** *In the setting of Definition H.1, if $n \ge 4d + 18\log(2/\beta)$ then with probability at least $1-\beta$ we have, for all $w \in \mathbb{R}$,*

$$\frac{\mu}{2}(w - \hat{\theta}_1)^2 \;\le\; L^{(w)}(Z) - L(Z) \;\le\; 2\mu(w - \hat{\theta}_1)^2,$$

where $\mu := \frac{1}{(\Sigma^{-1})_{11}}$. Recall that $L^{(w)}(Z)$ denotes the minimum achievable loss among parameters whose first coordinate is fixed to w.

Proof. Write the design matrix as $X = (x^{(1)}, X_{-1})$, where $x^{(1)} \in \mathbb{R}^n$ is the first column and $X_{-1} \in \mathbb{R}^{n\times(d-1)}$ are the remaining columns. For a fixed $w \in \mathbb{R}$, the constrained least-squares problem defining $L^{(w)}(Z)$ is

$$L^{(w)}(Z) = \min_{\theta_{-1}\in\mathbb{R}^{d-1}} \frac{1}{n}\|y - x^{(1)}w - X_{-1}\theta_{-1}\|_2^2.$$

Let P denote the orthogonal projector onto $\mathrm{col}(X_{-1})$ and set $M := I - P$ (so M is an orthogonal projector, hence symmetric and idempotent). Then

$$L^{(w)}(Z) = \frac{1}{n}\|M(y - x^{(1)}w)\|_2^2.$$

Define $r := My$ and $v := Mx^{(1)}$, so $L^{(w)}(Z) = \frac{1}{n}\|r - vw\|_2^2$. As a function of w, this is a one-dimensional quadratic with minimizer $w = \hat{w}$, where $\hat{w}$ is exactly the first coordinate of the unconstrained OLS solution, i.e. $\hat{w} = \hat{\theta}_1$. Therefore,

$$L^{(w)}(Z) - L(Z) = \frac{1}{n}\Big(\|r - vw\|_2^2 - \|r - v\hat{\theta}_1\|_2^2\Big) = \frac{v^\top v}{n}(w - \hat{\theta}_1)^2.$$

Thus, it remains to control the random scalar

$$c_Z := \frac{v^\top v}{n} = \frac{1}{n}x^{(1)\top}Mx^{(1)}.$$

We now show that c_Z concentrates around $\mu := 1/(\Sigma^{-1})_{11}$. Because $(x_1, \ldots, x_d)$ is jointly Gaussian with covariance Σ, the conditional variance of the first coordinate given the others is

$$\mathrm{Var}(x_1 \mid x_{2:d}) = \frac{1}{(\Sigma^{-1})_{11}} = \mu.$$

Conditioned on X_{-1}, the residualized column $v = Mx^{(1)}$ is Gaussian in $\mathrm{range}(M)$ with covariance μM:

$$v \mid X_{-1} \sim \mathcal{N}(0, \mu M).$$

Since M is an idempotent projector with rank $\mathsf{rank}(M) = n - (d-1) = k$, it follows that

$$\frac{1}{\mu} v^\top v \;\Big|\; X_{-1} \sim \chi^2_k,$$

and hence unconditionally $(1/\mu)v^\top v \sim \chi^2_k$. Let $U \sim \chi^2_k$ denote this variable, so $c_Z = \mu U/n$. Apply Claim H.4 with $t = \log(2/\beta)$:

$$\Pr\left(U \notin \left[k - 2\sqrt{k \log \frac{2}{\beta}},\; k + 2\sqrt{k \log \frac{2}{\beta}} + 2\log \frac{2}{\beta}\right]\right) \le \beta.$$

Now we need to impose two conditions. First condition we require is $k - 2\sqrt{kt} \ge n/2$, or equivalently, since $k = n - d + 1$,

$$n - d + 1 - 2\sqrt{(n-d+1)t} \ge n/2\,.$$

In order for the above bound to hold, it suffices to take $n \ge 4(d-1) + 18t$.

The other constraint we need to impose is that $k + 2\sqrt{kt} + 2t \le 2n$, since $k \le n$, in order to ensure it suffices to take $n \ge 16t$. Therefore, as long as $n \ge 4d + 18\log(2/\beta)$, we will have

$$\frac{1}{2} \le \frac{U}{n} \le 2$$

and therefore,

$$\frac{\mu}{2} \le c_Z \le 2\mu$$

as desired. □

Lemma H.8 (Leave-one-out loss)**.** *In the setting of Definition H.1, assume $n \ge d+1$, fix $i \in [n]$, and let Z_{-i} be the dataset with point i removed. Recall $L_\theta(Z_{-i}) = \frac{1}{n}\sum_{j \ne i}(y_j - x_j^\top \theta)^2$. Then with probability at least $1-\beta$ we have*

$$\Pr\left(|L(Z) - L(Z_{-i})| \ge \frac{\lambda \log(2/\beta)}{n}\right) \le \beta \qquad \textit{with} \qquad \lambda = 2s^2.$$

Proof. By the standard Sherman–Morrison identity for deletions in least-squares, we have

$$L(Z) - L(Z_{-i}) = \frac{1}{n} \cdot \frac{r_i^2}{1 - h_{ii}},$$

where $r_i = (y_i - x_i^T \hat{\theta}(Z))$ is the residual and $h_i = x_i^T (X^T X)^{-1} x_i$ the leverage score. Note that this is always positive. For any fixed dataset X, we use the following distributional fact:

$$\frac{r_i}{\sqrt{1-h_i}} \;\Big|\; X \sim \mathcal{N}(0, s^2).$$

In particular, its distribution is independent of X, so the same statement holds unconditionally.

Thus we can apply Claim H.3: for $G \sim \mathcal{N}(0,1)$ we have

$$\begin{aligned}\Pr\left[L(Z) - L(Z_{-i}) \ge \frac{2s^2 \log(2/\beta)}{n}\right] &= \Pr\left[\frac{s^2}{n} \cdot G^2 \ge \frac{2s^2 \log(2/\beta)}{n}\right] \\ &= \Pr\left[G^2 \ge 2\log(2/\beta)\right] \\ &\le \beta.\end{aligned}$$

Thus we can take $\lambda = 2s^2$. □

Lemma H.9 (Tail bound for $L(Z)$)**.** *In the setting of Definition H.1, for all $\beta \in (0,1)$ we have*

$$\Pr\left(L(Z) \ge \sigma^2\left(1 + \frac{\log(1/\beta)}{n}\right)\right) \le \beta \qquad \textit{with} \qquad \sigma^2 := 4s^2.$$

Proof. The loss of the empirical minimizer $\hat{\theta}$ on Z is at most the loss of the true minimizer θ:

$$\begin{aligned} L(Z) = L_{\hat{\theta}}(Z) &\leq L_{\theta}(Z) \\ &= \frac{1}{n}\sum_{i=1}^{n}\left(x_i^T\theta - y_i\right)^2 \\ &= \frac{1}{n}\sum_{i=1}^{n}\eta_i^2, \end{aligned} \tag{7}$$

where we have used the fact that $y_i = x_i^T\theta + \eta_i$. Since each η_i is drawn i.i.d. from $\mathcal{N}(0, s^2)$, Eq. (7) is distributed as $\frac{s^2}{n}U$ where $U \sim \chi_n^2$. Thus

$$\begin{aligned} \Pr\left[L(Z) \geq 2s^2 + \frac{4ts^2}{n}\right] &\leq \Pr\left[\frac{s^2}{n}U \geq 2s^2 + \frac{4ts^2}{n}\right] \\ &= \Pr\left[U \geq 2n + 4t\right] \\ &\leq e^{-t}. \end{aligned}$$

Taking $t = \log(1/\beta)$, we are done. □

NeurIPS Paper Checklist

1. **Claims**

   Question: Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope?

   Answer: [Yes]

   Justification: Yes. Our main claims are statements about the theorems we prove and how they extend and improve upon prior work.

   Guidelines:

   - The answer [N/A] means that the abstract and introduction do not include the claims made in the paper.
   - The abstract and/or introduction should clearly state the claims made, including the contributions made in the paper and important assumptions and limitations. A [No] or [N/A] answer to this question will not be perceived well by the reviewers.
   - The claims made should match theoretical and experimental results, and reflect how much the results can be expected to generalize to other settings.
   - It is fine to include aspirational goals as motivation as long as it is clear that these goals are not attained by the paper.

2. **Limitations**

   Question: Does the paper discuss the limitations of the work performed by the authors?

   Answer: [Yes]

   Justification: Yes, our work is entirely theoretical and we take care to lay out what our analysis does and does not cover.

   Guidelines:

   - The answer [N/A] means that the paper has no limitation while the answer [No] means that the paper has limitations, but those are not discussed in the paper.
   - The authors are encouraged to create a separate "Limitations" section in their paper.
   - The paper should point out any strong assumptions and how robust the results are to violations of these assumptions (e.g., independence assumptions, noiseless settings, model well-specification, asymptotic approximations only holding locally). The authors should reflect on how these assumptions might be violated in practice and what the implications would be.
   - The authors should reflect on the scope of the claims made, e.g., if the approach was only tested on a few datasets or with a few runs. In general, empirical results often depend on implicit assumptions, which should be articulated.
   - The authors should reflect on the factors that influence the performance of the approach. For example, a facial recognition algorithm may perform poorly when image resolution is low or images are taken in low lighting. Or a speech-to-text system might not be used reliably to provide closed captions for online lectures because it fails to handle technical jargon.
   - The authors should discuss the computational efficiency of the proposed algorithms and how they scale with dataset size.
   - If applicable, the authors should discuss possible limitations of their approach to address problems of privacy and fairness.
   - While the authors might fear that complete honesty about limitations might be used by reviewers as grounds for rejection, a worse outcome might be that reviewers discover limitations that aren't acknowledged in the paper. The authors should use their best judgment and recognize that individual actions in favor of transparency play an important role in developing norms that preserve the integrity of the community. Reviewers will be specifically instructed to not penalize honesty concerning limitations.

3. **Theory assumptions and proofs**

   Question: For each theoretical result, does the paper provide the full set of assumptions and a complete (and correct) proof?

Answer: [Yes]

Justification: All of our theoretical results state their assumptions and follow the standard theorem-lemma-proof structure.

Guidelines:

- The answer [N/A] means that the paper does not include theoretical results.
- All the theorems, formulas, and proofs in the paper should be numbered and cross-referenced.
- All assumptions should be clearly stated or referenced in the statement of any theorems.
- The proofs can either appear in the main paper or the supplemental material, but if they appear in the supplemental material, the authors are encouraged to provide a short proof sketch to provide intuition.
- Inversely, any informal proof provided in the core of the paper should be complemented by formal proofs provided in appendix or supplemental material.
- Theorems and Lemmas that the proof relies upon should be properly referenced.

4. **Experimental result reproducibility**

   Question: Does the paper fully disclose all the information needed to reproduce the main experimental results of the paper to the extent that it affects the main claims and/or conclusions of the paper (regardless of whether the code and data are provided or not)?

   Answer: [N/A]

   Justification: We have no experiments.

   Guidelines:

   - The answer [N/A] means that the paper does not include experiments.
   - If the paper includes experiments, a [No] answer to this question will not be perceived well by the reviewers: Making the paper reproducible is important, regardless of whether the code and data are provided or not.
   - If the contribution is a dataset and/or model, the authors should describe the steps taken to make their results reproducible or verifiable.
   - Depending on the contribution, reproducibility can be accomplished in various ways. For example, if the contribution is a novel architecture, describing the architecture fully might suffice, or if the contribution is a specific model and empirical evaluation, it may be necessary to either make it possible for others to replicate the model with the same dataset, or provide access to the model. In general. releasing code and data is often one good way to accomplish this, but reproducibility can also be provided via detailed instructions for how to replicate the results, access to a hosted model (e.g., in the case of a large language model), releasing of a model checkpoint, or other means that are appropriate to the research performed.
   - While NeurIPS does not require releasing code, the conference does require all submissions to provide some reasonable avenue for reproducibility, which may depend on the nature of the contribution. For example
     (a) If the contribution is primarily a new algorithm, the paper should make it clear how to reproduce that algorithm.
     (b) If the contribution is primarily a new model architecture, the paper should describe the architecture clearly and fully.
     (c) If the contribution is a new model (e.g., a large language model), then there should either be a way to access this model for reproducing the results or a way to reproduce the model (e.g., with an open-source dataset or instructions for how to construct the dataset).
     (d) We recognize that reproducibility may be tricky in some cases, in which case authors are welcome to describe the particular way they provide for reproducibility. In the case of closed-source models, it may be that access to the model is limited in some way (e.g., to registered users), but it should be possible for other researchers to have some path to reproducing or verifying the results.

5. **Open access to data and code**

Question: Does the paper provide open access to the data and code, with sufficient instructions to faithfully reproduce the main experimental results, as described in supplemental material?

Answer: [N/A]

Justification: We have no experiments.

Guidelines:

- The answer [N/A] means that paper does not include experiments requiring code.
- Please see the NeurIPS code and data submission guidelines (https://neurips.cc/public/guides/CodeSubmissionPolicy) for more details.
- While we encourage the release of code and data, we understand that this might not be possible, so [No] is an acceptable answer. Papers cannot be rejected simply for not including code, unless this is central to the contribution (e.g., for a new open-source benchmark).
- The instructions should contain the exact command and environment needed to run to reproduce the results. See the NeurIPS code and data submission guidelines (https://neurips.cc/public/guides/CodeSubmissionPolicy) for more details.
- The authors should provide instructions on data access and preparation, including how to access the raw data, preprocessed data, intermediate data, and generated data, etc.
- The authors should provide scripts to reproduce all experimental results for the new proposed method and baselines. If only a subset of experiments are reproducible, they should state which ones are omitted from the script and why.
- At submission time, to preserve anonymity, the authors should release anonymized versions (if applicable).
- Providing as much information as possible in supplemental material (appended to the paper) is recommended, but including URLs to data and code is permitted.

6. **Experimental setting/details**

   Question: Does the paper specify all the training and test details (e.g., data splits, hyperparameters, how they were chosen, type of optimizer) necessary to understand the results?

   Answer: [N/A]

   Justification: We have no experiments.

   Guidelines:

   - The answer [N/A] means that the paper does not include experiments.
   - The experimental setting should be presented in the core of the paper to a level of detail that is necessary to appreciate the results and make sense of them.
   - The full details can be provided either with the code, in appendix, or as supplemental material.

7. **Experiment statistical significance**

   Question: Does the paper report error bars suitably and correctly defined or other appropriate information about the statistical significance of the experiments?

   Answer: [N/A]

   Justification: We have no experiments.

   Guidelines:

   - The answer [N/A] means that the paper does not include experiments.
   - The authors should answer [Yes] if the results are accompanied by error bars, confidence intervals, or statistical significance tests, at least for the experiments that support the main claims of the paper.
   - The factors of variability that the error bars are capturing should be clearly stated (for example, train/test split, initialization, random drawing of some parameter, or overall run with given experimental conditions).
   - The method for calculating the error bars should be explained (closed form formula, call to a library function, bootstrap, etc.)

- The assumptions made should be given (e.g., Normally distributed errors).
- It should be clear whether the error bar is the standard deviation or the standard error of the mean.
- It is OK to report 1-sigma error bars, but one should state it. The authors should preferably report a 2-sigma error bar than state that they have a 96% CI, if the hypothesis of Normality of errors is not verified.
- For asymmetric distributions, the authors should be careful not to show in tables or figures symmetric error bars that would yield results that are out of range (e.g., negative error rates).
- If error bars are reported in tables or plots, the authors should explain in the text how they were calculated and reference the corresponding figures or tables in the text.

8. **Experiments compute resources**

   Question: For each experiment, does the paper provide sufficient information on the computer resources (type of compute workers, memory, time of execution) needed to reproduce the experiments?

   Answer: [N/A]

   Justification: We have no experiments.

   Guidelines:

   - The answer [N/A] means that the paper does not include experiments.
   - The paper should indicate the type of compute workers CPU or GPU, internal cluster, or cloud provider, including relevant memory and storage.
   - The paper should provide the amount of compute required for each of the individual experimental runs as well as estimate the total compute.
   - The paper should disclose whether the full research project required more compute than the experiments reported in the paper (e.g., preliminary or failed experiments that didn't make it into the paper).

9. **Code of ethics**

   Question: Does the research conducted in the paper conform, in every respect, with the NeurIPS Code of Ethics https://neurips.cc/public/EthicsGuidelines?

   Answer: [Yes]

   Justification: Yes. Our work is entirely theoretical and deals with no human subjects. Our work is designed to advance the state-of-the-art in private learning, which we expect to have positive social effects. We see no potential social harms.

   Guidelines:

   - The answer [N/A] means that the authors have not reviewed the NeurIPS Code of Ethics.
   - If the authors answer [No], they should explain the special circumstances that require a deviation from the Code of Ethics.
   - The authors should make sure to preserve anonymity (e.g., if there is a special consideration due to laws or regulations in their jurisdiction).

10. **Broader impacts**

    Question: Does the paper discuss both potential positive societal impacts and negative societal impacts of the work performed?

    Answer: [Yes]

    Justification: Our work is designed to advance the state-of-the-art in private learning, which we expect to have positive social effects. We see no potential social harms.

    Guidelines:

    - The answer [N/A] means that there is no societal impact of the work performed.
    - If the authors answer [N/A] or [No], they should explain why their work has no societal impact or why the paper does not address societal impact.

- Examples of negative societal impacts include potential malicious or unintended uses (e.g., disinformation, generating fake profiles, surveillance), fairness considerations (e.g., deployment of technologies that could make decisions that unfairly impact specific groups), privacy considerations, and security considerations.
- The conference expects that many papers will be foundational research and not tied to particular applications, let alone deployments. However, if there is a direct path to any negative applications, the authors should point it out. For example, it is legitimate to point out that an improvement in the quality of generative models could be used to generate Deepfakes for disinformation. On the other hand, it is not needed to point out that a generic algorithm for optimizing neural networks could enable people to train models that generate Deepfakes faster.
- The authors should consider possible harms that could arise when the technology is being used as intended and functioning correctly, harms that could arise when the technology is being used as intended but gives incorrect results, and harms following from (intentional or unintentional) misuse of the technology.
- If there are negative societal impacts, the authors could also discuss possible mitigation strategies (e.g., gated release of models, providing defenses in addition to attacks, mechanisms for monitoring misuse, mechanisms to monitor how a system learns from feedback over time, improving the efficiency and accessibility of ML).

11. **Safeguards**

    Question: Does the paper describe safeguards that have been put in place for responsible release of data or models that have a high risk for misuse (e.g., pre-trained language models, image generators, or scraped datasets)?

    Answer: [N/A]

    Justification: There are no such risks associated with our work.

    Guidelines:

    - The answer [N/A] means that the paper poses no such risks.
    - Released models that have a high risk for misuse or dual-use should be released with necessary safeguards to allow for controlled use of the model, for example by requiring that users adhere to usage guidelines or restrictions to access the model or implementing safety filters.
    - Datasets that have been scraped from the Internet could pose safety risks. The authors should describe how they avoided releasing unsafe images.
    - We recognize that providing effective safeguards is challenging, and many papers do not require this, but we encourage authors to take this into account and make a best faith effort.

12. **Licenses for existing assets**

    Question: Are the creators or original owners of assets (e.g., code, data, models), used in the paper, properly credited and are the license and terms of use explicitly mentioned and properly respected?

    Answer: [N/A]

    Justification: We did not use any existing assets.

    Guidelines:

    - The answer [N/A] means that the paper does not use existing assets.
    - The authors should cite the original paper that produced the code package or dataset.
    - The authors should state which version of the asset is used and, if possible, include a URL.
    - The name of the license (e.g., CC-BY 4.0) should be included for each asset.
    - For scraped data from a particular source (e.g., website), the copyright and terms of service of that source should be provided.
    - If assets are released, the license, copyright information, and terms of use in the package should be provided. For popular datasets, `paperswithcode.com/datasets` has curated licenses for some datasets. Their licensing guide can help determine the license of a dataset.

- For existing datasets that are re-packaged, both the original license and the license of the derived asset (if it has changed) should be provided.
- If this information is not available online, the authors are encouraged to reach out to the asset's creators.

13. **New assets**

    Question: Are new assets introduced in the paper well documented and is the documentation provided alongside the assets?

    Answer: [N/A]

    Justification: We release no new assets.

    Guidelines:

    - The answer [N/A] means that the paper does not release new assets.
    - Researchers should communicate the details of the dataset/code/model as part of their submissions via structured templates. This includes details about training, license, limitations, etc.
    - The paper should discuss whether and how consent was obtained from people whose asset is used.
    - At submission time, remember to anonymize your assets (if applicable). You can either create an anonymized URL or include an anonymized zip file.

14. **Crowdsourcing and research with human subjects**

    Question: For crowdsourcing experiments and research with human subjects, does the paper include the full text of instructions given to participants and screenshots, if applicable, as well as details about compensation (if any)?

    Answer: [N/A]

    Justification: Our work involves no crowdsourcing or human subjects.

    Guidelines:

    - The answer [N/A] means that the paper does not involve crowdsourcing nor research with human subjects.
    - Including this information in the supplemental material is fine, but if the main contribution of the paper involves human subjects, then as much detail as possible should be included in the main paper.
    - According to the NeurIPS Code of Ethics, workers involved in data collection, curation, or other labor should be paid at least the minimum wage in the country of the data collector.

15. **Institutional review board (IRB) approvals or equivalent for research with human subjects**

    Question: Does the paper describe potential risks incurred by study participants, whether such risks were disclosed to the subjects, and whether Institutional Review Board (IRB) approvals (or an equivalent approval/review based on the requirements of your country or institution) were obtained?

    Answer: [N/A]

    Justification: Our work involves no crowdsourcing or human subjects.

    Guidelines:

    - The answer [N/A] means that the paper does not involve crowdsourcing nor research with human subjects.
    - Depending on the country in which research is conducted, IRB approval (or equivalent) may be required for any human subjects research. If you obtained IRB approval, you should clearly state this in the paper.
    - We recognize that the procedures for this may vary significantly between institutions and locations, and we expect authors to adhere to the NeurIPS Code of Ethics and the guidelines for their institution.
    - For initial submissions, do not include any information that would break anonymity (if applicable), such as the institution conducting the review.

16. **Declaration of LLM usage**

Question: Does the paper describe the usage of LLMs if it is an important, original, or non-standard component of the core methods in this research? Note that if the LLM is used only for writing, editing, or formatting purposes and does *not* impact the core methodology, scientific rigor, or originality of the research, declaration is not required.

Answer: [N/A]

Justification: The core methods in this research did not involve LLMs in their development.

Guidelines:

- The answer [N/A] means that the core method development in this research does not involve LLMs as any important, original, or non-standard components.
- Please refer to our LLM policy in the NeurIPS handbook for what should or should not be described.