Submitted to the Annals of Statistics
arXiv: arXiv:0000.0000

THE COST OF PRIVACY: OPTIMAL RATES OF CONVERGENCE FOR PARAMETER ESTIMATION WITH DIFFERENTIAL PRIVACY

By T. Tony Cai, Yichen Wang, and Linjun Zhang

University of Pennsylvania and Rutgers University

Privacy-preserving data analysis is a rising challenge in contemporary statistics, as the privacy guarantees of statistical methods are often achieved at the expense of accuracy. In this paper, we investigate the tradeoff between statistical accuracy and privacy in mean estimation and linear regression, under both the classical low-dimensional and modern high-dimensional settings. A primary focus is to establish minimax optimality for statistical estimation with the (ε, δ)-differential privacy constraint. By refining the "tracing adversary" technique for lower bounds in the theoretical computer science literature, we improve existing minimax lower bound for low-dimensional mean estimation and establish new lower bounds for high-dimensional mean estimation and linear regression problems. We also design differentially private algorithms that attain the minimax lower bounds up to logarithmic factors. In particular, for high-dimensional linear regression, a novel private iterative hard thresholding algorithm is proposed. The numerical performance of differentially private algorithms is demonstrated by simulation studies and applications to real data sets.

1. Introduction. With the unprecedented availability of datasets containing sensitive personal information, there are increasing concerns that statistical analysis of such datasets may compromise individual privacy. These concerns give rise to statistical methods that provide privacy guarantees at the cost of statistical accuracy, which then motivates us to study the optimal tradeoff between privacy and accuracy in fundamental statistical problems such as mean estimation and linear regression.

A rigorous definition of privacy is a prerequisite for our study. Differential privacy, introduced in [17], is arguably the most widely adopted definition of privacy in statistical data analysis. The promise of a differentially private algorithm is protection of each individual's privacy from an adversary who has access to the algorithm's output and possibly even the rest of the data. Differential privacy has gained significant attention in academia [18, 1, 20, 16] and found its way into real world applications developed by Apple [11], Google [24], Microsoft [12], and the U.S. Census Bureau [2].

A usual approach to developing differentially private algorithms is per-

MSC 2010 subject classifications: Primary 62F30; secondary 62F12, 62J05.
Keywords and phrases: High-dimensional data; Differential privacy; Mean estimation; Linear regression; Minimax optimality.

turbing the output of non-private algorithms by random noise [17, 35, 18], and naturally the processed output suffers from some loss of accuracy, which has been extensively observed and studied in the literature [48, 42, 32, 5, 23]. Our paper intends to characterize quantitatively the tradeoff between differential privacy guarantees and statistical accuracy, under the statistical minimax risk framework. Specifically, we study this tradeoff in mean estimation and linear regression problems with the (ε, δ)-differential privacy constraint, which is formally defined as follows.

DEFINITION 1 (Differential Privacy [17]). A randomized algorithm $M : \mathcal{X}^n \to \mathcal{R}$ is (ε, δ)-differentially private if for every pair of adjacent data sets $\boldsymbol{X}, \boldsymbol{X}' \in \mathcal{X}^n$ that differ by one individual datum and every (measurable) $S \subseteq \mathcal{R}$,

$$\mathbb{P}\left(M(\boldsymbol{X}) \in S\right) \leq e^{\varepsilon} \cdot \mathbb{P}\left(M(\boldsymbol{X}') \in S\right) + \delta,$$

where the probability measure $\mathbb{P}$ is induced by the randomness of M only.

According to the definition, the two parameters ε and δ control the level of privacy against an adversary who attempts to detect the presence of a certain individual in the sample. The privacy constraint becomes more stringent as ε, δ tend to 0.

Our contributions and related literature.

Lower bounds based on tracing attacks. We establish the necessary cost of privacy by proving minimax risk lower bounds with the (ε, δ)-differential privacy constraint. Specifically, we improve existing minimax risk lower bounds for low-dimensional mean estimation and prove new lower bounds for linear regression problems as well as high-dimensional [1] mean estimation. These lower bound results are based on the tracing adversary argument, which originated in the theoretical computer science literature [9, 43]. Early works in this direction were primarily concerned with the accuracy of releasing in-sample quantities, such as k-way marginals, with differential privacy constraints. Some more recent works [21, 28] applied the idea to obtain lower bounds for estimating population quantities such as mean vectors of discrete and Gaussian distributions. Below is a brief summary of our results as compared to existing results; the details are in Sections 3 and 4.

(1) Improved lower bound for low-dimensional mean estimation. In Section 3.1, we show that the minimax squared ℓ_2 risk of sub-Gaussian mean

[1] In computer science literature, the term "high-dimension" refers to settings in which the dimension is allowed to grow with the sample size, and asymptotic dependence on the dimension is of interest. In statistics literature, including this paper, "high-dimension" typically implies that the dimension is greater than the sample size, so sparsity assumptions are often introduced to make the problem feasible.

estimation with (ε, δ)-differential privacy is at least $O\left(\frac{d^2 \log(1/\delta)}{n^2\varepsilon^2}\right)$ (Theorem 3.1), which improves the $O\left(\frac{d^2}{n^2\varepsilon^2}\right)$ minimax lower bound by [28] and matches the deterministic worst case lower bound by [43]. It is further shown that our lower bound is optimal as it can be attained by a differentially private algorithm, the noisy sample mean (Algorithm 1; Theorem 3.2).

(2) New lower bounds for linear regression and high-dimensional mean estimation. To the best of our knowledge, our minimax risk lower bounds for high-dimensional mean estimation and linear regression in both low and high dimensions are the first of their kind in the literature. In these three problems, the minimax squared ℓ_2 risk lower bounds are of the order $O\left(\frac{(s \log d)^2}{n^2\varepsilon^2}\right)$ (Theorem 3.3), $O\left(\frac{d^2}{n^2\varepsilon^2}\right)$ (Theorem 4.1), and $O\left(\frac{(s \log d)^2}{n^2\varepsilon^2}\right)$ (Theorem 4.3) respectively, where n, d and s denote the sample size, the dimension, and the sparsity of true parameter vector. For context, there exist several lower bound results for related but different problems: [44] found that the sample complexity lower bound of selecting the top-k largest coordinates of d-dimensional data depends linearly on k and only logarithmically on d; [5] established an excess empirical risk lower bound of $O\left(\frac{d}{n\varepsilon^2}\right)$ for (ε, δ)-differentially private empirical risk minimization, by explicitly constructing a worst-case strongly convex and Lipschitz objective function.

Differentially private algorithms. We show that the lower bound results are sharp up to logarithmic factors, by constructing differentially private algorithms with rates of convergence matching the corresponding lower bounds.

In low-dimensional problems, the algorithms (Algorithms 1 and 4) are similar to existing algorithms, such as the noisy Gaussian sample mean [29] or noisy gradient descent [5]. For low-dimensional regression, our contribution is in obtaining an upper bound of the parameter estimation error $\mathbb{E}\|\hat{\boldsymbol{\beta}}_{\text{private}} - \boldsymbol{\beta}_{\text{true}}\|_2^2 = \tilde{O}\left(\frac{d^2 \log(1/\delta)}{n^2\varepsilon^2}\right)$ (Theorem 4.2) for the noisy gradient descent algorithm, as opposed to the excess risk bound (or its empirical version) by previous works [5, 4]: $\mathbb{E}[\mathcal{L}_n(\hat{\boldsymbol{\beta}}_{\text{private}}) - \mathcal{L}_n(\hat{\boldsymbol{\beta}}_{\text{non-private}})] = O\left(\frac{\sqrt{d \log(1/\delta)}}{n\varepsilon}\right)$, where $\mathcal{L}_n$ is the least-square objective function of linear regression.

For high-dimensional sparse estimation, our algorithms, to the best of our knowledge, are the first results achieving optimal rates of convergence with the (ε, δ)-differential privacy constraint up to logarithmic factors. The high-dimensional mean estimation algorithm (Algorithms 3) is based on a novel application of the "peeling" algorithm first proposed by [22] for reporting top-k coordinates of a vector. The high-dimensional linear regression algorithm (Algorithm 5) can be understood as a private version

of iterative hard thresholding [7, 26], which, roughly speaking, is a projected gradient descent algorithm onto the set of sparse vectors. The focus of our theoretical analysis is again on the parameter estimation error $\mathbb{E}\|\hat{\boldsymbol{\beta}}_{\text{private}} - \boldsymbol{\beta}_{\text{true}}\|_2^2 = \tilde{O}\left(\frac{(s\log d)^2\log(1/\delta)}{n^2\varepsilon^2}\right)$ (Theorems 3.4 and 4.4), as opposed to excess risk results such as $\mathbb{E}[\mathcal{L}_n(\hat{\boldsymbol{\beta}}_{\text{private}}) - \mathcal{L}_n(\boldsymbol{\beta}_{\text{true}})] = O\left(\frac{s^3\log d}{n\varepsilon}\right)$ in [31] and $\mathbb{E}[\mathcal{L}_n(\hat{\boldsymbol{\beta}}_{\text{private}}) - \mathcal{L}_n(\hat{\boldsymbol{\beta}}_{\text{non-private}})] = O\left(\frac{\log d+\log(n/\delta)}{(n\varepsilon)^{2/3}}\right)$ in [45].

Other related literature. In theoretical computer science, [42] showed that under strong conditions for privacy parameters, some estimators attain the statistical convergence rates and hence privacy can be gained for free. [5, 23, 45] proposed differentially private algorithms for convex empirical risk minimization, principal component analysis, and high-dimensional sparse regression, and investigated the convergence rates of excess risk.

In the statistics literature, there has also been a series of works that studied differential privacy in statistical estimation. [48] observed that, locally differentially private schemes [30] seem to yield slower convergence rates than the optimal minimax rates in general; [15] developed a framework for deriving statistical minimax rates with the α-local privacy constraint; [40] proved several minimax optimal rates of convergence under α-local differential privacy and exhibited a mechanism that is minimax optimal for linear functionals based on randomized response. It has also been observed that α-local privacy is a much stronger notion of privacy than (ε, δ)-differential privacy that is hardly compatible with high-dimensional problems [15]. As we shall see in this paper, the cost of (ε, δ)-differential privacy in high-dimensional statistical estimation is quite different from that of α-local privacy.

Organization of the paper. The paper is organized as follows. Section 2 formally defines the "cost of privacy" in terms of statistical minimax risk and introduces our technical tools for upper and lower bounding the cost of privacy in various statistical problems. These technical tools are then applied to mean estimation and linear regression problems in Sections 3 and 4 respectively. The numerical performance of the mean estimation and linear regression algorithms are demonstrated by simulated experiments in Section 5 and by real data analysis in Section 6. Section 7 discusses implications of our results in other statistical estimation problems with privacy constraints. The proofs of our theoretical results are in Section 8 and the supplementary materials [10].

Notation. For real-valued sequences $\{a_n\}$ and $\{b_n\}$, we write $a_n \lesssim b_n$ if $a_n \le cb_n$ for some universal constant $c \in (0, \infty)$, and $a_n \gtrsim b_n$ if $a_n \ge c'b_n$ for some universal constant $c' \in (0, \infty)$. We say $a_n \asymp b_n$ if $a_n \lesssim b_n$ and $a_n \gtrsim b_n$. In this paper, $c, C, c_0, c_1, c_2, \cdots$, refer to universal constants, and their specific values may vary from place to place.

For a positive integer k, we write $[k]$ as short hand for $\{1, \cdots, k\}$. For a vector $\boldsymbol{v} \in \mathbb{R}^d$ and a subset $S \subseteq [d]$, we use $\boldsymbol{v}_S$ to denote the restriction of vector $\boldsymbol{v}$ to the index set S. We write $\mathrm{supp}(\boldsymbol{v}) := \{j \in [d] : v_j \neq 0\}$. $\|\boldsymbol{v}\|_p$ denotes the vector ℓ_p norm for $1 \leq p \leq \infty$, with an additional convention that $\|\boldsymbol{v}\|_0$ denotes the number of non-zero coordinates of $\boldsymbol{v}$. For a positive definite matrix Σ, we define $\|\boldsymbol{v}\|_\Sigma = \sqrt{\boldsymbol{v}^\top \Sigma \boldsymbol{v}}$. For $\boldsymbol{v} \in \mathbb{R}^d$ and $R > 0$, let $\Pi_R(\boldsymbol{v})$ denote the projection of $\boldsymbol{v}$ onto the ℓ_2 ball $\{\boldsymbol{u} \in \mathbb{R}^d : \|\boldsymbol{u}\|_2 \leq R\}$.

2. Problem Formulation. In this section, we start with a formal definition of the "cost of privacy" based on the minimax risk with differential privacy constraint, in Section 2.1. In Sections 2.2 and 2.3, we provide an overview of our technical tools for upper and lower bounding the cost of privacy.

2.1. *The Cost of Privacy.* We quantify the cost of differential privacy in statistical estimation via the minimax risk with differential privacy constraint, defined as follows.

Let $\mathcal{P}$ denote a family of distributions supported on a set $\mathcal{X}$, and let $\boldsymbol{\theta} : \mathcal{P} \to \Theta \subseteq \mathbb{R}^d$ denote a population quantity of interest. The statistician has access to a data set of n i.i.d. samples, $\boldsymbol{X} = (\boldsymbol{x}_1, ..., \boldsymbol{x}_n) \in \mathcal{X}^n$, drawn from some distribution $P \in \mathcal{P}$.

With the data, we estimate a population parameter $\boldsymbol{\theta}(P)$ by an estimator $M(\boldsymbol{X}) : \mathcal{X}^n \to \Theta$ that belongs to $\mathcal{M}_{\varepsilon,\delta}$, the collection of all (ε, δ)-differentially private procedures. The performance of $M(\boldsymbol{X})$ is measured by its distance to the truth $\boldsymbol{\theta}(P)$: let $\rho : \Theta \times \Theta \to \mathbb{R}^+$ be a metric induced by a norm $\|\cdot\|$ on Θ, namely $\rho(\boldsymbol{\theta}_1, \boldsymbol{\theta}_2) = \|\theta_1 - \theta_2\|$, and let $l : \mathbb{R}^+ \to \mathbb{R}^+$ be an increasing function, the minimax risk of estimating $\boldsymbol{\theta}(P)$ with differential privacy constraint is defined as

$$\inf_{M \in \mathcal{M}_{\varepsilon,\delta}} \sup_{P \in \mathcal{P}} \mathbb{E}\left[l(\rho(M(\boldsymbol{X}), \boldsymbol{\theta}(P)))\right]. \tag{2.1}$$

The quantity characterizes the worst-case performance over $\mathcal{P}$ of the best (ε, δ)-differentially private estimator. The difference between (2.1) and the usual, unconstrained minimax risk

$$\inf_{M} \sup_{P \in \mathcal{P}} \mathbb{E}\left[l(\rho(M(\boldsymbol{X}), \boldsymbol{\theta}(P)))\right]. \tag{2.2}$$

is the "cost of privacy". As (2.2) is well understood for mean estimation and linear regression problems, we focus on characterizing the constrained minimax risk (2.1) in this paper. More specifically, we establish upper and lower bounds of (2.1) with technical tools to be introduced in Sections 2.2 and 2.3.

2.2. *Construction of Differentially Private Algorithms.* It is frequently the case that differentially private algorithms are constructed by perturbing the output of a non-private algorithm with random noise. Among the most prominent examples are the Laplace and Gaussian mechanisms.

The Laplace and Gaussian mechanisms. As the name suggests, the Laplace and Gaussian mechanisms achieve differential privacy by perturbing an algorithm with Laplace and Gaussian noises respectively. The scale of such noises is determined by the sensitivity of the algorithm:

DEFINITION 2. For any algorithm f mapping a data set $\boldsymbol{X}$ to $\mathbb{R}^d$, The ℓ_p-sensitivity of f is

$$\Delta_p(f) = \sup_{\boldsymbol{X},\boldsymbol{X}' \text{ adjacent}} \|f(\boldsymbol{X}) - f(\boldsymbol{X}')\|_p.$$

The sensitivity of an algorithm f characterizes the magnitude of change in the output of f resulted from replacing one element in an input data set; naturally, we introduce some perturbation of comparable scale, so that the differentially private version of f is stable regardless of the presence or absence of any individual datum in the dataset.

For algorithms with finite ℓ_1-sensitivity, differential privacy can be attained by adding Laplace noises.

EXAMPLE 2.1 (The Laplace mechanism). For any algorithm f mapping a data set $\boldsymbol{X}$ to $\mathbb{R}^d$ such that $\Delta_1(f) < \infty$, $M_1(\boldsymbol{X}) := f(\boldsymbol{X}) + (\xi_1, \xi_2, \cdots, \xi_d)$, where $\xi_1, \xi_2, \cdots, \xi_d$ is an i.i.d. sample drawn from Laplace$(\Delta_1 f/\varepsilon)$, achieves $(\varepsilon, 0)$-differential privacy.

Adding Gaussian noises to algorithms with finite ℓ_2-sensitivity guarantees differential privacy.

EXAMPLE 2.2 (The Gaussian mechanism). For any algorithm f mapping a data set $\boldsymbol{X}$ to $\mathbb{R}^d$ such that $\Delta_2(f) < \infty$, $M_2(\boldsymbol{X}) := f(\boldsymbol{X}) + (\xi_1, \xi_2, \cdots, \xi_d)$, where $\xi_1, \xi_2, \cdots, \xi_k$ is an i.i.d. sample drawn from $N(0, 2(\Delta_2(f)/\varepsilon)^2 \log(1.25/\delta))$, achieves (ε, δ)-differential privacy.

Although conceptually simple, these mechanism can often lead to complex differentially private algorithms, thanks to the post-processing and composition properties of differential privacy.

Post-processing and Composition. Conveniently, post-processing a differentially private algorithm preserves privacy.

FACT 2.1 (Post-processing [17, 48]). Let f be an (ε, δ)-differentially private algorithm and g be an arbitrary, deterministic mapping that takes $f(\boldsymbol{X})$ as an input, then $g(f(\boldsymbol{X}))$ is (ε, δ)-differentially private.

Further, the privacy parameters are additive with respect to compositions of differentially private algorithms.

FACT 2.2 (Composition [17]). For $i = 1, 2$, let f_i be $(\varepsilon_i, \delta_i)$-differentially private, then $f_1 \circ f_2$ is $(\varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2)$-differentially private.

The mechanisms and composition theorem reviewed in this section shall later enable us to construct differentially private algorithms for mean estimation and linear regression.

2.3. *Minimax Risk Lower Bounds with Differential Privacy Constraint.* Our technique for proving lower bounds of the minimax risk (2.1) is based on the "tracing adversary" argument originally proposed by [9]. It has proven to be a powerful tool for obtaining lower bounds in the context of releasing sample quantities [43, 44] and for Gaussian mean estimation [21, 28]. In this paper, we refine the tracing adversary technique to prove a sharper lower bound for low-dimensional mean estimation compared to previous works [21, 28] as well as new lower bounds for sparse mean estimation and linear regression problems.

Informally, a tracing adversary (or tracing attack) is an algorithm that attempts to detect the absence/presence of a candidate datum $\tilde{\boldsymbol{x}}$ in a target data set $\boldsymbol{X}$, by looking at an estimator $M(\boldsymbol{X})$ computed from the data set. If one can construct a tracing adversary that is powerful given an accurate estimator, an argument by contradiction leads to a lower bound: suppose a differentially private estimator computed from the target data set is sufficiently accurate, the tracing adversary will be able to determine whether a given datum belongs to the data set or not, thereby contradicting with the differential privacy guarantee. The privacy guarantee and the tracing adversary together ensure that a differentially private estimator cannot be "too accurate". In Sections 3.1, 3.3, 4.1 and 4.3, we shall formally define and analyze such tracing attacks for mean estimation and linear regression problems. For now, we illustrate this general approach with a concrete example of sub-Gaussian mean estimation.

Example: a preliminary lower bound for mean estimation. To illustrate this approach, we consider a tracing attack proposed by [21] and show how its theoretical properties imply a minimax risk lower bound for differentially private mean estimation of d-dimensional sub-Gaussian(σ) distribution. Let $\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\}$ be an i.i.d. sample drawn from the d-dimensional product distribution supported on $\{-\sigma, \sigma\}^d$, which is clearly sub-Gaussian(σ), with unknown mean vector $\boldsymbol{\mu} \in [-\sigma, \sigma]^d$. The tracing attack is given by

$$\mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{x}, M(\boldsymbol{X})) = \langle \boldsymbol{x} - \boldsymbol{\mu}, M(\boldsymbol{X}) \rangle.$$

The theoretical properties of this tracing attack are presented in the following lemma.

LEMMA 2.1. *Let $\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\}$ be an i.i.d. sample drawn from the d-dimensional product distribution supported on $\{-\sigma, \sigma\}^d$ with unknown mean vector $\boldsymbol{\mu} \in [-\sigma, \sigma]^d$.*

1. *For each $i \in [n]$, let $\boldsymbol{X}_i'$ denote the data set obtained by replacing $\boldsymbol{x}_i$ in $\boldsymbol{X}$ with an independent copy, then for every $\delta > 0$, every $i \in [n]$ and every $\boldsymbol{\mu}$ we have*

$$\mathbb{P}(\mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{x}_i, M(\boldsymbol{X}_i')) > \sigma^2\sqrt{8d\log(1/\delta)}) < \delta.$$

2. *There is a universal constant c_1 such that, if $n < c_1\sqrt{d/\log(1/\delta)}$, we can find a prior distribution $\boldsymbol{\pi}$ of $\boldsymbol{\mu}$ so that*

$$\mathbb{P}_{\boldsymbol{X},\boldsymbol{\mu}}\left(\sum_{i\in[n]} \mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{x}_i, M(\boldsymbol{X})) \le n\sigma^2\sqrt{8d\log(1/\delta)}, \|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|_2 < c_2\sigma\sqrt{d}\right) < \delta$$

for an appropriate universal constant c_2.

The lemma is similar in spirit to Lemma 12 in [21] and proved with a new technical argument in Section B.1 of supplementary materials [10]. According to the lemma, when $M(\boldsymbol{X})$ is close to the sample mean $\bar{\boldsymbol{X}}$, the attack takes large values if the candidate datum belongs to the data set $\boldsymbol{X}$ from which $M(\boldsymbol{X})$ is computed.

We would like to point out that lemma 2.1 is valid without requiring differential privacy of $M(\boldsymbol{X})$. For a differentially private $M(\boldsymbol{X})$ in particular, the lemma makes available a lower bound for $\|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|$, as we have sketched informally: if $n < c_1\sqrt{d/\log(1/\delta)}$ and $M(\boldsymbol{X})$ is (ε, δ)-differentially private with $0 < \varepsilon < 1$ and $\delta = o(1/n)$, let $\mathcal{C} = \{\sum_{i\in[n]} \mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{x}_i, M(\boldsymbol{X})) \le n\sigma^2\sqrt{8d\log(1/\delta)}\}$,

$$\begin{aligned}
&\mathbb{P}_{\boldsymbol{X},\boldsymbol{\mu}}(\|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|_2 < c_2\sigma\sqrt{d}) \\
\le\ &\mathbb{P}_{\boldsymbol{X},\boldsymbol{\mu}}\left(\mathcal{C} \cap \{\|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|_2 < c_2\sigma\sqrt{d}\}\right) + \sum_{i\in[n]} \mathbb{P}_{\boldsymbol{X},\boldsymbol{\mu}}\left(\mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{x}_i, M(\boldsymbol{X})) > \sigma^2\sqrt{8d\log(1/\delta)}\right) \\
\le\ &\mathbb{P}_{\boldsymbol{X},\boldsymbol{\mu}}\left(\mathcal{C} \cap \{\|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|_2 < c_2\sigma\sqrt{d}\}\right) + n\left(e^{\varepsilon}\mathbb{P}(\mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{x}_i, M(\boldsymbol{X}_i')) > \sigma^2\sqrt{8d\log(1/\delta)}) + \delta\right) \\
\le\ &\delta + n(e^{\varepsilon}\delta + \delta) = o(1).
\end{aligned}$$

The second inequality is due to differential privacy; the third inequality uses Lemma 2.1. It follows that, when $n < c_1\sqrt{d/\log(1/\delta)}$, we have

(2.3)
$$\inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \sup_{\boldsymbol{\mu}} \mathbb{E}\|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|_2 \ge \inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \mathbb{E}_{\boldsymbol{\pi}}\mathbb{E}_{X|\boldsymbol{\mu}}\|M(\boldsymbol{X}) - \bar{\boldsymbol{X}}\|_2 \gtrsim \sigma\sqrt{d}.$$

It should be noted, however, that the lower bound result is unsatisfactory in two important ways. First, as formulated in Section 2.1, we are in fact interested in lower bounding a related but distinct quantity, $\inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \sup_{\boldsymbol{\mu}} \mathbb{E}\|M(\boldsymbol{X})-\boldsymbol{\mu}\|_2$. Second, the sample size range $n < c_1\sqrt{d/\log(1/\delta)}$ is somewhat artificial; for low-dimensional mean estimation problems, the usual setting of $n \gtrsim d$ is of greater interest. In Section 3.1, we shall resolve these issues and, on the basis of the same tracing attack and Lemma 2.1, establish an optimal lower bound for the mean estimation problem.

3. The Cost of Privacy in Mean Estimation. In this section, we study the cost of (ε,δ)-differential privacy in estimating the mean vector of a d-dimensional sub-Gaussian(σ) distribution. Formally, an $\mathbb{R}^d$-valued random variable $\boldsymbol{x}$ follows a sub-Gaussian(σ) distribution if for $\boldsymbol{\mu}=\mathbb{E}\boldsymbol{x}$ and any fixed vector $\|\boldsymbol{v}\|_2=1$, we have

$$\mathbb{E}\exp\left(\lambda\langle\boldsymbol{x}-\boldsymbol{\mu},\boldsymbol{v}\rangle\right)\le\exp(\lambda^2\sigma^2),\forall\lambda\in\mathbb{R}.$$

We begin with sharpening the preliminary lower bound (2.3), in Section 3.1. The lower bound is then shown to be optimal via an (ε,δ)-differentially private estimator with convergence rate attaining the lower bound.

We also study the cost of differential privacy in sparse mean estimation, where the unknown mean vector $\boldsymbol{\mu}\in\mathbb{R}^d$ has only a small fraction of non-zero coordinates. This sparse model is useful when the data's dimension d outnumbers the sample size n, rendering the usual sample mean estimator sub-optimal. Instead, if the unknown mean vector is indeed sparse, thresholding the sample mean have been shown to achieve optimal statistical accuracy [14, 27]. We establish in Section 3.3 a minimax risk lower bound for estimating sparse mean with differential privacy constraint, and match this lower bound with a differentially private estimator of the sparse mean in Section 3.4.

3.1. *Lower bound of low-dimensional mean estimation.* In this section, we prove a sharp lower bound for estimating a d-dimensional sub-Gaussian mean by improving the preliminary lower bound in Section 2.3. We consider the class of d-dimensional sub-Gaussian(σ) distributions with mean vector in $\Theta=\{\boldsymbol{\mu}\in\mathbb{R}^d:\|\boldsymbol{\mu}\|_\infty<\sigma\}$ and denote the class by $\mathcal{P}(\sigma,d,\Theta)$.

The first improvement is a relaxation of the sample size range $n \lesssim \sqrt{d/\log(1/\delta)}$.

LEMMA 3.1. *Let $\boldsymbol{Y}=\{\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_n\}$ be sampled with replacement from a set of deterministic vectors $\boldsymbol{Z}=\{\boldsymbol{z}_1,\boldsymbol{z}_2,\cdots,\boldsymbol{z}_m\}$ with $n=km$ and $k\ge 1$. There exists a choice of $\boldsymbol{Z}$ with each $\boldsymbol{z}_i\in\{-\sigma,\sigma\}^d$, $m=c_1\sqrt{d/\log(1/\delta)}\gtrsim 1$ and $k\asymp\log(1/\delta)/\varepsilon$ such that*

$$\mathbb{E}\|M(\boldsymbol{Y})-\mathbb{E}\boldsymbol{y}_1\|_2\gtrsim\sigma\sqrt{d}$$

for every (ε, δ)*-differentially private* M *if* $0 < \varepsilon < 1$, $n^{-1}\exp(-n\varepsilon) < \delta < n^{-(1+\omega)}$ *for some fixed constant* $\omega > 0$, *and* $\log(\delta)/\log(n)$ *is non-increasing in* n.

Lemma 3.1 is proved in Section 8.1. In essence, this lemma improves the lower bound (2.3) by extending its range of validity to $n \lesssim \sqrt{d\log(1/\delta)}/\varepsilon$, as the discrete uniform distribution described in the lemma is sub-Gaussian(σ) with $\boldsymbol{\mu} \in \Theta$ thanks to the choice of $\boldsymbol{z}_i \in \{-\sigma, \sigma\}^d$.

On the basis of Lemma 3.1, we are able to translate the lower bound result to the more interesting large n regime, as described by the following theorem.

THEOREM 3.1. *Let* $\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\}$ *be an i.i.d. sample drawn from some distribution in* $\mathcal{P}(d, \sigma, \Theta)$ *with mean* $\mathbb{E}\boldsymbol{x}_1 = \boldsymbol{\mu}$. *If* $0 < \varepsilon < 1$, $n^{-1}\exp(-n\varepsilon) < \delta < n^{-(1+\omega)}$ *for some fixed constant* $\omega > 0$ *with* $\log(\delta)/\log(n)$ *non-increasing in* n, $d/\log(1/\delta) \gtrsim 1$ *and* $n \gtrsim \sqrt{d\log(1/\delta)}/\varepsilon$, *we have*

$$\inf_{M \in \mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(d,\sigma,\Theta)} \mathbb{E}\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2^2 \gtrsim \sigma^2 \left(\frac{d}{n} + \frac{d^2\log(1/\delta)}{n^2\varepsilon^2}\right). \tag{3.1}$$

The theorem is proved in Section 8.2. The minimax lower bound characterizes the cost of privacy in the mean estimation problem: the cost of privacy dominates the statistical risk when $d\log(1/\delta)/n\varepsilon^2 \gtrsim 1$. This minimax lower bound matches the sample complexity lower bound in [43], which considered the deterministic worst case instead of the i.i.d. statistical setting. [28] studied the Gaussian mean estimation problem but did not obtain a tight bound with respect to δ; Theorem 3.1 improves the lower bound in [28] by $\log(1/\delta)$. In Section 3.2, we exhibit an algorithm for mean estimation that attains the convergence rate of $\sigma^2\left(\frac{d}{n} + \frac{d^2\log(1/\delta)}{n^2\varepsilon^2}\right)$, showing that the lower bound (3.1) is in fact rate-optimal.

3.2. *Algorithm for low-dimensional mean estimation.* In this section, we show that the minimax lower bound (3.1) can be attained by a differentially private estimator, thereby implying a tight characterization of the cost of privacy in low-dimensional mean estimation.

Let $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n$ be an i.i.d. sample drawn from a sub-Gaussian(σ) distribution on $\mathbb{R}^d$, and we denote $\mathbb{E}\boldsymbol{x}_1$ by $\boldsymbol{\mu} \in \mathbb{R}^d$. It is further assumed that $\|\boldsymbol{\mu}\|_\infty < c$ for some constant $c = O(1)$. We consider the following simple algorithm based on the Gaussian mechanism, Example 2.2.

Algorithm 3.1: Differentially Private Mean Estimation

Input : Data set $\boldsymbol{X} = \{\boldsymbol{x}_i\}_{i\in[n]}$, privacy parameters ε, δ, truncation level R.

1 Compute $\overline{\boldsymbol{X}}_R$: for $j \in [d]$, $\overline{\boldsymbol{X}}_{R,j} = n^{-1}\sum_{i\in[n]} \Pi_R(x_{ij})$;

2 Compute $\hat{\boldsymbol{\mu}} = \boldsymbol{X}_R + \boldsymbol{w}$, where $\boldsymbol{w} \sim N_d\left(\boldsymbol{0}, \frac{4R^2 d\log(1/\delta)}{n^2\varepsilon^2}\cdot \boldsymbol{I}\right)$;

Output: $\hat{\boldsymbol{\mu}}$.

The truncation step guarantees that, over a pair of data sets $\boldsymbol{X}$ and $\boldsymbol{X}'$ which differ by one single entry, $\|\overline{\boldsymbol{X}}_R - \overline{\boldsymbol{X}'}_R\|_2 < 2R\sqrt{d}/n$ and therefore the Gaussian mechanism applies. When R is selected so that most of the data is preserved, $\hat{\boldsymbol{\mu}}$ is an accurate estimator of the mean $\boldsymbol{\mu}$.

THEOREM 3.2. *If there exists a constant $T < \infty$ so that $\|\boldsymbol{x}\|_\infty < T$ with probability one, setting $R = T$ ensures that*

$$\mathbb{E}\|\hat{\boldsymbol{\mu}} - \boldsymbol{\mu}\|_2^2 \lesssim \sigma^2\left(\frac{d}{n} + \frac{d^2\log(1/\delta)}{n^2\varepsilon^2}\right).$$

Otherwise, choosing $R = K\sigma\sqrt{\log n}$ for a sufficiently large K guarantees

$$\mathbb{E}\|\hat{\boldsymbol{\mu}} - \boldsymbol{\mu}\|_2^2 \lesssim \sigma^2\left(\frac{d}{n} + \frac{d^2\log(1/\delta)\log n}{n^2\varepsilon^2}\right).$$

The theorem is proved in Section A.1 of the supplement [10]. The first case applies to distributions with bounded support, e.g. Bernoulli, with the rate of convergence exactly matching the lower bound (3.1). The second case includes unbounded sub-Gaussian distributions such as the Gaussian, where the convergence rate matches the lower bound up to a gap of $O(\log n)$. Overall, the upper and lower bounds suggest that the cost of (ε, δ)-differential privacy in low-dimensional mean estimation is $\tilde{O}\left(\frac{d^2\log(1/\delta)}{n^2\varepsilon^2}\right)$.

It should be noted that Algorithm 1 lacks some practicality: the truncation level R is a tuning parameter that needs to be set at the correct level for the convergence rate to hold; we included this somewhat simplistic algorithm here for the theoretical analysis of privacy cost. In Section 5, we consider data-driven and differentially private proxies of the theoretical choice of R and demonstrate their numerical performance. As the focus of this paper is theoretical properties of private estimators, we refer interested readers to [29] and [6] for more practical methods of differentially private mean estimation.

3.3. *Lower bound of sparse mean estimation.* We consider lower bounding the minimax risk of estimating the mean vector of a sub-Gaussian(σ) distribution when the mean vector is s^*-sparse. Concretely, we index this collection of distributions by the set of mean vectors $\Theta = \{\boldsymbol{\mu} \in \mathbb{R}^d : \|\boldsymbol{\mu}\|_0 \le s^*, \|\boldsymbol{\mu}\|_\infty < 1\}$, and denote this class of distributions by $\mathcal{P}(\sigma, d, s^*, \Theta)$. Let

$\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\}$ be an i.i.d. sample drawn from a sub-Gaussian(σ) distribution with mean vector $\boldsymbol{\mu} \in \Theta$, we would like to establish a lower bound of $\inf_{M \in \mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(\sigma,d,s^*,\Theta)} \mathbb{E}\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2^2$ as a function of privacy parameters (ε, δ) as well as d, n, s^* and σ.

As sketched in Section 2.3, our strategy for proving the lower bound requires the existence of a powerful tracing attack. For sparse mean estimation, one reasonable choice of tracing attack is given by

$$\mathcal{A}_{\boldsymbol{\mu},s^*}(\boldsymbol{x}, M(\boldsymbol{X})) = \langle (\boldsymbol{x} - \boldsymbol{\mu})_{\mathrm{supp}(\boldsymbol{\mu})}, M(\boldsymbol{X}) - \boldsymbol{\mu} \rangle. \tag{3.2}$$

In particular, this attack coincides with the tracing attack proposed by [44] for differentially private top-k selection.

Similar to our lower bound analysis for low-dimensional mean estimation, the key ingredient is to show that the attack typically takes a large value when $\tilde{\boldsymbol{x}}$ belongs to $\boldsymbol{X}$ and a small value otherwise. This is indeed the case for the tracing attack (3.2), as described by the following lemma.

LEMMA 3.2. *Let $\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n\}$ be an i.i.d. sample drawn from $N_d(\boldsymbol{\mu}, \sigma^2 \boldsymbol{I})$ with $\boldsymbol{\mu} \in \Theta$. If $s^* = o(d^{1-\omega})$ for some fixed $\omega > 0$, for every (ε, δ)-differentially private estimator M satisfying $\mathbb{E}_{\boldsymbol{X}|\boldsymbol{\mu}}\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2^2 = o(1)$ at every $\boldsymbol{\mu} \in \Theta$, the following are true.*

1. *For each $i \in [n]$, let $\boldsymbol{X}_i'$ denote the data set obtained by replacing $\boldsymbol{x}_i$ in $\boldsymbol{X}$ with an independent copy, then*

$$\mathbb{E}\mathcal{A}_{\boldsymbol{\mu},s^*}(\boldsymbol{x}_i, M(\boldsymbol{X}_i')) = 0, \mathbb{E}|\mathcal{A}_{\boldsymbol{\mu},s^*}(\boldsymbol{x}_i, M(\boldsymbol{X}_i'))| \le \sigma \sqrt{\mathbb{E}\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2^2}.$$

2. *There exists a prior distribution of $\boldsymbol{\pi} = \boldsymbol{\pi}(\boldsymbol{\mu})$ supported over Θ such that*

$$\sum_{i \in [n]} \mathbb{E}_{\boldsymbol{\pi}} \mathbb{E}_{\boldsymbol{X}|\boldsymbol{\mu}} \mathcal{A}_{\boldsymbol{\mu},s^*}(\boldsymbol{x}_i, M(\boldsymbol{X})) \gtrsim \sigma^2 s^* \log d.$$

The lemma is proved in Section B.2 of the supplement [10]. On the basis of Lemma 3.2, we have the following minimax risk lower bound.

THEOREM 3.3. *If $s^* = o(d^{1-\omega})$ for some fixed $\omega > 0$, $0 < \varepsilon < 1$ and $\delta < n^{-(1+\omega)}$ for some fixed $\omega > 0$, we have*

$$\inf_{M \in \mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(\sigma,d,s^*,\Theta)} \mathbb{E}\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2^2 \gtrsim \sigma^2 \left(\frac{s^* \log d}{n} + \frac{(s^* \log d)^2}{n^2 \varepsilon^2} \right). \tag{3.3}$$

The lower bound is proved in Section B.3 of the supplement [10]. In this lower bound, it is worth noting that the term due to privacy, similar to the statistical term, only depends logarithmically on the dimension d, suggesting that mean estimation in high dimensions remains viable despite the

(ε, δ)-differential privacy constraint. This is in marked contrast with high-dimensional statistical estimation under the (much more demanding) local differential privacy constraint [30, 15], where the minimax risk always depends linearly on d. In the next section, we propose a differentially private estimator that efficiently estimates the sparse mean vector and attains the lower bound (3.3) up to factors of $\log n$.

3.4. *Algorithm for sparse mean estimation.* Let $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n$ be an i.i.d. sample drawn from a sub-Gaussian(σ) distribution on $\mathbb{R}^d$, with mean $\mathbb{E}\boldsymbol{x}_1 = \boldsymbol{\mu} \in \mathbb{R}^d$. It is further assumed that $\|\boldsymbol{\mu}\|_0 \leq s^*$ and $\|\boldsymbol{\mu}\|_\infty < c$ for some constant $c = O(1)$.

In this section, we propose a differentially private algorithm for estimating the sparse mean vector $\boldsymbol{\mu}$. At a high level, the algorithm selects the large coordinates of the (truncated) sample mean vector in a differentially private manner, and sets the remaining coordinates to zero. We start with describing and analyzing the differentially private selection step.

The following "peeling" algorithm, developed by [22], is an efficient and differentially private method for selecting the top-s largest coordinates in terms of absolute value. In each of the s iterations, one coordinate is "peeled" from the original vector and added to the output set.

Algorithm 3.2: "Peeling" [22]

Input : vector-valued function $\boldsymbol{v} = \boldsymbol{v}(\boldsymbol{X}) \in \mathbb{R}^d$, data $\boldsymbol{X}$, sparsity s, privacy parameters ε, δ, noise scale λ.

Initialize $S = \emptyset$;

for i *in* 1 **to** s **do**

  Generate $\boldsymbol{w}_i \in \mathbb{R}^d$ with

  $$w_{i1}, w_{i2}, \cdots, w_{id} \overset{\text{i.i.d.}}{\sim} \text{Laplace}\left(\lambda \cdot \frac{2\sqrt{3s\log(1/\delta)}}{\varepsilon}\right);$$

  Append $j^* = \arg\max_{j \in [d] \setminus S} |v_j| + w_{ij}$ to S;

end

Set $\tilde{P}_s(\boldsymbol{v}) = \boldsymbol{v}_S$;

Generate $\tilde{\boldsymbol{w}}$ with $\tilde{w}_1, \cdots, \tilde{w}_d \overset{\text{i.i.d.}}{\sim} \text{Laplace}\left(\lambda \cdot \frac{2\sqrt{3s\log(1/\delta)}}{\varepsilon}\right)$;

Output: $\tilde{P}_s(\boldsymbol{v}) + \tilde{\boldsymbol{w}}_S$.

The algorithm is guaranteed to be differentially private when the vector $\boldsymbol{v} = v(\boldsymbol{X})$ has bounded change in value when any single datum in $\boldsymbol{X}$ is modified.

LEMMA 3.3 ([22]). *If for every pair of adjacent data sets $\boldsymbol{Z}, \boldsymbol{Z}'$ we have $\|\boldsymbol{v}(\boldsymbol{Z}) - \boldsymbol{v}(\boldsymbol{Z}')\|_\infty < \lambda$, then Algorithm 2 is an (ε, δ)-differentially private algorithm.*

Another important property of the Peeling algorithm is its (approximate) accuracy, proved in Section A.2 of the supplement.

LEMMA 3.4. *Let S and $\{\boldsymbol{w}\}_{i\in[s]}$ be defined as in Algorithm 2. For every $R_1 \subseteq S$ and $R_2 \in S^c$ such that $|R_1| = |R_2|$ and every $c > 0$, we have*

$$\|\boldsymbol{v}_{R_2}\|_2^2 \le (1+c)\|\boldsymbol{v}_{R_1}\|_2^2 + 4(1+1/c)\sum_{i\in[s]}\|\boldsymbol{w}_i\|_\infty^2.$$

Now returning to the original problem of sparse mean estimation, we construct a differentially estimator of the sparse mean by applying the "peeling" algorithm to a (truncated) sample mean, as follows.

Algorithm 3.3: Differentially Private Sparse Mean Estimation

Input : Data set $\boldsymbol{X} = \{\boldsymbol{x}_i\}_{i\in[n]}$, privacy parameters ε, δ, truncation level R, sparsity s.

1 Compute $\overline{\boldsymbol{X}}_R$: for $j \in [d]$, $\overline{\boldsymbol{X}}_{R,j} = n^{-1}\sum_{i\in[n]}\Pi_R(x_{ij})$;

2 Compute $\hat{\boldsymbol{\mu}} = \texttt{Peeling}(\overline{\boldsymbol{X}}_R, \boldsymbol{X}, s, \varepsilon, \delta, 2R/n)$;

Output: $\hat{\boldsymbol{\mu}}$.

The truncation step ensures that, over a pair of data sets $\boldsymbol{X}$ and $\boldsymbol{X}'$ which differ by one single entry, $\|\overline{\boldsymbol{X}}_R - \overline{\boldsymbol{X}'}_R\|_\infty < 2R/n$ and therefore the privacy guarantee, Lemma 3.3, applies. Algorithm 3 further inherits the accuracy of "Peeling" and leads to an accurate estimator of the sparse mean $\boldsymbol{\mu}$, as stated in the following theorem.

THEOREM 3.4. *If $R = K\sigma\sqrt{\log n}$ for a sufficiently large constant K, $s \ge s^*$ and $s \asymp s^*$, then with probability at least $1 - c_1\exp(-c_2\log n) - c_1\exp(-c_2\log d)$, it holds that*

$$\|\hat{\boldsymbol{\mu}} - \boldsymbol{\mu}\|_2^2 \lesssim \sigma^2\left(\frac{s^*\log d}{n} + \frac{(s^*\log d)^2\log(1/\delta)\log n}{n^2\varepsilon^2}\right).$$

Theorem 3.4 is proved in Section A.3. With the usual choice of $\delta = n^{-(1+\omega)}$, the convergence rate of Algorithm 3 attains the lower bound, Theorem 3.3, up to a gap of $\log^2 n$. While the convergence analysis of Algorithm 3 requires some theoretical choice of tuning parameters R and s, in Section 5 we discuss data-driven methods of selecting these tuning parameters that achieve reasonably good numerical performance.

4. The Cost of Privacy in Linear Regression. In this section, we consider the Gaussian linear model

$$f_{\boldsymbol{\beta}}(y|\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(\frac{-(y-\boldsymbol{x}^\top\boldsymbol{\beta})^2}{2\sigma^2}\right); \boldsymbol{x} \sim f_{\boldsymbol{x}}. \tag{4.1}$$

Given an i.i.d. sample $(\boldsymbol{y}, \boldsymbol{X}) = \{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$ drawn from the model, we study the cost of (ε, δ)-differential privacy in estimating the regression coefficients $\boldsymbol{\beta} \in \mathbb{R}^d$. The primary focus is on the high-dimensional setting (Sections 4.3, 4.4) where the dimension d dominates the sample size n, and the regression coefficient $\boldsymbol{\beta}$ is assumed to be sparse; the classical, low-dimensional case of $d = o(n)$ will also be considered (Sections 4.1, 4.2).

4.1. *Lower bound of low-dimensional linear regression.* Let $\mathcal{P}(\sigma, d, \Theta)$ denote the class of distributions $f_{\boldsymbol{\beta}}(y, \boldsymbol{x})$, as specified by (4.1), with $\boldsymbol{\beta} \in \Theta = \{\boldsymbol{\beta} \in \mathbb{R}^d : \|\boldsymbol{\beta}\|_2 \le 1\}$. With an i.i.d. sample $(\boldsymbol{y}, \boldsymbol{X}) = \{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$ drawn from a distribution in $\mathcal{P}(\sigma, d, \Theta)$, we shall establish a lower bound of $\inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(\sigma,d,\Theta)} \mathbb{E}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|^2_{\Sigma_{\boldsymbol{x}}}$ via the tracing attack argument.

Consider the attack given by

$$\mathcal{A}_{\boldsymbol{\beta}}((y, \boldsymbol{x}), M(\boldsymbol{y}, \boldsymbol{X})) = \big\langle M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}, (y - \boldsymbol{x}^\top\boldsymbol{\beta})\boldsymbol{x}\big\rangle. \tag{4.2}$$

Similar to the tracing attacks for mean estimation problems, the attack takes large value when $(y, \boldsymbol{x})$ belongs to $(\boldsymbol{y}, \boldsymbol{X})$ and small value otherwise.

LEMMA 4.1. *Let $(\boldsymbol{y}, \boldsymbol{X})$ be an i.i.d. sample drawn from some distribution in $\mathcal{P}(\sigma, d, \Theta)$ such that $\|\boldsymbol{x}\|_2 \le 1$ with probability 1, and $\Sigma_{\boldsymbol{x}} = \mathbb{E}\boldsymbol{x}\boldsymbol{x}^\top$ is diagonal and satisfies $0 < 1/L < d\lambda_{\min}(\Sigma_{\boldsymbol{x}}) \le d\lambda_{\max}(\Sigma_{\boldsymbol{x}}) < L$ for some constant $L = O(1)$. For every (ε, δ)-differentially private estimator M satisfying $\mathbb{E}_{\boldsymbol{y},\boldsymbol{X}|\boldsymbol{\beta}}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|_2^2 = o(1)$ at every $\boldsymbol{\beta} \in \Theta$, the following are true.*

1. *For each $i \in [n]$, let $(\boldsymbol{y}_i', \boldsymbol{X}_i')$ denote the data set obtained by replacing $(y_i, \boldsymbol{x}_i)$ in $(\boldsymbol{y}, \boldsymbol{X})$ with an independent copy, then $\mathbb{E}\mathcal{A}_{\boldsymbol{\beta}}((y_i, \boldsymbol{x}_i), M(\boldsymbol{y}_i', \boldsymbol{X}_i')) = 0$ and*
$$\mathbb{E}|\mathcal{A}_{\boldsymbol{\beta}}((y_i, \boldsymbol{x}_i), M(\boldsymbol{y}_i', \boldsymbol{X}_i'))| \le \sigma\sqrt{\mathbb{E}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|^2_{\Sigma_{\boldsymbol{x}}}}.$$
2. *There exists a prior distribution of $\boldsymbol{\pi} = \boldsymbol{\pi}(\boldsymbol{\beta})$ supported over Θ such that*
$$\sum_{i\in[n]} \mathbb{E}_{\boldsymbol{\pi}}\mathbb{E}_{\boldsymbol{y},\boldsymbol{X}|\boldsymbol{\beta}}\mathcal{A}_{\boldsymbol{\beta}}((y_i, \boldsymbol{x}_i), M(\boldsymbol{y}, \boldsymbol{X})) \gtrsim \sigma^2 d.$$

The lemma is proved in Section B.4 of the supplement [10]. These properties of tracing attack imply a minimax lower bound for (ε, δ)-differentially private estimation of $\boldsymbol{\beta}$.

THEOREM 4.1. *If $0 < \varepsilon < 1$ and $\delta < n^{-(1+\omega)}$ for some fixed $\omega > 0$, we have*

$$\inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(\sigma,d,\Theta)} \mathbb{E}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|^2_{\Sigma_{\boldsymbol{x}}} \gtrsim \sigma^2\left(\frac{d}{n} + \frac{d^2}{n^2\varepsilon^2}\right). \tag{4.3}$$

The lower bound is proved in Section B.5 of the supplement [10]. In next section, we show that the lower bound is sharp up to factors of $\log n$ by analyzing a differentially private algorithm for estimating $\boldsymbol{\beta}$.

4.2. *Algorithm for low-dimensional linear regression.* For the low-dimensional linear regression problem, we seek a differentially private (approximate) minimizer of the least square objective function

$$\mathcal{L}_n(\boldsymbol{\beta}) = \frac{1}{n}\sum_{i=1}^{n}(y_i - \boldsymbol{x}_i^\top \boldsymbol{\beta})^2.$$

We find this solution via the noisy gradient descent algorithm of [5]. We tailor the convergence analysis to the linear regression problem to obtain convergence in $O(\log n)$ iterations, as opposed to $O(n)$ iterations required by the general-purpose version in [5]. The algorithm and its theoretical properties are described in detail in this section.

Algorithm 4.1: Differentially Private Linear Regression

Input : $\mathcal{L}_n(\boldsymbol{\beta})$, data set $\{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$, step size η^0, privacy parameters ε, δ, noise scale B, number of iterations T, truncation level R, feasibility parameter C, initial value $\boldsymbol{\beta}^0$.

for t *in* 0 **to** $T-1$ **do**

  Generate $\boldsymbol{w}_t \in \mathbb{R}^d$ with $w_{t1}, w_{t2}, \cdots, w_{td} \overset{\text{i.i.d.}}{\sim} N\left(0, (\eta^0)^2 2B^2 \frac{\log(2T/\delta)}{n^2(\varepsilon/T)^2}\right)$;

  Compute $\boldsymbol{\beta}^{t+1} = \Pi_C\left(\boldsymbol{\beta}^t - (\eta^0/n)\sum_{i=1}^{n}(\boldsymbol{x}_i^\top \boldsymbol{\beta}^t - \Pi_R(y_i))\boldsymbol{x}_i + \boldsymbol{w}_t\right)$;

end

Output: $\boldsymbol{\beta}^T$.

The analysis of Algorithm 4 relies on some assumptions about $\boldsymbol{x}$ and $\boldsymbol{\beta}$.

(D1) Bounded design: there is a constant $c_{\boldsymbol{x}} < \infty$ such that $\|\boldsymbol{x}\|_2 < c_{\boldsymbol{x}}$ with probability 1.

(D2) Bounded moments of design: $\mathbb{E}\boldsymbol{x} = \mathbf{0}$ and the covariance matrix $\Sigma_{\boldsymbol{x}} = \mathbb{E}\boldsymbol{x}\boldsymbol{x}^\top$ satisfies $0 < 1/L < d \cdot \lambda_{\min}(\Sigma_{\boldsymbol{x}}) \le d \cdot \lambda_{\max}(\Sigma_{\boldsymbol{x}}) < L$ for some constant $0 < L < \infty$.

(P1) The true parameter vector $\boldsymbol{\beta}$ satisfies $\|\boldsymbol{\beta}\|_2 < c_0$ for some constant $0 < c_0 < \infty$.

In essence, the assumptions on design require that the rows of design matrix are normalized, and the assumed ℓ_2 bound of $\boldsymbol{\beta}$ is consistent with the parameter regime in our lower bound analysis, Section 4.1.

Assumptions (D1) and (P1) together guarantee that the algorithm is (ε, δ)-differentially private if the noise level B is sufficiently large.

LEMMA 4.2. *If assumptions (D1) and (P1) are true, then Algorithm 4 is (ε, δ)-differentially private as long as $B \ge 4(R + c_0 c_{\boldsymbol{x}})c_{\boldsymbol{x}}$ and $C \le c_0$.*

The lemma is proved in Section A.4 of the supplement [10]. If (D2) is true as well, we obtain the following theorem which describes the convergence rate of Algorithm 4.

THEOREM 4.2. *Let* $\{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$ *be an i.i.d. sample from the linear model* (4.1). *Suppose assumptions (D1), (D2), (P1) are true. Let the parameters of Algorithm* 4 *be chosen as follows.*

- *Set step size* $\eta^0 = d/2L$, *where* L *is the constant defined in assumption (D2).*
- *Set* $R = \sigma\sqrt{2\log n}$, $B = 4(R + c_0 c_{\boldsymbol{x}})c_{\boldsymbol{x}}$ *and* $C = c_0$, *in accordance with Lemma 4.2.*
- *Number of iterations* T. *Let* $T = (8L^2)\log(c_0^2 n)$, *where* L *is the constant defined in assumption (D2).*
- *Initialization* $\boldsymbol{\beta}^0 = \mathbf{0}$.

If $n \geq K \cdot \left(Rd^{3/2}\sqrt{\log(1/\delta)}\log n \log\log n/\varepsilon\right)$ *for a sufficiently large constant* K, *the output of Algorithm 4 satisfies*

$$\|\boldsymbol{\beta}^T - \boldsymbol{\beta}^*\|_{\Sigma_{\boldsymbol{x}}}^2 \lesssim \sigma^2\left(\frac{d}{n} + \frac{d^2\log(1/\delta)\log^3 n}{n^2\varepsilon^2}\right), \tag{4.4}$$

with probability at least $1 - c_1\exp(-c_2 n) - c_1\exp(-c_2 d) - c_1\exp(-c_2\log n)$.

Theorem 4.2 is proved in Section A.5 of the supplement [10]. For practical application of the algorithm, we note that the theoretical choice of truncation level R, which ensures the privacy protection of the algorithm, depends on the often unknown quantity σ. We provide a data-driven, differentially private alternative to this theoretical choice and demonstrate its numerical performance in Section 5.

4.3. *Lower bound of high-dimensional linear regression.* We next consider the high-dimensional linear regression problem where d potentially dominates sample size n, but the estimand $\boldsymbol{\beta}$ is sparse. Concretely, let $\mathcal{P}(\sigma, d, s^*, \Theta)$ denote the class of distributions $f_{\boldsymbol{\beta}}(y, \boldsymbol{x})$, as specified by (4.1), with $\boldsymbol{\beta} \in \Theta = \{\boldsymbol{\beta} \in \mathbb{R}^d : \|\boldsymbol{\beta}\|_0 \leq s^*, \|\boldsymbol{\beta}\|_2 \leq 1\}$. With an i.i.d. sample $(\boldsymbol{y}, \boldsymbol{X}) = \{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$ drawn from a distribution in $\mathcal{P}(\sigma, d, s^*, \Theta)$, we consider lower bounding $\inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(\sigma,d,s^*,\Theta)} \mathbb{E}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|_{\Sigma_{\boldsymbol{x}}}^2$ via the tracing attack argument.

Consider the attack given by

$$\mathcal{A}_{\boldsymbol{\beta},s^*}((y, \boldsymbol{x}), M(\boldsymbol{y}, \boldsymbol{X})) = \big\langle (M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta})_{\mathrm{supp}(\boldsymbol{\beta})}, (y - \boldsymbol{x}^\top\boldsymbol{\beta})\boldsymbol{x}\big\rangle. \tag{4.5}$$

Similar to the tracing attacks for mean estimation problems, the attack takes large value when $(y, \boldsymbol{x})$ belongs to $(\boldsymbol{y}, \boldsymbol{X})$ and small value otherwise.

LEMMA 4.3. *Let $(\boldsymbol{y}, \boldsymbol{X})$ be an i.i.d. sample drawn from some distribution in $\mathcal{P}(\sigma, d, s^*, \Theta)$. Let $S = \operatorname{supp}(\boldsymbol{\beta})$; assume that $\|\boldsymbol{x}_S\|_2 \le 1$ and $\boldsymbol{x}_{S^c} = \mathbf{0}$ with probability 1, and that the restricted covariance matrix $\Sigma_S = \{\mathbb{E}(\boldsymbol{x}\boldsymbol{x}^\top)\}_{i,j\in S}$ is diagonal and satisfies $0 < 1/L < s^*\lambda_{\min}(\Sigma_{\boldsymbol{x}}) \le s^*\lambda_{\max}(\Sigma_{\boldsymbol{x}}) < L$ for some constant $L = O(1)$.*

If $s^* = o(d^{1-\omega})$ for some fixed $\omega > 0$, then for every (ε, δ)-differentially private estimator M satisfying $\mathbb{E}_{\boldsymbol{y},\boldsymbol{X}|\boldsymbol{\beta}}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|_2^2 = o(1)$ at every $\boldsymbol{\beta} \in \Theta$, the following are true.

1. *For each $i \in [n]$, let $(\boldsymbol{y}_i', \boldsymbol{X}_i')$ denote the data set obtained by replacing $(y_i, \boldsymbol{x}_i)$ in $(\boldsymbol{y}, \boldsymbol{X})$ with an independent copy, then $\mathbb{E}\mathcal{A}_{\boldsymbol{\beta},s^*}((y_i, \boldsymbol{x}_i), M(\boldsymbol{y}_i', \boldsymbol{X}_i')) = 0$ and*

$$\mathbb{E}|\mathcal{A}_{\boldsymbol{\beta},s^*}((y_i, \boldsymbol{x}_i), M(\boldsymbol{y}_i', \boldsymbol{X}_i'))| \le \sigma\sqrt{\mathbb{E}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|_{\Sigma_{\boldsymbol{x}}}^2}.$$

2. *There exists a prior distribution of $\boldsymbol{\pi} = \boldsymbol{\pi}(\boldsymbol{\beta})$ over Θ such that*

$$\sum_{i\in[n]} \mathbb{E}_{\boldsymbol{\pi}}\mathbb{E}_{\boldsymbol{y},\boldsymbol{X}|\boldsymbol{\beta}}\mathcal{A}_{\boldsymbol{\beta},s^*}((y_i, \boldsymbol{x}_i), M(\boldsymbol{y}, \boldsymbol{X})) \gtrsim \sigma^2 s^* \log d.$$

The lemma is proved in Section B.6 of the supplement [10]. These properties of tracing attack (4.5) imply a minimax lower bound for (ε, δ)-differentially private estimation of $\boldsymbol{\beta}$.

THEOREM 4.3. *If $s^* = o(d^{1-\omega})$ for some fixed $\omega > 0$, $0 < \varepsilon < 1$ and $\delta < n^{-(1+\omega)}$ for some fixed $\omega > 0$, we have*

$$\inf_{M\in\mathcal{M}_{\varepsilon,\delta}} \sup_{\mathcal{P}(\sigma,d,s^*,\Theta)} \mathbb{E}\|M(\boldsymbol{y}, \boldsymbol{X}) - \boldsymbol{\beta}\|_{\Sigma_{\boldsymbol{x}}}^2 \gtrsim \sigma^2\left(\frac{s^*\log d}{n} + \frac{(s^*\log d)^2}{n^2\varepsilon^2}\right). \tag{4.6}$$

The lower bound is proved in Section B.7 of the supplement [10]. Similar to the cost of privacy in high-dimensional mean estimation, the lower bound here depends only logarithmically on dimension d. We show in the next section that this lower bound is achieved up to factors of $\log n$ by an (ε, δ)-differentially private algorithm.

4.4. *Algorithm for high-dimensional linear regression.* When the dimension of $\boldsymbol{\beta}$ exceeds the sample size, directly minimizing $\mathcal{L}_n(\boldsymbol{\beta}) = n^{-1}\sum_{i=1}^n (y_i - \boldsymbol{x}_i^\top\boldsymbol{\beta})^2$ no longer leads to an accurate estimate of $\boldsymbol{\beta}$, as seen from the rank deficiency of $\nabla^2\mathcal{L}_n(\boldsymbol{\beta}) = n^{-1}\boldsymbol{X}^\top\boldsymbol{X}$. As a consequence, the differentially private, noisy gradient algorithm for the low-dimensional setting is no longer applicable.

To leverage the sparsity of $\boldsymbol{\beta}$, we recall the "peeling" algorithm for sparse mean estimation in Section 3.4, and arrive at the following modification of Algorithm 4.

Algorithm 4.2: Differentially Private Sparse Linear Regression

Input : $\mathcal{L}_n(\boldsymbol{\beta})$, data set $(\boldsymbol{y}, \boldsymbol{X}) = \{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$, step size η^0, privacy parameters ε, δ, noise scale B, number of iterations T, truncation level R, feasibility parameter C, sparsity s, initial value $\boldsymbol{\beta}^0$.

for t *in* 0 **to** $T-1$ **do**

  Compute $\boldsymbol{\beta}^{t+0.5} = \boldsymbol{\beta}^t - (\eta^0/n)\sum_{i=1}^n(\boldsymbol{x}_i^\top\boldsymbol{\beta}^t - \Pi_R(y_i))\boldsymbol{x}_i$;

  $\boldsymbol{\beta}^{t+1} = \Pi_C\left(\texttt{Peeling}(\boldsymbol{\beta}^{t+0.5}, (\boldsymbol{y}, \boldsymbol{X}), s, \varepsilon/T, \delta/T, \eta^0 B/n)\right)$.

end

Output: $\boldsymbol{\beta}^T$.

If the "Peeling" step is replaced by non-private, exact projection of the gradient step onto $\{\boldsymbol{v} \in \mathbb{R}^d : \|\boldsymbol{v}\|_0 \le s\}$, we recover the well-known iterative hard thresholding algorithm [7, 26] for high-dimensional sparse regression.

The analysis of Algorithm 5 requires some assumptions similar to their low-dimensional counterparts in Section 4.2, as follows.

(P1') The true parameter vector $\boldsymbol{\beta}$ satisfies $\|\boldsymbol{\beta}\|_2 < c_0$ for some constant $0 < c_0 < \infty$ and $\|\boldsymbol{\beta}\|_0 \le s^* = o(n)$.

(D1') Bounded design: for every index set $I \subseteq [d]$ with $|I| = o(n)$, there is a constant $c_{\boldsymbol{x}} < \infty$ such that $\sqrt{|I|}\|\boldsymbol{x}_I\|_\infty < c_{\boldsymbol{x}}$ with probability 1.

(D2') Bounded moments of design: $\mathbb{E}\boldsymbol{x} = \boldsymbol{0}$ and for every index set $I \subseteq [d]$ with $|I| = o(n)$, the (restricted) covariance matrix $\Sigma_I = \mathbb{E}\boldsymbol{x}_I\boldsymbol{x}_I^\top$ satisfies $0 < 1/L < |I| \cdot \lambda_{\min}(\Sigma_I) \le |I| \cdot \lambda_{\max}(\Sigma_I) < L$ for some constant $0 < L < \infty$.

These assumptions can be understood as restricted versions of their counterparts, (P1), (D1) and (D2), in the low-dimensional case, Section 4.2. When assumptions (P1') and (D1') hold, the algorithm is guaranteed to be (ε, δ)-differentially private as long as the noise level B is chosen properly.

LEMMA 4.4. *If assumption (P1') and (D1') are true, then Algorithm 5 is (ϵ, δ)-differentially private as long as $B \ge 4(R + c_0 c_{\boldsymbol{x}})c_{\boldsymbol{x}}/\sqrt{s}$.*

The lemma is proved in Section A.6. With assumption (D2') in addition, we can obtain the following convergence result for Algorithm 5.

THEOREM 4.4. *Let $\{(y_i, \boldsymbol{x}_i)\}_{i\in[n]}$ be an i.i.d. sample from the linear model (4.1). Suppose assumptions (P1'), (D1') and (D2') are true. Let $R = \sigma\sqrt{2\log n}$, $C = c_0$ and $B = 4(R + c_0 c_{\boldsymbol{x}})c_{\boldsymbol{x}}/\sqrt{s}$ in accordance with Lemma 4.4, and $\boldsymbol{\beta}^0 = \boldsymbol{0}$. Then there exists some absolute constant ρ such that, if $s = \rho L^4 s^*$, $\eta^0 = s/6L$, $T = \rho L^2 \log(8c_0^2 Ln)$ and $n \ge K \cdot \left(R(s^*)^{3/2}\log d\sqrt{\log(1/\delta)}\log n/\varepsilon\right)$ for a sufficiently large constant K, the bound*

$$\|\boldsymbol{\beta}^T - \boldsymbol{\beta}\|_{\Sigma_{\boldsymbol{x}}}^2 \lesssim \sigma^2\left(\frac{s^*\log d}{n} + \frac{(s^*\log d)^2\log(1/\delta)\log^3 n}{n^2\varepsilon^2}\right) \tag{4.7}$$

holds with probability at least $1-c_1\exp(-c_2\log(d/s^*\log n))-c_1\exp(-c_2 n)-c_1\exp(-c_2\log n)$.

The theorem is proved in Section 8.3. This convergence rate attains the corresponding lower bound (4.6) up to factors of $\log n$, for the usual choice of $\delta = n^{-(1+\omega)}$. For selecting tuning parameters R and s in Algorithm 5, we demonstrate in Section 5 data-driven and differentially private alternatives to the theoretical choices required by Theorem 4.4.

5. Simulation Studies. In this section, we perform simulation studies of our algorithms to evaluate their numerical performance and demonstrate the cost of privacy in various estimation problems. The data are generated as follows.

Mean estimation $\boldsymbol{x}_1, ..., \boldsymbol{x}_n$ are independently drawn from $N_d(\boldsymbol{\mu}, \boldsymbol{I}_d)$. Over repetitions of the experiments, the coordinates of $\boldsymbol{\mu}$ are sample i.i.d. from Uniform$(-10, 10)$ for the low-dimensional problem; in the high-dimensional case, the first s^* coordinates of $\boldsymbol{\mu}$ are sampled i.i.d. from Uniform$(-10, 10)$ and the other coordinates are set to 0.

Linear regression The data $(\boldsymbol{x}_1, y_1), ..., (\boldsymbol{x}_n, y_n)$ are generated from the linear model $y_i = \boldsymbol{x}_i^\top \boldsymbol{\beta} + \epsilon_i$. The entries of design matrix are sampled i.i.d from the uniform distribution over $(-1/\sqrt{d}, 1/\sqrt{d})$ so that the row normalization assumption (D1) in Section 4 is satisfied; $\epsilon_1, ...\epsilon_n$ is an i.i.d sample from $N(0, 1)$. $\boldsymbol{\beta}$ is sampled uniformly from the unit sphere $\{\boldsymbol{v} \in \mathbb{R}^d : \|\boldsymbol{v}\|_2 = 1\}$ for the low-dimensional problem; in the high-dimensional problem, the vector of first s coordinates is sampled uniformly from the unit sphere $\{\boldsymbol{v} \in \mathbb{R}^{s^*} : \|\boldsymbol{v}\|_2 = 1\}$, and the other coordinates are set to 0.

We shall carry out three sets of experiments with the simulated data:

- Compare the performance of our algorithms under different choices of R, the truncation tuning parameter.
- Compare the performance of the high-dimensional algorithms under different choices of s, the sparsity tuning parameter.
- Compare our algorithms with their non-private counterparts, and with other differentially private algorithms in the literature.

5.1. *Tuning of truncation level.* For each of our four algorithms, we consider three methods of determining the truncation tuning parameter R.

- No truncation.
- The theoretical choice: R is set to be the theoretical value of $4\sigma\sqrt{\log n}$.
- Data-driven: compute differentially private estimates of the data set's 2.5% and 97.5% percentiles by Algorithm 1′ in [32] (see "Extension to distributions supported on $(-\infty, \infty)$", pp. 6), and truncate the data set at these levels.

As shown in Figure 1 below, the data-driven method incurs comparable errors to the no truncation case and the theoretical choice of R, suggesting that it is a viable method for choosing R in practice. It should be cautioned that the optimistic performance of constant quantile truncation benefits from the symmetry and light-tailedness of the Gaussian distribution; it may not be applicable to all types of data distribution.

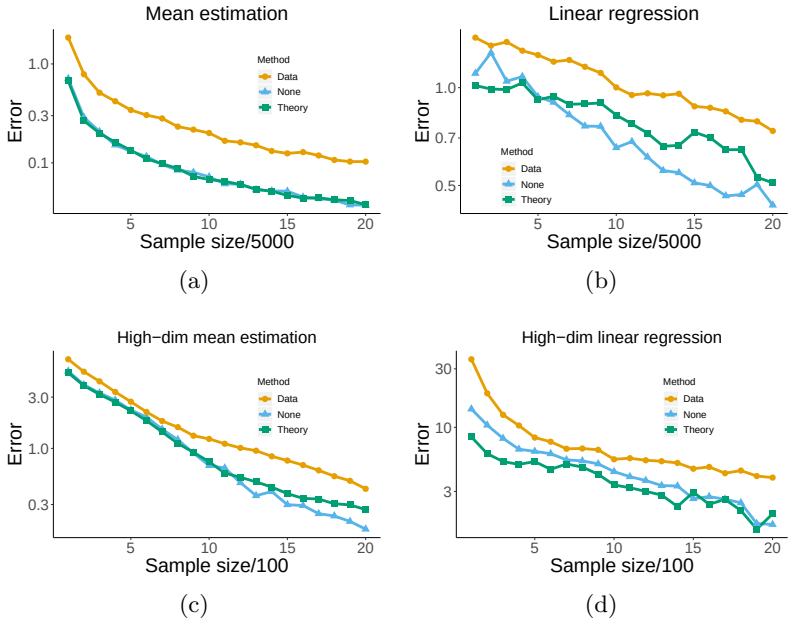
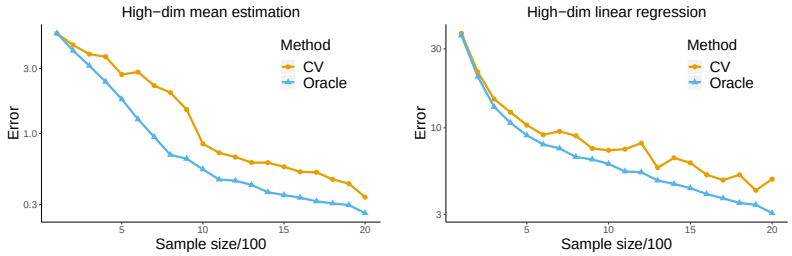


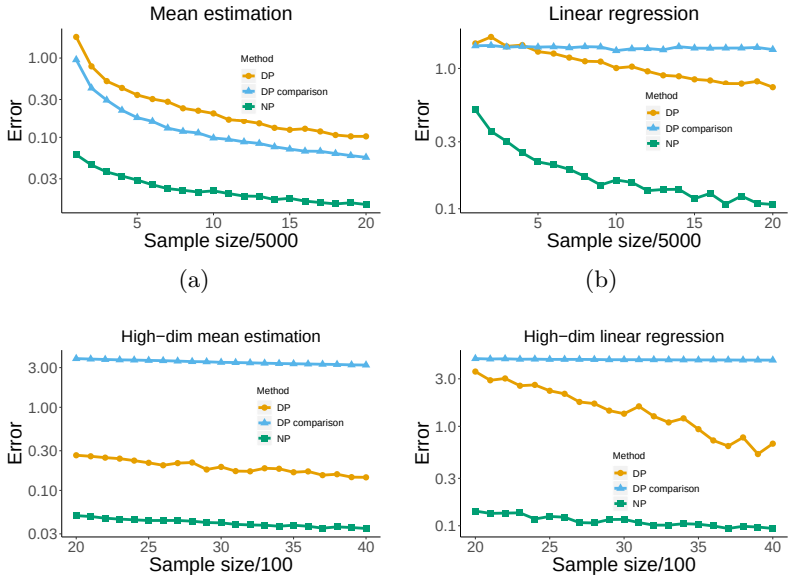
Fig 1: Average ℓ_2-error over 100 repetitions plotted against sample size n, with privacy level set at $(0.5, 10/n^{1.1})$. (a) & (b): mean estimation and linear regression with $d = 20$ and n from 5000 to 100000. (c) & (d): high-dimensional mean estimation and linear regression with n increasing from 100 to 2000, $d = n$, and $s = 20$.

5.2. *Tuning of s.* Our algorithms for high-dimensional problems require a sparsity tuning parameter s. We compare their performances when supplied with the true sparsity s^* and when s is chosen by 5-fold cross validation. The cross-validation error is first computed over a uniform grid of values from $s^*/2$ to $2s^*$. We then truncate these cross-validation errors with Algorithm $1'$ in [32], so that the truncated cross-validation errors have bounded sensitivity. With bounded sensitivity, the exponential mechanism [35] can be applied to the (truncated) cross-validation errors to select a value of s in a differentially private manner.



(a) (b)

Fig 2: Average ℓ_2-error over 50 repetitions plotted against sample size n, with privacy level set at $(0.5, 10/n^{1.1})$. (a) & (b): high-dimensional mean estimation and linear regression with n increasing from 100 to 2000, $d = n$, and $s = 20$.



(a) (b)

(c) (d)

Fig 3: Average ℓ_2-error over 100 repetitions plotted against sample size n, with privacy level set at $(0.5, 10/n^{1.1})$. (a) & (b): mean estimation and linear regression with fixed $d = 20$ and n increasing from 5000 to 100000. (c) & (d): high-dimensional mean estimation and linear regression with n increasing from 2000 to 4000, $d = 2n$, and $s = 20$.

Informed by the previous section on tuning R, the truncation tuning parameters for experiments in this section are selected by the data-driven method. In each problem, as the plots show, selecting s by cross validation leads to errors comparable with their counterparts when the algorithms are supplied with the true sparsity s^*.

5.3. *Comparisons with other algorithms.* We compare our algorithms with their non-private counterparts, as well as other differentially private algorithms in the literature. For the low-dimensional problems, we consider Algorithm 4 in [29] for mean estimation and Algorithm 1 in [41] for regression. For the high-dimensional problems, we compare with the method in [45].

There are significant gaps in performance between our algorithms and those in [41, 45]. It is important to note, however, that the primary strength of Algorithm 1 in [41] is its ability to produce accurate test statistics with differential privacy, and the algorithm by [45] is primarily targeted at minimizing the excess empirical risk, so these numerical experiments may not be fully reflective of their advantages.

To further understand the improved numerical performance, we report here some observations from the numerical experiments. For the private Johnson-Lindenstrauss projection algorithm in [41], we observed that the ridge regression subroutine of the algorithm is frequently activated even when n is very large, resulting in a ridge regression solution with regularization parameter of order $O(\log(1/\delta)/\varepsilon)$ and leading to significant bias. For the private Frank-Wolfe algorithm in [45], the solution is often non-sparse with large values outside the true support of $\boldsymbol{\beta}$, while our algorithm guarantees a sparse solution by construction and converges to the non-private solution as n grows.

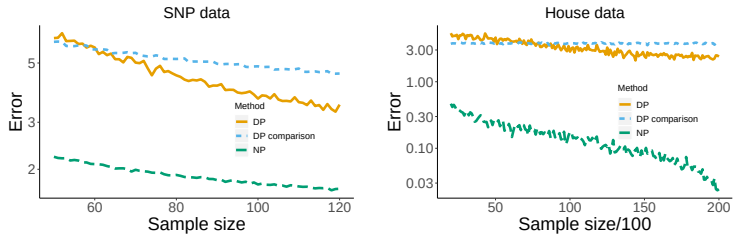
6. Data Analysis. In this section, we demonstrate the numerical performance of the differentially private algorithms on real data sets.

6.1. *SNP array of adults with schizophrenia.* We analyze the SNP array data of adults with schizophrenia, collected by [34], to illustrate the performance of our high-dimensional sparse mean estimator. In the dataset, there are 387 adults with schizophrenia, 241 of which are labeled as "average IQ" and 146 of which are labeled as "low IQ". The SNP array is obtained by genotyping the subjects with the Affymetrix Genome-Wide Human SNP 6.0 platform. For our analysis, we focus on the 2000 SNPs with the highest minor allele frequencies (MAFs); the full dataset is available at https://www.ncbi.nlm.nih.gov/geo/query/acc.cgi?acc=GSE106818.

Privacy-perserving data analysis is very much relevant for this dataset and genetic data in general, because as [25] shows, an adversary can infer the absence/presence of an individual 's genetic data in a large dataset by cross-referencing summary statistics, such as MAFs, from multiple genetic datasets. As MAFs can be calculated from the mean of an SNP array, differentially-private estimators of the mean allow reporting the MAFs without compromising any individual's privacy.

The data set takes the form of a 387×2000 matrix. The entries of the matrix take values 0, 1 or 2, representing the number of minor allele(s) at

each SNP, and therefore the MAF of each SNP location in this sample can be obtained by computing the mean of the rows in this matrix. Sparsity is introduced by considering the difference in MAFs of the two IQ groups: the MAFs of the two groups are likely to differ at a small number of SNP locations among the 2000 SNPs considered.



(a) (b)

Fig 4: (a): The estimate of $\mathbb{E}[\|\hat{\boldsymbol{\mu}} - \boldsymbol{\mu}\|_2]$ for the differentially private sparse mean estimator as sample size increases from 50 to 120, with $s = 20$.
(b): The estimate of $\mathbb{E}[\|\hat{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2]$ for the differentially private OLS estimator, compared with its differentially private counterpart, as sample size increases from 2000 to 20000.

For m ranging from 10 to 120, we subsample m subjects from each of the two IQ groups, say $\{\boldsymbol{x}_{11}, \boldsymbol{x}_{12}, \cdots \boldsymbol{x}_{1m}\}$ and $\{\boldsymbol{x}_{21}, \boldsymbol{x}_{22}, \cdots \boldsymbol{x}_{2m}\}$, and apply our sparse mean estimator to $\{\boldsymbol{x}_{11} - \boldsymbol{x}_{21}, \boldsymbol{x}_{12} - \boldsymbol{x}_{22}, \cdots \boldsymbol{x}_{1m} - \boldsymbol{x}_{2m}\}$ with $s = 20$ and privacy parameters $(\varepsilon, \delta) = (0.5, 10/n^{1.1})$. The error of this estimator is then calculated by comparing with the mean of the entire sample. This procedure is repeated 100 times to obtain Figure 4(a), which displays the estimate of $\mathbb{E}[\|\hat{\boldsymbol{\mu}} - \boldsymbol{\mu}\|_2]$ as m increases from 50 to 120. We also plotted the corresponding curve for the method in [45] for comparison.

6.2. *Housing prices in California.* For the linear regression problem, we analyze a housing price dataset with economic and demographic covariates, constructed by [38] and available for download at `http://lib.stat.cmu.edu/datasets/houses.zip`. In this dataset, each subject is a block group in California in the 1990 Census; there are 20640 block groups in this dataset. The response variable is the median house value in the block group; the covariates include the median income, median age, total population, number of households, and the total number of rooms of all houses in the block group. In general, summary statistics such as mean or median do not have any differential privacy guarantees, so the absence of information on individual households in the dataset does not preclude an adversary from extracting sensitive individual information from the summary statistics. Privacy-preserving methods are still desirable in this case.

For m ranging from 100 to 20600, we subsample m subjects from the dataset to compute the differentially private OLS estimate, with privacy parameters $(\varepsilon, \delta) = (0.5, 10/n^{1.1})$. The error of this estimator is then calculated by comparing with the non-private OLS estimator computed using the entire sample. This procedure is repeated 100 times to obtain Figure 4(b), which displays the estimate of $\mathbb{E}[\|\hat{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2]$ as m increases from 2000 to 20000. The design matrix is standardized before applying the algorithm. The corresponding curve for the method in [41] is also plotted for comparison.

7. Discussion. Our paper investigates the tradeoff between statistical accuracy and privacy, by providing minimax lower bounds with differential privacy constraint and proposing differentially private algorithms with rates of convergence attaining the lower bounds up to logarithmic factors. For the lower bounds, we considered a technique based on tracing adversary and illustrated its utility by establishing minimax lower bounds for differentially private mean estimation and linear regression. These lower bounds are shown to be tight up to logarithmic factors via analysis of differentially private algorithms with matching rates of convergence.

Beyond the theoretical results, numerical performance of the private algorithms are demonstrated in simulations and real data analysis. The results suggest that the proposed algorithms have robust performance with respect to various choices of tuning parameters, achieve accuracy comparable to or better than that of existing differentially private algorithms, and can compute efficiently for sample sizes and dimensions up to tens of thousands. The numerical results corroborate the cost of privacy delineated in the theorems by exhibiting shrinking but non-vanishing gaps of accuracy between the private algorithms and their non-private counterparts. The theoretical and numerical results together can inform practitioners of differential privacy the necessary sacrifice of accuracy at a prescribed level of privacy, or the appropriate choice of privacy parameters if a given level of accuracy is desired.

There are many promising avenues for future research. It is of significant interest to study the optimal tradeoff of privacy and accuracy in statistical problems beyond mean estimation and linear regression. Examples include covariance/precision matrix estimation, graphical model recovery, nonparametric regression, and principal component analysis. Along the way, it is of importance to further develop general approaches of designing privacy-preserving algorithms, as well as more general lower bound techniques than those presented in this work.

One natural extension is uncertainty quantification with privacy constraints, which is largely unexplored in the statistics literature. Notably, [29] established the rate-optimal length of differentially private confidence intervals for the (one-dimensional) Gaussian mean. The technical tools developed in our paper may provide insights for constructing optimal statistical

inference procedures in the context of, say, high-dimensional sparse mean estimation and linear regression.

Yet another intriguing direction of research is the cost of other notions of privacy, such as concentrated differential privacy [19], Rényi differential privacy [36], and Gaussian differential privacy [13]. These notions of privacy have found important applications such as stochastic gradient Langevin dynamics, stochastic Monte Carlo sampling [47] and deep learning [8].

8. Proofs.

In this section, we prove the lower bound of low-dimensional mean estimation, Lemma 3.1 and Theorem 3.1, and the upper bound of high-dimensional linear regression, Theorem 4.4.

8.1. *Proof of Lemma 3.1.*

PROOF OF LEMMA 3.1. Let $k = (C/2)\log(\frac{1}{n\delta})/\varepsilon$, with the value of $0 < C < 1$ to be chosen later. By the assumed regime of δ as a function of n, we have $k \asymp \log(1/\delta)/\varepsilon$ and $k < n/2$. We assume that k divides n without the loss of generality.

For an arbitrary $M \in \mathcal{M}_{\varepsilon,\delta}$, we define $M_k(\boldsymbol{Z}) \equiv M(\boldsymbol{Y})$. Because M is (ε, δ)-differentially private, M_k is also differentially private by post-processing. To lower bound $\mathbb{E}[\|M(\boldsymbol{Y}) - \mathbb{E}\boldsymbol{y}_1\|_2|\boldsymbol{Z}]$, we observe that it suffices to find some appropriate distribution of $\boldsymbol{Z}$ so that $\mathbb{E}\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2$ can be lower bounded: as $\|M(\boldsymbol{Y}) - \mathbb{E}\boldsymbol{y}_1\|_2 = \|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2$ by construction, there must be a realization of $\boldsymbol{Z}$ such that $\mathbb{E}[\|M(\boldsymbol{Y}) - \mathbb{E}\boldsymbol{y}_1\|_2|\boldsymbol{Z}]$ is also lower bounded.

Since the sample size of $\boldsymbol{Z}$ does satisfy the assumption of the preliminary lower bound (2.3), the bound applies provided that M_k is a differentially private algorithm with respect to $\boldsymbol{Z}$. To this end, we consider the group privacy lemma:

LEMMA 8.1 (group privacy, [43]). *For every $m \geq 1$, if M is (ε, δ)-differentially private, then for every pair of datasets $\boldsymbol{X} = \{\boldsymbol{x}_k\}_k$ and $\boldsymbol{Z} = \{\boldsymbol{z}_k\}_k$ satisfying $\sum_i \mathbb{1}(\boldsymbol{x}_i \neq \boldsymbol{z}_i) \leq m$, and every measurable set S,*

$$\mathbb{P}(M(\boldsymbol{X}) \in S) \leq e^{\varepsilon m}\mathbb{P}(M(\boldsymbol{Z}) \in S) + \frac{e^{\varepsilon m} - 1}{e - 1} \cdot \delta.$$

The group privacy lemma suggests that, to characterize the privacy parameters of M_k, it suffices to upper-bound the number of changes in $\boldsymbol{Y}$ incurred by replacing one element of $\boldsymbol{Z}$. Let m_i denote the number of times that $\boldsymbol{z}_i$ appears in a sample of size n drawn with replacement from $\boldsymbol{Z}$, then our quantity of interest here is simply $\max_{i\in[n/k]} m_i$.

To analyze $\max_{i\in[n/k]} m_i$, we first show that δ as a function of n must satisfy one of the following two statements.

1. There is a fixed constant τ such that $\frac{n}{(n/k)\log(n/k)} \leq C\tau/\varepsilon$ when n is sufficiently large.

2. Case 1 fails to hold: we have $k > (C/2)\tau/\varepsilon \log(n/k)$ for any constant τ, as long as n is sufficiently large.

The dichotomy is made possible by the assumption that $\log(\delta)/\log(n)$ is non-increasing in n and $\delta < n^{-(1+\omega)}$ for some fixed $\omega > 0$. Under this assumption, we have either $\lim_{n\to\infty} \log(\delta)/\log(n) = c < -1$ or $\lim_{n\to\infty} \log(\delta)/\log(n) = -\infty$.

For the first case, we have $k = (C/2)\log(\frac{1}{n\delta})/\varepsilon = (C/2\varepsilon) \cdot (\log(1/\delta) - \log(n)) \in ((C/2\varepsilon) \cdot c_1 \log n, (C/2\varepsilon) \cdot c_2 \log n)$ for some $c_1, c_2 > 0$ when n is sufficiently large. Therefore

$$\frac{n}{(n/k)\log(n/k)} = \frac{k}{\log(n/k)} \le \frac{c_2 \cdot (C/2\varepsilon) \cdot \log n}{\log(2n\varepsilon/(C \cdot c_1 \cdot \log n))} \le C\tau/\varepsilon,$$

for some $\tau > 0$. This corresponds to the first statement.

For the second case $\lim_{n\to\infty} \log(\delta)/\log(n) = -\infty$, we then have for any constant $c_3 > 0$ and sufficiently large n, $\log(1/\delta) > c_3 \log(n)$. Then $k = (C/2)\log(\frac{1}{n\delta})/\varepsilon = (C/2\varepsilon) \cdot (\log(1/\delta) - \log(n)) \ge (C/2\varepsilon) \cdot (c_3 - 1)\log n$. Consequently we have

$$\frac{k}{\log(n/k)} > \frac{(c_3 - 1) \cdot (C/2\varepsilon) \cdot \log n}{\log(n)} \le (c_3 - 1) \cdot (C/2\varepsilon)$$

for sufficiently large n. Since c_3 can take value of any positive number, this corresponds to the second statement.

Case 1. As $(m_1, m_2, \cdots, m_{n/k})$ follows a uniform multinomial distribution, we consider a useful result from [39], stated below:

LEMMA 8.2 ([39]). *If $(y_1, y_2, \cdots, y_d)$ follows a uniform multinomial(ℓ) distribution, and $\frac{\ell}{d \log d} \le c$ for some constant c not depending on ℓ and d, then for every $\zeta > 0$,*

$$\mathbb{P}\left(\max_{i\in[d]} y_i > (r_c + \zeta)\log d\right) = o(1),$$

where r_c is the unique root of $1 + y(\log c - \log y + 1) - c = 0$ that is strictly greater than c.

It follows that $\mathbb{P}(\max_i m_i \le r \log n) = 1 - o(1)$, where r is the unique root of $1 + x(\log(C\tau/\varepsilon) - \log x + 1) - (C\tau/\varepsilon) = 0$ that is greater than $C\tau/\varepsilon$. Such a root exists, because $f_{C,\tau,\varepsilon}(x) := 1 + x(\log(C\tau/\varepsilon) - \log x + 1) - (C\tau/\varepsilon)$ is strictly concave and achieves the global maximum value of 1 at $x = C\tau/\varepsilon$.

Let $\mathcal{E} := \{\max_i m_i \le r \log n\}$. Under $\mathcal{E}$, Lemma 8.1 implies that M_k is an $(\varepsilon r \log n,\ \delta e^{\varepsilon r \log n})$-differentially private algorithm. We may essentially repeat the lower bound argument leading to the preliminary lower bound (2.3), as follows. Let $\boldsymbol{Z} = \{\boldsymbol{z}_1, \boldsymbol{z}_2, \cdots, \boldsymbol{z}_{n/k}\}$ be sampled i.i.d, from the data distribution specified in Lemma 2.1 including the prior distribution

on $\boldsymbol{\mu} = \mathbb{E}z_1$, so that Lemma 2.1 applies to $\boldsymbol{Z}$. For every $i \in [n/k]$, let $\mathcal{C} = \{\sum_{i\in[n/k]} \mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{z}_i, M_k(\boldsymbol{Z})) \le (n/k)\sigma^2\sqrt{8d\log(1/\delta)}\}$. We have

$$\begin{aligned}
&\mathbb{P}(\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2 < c\sigma\sqrt{d}) \le \mathbb{P}(\mathcal{E}^c) + \mathbb{P}\left(\mathcal{C} \cap \{\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2 < c\sigma\sqrt{d}\}\right) + \mathbb{P}(\mathcal{C}^c)\\
&\le \mathbb{P}(\mathcal{E}^c) + \mathbb{P}\left(\mathcal{C} \cap \{\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2 < c\sigma\sqrt{d}\}\right) + \sum_{i\in[n/k]} \mathbb{P}\left(\mathcal{A}_{\boldsymbol{\mu}}(\boldsymbol{z}_i, M_k(\boldsymbol{Z})) > \sigma^2\sqrt{8d\log(1/\delta)}\right)\\
&\le o(1) + \delta + n(e^{\varepsilon r\log n}\delta + \delta e^{\varepsilon r\log n}) = o(1) + \delta + 2n^{-\tau+\varepsilon r}.
\end{aligned}$$

This probability is always bounded away from 1, because $\varepsilon r < \tau$ with appropriately chosen C: since $f_{C,\tau,\varepsilon}(\tau/\varepsilon) = (\tau/\varepsilon)(1 + \log C - C) + 1$ and $0 < \varepsilon < 1$, for every $\tau > 0$ there is a sufficiently small $0 < C < 1$ such that $f_{C,\tau,\varepsilon}(\tau/\varepsilon) < 0$. Since $f_{C,\tau,\varepsilon}(C\tau/\varepsilon) = 1$ is the global maximum, we have $r < \tau/\varepsilon$, or equivalently $\varepsilon r < \tau$, as desired.

Case 2. each m_i is a sum of n independent Bernoulli(k/n) random variables. Chernoff's inequality implies that

$$\mathbb{P}\left(\max_i m_i > \frac{1}{\varepsilon}\log\left(\frac{1}{2n\delta}\right)\right) \le \frac{n}{k}\cdot\exp\left(-\frac{(1/2C-1)}{3}k\right).$$

Recall that $k = (C/2)\log(\frac{1}{2n\delta})/\varepsilon$ by construction. By the assumption of Case 2, we have $k > (C/2)\tau/\varepsilon\log(n/k)$ for any constant τ, as long as n is sufficiently large. Then we have

$$\mathbb{P}\left(\max_i m_i > \frac{1}{\varepsilon}\log\left(\frac{1}{2n\delta}\right)\right) \le \left(\frac{n}{k}\right)^{1-(1-C/2)\tau/3\varepsilon}.$$

The probability can be made arbitrarily small by fixing $C = 1/2$ and choosing large τ. Now that we have a high-probability bound for $\max_i m_i$, the group privacy lemma and union bound, as in Case 1, imply that $\mathbb{P}(\mathcal{C}) = o(1)$, and therefore by Lemma 2.1

$$\begin{aligned}
&\mathbb{P}(\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2 < c\sigma\sqrt{d})\\
\le&\mathbb{P}(\mathcal{E}^c) + \mathbb{P}\left(\mathcal{C} \cap \{\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2 < c\sigma\sqrt{d}\}\right) + \mathbb{P}(\mathcal{C}^c) = o(1).
\end{aligned}$$

In each of the two cases, we found that $\mathbb{P}(\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2 < c\sigma\sqrt{d}) = o(1)$. The proof is now complete by the reduction from $\mathbb{E}\left[\|M(\boldsymbol{Y}) - \mathbb{E}\boldsymbol{y}_1\|_2|\boldsymbol{Z}\right]$ to $\mathbb{E}\|M_k(\boldsymbol{Z}) - \bar{\boldsymbol{Z}}\|_2$. □

8.2. *Proof of Theorem 3.1.* It suffices to prove the second term of the minimax lower bound, as the first term is the statistical minimax lower bound for sub-Gaussian mean estimation.

For $i \in [n]$, consider $\boldsymbol{x}_i = \boldsymbol{0} \in \mathbb{R}^d$ with probability $1-\alpha$ and $\boldsymbol{x}_i = \boldsymbol{y}_i$ with probability α, where $\boldsymbol{y}_i$ follows the discrete uniform distribution specified in Lemma 3.1. When $n \gtrsim \sqrt{d\log(1/\delta)}/\varepsilon$, there exists some $0 < \alpha < 1$ such

that $\alpha n \asymp \sqrt{d\log(1/\delta)}/\varepsilon$. The distribution of $\boldsymbol{x}_i$ is indeed sub-Gaussian(σ) with $\boldsymbol{\mu} \in \Theta$.

Consider the random index set $\mathcal{S} = \{i \in [n] : \boldsymbol{x}_i \neq \mathbf{0}\}$. For every $M \in \mathcal{M}_{\varepsilon,\delta}$, we have

$$\mathbb{E}[\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2] \geq \sum_{\mathcal{S}=S\subseteq[n],|S|\leq n\alpha} \mathbb{E}[\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2|\mathcal{S} = S]\mathbb{P}(\mathcal{S} = S).$$

Now for each fixed S, define $\tilde{M}(\boldsymbol{X}_S) = \alpha^{-1}M(\{\boldsymbol{x}_i : i \in S\} \cup \{\mathbf{0}\}^{n-|S|})$. We note that $\tilde{M}(\boldsymbol{X}_S)$ is an (ε, δ)-differentially private algorithm with respect to $\boldsymbol{X}_S = \{\boldsymbol{x}_i : i \in S\}$, by observing that modifying any single datum in $\boldsymbol{X}_S$ incurs the same privacy loss to M as it does to $\tilde{M}$. By construction, it also holds that $\boldsymbol{\mu} = \mathbb{E}\boldsymbol{x}_1 = \alpha\mathbb{E}\boldsymbol{y}_1$. We then have

$$\begin{aligned}\mathbb{E}[\|M(\boldsymbol{X}) - \boldsymbol{\mu}\|_2|\mathcal{S} = S] &\geq \mathbb{E}[\|\alpha\tilde{M}(\boldsymbol{X}_S) - \alpha\mathbb{E}\boldsymbol{y}_1\|_2|\mathcal{S} = S] \\ &\geq \alpha\mathbb{E}[\|\tilde{M}(\boldsymbol{X}_S) - \mathbb{E}\boldsymbol{y}_1\|_2] \gtrsim \alpha\sigma\sqrt{d} \asymp \sigma\frac{d\sqrt{\log(1/\delta)}}{n\varepsilon}.\end{aligned}$$

For the last inequality, we invoked the lower bound proved in Lemma 3.1, since the sample size of $\boldsymbol{X}_s$ is at most $\alpha n \asymp \sqrt{d\log(1/\delta)}/\varepsilon$. The proof is complete.

8.3. *Proof of Theorem 4.4.*

PROOF OF THEOREM 4.4. Let $\hat{\boldsymbol{\beta}} = \arg\min_{\|\boldsymbol{\beta}\|_2\leq c_0, \|\boldsymbol{\beta}\|_0\leq s^*} \mathcal{L}_n(\boldsymbol{\beta})$. While global strong convexity and smoothness are no longer possible when $d > n$, because $\boldsymbol{\beta}^t$ and $\hat{\boldsymbol{\beta}}$ are sparse, we have following fact known as restricted strong convexity (RSC) and restricted smoothness (RSM) [37, 3, 33].

FACT 8.1. Under assumptions of Theorem 4.4, it holds with probability at least $1 - c_1\exp(-c_2 n)$ that

$$\frac{1}{8Ls}\|\boldsymbol{\beta}^t - \hat{\boldsymbol{\beta}}\|_2^2 \leq \langle\nabla\mathcal{L}_n(\boldsymbol{\beta}^t) - \nabla\mathcal{L}_n(\hat{\boldsymbol{\beta}}), \boldsymbol{\beta}^t - \hat{\boldsymbol{\beta}}\rangle \leq \frac{4L}{s}\|\boldsymbol{\beta}^t - \hat{\boldsymbol{\beta}}\|_2^2. \tag{8.1}$$

Under the event $\mathcal{E}_1 = \{\Pi_R(y_i) = y_i, \forall i \in [n]\}$, Fact 8.1 implies that $\mathcal{L}_n(\boldsymbol{\beta}^t) - \mathcal{L}_n(\hat{\boldsymbol{\beta}})$ decays exponentially fast in t.

LEMMA 8.3. *Under assumptions of Theorem 4.4 and event $\mathcal{E}_1$,* (8.1) *implies that there exists an absolute constant ρ such that*

$$\mathcal{L}_n(\boldsymbol{\beta}^{t+1}) - \mathcal{L}_n(\hat{\boldsymbol{\beta}}) \leq \left(1 - \frac{1}{\rho L^2}\right)\left(\mathcal{L}_n(\boldsymbol{\beta}^t) - \mathcal{L}_n(\hat{\boldsymbol{\beta}})\right) + c_3\left(\sum_{i\in[s]}\|\boldsymbol{w}_i^t\|_\infty^2 + \|\tilde{\boldsymbol{w}}_{S^{t+1}}^t\|_2^2\right), \tag{8.2}$$

for every t, where $\boldsymbol{w}_1^t, \boldsymbol{w}_2^t, \cdots, \boldsymbol{w}_s^t$ are the Laplace noise vectors added to $\boldsymbol{\beta}^t - (\eta^0/n)\sum_{i=1}^n (\boldsymbol{x}_i^\top \boldsymbol{\beta}^t - \Pi_R(y_i))\boldsymbol{x}_i$ when the support of $\boldsymbol{\beta}^{t+1}$ is iteratively selected by "Peeling", S^{t+1} is the support of $\boldsymbol{\beta}^{t+1}$, and $\tilde{\boldsymbol{w}}^t$ is the noise vector added to the selected s-sparse vector.

We take Lemma 8.3, which is proved in Section A.7 of the supplement [10], to prove Theorem 4.4. We iterate (8.2) over t and notate $\boldsymbol{W}_t = c_3\left(\sum_{i\in[s]} \|\boldsymbol{w}_i^t\|_\infty^2 + \|\tilde{\boldsymbol{w}}_{S^{t+1}}^t\|_2^2\right)$ to obtain

$$\begin{aligned}\mathcal{L}_n(\boldsymbol{\beta}^T) - \mathcal{L}_n(\hat{\boldsymbol{\beta}}) &\le \left(1 - \frac{1}{\rho L^2}\right)^T \left(\mathcal{L}_n(\boldsymbol{\beta}^0) - \mathcal{L}_n(\hat{\boldsymbol{\beta}})\right) + \sum_{k=0}^{T-1}\left(1 - \frac{1}{\rho L^2}\right)^{T-k-1} \boldsymbol{W}_k \\ &\le \left(1 - \frac{1}{\rho L^2}\right)^T 8Lc_0^2 + \sum_{k=0}^{T-1}\left(1 - \frac{1}{\rho L^2}\right)^{T-k-1} \boldsymbol{W}_k. \qquad (8.3)\end{aligned}$$

The second inequality is a consequence of the upper inequality in (8.1) and the ℓ_2 bounds of $\boldsymbol{\beta}^0$ and $\hat{\boldsymbol{\beta}}$. We can also bound $\mathcal{L}_n(\boldsymbol{\beta}^T) - \mathcal{L}_n(\hat{\boldsymbol{\beta}})$ from below by the lower inequality in (8.1):

$$\mathcal{L}_n(\boldsymbol{\beta}^T) - \mathcal{L}_n(\hat{\boldsymbol{\beta}}) \ge \mathcal{L}_n(\boldsymbol{\beta}^T) - \mathcal{L}_n(\boldsymbol{\beta}^*) \ge \frac{1}{16Ls}\|\boldsymbol{\beta}^T - \boldsymbol{\beta}^*\|_2^2 - \langle \nabla\mathcal{L}_n(\boldsymbol{\beta}^*), \boldsymbol{\beta}^* - \boldsymbol{\beta}^T\rangle. \qquad (8.4)$$

Now (8.3) and (8.4) imply that, with $T = (\rho L^2)\log(8c_0^2 Ln)$,

$$\frac{1}{16Ls}\|\boldsymbol{\beta}^T - \boldsymbol{\beta}^*\|_2^2 \le \|\nabla\mathcal{L}_n(\boldsymbol{\beta}^*)\|_\infty\sqrt{s+s^*}\|\boldsymbol{\beta}^* - \boldsymbol{\beta}^T\|_2 + \frac{1}{n} + \sum_{k=0}^{T-1}\left(1 - \frac{1}{\rho L^2}\right)^{T-k-1} \boldsymbol{W}_k. \qquad (8.5)$$

To further bound $\|\boldsymbol{\beta}^T - \boldsymbol{\beta}^*\|_2^2$, we observe that under $\mathcal{E}_1$ and two other events

$$\mathcal{E}_2 = \left\{\max_t \boldsymbol{W}_t \le K\frac{R^2(s^*)^3\log^2 d\log(1/\delta)\log^2 n}{n^2\varepsilon^2}\right\},$$
$$\mathcal{E}_3 = \left\{\|\nabla\mathcal{L}_n(\boldsymbol{\beta}^*)\|_\infty \le 4\sigma\|\boldsymbol{x}\|_\infty\sqrt{\frac{\log d}{n}}\right\},$$

(8.5) and assumptions (D1'), (D2') yield

$$\|\boldsymbol{\beta}^T - \boldsymbol{\beta}\|_{\Sigma_{\boldsymbol{x}}}^2 \lesssim \sigma^2\left(\frac{s^*\log d}{n} + \frac{(s^*\log d)^2\log(1/\delta)\log^3 n}{n^2\varepsilon^2}\right).$$

It remains to show that the events $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ occur simultaneously with high probability. We have $\mathbb{P}(\mathcal{E}_1^c) \le c_1\exp(-c_2\log n)$ because $y_1, y_2, \cdots, y_n \overset{\text{i.i.d.}}{\sim} N(0,\sigma^2)$ and $R \asymp \sigma\sqrt{\log n}$.

For $\mathcal{E}_2$, we invoke Lemma A.1 in the supplement [10]. For each iterate t, the individual coordinates of $\tilde{\boldsymbol{w}}^t$, $\boldsymbol{w}_i^t$ are sampled i.i.d. from the Laplace distribution with scale $\eta^0 \cdot \frac{2B\sqrt{3s\log(T/\delta)}}{n\varepsilon/T}$, where the noise scale $B \lesssim R/\sqrt{s}$ and $T \asymp \log n$ by our choice. If $n \geq K \cdot \left(R(s^*)^{3/2}\log d\sqrt{\log(1/\delta)}\log n/\varepsilon\right)$ for a sufficiently large constant K, Lemma A.1 and the union bound imply that, with probability at least $1 - c_1\exp(-c_2\log(d/(s^*\log n))$, $\max_t \boldsymbol{W}_t$ is bounded by $K\frac{R^2(s^*)^3\log^2 d\log(1/\delta)\log^2 n}{n^2\varepsilon^2}$ for some appropriate constant K. For $\mathcal{E}_3$, under assumptions (D1') and (D2'), it is a standard probabilistic result (see, for example, [46] pp. 210-211) that $\mathbb{P}(\mathcal{E}_3^c) \leq 2e^{-2\log d}$. □

9. Ackowledgement. We would like to thank the Associate Editor and referees for their helpful suggestions and comments that lead to a great improvement of the paper. We also thank Chi-Yun Wu for advice on Section 6. The research of T. Cai was supported in part by NSF grants DMS-1712735 and DMS-2015259 and NIH grants R01-GM129781 and R01-GM123056. The research of L. Zhang was supported in part by NSF grant NSF DMS-2015378.

References.

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *ACM CCS 2016*, pages 308–318. ACM, 2016.

[2] John M. Abowd. The challenge of scientific reproducibility and privacy protection for statistical agencies. In *Census Scientific Advisory Committee*, 2016.

[3] Alekh Agarwal, Sahand Negahban, and Martin J Wainwright. Fast global convergence rates of gradient methods for high-dimensional statistical recovery. In *Advances in Neural Information Processing Systems*, pages 37–45, 2010.

[4] Raef Bassily, Vitaly Feldman, Kunal Talwar, and Abhradeep Guha Thakurta. Private stochastic convex optimization with optimal rates. In *Advances in Neural Information Processing Systems*, pages 11282–11291, 2019.

[5] Raef Bassily, Adam Smith, and Abhradeep Thakurta. Private empirical risk minimization: Efficient algorithms and tight error bounds. In *FOCS 2014*, pages 464–473. IEEE, 2014.

[6] Sourav Biswas, Yihe Dong, Gautam Kamath, and Jonathan Ullman. Coinpress: Practical private mean and covariance estimation. *arXiv preprint arXiv:2006.06618*, 2020.

[7] Thomas Blumensath and Mike E Davies. Iterative hard thresholding for compressed sensing. *Applied and computational harmonic analysis*, 27(3):265–274, 2009.

[8] Zhiqi Bu, Jinshuo Dong, Qi Long, and Weijie J Su. Deep learning with gaussian differential privacy. *arXiv preprint arXiv:1911.11607*, 2019.

[9] Mark Bun, Jonathan Ullman, and Salil Vadhan. Fingerprinting codes and the price of approximate differential privacy. In *STOC 2014*, pages 1–10. ACM, 2014.

[10] T. Tony Cai, Yichen Wang, and Linjun Zhang. Supplement to "the cost of privacy: optimal rates of convergence for parameter estimation with differential privacy". 2020.

[11] Apple Differential Privacy Team. Privacy at scale. 2017.

[12] Bolin Ding, Janardhan Kulkarni, and Sergey Yekhanin. Collecting telemetry data privately. In *NeurIPS 2017*, pages 3571–3580, 2017.

[13] Jinshuo Dong, Aaron Roth, and Weijie J Su. Gaussian differential privacy. *arXiv preprint arXiv:1905.02383*, 2019.

[14] David L Donoho. Statistical estimation and optimal recovery. *The Annals of Statistics*, pages 238–270, 1994.
[15] John C Duchi, Michael I Jordan, and Martin J Wainwright. Minimax optimal procedures for locally private estimation. *J. Am. Stat. Assoc.*, 113(521):182–201, 2018.
[16] Cynthia Dwork and Vitaly Feldman. Privacy-preserving prediction. *arXiv preprint arXiv:1803.10266*, 2018.
[17] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *TCC 2006*, pages 265–284. Springer, 2006.
[18] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.
[19] Cynthia Dwork and Guy N Rothblum. Concentrated differential privacy. *arXiv preprint arXiv:1603.01887*, 2016.
[20] Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. Exposed! a survey of attacks on private data. *Annu. Rev. Stat. Appl.*, 4:61–84, 2017.
[21] Cynthia Dwork, Adam Smith, Thomas Steinke, Jonathan Ullman, and Salil Vadhan. Robust traceability from trace amounts. In *FOCS 2015*, pages 650–669. IEEE, 2015.
[22] Cynthia Dwork, Weijie J Su, and Li Zhang. Differentially private false discovery rate control. *arXiv preprint arXiv:1807.04209*, 2018.
[23] Cynthia Dwork, Kunal Talwar, Abhradeep Thakurta, and Li Zhang. Analyze gauss: optimal bounds for privacy-preserving principal component analysis. In *STOC 2014*, pages 11–20. ACM, 2014.
[24] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *ACM CCS 2014*, pages 1054–1067. ACM, 2014.
[25] Nils Homer, Szabolcs Szelinger, Margot Redman, David Duggan, Waibhav Tembe, Jill Muehling, John V Pearson, Dietrich A Stephan, Stanley F Nelson, and David W Craig. Resolving individuals contributing trace amounts of dna to highly complex mixtures using high-density snp genotyping microarrays. *PLoS genetics*, 4(8):e1000167, 2008.
[26] Prateek Jain, Ambuj Tewari, and Purushottam Kar. On iterative hard thresholding methods for high-dimensional m-estimation. In *NeurIPS 2014*, pages 685–693, 2014.
[27] Iain M Johnstone. On minimax estimation of a sparse normal mean vector. *Ann. Stat.*, 22:271–289, 1994.
[28] Gautam Kamath, Jerry Li, Vikrant Singhal, and Jonathan Ullman. Privately learning high-dimensional distributions. *arXiv preprint arXiv:1805.00216*, 2018.
[29] Vishesh Karwa and Salil Vadhan. Finite sample differentially private confidence intervals. *arXiv preprint arXiv:1711.03908*, 2017.
[30] Shiva Prasad Kasiviswanathan, Homin K Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. What can we learn privately? *SIAM Journal on Computing*, 40(3):793–826, 2011.
[31] Daniel Kifer, Adam Smith, and Abhradeep Thakurta. Private convex empirical risk minimization and high-dimensional regression. In *COLT 2012*, pages 25.1–25.40, 2012.
[32] Jing Lei. Differentially private m-estimators. In *NeurIPS 2011*, pages 361–369, 2011.
[33] Po-Ling Loh and Martin J Wainwright. Regularized m-estimators with nonconvexity: Statistical and algorithmic theory for local optima. *The Journal of Machine Learning Research*, 16(1):559–616, 2015.
[34] Chelsea Lowther, Daniele Merico, Gregory Costain, Jack Waserman, Kerry Boyd, Abdul Noor, Marsha Speevak, Dimitri J Stavropoulos, John Wei, Anath C Lionel, et al. Impact of IQ on the diagnostic yield of chromosomal microarray in a community sample of adults with schizophrenia. *Genome Med.*, 9(1):105, 2017.
[35] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *FOCS 2007*, volume 7, pages 94–103, 2007.

[36] Ilya Mironov. Renyi differential privacy. In *CSF 2017*, pages 263–275. IEEE, 2017.
[37] Sahand Negahban, Bin Yu, Martin J Wainwright, and Pradeep K Ravikumar. A unified framework for high-dimensional analysis of m-estimators with decomposable regularizers. In *Advances in neural information processing systems*, pages 1348–1356, 2009.
[38] R Kelley Pace and Ronald Barry. Sparse spatial autoregressions. *Stat. Probab. Lett.*, 33(3):291–297, 1997.
[39] Martin Raab and Angelika Steger. Balls into bins – a simple and tight analysis. In *International Workshop RANDOM'98*, pages 159–170. Springer, 1998.
[40] Angelika Rohde and Lukas Steinberger. Geometrizing rates of convergence under differential privacy constraints. *arXiv preprint arXiv:1805.01422*, 2018.
[41] Or Sheffet. Differentially private ordinary least squares. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 3105–3114. JMLR. org, 2017.
[42] Adam Smith. Privacy-preserving statistical estimation with optimal convergence rates. In *STOC 2011*, pages 813–822. ACM, 2011.
[43] Thomas Steinke and Jonathan Ullman. Between pure and approximate differential privacy. *Journal of Privacy and Confidentiality*, 7(2), 2017.
[44] Thomas Steinke and Jonathan Ullman. Tight lower bounds for differentially private selection. In *FOCS 2017*, pages 552–563. IEEE, 2017.
[45] Kunal Talwar, Abhradeep Guha Thakurta, and Li Zhang. Nearly optimal private lasso. In *NeurIPS 2015*, pages 3025–3033, 2015.
[46] Martin J Wainwright. *High-dimensional statistics: A non-asymptotic viewpoint*, volume 48. Cambridge University Press, 2019.
[47] Yu-Xiang Wang, Stephen Fienberg, and Alex Smola. Privacy for free: Posterior sampling and stochastic gradient monte carlo. In *ICML*, pages 2493–2502, 2015.
[48] Larry Wasserman and Shuheng Zhou. A statistical framework for differential privacy. *J. Am. Stat. Assoc.*, 105(489):375–389, 2010.

DEPARTMENT OF STATISTICS
THE WHARTON SCHOOL
UNIVERSITY OF PENNSYLVANIA
PHILADELPHIA, PENNSYLVANIA 19104
USA
E-MAIL: tcai@wharton.upenn.edu
wangyc@wharton.upenn.edu
linjun.zhang@rutgers.edu
URL: http://www-stat.wharton.upenn.edu/∼tcai/
URL: https://linjunz.github.io/