Model-Protected Multi-Task Learning

Jian Liang, Ziqi Liu, Jiayu Zhou, Xiaoqian Jiang, Changshui Zhang, Fellow, IEEE, Fei Wang

Abstract—Multi-task learning (MTL) refers to the paradigm of learning multiple related tasks together. By contrast, single-task learning (STL) learns each individual task independently. MTL often leads to better trained models because they can leverage the commonalities among related tasks. However, because MTL algorithms will “transmit” information on different models across different tasks, MTL poses a potential security risk. Specifically, an adversary may participate in the MTL process through a participating task, thereby acquiring the model information for another task. Previously proposed privacy-preserving MTL methods protect data instances rather than models, and some of them may underperform in comparison with STL methods. In this paper, we propose a privacy-preserving MTL framework to prevent the information on each model from leaking to other models based on a perturbation of the covariance matrix of the model matrix, and we study two popular MTL approaches for instantiation, namely, MTL approaches for learning the low-rank and group-sparse patterns of the model matrix. Our methods are built upon tools for differential privacy. Privacy guarantees and utility bounds are provided. Heterogeneous privacy budgets are considered. Our algorithms can be guaranteed not to underperform comparing with STL methods. Experiments demonstrate that our algorithms outperform existing privacy-preserving MTL methods on the proposed model-protection problem.

Index Terms—Multi-Task Learning, Model Protection, Differential Privacy, Covariance Matrix, Low-Rank Subspace Learning.

1 INTRODUCTION

MULTI-TASK LEARNING (MTL) [12] refers to the paradigm of learning multiple related tasks together. By contrast, single-task learning (STL) refers to the paradigm of learning each individual task independently. MTL often leads to better trained models because the commonalities among related tasks may assist in the learning process for each specific task. For example, the capability of an infant to recognize a cat might help in the development of his/her capability to recognize a dog. In recent years, MTL has received considerable interest in a broad range of application areas, including computer vision [38, 62], natural language processing [2] and health informatics [52, 55].

Because MTL approaches explore and leverage the commonalities among related tasks within the learning process, either explicitly or implicitly, they pose a potential security risk. Specifically, an adversary may participate in the MTL process through a participating task, thereby acquiring the model information for another task. Consider the example of adversarial attacks [53, 41, 36], which have recently received significant research attention. In such an attack, adversarial perturbations are added to data samples to fool the models to infer incorrect predictions. Knowledge of the architecture and parameters of the attacked model will make the execution of a successful attack much easier; such a scenario is termed a white-box attack [59]. A black-box attack, in which at least the parameter values are not known to the adversary, is much more complicated and requires more conditions to be satisfied [59, 46]. Therefore, the leakage of information on one model to adversaries can escalate a black-box attack into a white-box attack. Such attacks are effective not only against deep neural networks but also against linear models such as logistic regression models and support vector machines [45], and they do not even necessarily require access to the data samples; instead, it may be possible to add one adversarial perturbation to the data-recording device, which may universally flip the predictions of most data samples [42].

We consider a concrete example in which an adversary hacks the models of interest without requiring any individual’s data. This example involves fooling a face-validation system. An adversary Jack from company A hacks the face-validation model of company B through the joint learning of models related to both companies. Jack then creates a mask containing an adversarial perturbation and pastes it onto the face-validation camera of company B to cause company B’s model to generate incorrect predictions for most employees of B, thereby achieving a successful white-box attack. Furthermore, we assume that Jack may even have an opportunity to act as a user of company B’s model. Given the model of company B, Jack can easily disguise himself to cause the model to predict that he is a valid employee of B, thereby achieving another successful white-box attack. However, if Jack has no information on the model, such attacks will be much more difficult. Similar white-box attacks can be generalized to many other applications.

As another example, we consider personalized predictive modeling [43, 61], which has become a fundamental methodology in health informatics. In this type of modeling, a custom-made model is built for each person. In modern health informatics, such a model may contain sensitive in-
formation, such as how and why a specific patient whether or not developed a specific disease. Such information is a different type of privacy from that of any single data record, and also requires protection. However, the joint training of personalized models may allow such causes of disease to be leaked to an adversary whose model is also participating in the joint training.

Because of the concerns discussed above, it is necessary to develop a secure training strategy for MTL approaches to prevent information on each model from leaking to other models.

However, few privacy-preserving MTL approaches have been proposed to date [40, 9, 47, 50, 29]. Moreover, such approaches protect only the security of data instances rather than that of models/predictors. A typical focus of research is distributed learning [40, 9], in which the datasets for different tasks are distributively located. The local task models are trained independently using their own datasets before being aggregated and injected with useful knowledge shared across tasks. Such a procedure mitigates the privacy problem by updating each local model independently. However, these methods do not provide theoretical guarantees of privacy.

Pathak et al. [47] proposed a privacy-preserving distributed learning scheme with privacy guarantees using tools offered by differential privacy [20], which provides a strong, cryptographically motivated definition of privacy based on rigorous mathematical theory and has recently received significant research attention due to its robustness to known attacks [15, 24]. This scheme is useful when one wishes to prevent potential attackers from acquiring information on any element of the input dataset based on a change in the output distribution. Pathak et al. [47] first trained local models distributively and then averaged the decision vectors of the tasks before adding noise based on the output perturbation method of [19]. However, because only averaging is performed in this method, it has a limited ability to cover more complicated relations among tasks, such as low-rank [4], group-sparse [54], clustered [27] or graph-based [63] task structures. Gupta et al. [29] proposed a scheme for transforming multi-task relationship learning [63] into a differentially private version, in which the output perturbation method is also adopted. However, their method requires a closed-form solution (obtained by minimizing the least-square loss function) to achieve a theoretical privacy guarantee; thus, it cannot guarantee the privacy for methods like logistic regression who needs iterative optimization procedures. Moreover, on their synthetic datasets, their privacy-preserving MTL methods underperformed even compared with non-private STL methods (which can guarantee optimal privacy against the leakage of information across tasks), which suggests that there is no reason to use their proposed methods. In addition, they did not study the additional privacy leakage due to the iterative nature of their algorithm (see Kairouz et al. [35]), and they did not study the utility bound for their method. The approaches of both Pathak et al. [47] and Gupta et al. [29] protect a single data instance instead of the predictor/model of each task, and they involve adding noise directly to the predictors, which is not necessary for avoiding the leakage of information across tasks and may induce excessive noise and thus jeopardize the utility of the algorithms.

To overcome these shortcomings, in this paper, we propose model-protected multi-task learning (MP-MTL), which enables the joint learning of multiple related tasks while simultaneously preventing leakage of the models for each task.

Without loss of generality, our MP-MTL method is designed based on linear multi-task models [32, 39], in which we assume that the model parameters are learned by minimizing an objective that combines an average empirical prediction loss and a regularization term. The regularization term captures the commonalities among the different tasks and couples their model parameters. The solution process for this type of MTL method can be viewed as a recursive two-step procedure. The first step is a decoupled learning procedure in which the model parameters for each task are estimated independently using some pre-computed shared information among tasks. The second step is a centralized transfer procedure in which some of the information shared among tasks is extracted for distribution to each task for the decoupled learning procedure in the next step. Our MP-MTL mechanism protects the models by adding perturbations during this second step. Note that we assume a curator that collects models for joint learning but never needs to collect task data. We develop a rigorous mathematical definition of the MP-MTL problem and propose an algorithmic framework to obtain the solution. We add perturbations to the covariance matrix of the parameter matrix because the tasks’ covariance matrix is widely used as a fundamental ingredient from which to extract useful knowledge to share among tasks [39, 63, 32, 5, 64, 52]. Consequently, our technique can cover a wide range of MTL algorithms. Fig. 1 illustrates the key ideas of the main framework.

Several methods have been proposed for the private release of the covariance matrix [34, 21, 10]. Considering an additive noise matrix, according to our utility analysis, the overall utility of the MTL algorithm depends on the spectral norm of the noise matrix. A list of the bounds on the spectral norms of additive noise matrices can be found in Jiang et al. [34]. We choose to add Wishart noise [34] to the covariance matrix for four reasons: (1) For a given privacy budget,
this type of noise matrix has a better spectral-norm bound than that of Laplace noise matrix [34]. (2) Unlike Gaussian noise matrix which enables an \((\epsilon, \delta)-\)private method with a positive \(\delta\), this approach enables an \((\epsilon, 0)-\)private method and can be used to build an iterative method that is entirely \((\epsilon, 0)-\)private, which provides a stronger privacy guarantee. (3) Unlike in the case of Gaussian and Laplace noise matrices, Wishart noise matrix is positive definite. Thus, it can be guaranteed that our method will not underperform compared with STL methods under high noise level, which means that participation in the joint learning process will have no negative effect on the training of any task model. (4) This approach allows arbitrary changes to any task, unlike the method of Blocki et al. [10]. The usage of the perturbed covariance matrix depends on the specific MTL method applied.

We further develop two concrete approaches as instantiations of our framework, each of which transforms an existing MTL algorithm into a private version. Specifically, we consider two popular types of basic MTL models: 1) a model that learns a low-rank subspace by means of a trace norm penalty [32] and 2) a model that performs shared feature selection by means of a group \(\ell_1 (\ell_{2,1})\) norm penalty [39]. In both cases, the covariance matrix is used to build a linear transform matrix with which to project the models into new feature subspaces, among which the most useful subspaces are selected. Privacy guarantees are provided. Utility analyses are also presented for both convex and strongly convex prediction loss functions and for both the basic and accelerated proximal-gradient methods. To the best of our knowledge, we are the first to present a utility analysis for differentially private MTL algorithms that allow heterogeneous tasks. By contrast, the distributed tasks studied by Pathak et al. [47] are homogeneous; i.e., the coding procedures for both features and targets are the same for different tasks. Furthermore, heterogeneous privacy budgets are considered for different iterations of our algorithms, and a utility analysis for budget allocation is presented. The utility results under the best budget allocation strategies are summarized in Table 1 (the notations used in the table are defined in the next section). In addition, we analyze the difference between our MP-MTL scheme and the existing privacy-preserving MTL strategies, which ensure the security of data instances. We also validate the effectiveness of our approach on benchmark and real-world datasets. Since existing privacy-preserving MTL methods only protect single data instances, they are transformed into methods that can protect task models using our theoretical results. The experimental results demonstrate that our algorithms outperform existing privacy-preserving MTL methods on the proposed model-protection problem.

The contributions of this paper are highlighted as follows.

- We are the first to propose and address the model-protection problem in MTL setting.
- We develop a general algorithmic framework to solve the MP-MTL problem to obtain secure estimates of the model parameters. We derive concrete instantiations of our algorithmic framework for two popular types of MTL models, namely, models that learn the low-rank and group-sparse patterns of the model matrix. It can be guaranteed that our algorithms will not underperform in comparison with STL methods under high noise level.
- Privacy guarantees are provided. To the best of our knowledge, we are the first to provide privacy guarantees for differentially private MTL algorithms that allow heterogeneous tasks and that minimize the logistic loss and other loss functions that do not have closed-form solutions.
- Utility analyses are also presented for both convex and strongly convex prediction loss functions and for both the basic and accelerated proximal-gradient methods. To the best of our knowledge, we are the first to present utility bounds for differentially private MTL algorithms that allow heterogeneous tasks. Heterogeneous privacy budgets are considered, and a utility analysis for budget allocation is presented.
- Existing privacy-preserving MTL methods that protect data instances are transformed into methods that can protect task models. Experiments demonstrate that our algorithms significantly outperform them on the proposed model-protection problem.

The remainder of this paper is organized as follows. Section 2 introduces the background on MTL problems and the definition of the proposed model-protection problem. The algorithmic framework and concrete instantiations of the proposed MP-MTL method are presented in Section 3, along with the analyses of utility and privacy-budget allocation. Section 4 presents an empirical evaluation of the proposed approaches, followed by the conclusions in Section 5.

### 2 Preliminaries and the Proposed Problem

In this section, we first introduce the background on MTL problems and then introduce the definition of model protection.

The notations and symbols that will be used throughout the paper are summarized in Table 2.

Extensive MTL studies have been conducted on linear models using regularized approaches. The basic MTL algorithm that we will consider is as follows:

\[
\hat{W} = \arg \min_{W} \sum_{i=1}^{m} L_i(X_i, W_i, y_i) + \lambda g(W),
\]  

(1)
where \( m \) is the number of tasks. The datasets for the tasks are denoted by \( D^m = (X^m, y^m) = \{(X_1, y_1), \ldots, (X_m, y_m)\} \), where for each \( i \in [m] \), \( D_i = (X_i, y_i) \), where \( X_i \in \mathbb{R}^{n_i \times d} \) and \( y_i \in \mathbb{R}^{n_i \times 1} \) denote the data matrix and target vector of the \( i \)-th task with \( n_i \) samples and dimensionality \( d \), respectively. \( \mathcal{L}_i \) is the prediction loss function for the \( i \)-th task. In this paper, we will focus on linear MTL models, where \( w_i \) denotes the predictor/decision vector for task \( i \) and \( W = [w_1, w_2, \ldots, w_m] \in \mathbb{R}^{k \times m} \) is the model parameter matrix. \( g(\cdot) \) is a regularization term that represents the structure of the information shared among the tasks, for which \( \lambda \) is the pre-fixed hyper-parameter. As a special case, STL can be described by (1) with \( \lambda = 0 \).

The key to multi-task learning is to relate the tasks via a shared representation, which, in turn, benefits the tasks to be learned. Each possible shared representation encodes certain assumptions regarding the task relatedness.

A typical assumption is that the tasks share a latent low-dimensional subspace [4, 16, 58]. The formulation also leads to a low-rank structure of the model matrix. Because optimization problems involving rank functions are intractable, a trace norm regularization method is typically used [3, 32, 48]:

\[
\min_W \sum_{i=1}^{m} \mathcal{L}_i(X_i w_i, y_i) + \lambda \|W\|_*.
\]

Another typical assumption is that all tasks share a subset of important features. Such taskrelatedness can be captured by imposing a group-sparse penalty on the predictor matrix to select shared features across tasks [54, 57, 39]. One commonly used group-sparse penalty is the group \( \ell_1 \) penalty [39, 44]:

\[
\min_W \sum_{i=1}^{m} \mathcal{L}_i(X_i w_i, y_i) + \lambda \|W\|_{2,1}.
\]

Now, we will present a compact definition of the model-protection problem in the context of MTL and discuss the general approach without differential privacy. As can be seen from (1), as a result of the joint learning process, \( \hat{w}_j \) may contain some information on \( \tilde{w}_i \), for \( i, j \in [m] \) and \( i \neq j \). Then, it is possible for the owner of task \( j \) to use such information to attack task \( i \). Thus, we define the model-protection problem as follows.

**Definition 1 (Model-Protection Problem for MTL).** The model-protection problem for MTL has three objectives:

1) minimizing the information on \( \tilde{w}_i \), that can be inferred from \( \hat{w}_{[\neg i]} \), for all \( i \in [m] \);

2) maximizing the prediction performance of \( \hat{w}_i \), for all \( i \in [m] \); and

3) sharing useful predictive information among tasks.

Now, we consider two settings:

1) A non-iterative setting, in which a trusted curator collects independently trained models, denoted by \( w_1, \ldots, w_m \), for all tasks without their associated data to be used as input. After the joint learning procedure, the curator outputs the updated models, denoted by \( \hat{W} \), and sends each updated model to each task privately. In this setting, the model collection process and the joint learning process are each performed only once.

2) An iterative setting, in which the model collection and joint learning processes are performed iteratively. Such a setting is more general.

One may observe that we assume the use of a trusted curator that collects the task models; this assumption will raise privacy concerns in settings in which the curator is untrusted. Such concerns are related to the demand for secure multi-party computation (SMC) [47, 25], the purpose of which is to avoid the leakage of data instances to the curator. Our extended framework considering SMC is presented in the supplementary material.

We note that the two types of problems represented by (2) and (3) are unified in the multi-task feature learning framework, which is based on the covariance matrix of the tasks' predictors [6, 22, 7]. Many other MTL methods also fall under this framework, such as the learning of clustered structures among tasks [27, 64] and the inference of task relations [63, 23, 11]. As such, we note that the tasks’ covariance matrix constitutes a major source of shared knowledge in MTL methods, and hence, it is regarded as the primary target for model protection.

Therefore, we address the model-protection problem by first rephrasing the first objective in Definition 1 as follows: minimizing the changes in \( \tilde{w}_{[\neg i]} \) and the tasks' covariance matrix \( \mathbb{W}^T \mathbb{W} \) or \( \mathbb{W}^T \mathbb{W} \) when task \( i \) participates in the joint learning process, for all \( i \in [m] \). Thus, the model of this new task is protected.

Then, we find that the concept of differential privacy (minimizing the change in the output distribution) can be adopted to further rephrase this objective as follows: minimizing the changes in the distribution of \( \tilde{w}_{[\neg i]} \) and the tasks’ covariance matrix when task \( i \) participates in the joint learning process, for all \( i \in [m] \).

In differential privacy, algorithms are randomized by introducing some kind of perturbation.

**Definition 2 (Randomized Algorithm).** A randomized algorithm \( A: \mathcal{D} \rightarrow \theta \in C \) is associated with some mapping \( A: \mathcal{D} \rightarrow \theta \in C \). Algorithm \( A \) outputs \( A(\mathcal{D}) = \theta \) with a density \( p(A(\mathcal{D}) = \theta) \) for each \( \theta \in C \). The probability space is over some kind of perturbation introduced into algorithm \( A \).

In this paper, \( A \) denotes some randomized machine learning estimator, and \( \theta \) denotes the model parameters that we wish to estimate. Perturbations can be introduced into the original learning system via the (1) input data [37, 8], (2) model parameters [13, 33], (3) objective function [14, 60], or (4) optimization process [51, 56].

The formal definition of differential privacy is as follows.
Definition 3 (Dwork et al. [20]). A randomized algorithm $A$ provides $(\epsilon, \delta)$-differential privacy if, for any two adjacent datasets $D$ and $D'$ that differ by a single entry and for any set $S$,

$$\Pr(A(D) \in S) \leq \exp(\epsilon) \Pr(A(D') \in S) + \delta,$$

where $A(D)$ and $A(D')$ are the outputs of $A$ on the inputs $D$ and $D'$, respectively.

The privacy loss pair $(\epsilon, \delta)$ is referred to as the privacy budget/loss and quantifies the privacy risk of algorithm $A$. The intuition is that it is difficult for a potential attacker to infer whether a certain data point has been changed (or added to the dataset $D$) based on a change in the output distribution. Consequently, the information of any single data point is protected.

Furthermore, note that differential privacy is defined in terms of application-specific adjacent input databases. In our setting, it is the pair of each task’s model and dataset to be treated as the “single entry” by Definition 3.

Several mechanisms exist for introducing a specific type of perturbation. A typical type is calibrated to the sensitivity of the original “unrandomized” machine learning estimator $f: D \rightarrow \Theta \in \mathbb{R}^d$. The sensitivity of an estimator is defined as the maximum change in its output due to an replacement of any single data instance.

Definition 4 (Dwork et al. [20]). The sensitivity of a function $f: D \rightarrow \mathbb{R}^d$ is defined as

$$S(f) = \max_{D, D'} \| f(D) - f(D')\|$$

for all datasets $D$ and $D'$ that differ by at most one instance, where $\| \cdot \|$ can be any norm, e.g., the $\ell_1$ or $\ell_2$ norm.

The use of additive noise, such as Laplace noise [20], Gaussian noise [21] or Wishart noise [34], with a standard deviation proportional to the sensitivity from the distribution of its view: $\tilde{w}_{[-i]}$. Thus, the information on the new task’s model is protected. Note that for different tasks, the views of an adversary are different.

We can redefine the non-iterative MP-MTL algorithm in the form of differential privacy.

Let $\overline{D} = \{(\hat{w}_1, D_1), \ldots, (\hat{w}_m, D_m)\}$ be an augmented dataset; i.e., let $(\hat{w}_i, D_i)$ be treated as the $i$-th “data instance” of the augmented dataset $\overline{D}$ for all $i \in [m]$. Thus, the $m$ datasets and $m$ models associated with the $m$ tasks are transformed into a single dataset $\overline{D}$ with $m$ “data instances”.

Then, we define $m$ outputs $\theta = (\theta_1, \ldots, \theta_m)$ such that for all $i \in [m]$, $\theta_i \in C_i$ denotes the view of an adversary for the $i$-th task, which includes $\hat{w}_{[-i]}$. Then, an $(\epsilon, \delta)$-non-iterative MP-MTL algorithm $A(B)$ should satisfy $m$ inequalities: for all $i \in [m]$, for all neighboring datasets $D$ and $D'$ that differ by the $i$-th “data instance”, and for any set $S_i \subseteq C_i$, we have

$$\Pr(\theta_i \in S_i \mid B = \overline{D}) \leq e^\epsilon \Pr(\theta_i \in S_i \mid B = \overline{D'}) + \delta.$$  

3.1 The General Framework for MP-MTL

We first present our main ideas for modeling our MP-MTL framework in the non-iterative setting before extending it to the general iterative setting.

3.1.1 Non-Iterative Setting

Formally, we define a non-iterative MP-MTL algorithm as follows.

Definition 5 (Non-iterative MP-MTL). For a randomized MTL algorithm $A(B)$ that uses $W \in \mathbb{R}^{d \times m}$ and the datasets $D^m = (X^m, y^m)$ as input and outputs $\overline{W} \in \mathbb{R}^{d \times m}$, $A$ is an $(\epsilon, \delta)$ non-iterative MP-MTL algorithm if for all $i \in [m]$, neighboring input pairs $(W_i, D^m)$ and $(W_i', D^m)$ that differ only by the $i$-th task, such that $w_i \neq w_i'$ or $D_i \neq D_i'$, the following holds for some constants $\epsilon, \delta \geq 0$ and for any set $S \subseteq \mathbb{R}^{d \times (m-1)}$:

$$\Pr(\hat{w}_{[-i]} \in S \mid B = (w_{[-i]}', D_{[-i]}, w_i, D_i)) \leq e^\epsilon \Pr(\hat{w}_{[-i]} \in S \mid B = (w_{[-i]}', D_{[-i]}, w_i', D_i')) + \delta.$$  

Remark 1. Note that the curator requires only the models $W$ as input, not the datasets. The datasets are held privately by the owners of their respective tasks and are only theoretically considered as inputs for the entire MTL algorithm.

As such, for the $i$-th task ($i \in [m]$), we assume that potential adversaries may acquire $\hat{w}_{[-i]}$, and we wish to protect both the input model $w_i$ and the dataset $D_i$. Note that although we ultimately wish to protect $w_i$, i.e., the output model for the $i$-th task, all information related to the $i$-th task in $w_i$ comes from the input model $w_i$ and the dataset $D_i$, and the latter are the only objects that any algorithm can directly control because they are the inputs.

For the sake of intuition, we set $w'_i$ and $D'_i$ in Definition 5 to 0 and the empty set, respectively; then, the goal of MP-MTL is to ensure that when the model for a new task is provided to the curator, an adversary, including another existing task, cannot discover significant anomalous information from the distribution of its view: $\hat{w}_{[-i]}$. Thus, the information on the new task’s model is protected. Note that for different tasks, the views of an adversary are different.

We can redefine the non-iterative MP-MTL algorithm as follows:

$$\Pr(\theta_i \in S_i \mid B = \overline{D}) \leq e^\epsilon \Pr(\theta_i \in S_i \mid B = \overline{D'}) + \delta.$$  

STL can be easily shown to be optimal for avoiding information leakage across tasks because the individual task models are learned independently.

Lemma 1. For any STL algorithm $A(B)$ that uses $W \in \mathbb{R}^{d \times m}$ and datasets $(X^m, y^m)$ as input, outputs $\overline{W} \in \mathbb{R}^{d \times m}$ and learns each task independently, $A$ is a $(0, 0)$ non-iterative MP-MTL algorithm.

We learn from this lemma that if there is no information sharing across tasks, then no leakage across tasks occurs.
3.1.2 Iterative Setting

Consider an iterative MP-MTL algorithm $A$ with a number of iterations $T$. For $t = 1, \ldots, T$, a trusted curator collects the models, denoted by $w_1^{(t-1)}, \ldots, w_m^{(t-1)}$, for all tasks. Then, model-protected MTL is performed, and the updated models $\tilde{w}_1^{(t)}, \ldots, \tilde{w}_m^{(t)}$ are output and sent back to their respective tasks.

In such a setting, for all $i \in [m]$, for the $i$-th task, we wish to protect dataset $D_i = (X_i, y_i)$ and the entire input sequence of its model $(w_1^{(0)}, \ldots, w_i^{(T-1)})$ (denoted by $w_i^{(0:T-1)}$ for short). For the $i$-th task, the output sequence $\tilde{w}_i^{(1:T)}$ is the view of a potential adversary.

We formally define an iterative MP-MTL algorithm as follows.

Definition 6 (Iterative MP-MTL). Let $A$ be a randomized iterative MTL algorithm with $N$ iterations. In the first iteration, $A$ performs the mapping $(\tilde{W}^{(0)}) \in \mathbb{R}^{d \times m} \rightarrow \theta_1 \in C_1$, where $\theta_1$ includes $\tilde{W}^{(1)} \in \mathbb{R}^{d \times m}$. For $t = 2, \ldots, T$, in the $t$-th iteration, $A$ performs the mapping $(\tilde{W}^{(t-1)}) \in \mathbb{R}^{d \times m}, D_t, \theta_1, \ldots, \theta_{t-1}) \rightarrow \theta_t \in C_t$, where $\theta_t$ includes $\tilde{W}^{(t)} \in \mathbb{R}^{d \times m}$. $A$ is an $(\epsilon, \eta)$ iterative MP-MTL algorithm if for all $i \in [m]$, for all $t \in [T]$, and for neighboring input pairs $(\tilde{W}^{(t-1)}, D_t)$ and $(\tilde{W}^{′(t-1)}, (D'_t)^m)$ that differ only by the $i$-th task, such that $w_i^{(t-1)} \neq (w'_i)^{(t-1)}$ or $D_i \neq D'_i$, the following holds for some constants $\epsilon, \delta > 0$ and for any set $S \subseteq \mathbb{R}^{d \times (m-1) \times T}$:

$$P(\tilde{w}^{(1:T)}_{-i} \in S | \bigcap_{i=1}^{T} B_i = (\tilde{W}^{(t-1)}, D_t, \theta_{1:t-1}))$$

$$\leq e^\epsilon P(\tilde{w}^{(1:T)}_{-i} \in S | \bigcap_{i=1}^{T} B_i = ((\tilde{W}^{′(t-1)}, (D'_t)^m), \theta_{1:t-1})) + \delta,$$

where for all $t \in [T], B_t$ denotes the input for the $t$-th iteration and

$$\theta_{1:t-1} = \begin{cases} \emptyset, & t = 1 \\ \theta_1, \theta_2, \ldots, \theta_{t-1}, & t \geq 2. \end{cases}$$

We can also redefine the iterative MP-MTL algorithm in the form of differential privacy by considering an augmented dataset $\tilde{D}_t = \{(w_1^{(t-1)}, D_1), \ldots, (w_m^{(t-1)}, D_m)\}$, i.e., by treating $(w_i^{(t-1)}, D_i)$ as the $i$-th “data instance” of the data set $\tilde{D}_t$, for all $i \in [m]$, in the $t$-th iteration, for all $t \in [T]$. The details are similar to those in the non-iterative setting and are omitted here.

Obviously, any non-iterative MP-MTL algorithm is an iterative MP-MTL algorithm with $T = 1$.

Our MP-MTL framework is elaborated in Algorithm 1, which is iterative in nature. As mentioned in Section 2, we choose to protect the tasks’ covariance matrix, which is denoted by $\Sigma = WW^T$ or $\Sigma = W^TW$, depending on the chosen MTL method. As previously stated, Wishart noise [34] is added. Fig. 1 illustrates the key concepts of the framework. This framework is generally applicable for many optimization schemes, such as proximal gradient methods [32, 39], alternating methods [5] and Frank-Wolfe methods [30].

Remark 2. In Algorithm 1, the datasets $(X^m, y^m)$ are only used in STL algorithms that can be performed locally.

Algorithm 1 MP-MTL framework

Input: Datasets $(X^m, y^m) = \{(X_i, y_i), \ldots, (X_m, y_m)\}$, where $i \in [m], X_i \in \mathbb{R}^{n_i \times d}$ and $y_i \in \mathbb{R}^{n_i \times 1}$. Privacy loss $\epsilon, \delta \geq 0$.

Number of iterations $T$. Initial shared information matrix $M^{(0)}$. Initial task models $W^{(0)}$, which can be acquired via arbitrary STL methods.

Output: $\tilde{W}^{(1:T)}$

1: For $t = 1, \ldots, T$, set $\epsilon_t$ such that $\epsilon \leq \epsilon_t$, where

$$\epsilon_t = \min \left\{ \sum_{t=1}^{T} \epsilon_t, \min_{1 \leq t \leq T} \left( \frac{e^{\epsilon} - 1}{e^{\epsilon} + 1} \right) + \left( \frac{1}{T} \sum_{t=1}^{T} 2e^{\epsilon} \log \left( \frac{1}{\delta} \right) \right) \right\}.$$ 

2: for $t = 1 \ldots T$ do

3: Compute the sensitivity vector $s^{(t-1)} = [s_1^{(t-1)}, \ldots, s_m^{(t-1)}]^T$, which is defined as follows for all $i \in [m]$:

$$(s_i^{(t-1)} = \max_{w_i^{(t-1)}} ||W_i^{(t-1)}||_2^2 = ||W_i^{(t-1)}||_2^2).$$

4: $\Sigma^{(t)} = W^{(t-1)}(W^{(t-1)})^T$ (or $\Sigma^{(t)} = W^{(t-1)}(W^{t-1})^T W^{(t-1)})$.

5: $\Sigma_t = \Sigma^{(t)} + E$, where $E \sim N(0, K_{max}^{(t)}}(\mathbf{L}_d)$ (or $E \sim N(m + 1, \max \{s_i^{(t-1)} \mathbf{L}_d \}$) and diag$(\mathbf{v})$ transforms a vector into a diagonal matrix.

6: Perform an arbitrary mapping $f: \Sigma^{(t)} \rightarrow M^{(t)}$, e.g., take the diagonal elements of $\Sigma^{(t)}$ or the singular value decomposition of $\Sigma^{(t)}$.

7: $w_i^{(t-1)} = A_{STL}(M^{(t)}, w_i^{(t-1)}{X}_i, y_i)$, for all $i \in [m]$, where $A_{STL}$ is an arbitrary STL algorithm for the $i$-th task and the $w_i^{(t-1)}$ are used for initialization.

8: Set the input for the next iteration: $W^{(t)} = \tilde{W}^{(t)}$.

9: end for

3.2 Instantiations of the MP-MTL Framework

In this section, we introduce two instantiations of our MP-MTL framework described in Algorithm 1. These two instantiations are related to the MTL problems represented by (2) and (3). We focus on the proximal gradient descent methods presented by Ji and Ye [32] and Liu et al. [39] for Problems (2) and (3), respectively.

First, we instantiate the MP-MTL framework for Problem (2), the low-rank case, as shown in Algorithm 2. Generally speaking, the algorithm uses an accelerated proximal gradient method. Steps 5 to 9 approximate the following proximal operator:

$$\tilde{W}^{(t-1)} = \arg \min_{W} \frac{1}{2\eta} ||W - \tilde{W}^{(t-1)}||_F^2 + \lambda ||W||_*.$$ 

Fig. 2 provides a running example for model leakage and model protection under different settings of Algorithm 2.
Algorithm 2 MP-MTL Low-Rank Estimator

Input: Datasets $(X^m, y^m) = \{(X_1, y_1), \ldots, (X_m, y_m)\}$, where $\forall i \in [m], X_i \in \mathbb{R}^{n_i \times d}$ and $y_i \in \mathbb{R}^{n_i \times 1}$. Privacy loss $\epsilon, \delta \geq 0$. Number of iterations $T$. Step size $\eta$. Regularization parameter $\lambda > 0$. Norm clipping parameter $K > 0$. Acceleration parameters $\{\beta_t\}$. Initial task models $W^{(0)}$.

Output: $\tilde{W}^{(1:T)}$.
1: For $t \in [T]$, set $\epsilon_t$ such that $\epsilon \leq \epsilon_t$, where $\tilde{\epsilon}$ is defined in (7).
2: for $t = 1 \rightarrow T$ do
3: Norm clipping: $\tilde{w}_i^{(t-1)} = w_i^{(t-1)} / \max(1, \frac{\|w_i^{(t-1)}\|_2}{K})$, for all $i \in [m]$. Let $\tilde{W}^{(0)} = \tilde{W}^{(0)}$.
4: Compute sensitivity: $s_i^{(t-1)} = 2K$ for all $i \in [m]$.
5: $\tilde{\Sigma}^{(t)} = \tilde{W}^{(t)}(\tilde{W}^{(t-1)})^T$.
6: $\Sigma^{(t)} = \tilde{\Sigma}^{(t)} + E$, where $E \sim W_d(d + 1, \max\{s_i^{(t-1)}\}/2\epsilon_t)I_d$ is a sample from the Wishart distribution.
7: Perform singular vector decomposition: $U \Lambda U^T = \Sigma^{(t)}$.
8: Let $S_{\lambda,i}^\lambda$ be a diagonal matrix, and let $S_{\eta,i} = \max\{0, 1 - \eta\lambda/\sqrt{\Sigma^{(t)}_{ii}}\}$, for $i = 1, \ldots, \min\{d, m\}$.
9: Let $\tilde{w}^{(t)}_i = US_{\lambda,i}^\lambda U^T \tilde{w}^{(t-1)}_i$, for all $i \in [m]$.
10: Let $\tilde{z}^{(t)}_i = \tilde{w}^{(t)}_i + \beta_t(\tilde{w}^{(t)}_i - \tilde{w}^{(t-1)}_i)$, for all $i \in [m]$.
11: Let $w_i^{(t)} = z_i^{(t)} - \eta \frac{\partial C(X, \tilde{w}^{(t)}_i)}{\partial z_i^{(t)}}$, for all $i \in [m]$.
12: end for

The approximation error bounds for both the proximal operators are provided in Section 3.4.

Algorithm 3 MP-MTL Group-Sparse Estimator

Input: Datasets $(X^m, y^m) = \{(X_1, y_1), \ldots, (X_m, y_m)\}$, where $\forall i \in [m], X_i \in \mathbb{R}^{n_i \times d}$ and $y_i \in \mathbb{R}^{n_i \times 1}$. Privacy loss $\epsilon, \delta \geq 0$. Number of iterations $T$. Step size $\eta$. Regularization parameter $\lambda > 0$. Norm clipping parameter $K > 0$. Acceleration parameters $\{\beta_t\}$. Initial task models $W^{(0)}$.

Output: $\tilde{W}^{(1:T)}$.
1: For $t \in [T]$, set $\epsilon_t$ such that $\epsilon \leq \epsilon_t$, where $\tilde{\epsilon}$ is defined in (7).
2: for $t = 1 \rightarrow T$ do
3: Norm clipping: $\tilde{w}_i^{(t-1)} = w_i^{(t-1)} / \max(1, \frac{\|w_i^{(t-1)}\|_2}{K})$, for all $i \in [m]$. Let $\tilde{W}^{(0)} = \tilde{W}^{(0)}$.
4: Compute sensitivity: $s_i^{(t-1)} = 2K$ for all $i \in [m]$.
5: $\tilde{\Sigma}^{(t)} = \tilde{W}^{(t)}(\tilde{W}^{(t-1)})^T$.
6: $\Sigma^{(t)} = \tilde{\Sigma}^{(t)} + E$, where $E \sim W_d(d + 1, \max\{s_i^{(t-1)}\}/2\epsilon_t)I_d$ is a sample from the Wishart distribution.
7: Let $S_{\lambda,i}^\lambda$ be a diagonal matrix, where for $i = 1, \ldots, d, S_{\eta,i} = \max\{0, 1 - \eta\lambda/\sqrt{\Sigma_{ii}^{(t)}}\}$.
8: Let $\tilde{w}^{(t)}_i = S_{\lambda,i}^\lambda \tilde{w}^{(t-1)}_i$, for all $i \in [m]$.
9: Let $\tilde{z}^{(t)}_i = \tilde{w}^{(t)}_i + \beta_t(\tilde{w}^{(t)}_i - \tilde{w}^{(t-1)}_i)$, for all $i \in [m]$.
10: Let $w_i^{(t)} = z_i^{(t)} - \eta \frac{\partial C(X, \tilde{w}^{(t)}_i)}{\partial z_i^{(t)}}$, for all $i \in [m]$.
11: end for

Second, we instantiate the MP-MTL framework for Problem (3), the group-sparse case, as shown in Algorithm 3. Steps 5 to 8 approximate the following proximal operator:

$$\tilde{W}^{(t-1)} = \arg \min_w \frac{1}{2\eta} \|W - \tilde{W}^{(t-1)}\|_F^2 + \lambda \|W\|_{2,1}. \tag{9}$$

3.3 Privacy Guarantees

Theorem 1. Algorithm 1 is an $(\epsilon, \delta)$ iterative MP-MTL algorithm.

Corollary 1. Algorithm 1 and Algorithm 3 are $(\epsilon, \delta)$ iterative MP-MTL algorithms.

3.4 Utility Analyses

Building upon the utility analysis of the Wishart mechanism presented by Jiang et al. [34], the convergence analysis of inexact proximal-gradient descent presented by Schmidt et al. [49] and the optimal solutions for proximal operators presented by Ji and Ye [32] and Liu et al. [39], we study the utility bounds for Algorithm 2 and Algorithm 3.

We define the following parameter space for a constant $K > 0$:

$$\mathcal{W} = \{W \in \mathbb{R}^{d \times m} : \max_{i \in [m]} \|w_i\|_2 \leq K\}.$$
We consider $f(W) = \frac{1}{2} \sum_{i=1}^{m} C_i (X_i, w_i, y_i)$. We assume that $m f(W)$ is convex and has an $L$-Lipschitz-continuous gradient (as defined in Schmidt et al. [49]). Let $W_* = \arg \min_{W} m f(W) + \lambda g(W)$, where $g(\cdot) = \| \cdot \|_*$ for Algorithm 2 and $g(\cdot) = \| \cdot \|_{2,1}$ for Algorithm 3. Without loss of generality, we assume that $W_* \in W$ and $f(\tilde{W}^{(t)}) - f(W_*) = O(K^2 L m)$. We adopt the notation $q = \min(d, m)$.

We have studied the utility bounds for three cases of $\{ \epsilon_i \}$ in (7). Here, we report the results for the following case:

$$
\epsilon = \sum_{i=1}^{T} \left( \epsilon_i - 1 \right) \epsilon_i + \sqrt{2 \sum_{i=1}^{T} 2 \epsilon_i^2 \log \left( 1 + \frac{\sqrt{\sum_{i=1}^{T} 2 \epsilon_i^2}}{\delta} \right)}.
$$

Such a case assumes $\delta > 0$ and is suitable for small privacy budgets, such as $\epsilon + c \delta < 1$. The results for the other two cases of $\{ \epsilon_i \}$ can be found in the supplementary material.

The number of tasks are assumed sufficient as follows.

**Assumption 1.** For Algorithm 2, assume that for sufficiently large $C > 0$,

$$
m > \frac{Cd^2 \log^2(d)(\log(e + \sqrt{2d}) + 2c)}{\epsilon}.
$$

For Algorithm 3, assume that for sufficiently large $C > 0$,

$$
m > \frac{C \log(d)}{\log(e + \sqrt{2d}) + 2\epsilon}.
$$

We first present approximation error bounds for proximal operators with respect to an arbitrary noisy matrix $E$.

**Lemma 2.** Consider Algorithm 2. For $t \in [T]$, in the $t$-th iteration, let $C = \tilde{W}^{(t-1)}$. Let $r_c = \text{rank}(C) \leq q$ be the rank of $C$. Suppose that there exists an index $k \leq q$ such that $\sigma_k(C) > \eta \lambda$ and $\sigma_{k+1}(C) \leq \eta \lambda$. Assume that $2\sigma_1(E) \leq \sqrt{\sigma_j(C)} - \sigma_{j+1}(C)$ for $j \in [k]$. Then, for any random matrix $E \in \mathbb{R}^{d \times d}$, the following holds:

$$
\frac{1}{2\eta} \left[ \| \tilde{W}^{(t)} - C \|_F^2 + \lambda \| \tilde{W}^{(t)} \|_* \right] - \left\{ \min \left[ \frac{1}{2} \left[ \| W - C \|_F^2 + \lambda \| W \|_* \right] \right] \right\} \leq \frac{1}{\eta} \left( \frac{\sigma_k(C)}{\eta \lambda} + \sigma_k(C) \right) + \frac{\left( \frac{k^2}{\eta \lambda} + 2k \right) \sigma_1(E) + \max(0, r_c - k) \sqrt{\sigma_1(E)} }{2\eta}.
$$

**Lemma 3.** Consider Algorithm 3. For $t \in [T]$, in the $t$-th iteration, let $C = \tilde{W}^{(t-1)}$. Let the indices of non-zero rows of $C$ be denoted by $I_c = \{ j : C_{j} \neq 0 \}$, and let $r_{c,s} = |I_c| \leq d$. Let $Z_0 = \mathbb{C}^{I_c}$. Suppose that there exists an integer $k \leq d$ such that $\sum_{j=1}^{d} I(j,\delta) \geq n \lambda k$, where $I(\cdot)$ is the indicator function. Then, for any random matrix $E \in \mathbb{R}^{d \times d}$, the following holds:

$$
\frac{1}{2\eta} \left[ \| \tilde{W}^{(t)} - C \|_F^2 + \lambda \| \tilde{W}^{(t)} \|_{2,1} \right] - \left\{ \min \left[ \frac{1}{2} \left[ \| W - C \|_F^2 + \lambda \| W \|_* \right] \right] \right\} \leq \frac{1}{\eta} \left( \frac{r_{c,s}}{\eta \lambda} \left( \max_{j \in [d]} C_{j}^2 \right) + \max_{j \in [d]} \| C \|_{2,1} \right) \leq \frac{k}{2\eta \lambda} \max_{j \in [d]} E_{jj} + \max(0, r_{c,s} - k) \max_{j \in [d]} \| E_{jj} \|_1.
$$

We find that the approximation error bounds for both algorithms depend on $\sigma_1(E)$ (note that $\max_{j} |E_{jj}| \leq \sigma_1(E)$).

Now, we present guarantees regarding both utility and run time. In the following, $E$ is assumed to be the Wishart random matrix defined in each algorithm. We consider heterogeneous privacy budgets and set $c_t = \Theta(t^\alpha)$ for $\alpha \in \mathbb{R}$ and $t \in [T]$ for the convex case.

**Theorem 2.** (Low rank - Convexity). Consider Algorithm 2. For an index $k \leq q$ that satisfies the conditions given in Lemma 2 for all $t \in [T]$, $\eta = 1/L$, and $\lambda = \Theta(LK \sqrt{m})$, assume that $c_t \leq 4Kk^2d(\log d)/q^2$ for $t \in [T]$.

**No acceleration:** If we set $\beta_t = 0$ for $t \in [m]$, then we also set

$$
T = \Theta \left( \frac{(\alpha/2 - 1)^2 \sqrt{2\alpha + 1} \sqrt{\me}}{kd \log d \sqrt{\log(e + \sqrt{2d}) + 2\epsilon}} \phi(\alpha)^2 \right)
$$

for $E = f \left( \frac{1}{T} \sum_{t=1}^{T} \tilde{W}^{(t)} \right) - f(W_*)$, we have, with high probability,

$$
E = O \left( K^2 L \left[ \frac{kd \log d \sqrt{\log(e + \sqrt{2d}) + 2\epsilon}}{(\alpha/2 - 1)^2 \sqrt{2\alpha + 1} \sqrt{\me}} \phi(\alpha)^2 \right] \right),
$$

where

$$
\phi(\alpha) = \left\{ \begin{array}{ll}
2/(\alpha + 1), & \alpha > 4; \\
2/5, & -1/2 < \alpha < 2; \\
1/(2 - \alpha), & \alpha < -1/2.
\end{array} \right.
$$

**Use acceleration:** If we set $\beta_t = (t - 1)/(t + 2)$ for $t \in [m]$, then if we also set

$$
T = \Theta \left( \frac{(\alpha/2 - 2)^2 \sqrt{2\alpha + 1} \sqrt{\me}}{kd \log d \sqrt{\log(e + \sqrt{2d}) + 2\epsilon}} \phi(\alpha)^2 \right)
$$

for $E = f \left( \frac{1}{T} \sum_{t=1}^{T} \tilde{W}^{(t)} \right) - f(W_*)$, we have, with high probability,

$$
E = O \left( K^2 L \left[ \frac{kd \log d \sqrt{\log(e + \sqrt{2d}) + 2\epsilon}}{(\alpha/2 - 2)^2 \sqrt{2\alpha + 1} \sqrt{\me}} \phi(\alpha)^2 \right] \right),
$$

where

$$
\phi(\alpha) = \left\{ \begin{array}{ll}
4/(\alpha + 1), & \alpha > 4; \\
4/9, & -1/2 < \alpha < 4; \\
2/(4 - \alpha), & \alpha < -1/2.
\end{array} \right.
$$

**Theorem 3.** (Group sparse - Convexity). Consider Algorithm 3. For an index $k \leq d$ that satisfies the condition given in Lemma 3 for all $t \in [T]$, $\eta = 1/L$, and $\lambda = \Theta(LKd \sqrt{m})$, assume that $c_t \leq k^2 \log(d)/4K(d - k)^2 m$ for $t \in [T]$.

**No acceleration:** If we set $\beta_t = 0$ for $t \in [m]$, then if we also set

$$
T = \Theta \left( \frac{(\alpha/2 - 1)^2 \sqrt{2\alpha + 1} \sqrt{\me}}{kd \log d \sqrt{\log(e + \sqrt{2d}) + 2\epsilon}} \phi(\alpha)^2 \right)
$$

for $E = f \left( \frac{1}{T} \sum_{t=1}^{T} \tilde{W}^{(t)} \right) - f(W_*)$, we have, with high probability,

$$
E = O \left( K^2 L \left[ \frac{kd \log d \sqrt{\log(e + \sqrt{2d}) + 2\epsilon}}{(\alpha/2 - 1)^2 \sqrt{2\alpha + 1} \sqrt{\me}} \phi(\alpha)^2 \right] \right),
$$

where

$$
\phi(\alpha) \text{ is defined in (13)}.
$$
Use acceleration: If we set $\beta_t = (t-1)/(t+2)$ for $t \in [m]$, then if we also set

$$T = \Theta\left(\frac{(\alpha/2 - 2)^2 \sqrt{2\alpha + 1} K m}{k \log d} \frac{\phi(\alpha/2)}{\log(e + \sqrt{2}\delta)} + 2e\right)^{\phi(\alpha)/2}$$

for $E = f(\tilde{W}(T)) - f(W_*)$, we have, with high probability,

$$E = O\left(K \left[ k \log d \frac{\sqrt{\log(e + \sqrt{2}\delta)} + 2e}{(Q_0/\sqrt{Q} - 1)^2 \sqrt{1 - Q^2} K m e} \right] \right),$$

where $\phi(\alpha)$ is defined in (15).

Now, we further assume that $mf(W)$ is $\mu$-strongly convex and has an $L$-Lipschitz-continuous gradient, where $\mu < L$. We set $\epsilon_t = \Theta(Q^{-1})$ for $Q > 0$ and $t \in [T]$ for this case.

**Theorem 4** (Low rank - Strong convexity). Consider Algorithm 2. For an index $k \leq q$ that satisfies the conditions given in Lemma 2 for all $t \in [T]$, $\eta = 1/L$, and $\lambda = \Theta(LK \sqrt{m})$, assume that $\epsilon_t \leq 4Kd^2/\log^3 d$ for $t \in [T]$.

**No acceleration:** If we set $\beta_t = 0$ for $t \in [m]$, then if we let $Q_0 = 1 - \mu/L$ and set

$$T = \Theta\left(\log_1/(\phi(Q,Q^\alpha)) \frac{(Q_0^\alpha - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}}{k \log d \frac{\sqrt{\log(e + \sqrt{2}\delta)} + 2e}{(Q_0/\sqrt{Q} - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}} \right)^{\phi(\alpha)/2},$$

for $E = \frac{1}{\sqrt{m}} \left\| \tilde{W}(T) - W_* \right\|_F$, we have, with high probability,

$$E = O\left(\log_1/(\phi(Q,Q^\alpha)) \frac{(Q_0^\alpha - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}}{k \log d \frac{\sqrt{\log(e + \sqrt{2}\delta)} + 2e}{(Q_0/\sqrt{Q} - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}} \right)^{\phi(\alpha)/2} K,$$

where $\phi(\alpha)$ is defined in (19).

**Use acceleration:** If we set $\beta_t = (1 - \sqrt{\mu/L})/(1 + \sqrt{\mu/L})$ for $t \in [m]$, then if we let $Q_0 = 1 - \sqrt{\mu/L}$ and set

$$T = \Theta\left(\log_1/(\phi(Q,Q^\alpha)) \frac{(Q_0^\alpha - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}}{k \log d \frac{\sqrt{\log(e + \sqrt{2}\delta)} + 2e}{(Q_0/\sqrt{Q} - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}} \right)^{\phi(\alpha)/2},$$

for $E = f(\tilde{W}(T)) - f(W_*)$, we have, with high probability,

$$E = O\left(\log_1/(\phi(Q,Q^\alpha)) \frac{(Q_0^\alpha - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}}{k \log d \frac{\sqrt{\log(e + \sqrt{2}\delta)} + 2e}{(Q_0/\sqrt{Q} - 1)^2 \sqrt{1 - Q^2} \sqrt{m e}} \right)^{\phi(\alpha)/2} Q_0.$$

where $\phi(\alpha)$ is defined in (19).

3.5 **Privacy Budget Allocation**

In this section, we optimize the utility bounds presented in Section 3.4 with respect to the corresponding budget allocation strategies.

**Theorem 6.** Consider Algorithm 2 and Algorithm 3. For a convex $f$, use Theorem 2 and Theorem 3.

(1) No acceleration: The bounds given in (12) and (16) both reach their respective minima w.r.t. $\alpha$ at $\alpha = 0$. Meanwhile, $\phi(\alpha) = 2/5$.

(2) Use acceleration: The bounds given in (14) and (17) both reach their respective minima w.r.t. $\alpha$ at $\alpha = 2/5$. Meanwhile, $\phi(\alpha) = 4/9$.

For a strongly convex $f$, use Theorem 4 and Theorem 5.

(1) No acceleration: The bounds given in (18) and (20) both reach their respective minima w.r.t. $Q$ at $Q = Q_0^{2/5}$. Meanwhile, $\log_1/(\phi(Q,Q^\alpha)) Q_0 = 1/2$.

(2) Use acceleration: The bounds given in (21) and (22) both reach their respective minima w.r.t. $Q$ at $Q = (Q_0^{1/5})$. Meanwhile, $\log_1/(\phi(Q,Q^\alpha)) Q_0 = 1$.

Results corresponding to the optimized budget allocation strategies (with $\delta > 0$) are summarized in Table 1, where the terms with respect to $\sqrt{\log(e + \sqrt{2}\delta)} + 2e$ are omitted, and the results associated with the setting $\epsilon = \sum_{t=1}^T \epsilon_t$ and $\delta = 0$ are also included, which provides $(\epsilon, 0)$-iterative MP-MLT algorithms.

We learn from Theorem 6 that (1) for all four settings, a non-decreasing series of $\epsilon_t$ results in a good utility bound, since $\alpha = 0, 2/5 \geq 0$ and $Q = Q_0^{2/5}, (Q_0^{1/5}) < 1$. Intuitively, this means adding non-increasing noises over iterations, which is reasonable since initial iterations may move quickly in the parameter space while the last iterations may only fine-tune the model by a little. (2) Both the strong-convexity condition and the acceleration strategy improve the utility bounds.

Now, we introduce our concrete strategy for setting $\{\epsilon_t\}$ in both Algorithm 2 and Algorithm 3. We assume that $T, \epsilon$ and $\delta$ are given.
For a convex $f$, if no acceleration is to be used, then set $\beta_t = 0$ for $t \in [m]$ and set $\alpha \in \mathbb{R}$ (e.g., $\alpha = 0$); otherwise, set $\beta_t = (t - 1)/(t + 2)$ for $t \in [m]$ and set $\alpha \in \mathbb{R}$ (e.g., $\alpha = 2/5$). Then, for $t \in [T]$, let $\epsilon_t = \epsilon_0^{\alpha t}$ and find the largest $\epsilon_0$ that satisfies $\bar{c} \leq \epsilon$, where $\bar{c}$ is defined in (7).

For a $\mu$-strongly convex $f(W)$ with a known value of $\mu$ (e.g., $\mu = \frac{1}{2} \|w\|^2$ is added to each $\lambda_i$), if no acceleration is to be used, then set $\beta_t = 0$ for $t \in [m]$ and set $Q > 0$ (e.g., $Q = (1 - \mu/L)^{2/3}$, if $L$ is known); otherwise, if $L$ is known, set $\beta_t = (1 - \sqrt{\mu/L})/(1 + \sqrt{\mu/\epsilon})$ for $t \in [m]$ and set $Q > 0$ (e.g., $Q = (1 - \sqrt{\mu/L})^{1/3}$). Then, for $t \in [T]$, let $\epsilon_t = \epsilon_0 Q^{-t}$ and find the largest $\epsilon_0$ that satisfies $\bar{c} \leq \epsilon$, where $\bar{c}$ is defined in (7).

### 3.6 Relationship with Data-Protected MTL

In contrast with the proposed model-protected MTL approach, privacy-preserving MTL algorithms that prevent a single data instance for one task from leaking to other tasks can be regarded as data-protected MTL (DP-MTL) algorithms. The methods of Pathak et al. [47] and Gupta et al. [29] both fall into this category. Here, we explicitly define only the general iterative DP-MTL algorithm, since algorithms of the non-iterative type can be seen as a special case with $T = 1$.

**Definition 7** (Iterative DP-MTL). Let $A$ be a randomized iterative MTL algorithm with a number of iterations $T$. In the first iteration, $A$ performs the mapping $(W^{(0)}) \in \mathbb{R}^{d \times m}, D^m) \rightarrow \theta_1 \in C_1$, where $\theta_1$ includes $W^{(1)} \in \mathbb{R}^{d \times m}$. For $t = 2, \ldots, T$, in the $t$-th iteration, $A$ performs the mapping $(W^{t-1}) \in \mathbb{R}^{d \times m}, D^m, \theta_1, \ldots, \theta_{t-1}) \rightarrow \theta_t \in C_t$, where $\theta_t$ includes $W^{(t)} \in \mathbb{R}^{d \times m}$. $A$ is an $(\epsilon, \delta)$ iterative DP-MTL algorithm if for all $i \in [m]$ and for all neighboring datasets $D^m$ and $(D')^m$ that differ by a single data instance for the $i$-th task, the following holds for some constants $\epsilon', \delta \geq 0$ and for any set $S \subseteq \mathbb{R}^{d \times (m-1) \times T}$:

\[
P(W^{(1:T)}_{[-i]} \in S | \bigcap_{t=1}^T B_t = (W^{(t-1)}, D^m, \theta_{1:t-1})) \leq \epsilon' P(W^{(1:T)}_{[-i]} \in S | \bigcap_{t=1}^T B_t = (W^{t-1}, (D')^m, \theta_{1:t-1})) + \delta,
\]

where for all $t \in [T]$, $B_t$ denotes the input for the $t$-th iteration,

$$\theta_{1:t-1} = \begin{cases} \emptyset, & t = 1, \\ \theta_1, \theta_2, \ldots, \theta_{t-1}, & t \geq 2, \end{cases}$$

and $(W')^{t-1}$ is associated with the setting in which a single data instance for the $i$-th task has been replaced.

**Proposition 2.** The methods of both Pathak et al. [47] and Gupta et al. [29] are iterative DP-MTL algorithms with $T = 1$ and $T \geq 1$, respectively.

The following proposition addresses the relationship between MP-MTL and DP-MTL.

**Proposition 3.** For tasks’ sample sizes $n_1, \ldots, n_m$, any $(\epsilon, \delta)$ iterative DP-MTL algorithm is a $(\epsilon/n, \delta/(n \exp(\epsilon)))$ iterative MP-MTL algorithm, where $n = \max_{i \in [m]} n_i$.

Therefore, by Proposition 3, to guarantee an $(\epsilon, \delta)$ iterative MP-MTL algorithm, one can use an $(\epsilon/n, \delta/(n \exp(\epsilon)))$ iterative DP-MTL algorithm.

### 4 Experiments

In this section, we evaluate the proposed MP-MTL method. As two instantiations of our method, Algorithm 2 and Algorithm 3 are evaluated with respect to their ability to capture the low-rank and group-sparse patterns, respectively, in the model matrix. We use both synthetic and real-world datasets to evaluate these algorithms. All the algorithms were implemented in MATLAB.

#### 4.1 Methods for Comparison

We use the least-square loss and the logistic loss for least-square regression and binary classification problems, respectively.

For each setting, we evaluate three types of methods: 1) non-private STL methods, in which each task is learned independently without the introduction of any perturbation; 2) privacy-preserving MTL methods, including our MP-MTL method and existing differentially private MTL methods; and 3) non-private MTL methods, corresponding to the original MTL methods without the introduction of any perturbation.

For comparison with existing differentially private MTL methods, because few such approaches have been proposed, we firstly consider the Differentially Private Multi-Task Relationship Learning (DP-MTRL) method proposed by Gupta et al. [29]. The authors of this method did not consider the increase in privacy loss resulting from their iterative update procedure. This problem is solved in our comparison by using the same composition technique as in our method (Equation 7).

We have also modified the DP-MTRL method to consider the Lipschitz constants of the loss functions when computing the sensitivities in the 4-th step of the algorithm, which were omitted in the Algorithm 1 presented in the cited paper. For all $i \in [m]$, the Lipschitz constant $L_i$ of the loss function $L_i$ is estimated as $L_i = \max_{x \in [n]} |L_i'(x, w_i, y_i)|$, which is smaller than the true value. Thus, intuitively, we add less noise in their algorithm than should be added.

In the case of binary classification, we let DP-MTRL still minimize the least-square loss, because in each of its outer iterations (which alternate compute the parameter matrix and its covariance matrix), DP-MTRL requires a closed-form solution to guarantee the theoretical privacy results. However, for the logistic loss, iterative optimization is required in each outer iteration; consequently, the requirement of a closed-form solution cannot be satisfied. Therefore, DP-MTRL provides no privacy guarantee for the logistic loss. Moreover, it is not trivial to modify the DP-MTRL algorithm for loss functions that require iterative optimization in each outer iteration because additional leakage will occur in each inner iteration.

The differentially private aggregation (DP-AGGR) method proposed by Pathak et al. [47], which outputs an averaged model as the final solution, is also considered for comparison.
Differentially private STL methods are not considered because 1) empirically, they are always outperformed by non-private STL methods [15, 56], and 2) our MP-MTL method always outperforms STL methods, as will be presented later.

### 4.2 Experimental Setting

For the non-private methods, the regularization parameters and the numbers of iterations were optimized via 5-fold cross-validation on the training data, and acceleration was used without considering the strong convexity of the loss function \( f \). For the private methods, the regularization parameters, the number of iterations, the optimization strategy (whether to use acceleration and whether to consider strong convexity via adding \( \ell_2 \) norm penalties), and the budget allocation hyper-parameters (\( \alpha \) and \( Q \)) under each privacy loss \( \epsilon \) were optimized via 5-fold cross-validation on the training data. In the case where strong convexity was considered, \( \frac{e}{2} \| w_i \|_2^2 \) was added to each \( C_i \), with \( \mu = 1e^{-3} \).

For all the experiments, the \( \delta \) values in the MP-MTL algorithms were set to \( 1/m \log(m) \), where \( m \) is the number of tasks, as suggested by Abadi et al. [1], and the \( \delta \) values in the DP-MTL methods, i.e., DP-MTRL and DP-AGGR, were set in accordance with Proposition 3.

All experiments were replicated 100 times under each model setting.

### 4.3 Evaluation Metrics

We adopt evaluation metrics commonly-encountered in MTL approaches. For least-square regression, we use the nMSE [17, 26], which is defined as the mean squared error (MSE) divided by the variance of the target vector as the evaluation criterion. For binary classification, we use the average AUC [18], which is defined as the mean value of the area under the ROC curve for each task.

### 4.4 Simulation

We created a synthetic dataset as follows. The number of tasks was \( m = 320 \), the number of training samples for each task was \( n_i = 30 \), and the feature dimensionality of the training samples was \( d = 30 \). The entries of the training data \( \mathbf{X}_i \in \mathbb{R}^{n_i \times d} \) (for the \( i \)-th task) were randomly generated from the normal distribution \( \mathcal{N}(0, 1) \) before being normalized such that the \( \ell_2 \) norm of each sample was one.

To obtain a low-rank pattern, a covariance matrix \( \mathbf{\Sigma} \in \mathbb{R}^{m \times m} \) was firstly generated, as shown in Fig. 3 (a). Then the model parameter matrix \( \mathbf{W} \in \mathbb{R}^{d \times m} \) (see Fig. 3 (d)) was generated from a Matrix Variate Normal (MVN) distribution [28], i.e., \( \mathbf{W} \sim \text{MVN}(0, \mathbf{I}, \mathbf{\Sigma}) \).

To obtain a group-sparse pattern, the model parameter matrix \( \mathbf{W} \in \mathbb{R}^{d \times m} \) was generated such that the first 4 rows were non-zero. The values of the non-zero entries were generated from a uniform distribution in the range \([-50, -1] \cup [1, 50] \). Without loss of generality, we consider only the simulation of least-square regression. The results for logistic regression are similar. The response (target) vector for each task was \( \mathbf{y}_i = \mathbf{X}_i \mathbf{w}_i + \mathbf{e}_i \in \mathbb{R}^{n_i} \) (\( i \in [m] \)), where each entry in the vector \( \mathbf{e}_i \) was randomly generated from \( \mathcal{N}(0, 1) \).

The test set was generated in the same manner; the number of test samples was \( 9n_i \).

![Figure 3. Task relationships and output model matrices for the synthetic data experiments: (a), (b) and (c) are task relationship matrices, (d), (e) and (f) are the output model matrices. The results shown are the average of 100 runs with \( \epsilon = 0.1 \).](image)

![Figure 4. Evaluations for budget allocation strategies. In (a), we set \( \epsilon_t = \Theta(t^\alpha) \), for \( t \in [T] \); in (b), we set \( \epsilon_t = \Theta(Q_t^{-2}) \), for \( t \in [T] \). \( Q_0 = 1 - \sqrt{p} \approx 0.9684 \). The results shown are averages of 100 runs with \( \epsilon = 0.1 \). For the non-private MTL method, the nMSE was 0.0140.](image)

### 4.4.1 Privacy Budget Allocation

The budget allocation strategies in Section 3.5 were evaluated based on the synthetic data associated with the low-rank model matrix. The results shown in Fig. 4 are from 5-fold cross-validation on the training data. The prediction performances increase when acceleration is used, and achieve local optima at small positive values of the horizontal axes, which is consistent with our utility analyses. A local optima exists in the negative horizontal axis in Fig. 4 (b) when acceleration is used—perhaps because \( m \) is not large enough as assumed in Assumption 1.

### 4.4.2 Noise-To-Signal Ratio

Based on the setting in Section 4.4.1, noise-to-signal ratios under the best budget allocation strategy (using acceleration and considering basic convexity) are shown in Fig. 5. In contrast, for DP-MTRL, \( \log_{10}(\| \mathbf{E} \|_F / \| \mathbf{\Sigma}^{(t)} \|_F) = 0.2670 \pm 0.0075 \) with the best iteration number \( T = 1 \). The output model matrices of both our method and DP-MTRL are shown in Fig. 3 (e) and (f), respectively, along with their respective covariance matrices shown in Fig. 3 (b) and (c). These plots suggest that high level of noises added in our method had little influence on the output model matrix and the pattern in its covariance matrix, because our method adds noise only to the knowledge-sharing process and our method degrades to an STL method under high noise level.
We also evaluate the considered methods on the following two real datasets.

### School Data

The School dataset is a popular dataset for MTL [26] that consists of the exam scores of 15,362 students from 139 secondary schools. Each student is described by 27 attributes, including both school-specific and student-specific information, such as gender and ethnic group. The problem of predicting exam scores for the students can be formulated as an MTL problem: the number of tasks is $m = 139$, the data dimensionality is $d = 27$, and the number of data samples is $\sum_i n_i = 15,362$.

### LSOA II Data

These data are from the Second Longitudinal Study of Aging (LSOA II)\(^2\). LSOA II was a collaborative study conducted by the National Center for Health Statistics (NCHS) and the National Institute of Aging from 1994 to 2000. A national representative sample of 9,447 subjects of 70 years of age and older were selected and interviewed. Three separate interviews were conducted with each subject, one each during the periods of 1994-1996, 1997-1998, and 1999-2000, and referred to as WAVE 1, WAVE 2, and WAVE 3, respectively. Each wave of interviews included multiple modules covering a wide range of assessments. We used data from WAVE 2 and WAVE 3, which include a total of 4,299 sample subjects and 44 targets (each subject corresponded to 44 targets), and 188 features were extracted from the WAVE 2 interviews. The targets include $m = 41$ binary outcomes used in this study. These outcomes fall into several categories: 7 measures of fundamental daily activity, 13 of extended daily activity, 5 of social involvement, 8 of medical condition, 4 of cognitive ability, and 4 of sensation condition.

The features include records of demographics, family structure, daily personal care, medical history, social activity, health opinions, behavior, nutrition, health insurance and income and assets, the majority of which are binary measures.

Both the targets and the features have missing values due to non-response and questionnaire filtering. The average missing value rates of the targets and features are 13.7% and 20.2%, respectively. To address the missing values among the features, we adopted the following preprocessing procedure. For the continuous features, missing values were imputed with the sample mean. For binary features, it is better to treat the missing values as a third category, as the absence of a value may also carry important information. Therefore, two dummy variables were created for each binary feature with missing values (no third variable is necessary in such a case). This resulted in a total of $d = 295$.

\(^{1}\) http://www.cs.ucl.ac.uk/staff/a.argyriou/code/

\(^{2}\) https://www.cdc.gov/nchs/lsoa/lsoa2.htm.
features. To address the missing values among the targets, we include the samples associated with observed targets for each task, resulting in $\max_{i \in [m]} R_i = 3,473$.

For both the real-world datasets, We randomly selected 30% of the samples (from each task) to form the training set and used the remaining samples as the test set. For all tasks, each data point was normalized to have unit length.

4.5.2 Privacy-Accuracy Tradeoff

From Fig. 8, we can observe results similar to those seen in Fig. 6. In addition, our MP-MTL algorithms outperform DP-MTRL and DP-AGGR, especially when $\epsilon$ is small. This is because DP-MTRL and DP-AGGR introduce excessive noise to protect the model and all data instances of every individual task simultaneously. DP-AGGR underperforms compared with the STL method because its model averaging approach assumes that the tasks are homogeneous. Note that we have tuned the regularization parameters for both DP-MTRL and DP-AGGR for acceptable accuracies. In Fig. 8 (b), the aAUC values of our Algorithms (2 and 3) increase slowly because the feature dimension is large and the number of tasks is insufficient, which is consistent with our utility analyses.

Since the MTL behavior may change when the training-data percentage (the size of the training data divided by the size of the entire dataset) changes, we evaluated the methods on both real-world datasets at different training-data percentages and achieved similar results; see the supplementary material for more details.

5 Conclusions

In this paper, we discussed the potential security risks of multi-task learning approaches and presented a rigorous mathematical formulation of the model-protected multi-task learning (MP-MTL) problem. We proposed an algorithmic framework for implementing MP-MTL along with two concrete instantiations of this framework, which learn the low-rank and group-sparse patterns in the model matrix. We demonstrated that our algorithms are guaranteed not to underperform compared with single-task learning methods under high noise level. Privacy guarantees were also provided. Utility analyses suggested that both the strong-convexity condition and the acceleration strategy improve the utility bounds. A utility analysis for budget allocation yielded a recommendation for privacy budgets that are non-decreasing over the iterations. Experiments demonstrated that our algorithms significantly outperform existing privacy-preserving MTL methods on the proposed model-protection problem. Some interesting future directions of research include developing concrete MP-MTL algorithms for other MTL approaches and other optimization schemes.

ACKNOWLEDGMENTS

This research was supported in part by the National Science Foundation (NSF) under grants IIS-1565596, III-1615597 and IIS-1650723; the Office of Naval Research (ONR) under grant number N00014-14-1-0631; and the National Institutes of Health (NIH) under grants R00LM011392 and R21LM012060. In addition, we would like to thank Yuxiang Wang from the School of Computer Science at Carnegie Mellon University for his valuable comments on how to improve the properties of iterative MP-MTL algorithms.

REFERENCES

[1] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, L. Mironov, K. Talwar, and L. Zhang. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 308–318. ACM, 2016.

[2] M. B. Almeida and A. F. Martins. Fast and robust compressive summarization with dual decomposition and multi-task learning. In ACL (1), pages 196–206, 2013.

[3] Y. Amit, M. Fink, N. Srebro, and S. Ullman. Uncovering shared structures in multiclass classification. In Proceedings of the 24th ICML, pages 17–24, 2007.

[4] R. K. Ando and T. Zhang. A framework for learning predictive structures from multiple tasks and unlabeled data. The Journal of Machine Learning Research, 6:1817–1853, 2005.

[5] A. Argyriou, T. Evgeniou, and M. Pontil. Multi-task feature learning. Advances in neural information processing systems, 19:41, 2007.

[6] A. Argyriou, M. Pontil, Y. Ying, and C. A. Micchelli. A spectral regularization framework for multi-task structure learning. In Advances in Neural Information Processing Systems, pages 25–32, 2007.

[7] A. Argyriou, T. Evgeniou, and M. Pontil. Convex multi-task feature learning. Machine Learning, 73(3):243–272, 2008.

[8] B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy, Accuracy, and Consistency Too: A Holistic Solution to Contingency Table Release. In Proceedings of the 26th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS), pages 273–282, 2007.

[9] I. M. Baytas, M. Yan, A. K. Jain, and J. Zhou. Asynchronous multi-task learning. In Data Mining (ICDM), 2016 IEEE 16th International Conference on, pages 11–20. IEEE, 2016.

[10] J. Blocki, A. Blum, A. Datta, and O. Sheffet. The johnson-lindenstrauss transform itself preserves differential privacy. In Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on, pages 410–419. IEEE, 2012.

[11] E. V. Bonilla, K. M. A. Chai, and C. K. Williams. Multi-task gaussian process prediction. In NIPS, volume 20, pages 153–160, 2007.
[12] R. Caruana. Multitask learning. *Machine learning*, 28(1): 41–75, 1997.

[13] K. Chaudhuri and C. Monteleoni. Privacy-preserving logistic regression. In *Advances in Neural Information Processing Systems*, pages 289–296, 2008.

[14] K. Chaudhuri, C. Monteleoni, and A. Sarwate. Differentially Private Empirical Risk Minimization. *Journal of Machine Learning Research (JMLR)*, 12:1069–1109, jul 2011.

[15] K. Chaudhuri, C. Monteleoni, and A. D. Sarwate. Differentially private empirical risk minimization. *The Journal of Machine Learning Research*, 12:1069–1109, 2011.

[16] J. Chen, L. Tang, J. Liu, and J. Ye. A convex formulation for learning shared structures from multiple tasks. In *Proceedings of the 26th ICML*, pages 137–144, 2009.

[17] J. Chen, J. Zhou, and J. Ye. Integrating low-rank and group-sparse structures for robust multi-task learning. In *Proceedings of the 17th ACM SIGKDD Conference*, pages 42–50. ACM, 2011.

[18] J. Chen, J. Liu, and J. Ye. Learning incoherent sparse and low-rank patterns from multiple tasks. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 5(4):22, 2012.

[19] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference*, pages 265–284. Springer, 2006.

[20] C. Dwork, A. Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

[21] C. Dwork, K. Talwar, A. Thakurta, and L. Zhang. Analyze gauss: optimal bounds for privacy-preserving principal component analysis. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 11–20. ACM, 2014.

[22] A. Evgeniou and M. Pontil. Multi-task feature learning. In *Advances in neural information processing systems*, volume 19, page 41. The MIT Press, 2007.

[23] H. Fei and J. Huan. Structured feature selection and task relationship inference for multi-task learning. *Knowledge and information systems*, 35(2):345–364, 2014.

[24] S. R. Ganta, S. P. Kasiviswanathan, and A. Smith. Composition attacks and auxiliary information in data privacy. In *Proceedings of the 14th ACM SIGKDD Conference*, pages 265–273. ACM, 2008.

[25] O. Goldreich. Secure multi-party computation. *Manuscript. Preliminary version*, pages 86–97, 1998.

[26] P. Gong, J. Ye, and C. Zhang. Robust multi-task feature learning. In *Proceedings of the 18th ACM SIGKDD Conference*, pages 895–903. ACM, 2012.

[27] Q. Gu and J. Zhou. Learning the shared subspace for multi-task clustering and transductive transfer classification. In *Proceedings of ICDM*, pages 159–168. IEEE, 2009.

[28] A. K. Gupta and D. K. Nagar. *Matrix variate distributions*, volume 104. CRC Press, 1999.

[29] S. K. Gupta, S. Rana, and S. Venkatesh. Differentially private multi-task learning. In *Pacific-Asia Workshop on Intelligence and Security Informatics*, pages 101–113. Springer, 2015.

[30] M. Jaggi. Revisiting frank-wolfe: Projection-free sparse convex optimization. In *ICML* (1), pages 427–435, 2013.

[31] A. Jalali, S. Sanghavi, C. Ruan, and P. K. Ravikumar. A dirty model for multi-task learning. In *Advances in Neural Information Processing Systems*, pages 964–972, 2010.

[32] S. Ji and J. Ye. An accelerated gradient method for trace norm minimization. In *Proceedings of the 26th annual international conference on machine learning*, pages 457–464. ACM, 2009.

[33] Z. Ji, X. Jiang, H. Li, L. Xiong, and L. Ohno-Machado. Select and Label (S & L): A Task-Driven Privacy-Preserving Data Synthesization Framework. In *Translational Bioinformatics Conference (TBC)*, Qingdao, China, 2014.

[34] W. Jiang, C. Xie, and Z. Zhang. Wishart mechanism for differentially private principal components analysis. In *Thirtythird AAAI Conference on Artificial Intelligence*, 2016.

[35] P. Kairouz, S. Oh, and P. Viswanath. The composition theorem for differential privacy. *IEEE Transactions on Information Theory*, 2017.

[36] A. Kurakin, I. Goodfellow, and S. Bengio. Adversarial examples in the physical world. *arXiv preprint arXiv:1607.02533*, 2016.

[37] H. Li, L. Xiong, and X. Jiang. Differentially Private Synthesis of Multi-Dimensional Data using Copula Functions. In *17th International Conference on Extending Database Technology (EDBT) 2014*, Athens, Greece, 2014.

[38] J. Li, Y. Tian, T. Huang, and W. Gao. Probabilistic multi-task learning for visual saliency estimation in video. *International Journal of Computer Vision*, 90(2):150–165, 2010.

[39] J. Liu, S. Ji, and J. Ye. Multi-task feature learning via efficient l 1,2-norm minimization. In *Proceedings of the twenty-fifth conference on uncertainty in artificial intelligence*, pages 339–348. AUAI Press, 2009.

[40] G. Mathew and Z. Obradovic. Distributed privacy preserving decision support system for predicting hospitalization risk in hospitals with insufficient data. In *Machine Learning and Applications (ICMLA), 2012 11th International Conference on*, volume 2, pages 178–183. IEEE, 2012.

[41] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard. Deepfool: a simple and accurate method to fool deep neural networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 2574–2582, 2016.

[42] K. R. Mopuri, U. Garg, and R. V. Babu. Fast feature fool: A data independent approach to universal adversarial perturbations. *arXiv preprint arXiv:1707.05572*, 2017.

[43] K. Ng, J. Sun, J. Hu, and F. Wang. Personalized predictive modeling and risk factor identification using patient similarity. *AMIA Summits on Translational Science Proceedings*, 2015:132, 2015.

[44] F. Nie, H. Huang, X. Cai, and C. H. Ding. Efficient and robust feature selection via joint 2, 1-norms minimization. In *Advances in neural information processing systems*, pages 1813–1821, 2010.

[45] N. Papernot, P. McDaniel, and I. Goodfellow. Transferability in machine learning: from phenomea to black-box attacks using adversarial samples. *arXiv preprint arXiv:1605.07277*, 2016.

[46] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami. Practical black-box attacks against deep learning systems using adversarial examples. *arXiv preprint arXiv:1602.02697*, 2016.

[47] M. Pathak, S. Rane, and B. Raj. Multiparty differential privacy via aggregation of locally trained classifiers. In *Advances in Neural Information Processing Systems*, pages 1876–1884, 2010.

[48] T. K. Pong, P. Tseng, S. Ji, and J. Ye. Trace norm regularization: reformulations, algorithms, and multi-task learning. *SIAM Journal on Optimization*, 20(6):3465–3489, 2010.

[49] M. Schmidt, N. L. Roux, and F. R. Bach. Convergence rates of inexact proximal-gradient methods for convex optimization. *SIAM Journal on Optimization*, 20(6):3465–3489, 2010.

[50] M. Schmidt, N. L. Roux, and F. R. Bach. Convergence rates of inexact proximal-gradient methods for convex optimization. *SIAM Journal on Optimization*, 20(6):3465–3489, 2010.

[51] M. Schmidt, N. L. Roux, and F. R. Bach. Convergence rates of inexact proximal-gradient methods for convex optimization. *SIAM Journal on Optimization*, 20(6):3465–3489, 2010.

[52] M. Schmidt, N. L. Roux, and F. R. Bach. Convergence rates of inexact proximal-gradient methods for convex optimization. *SIAM Journal on Optimization*, 20(6):3465–3489, 2010.

[53] R. Shokri and V. Shmatikov. Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, pages 1310–1321. ACM, 2015.

[54] S. Song, K. Chaudhuri, and A. D. Sarwate. Stochastic gradient descent with differentially private updates. In *2013 IEEE Global Conference on Signal and Information Processing*, pages 245–248. IEEE, dec 2013. ISBN 978-1-4799-0248-4. doi: 10.1109/GlobalSIP.2013.6738661.

[55] S. Song, K. Chaudhuri, and A. D. Sarwate. Stochastic gradient descent with differentially private updates. In *2013 IEEE Global Conference on Signal and Information Processing*, pages 245–248. IEEE, dec 2013. ISBN 978-1-4799-0248-4. doi: 10.1109/GlobalSIP.2013.6738661.
1145–1154. ACM, 2015.

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

[54] B. A. Turlach, W. N. Venables, and S. J. Wright. Simultaneous variable selection. Technometrics, 47(3):349–363, 2005.

[55] X. Wang, F. Wang, J. Hu, and R. Sorrentino. Exploring joint disease risk prediction. In AMIA Annual Symposium Proceedings, volume 2014, page 1180. American Medical Informatics Association, 2014.

[56] Y.-X. Wang, S. Fienberg, and A. Smola. Privacy for Free: Posterior Sampling and Stochastic Gradient Monte Carlo. In Proceedings of the 32nd International Conference on Machine Learning (ICML-15), pages 2493–2502, 2015.

[57] S. J. Wright, R. D. Nowak, and M. A. Figueiredo. Sparse reconstruction by separable approximation. IEEE Transactions on Signal Processing, 57(7):2479–2493, 2009.

[58] M. Xu and J. D. Lafferty. Conditional sparse coding and grouped multivariate regression. In Proceedings of the 29th ICML, pages 1479–1486, 2012.

[59] V. Zantedeschi, M.-I. Nicolae, and A. Rawat. Efficient defenses against adversarial attacks. arXiv preprint arXiv:1707.06728, 2017.

[60] J. Zhang, Z. Zhang, X. Xiao, Y. Yang, and M. Winslett. Functional mechanism. Proceedings of the VLDB Endowment, 5(11):1364–1375, jul 2012. ISSN 21508097. doi: 10.14778/2350229.2350253.

[61] P. Zhang, F. Wang, J. Hu, and R. Sorrentino. Towards personalized medicine: leveraging patient similarity and drug similarity analytics. AMIA Summits on Translational Science Proceedings, 2014:132, 2014.

[62] T. Zhang, B. Ghanem, S. Liu, and N. Ahuja. Robust visual tracking via multi-task sparse learning. In IEEE CVPR Conference, pages 2042–2049. IEEE, 2012.

[63] Y. Zhang and D.-Y. Yeung. A convex formulation for learning task relationships in multi-task learning. In Proceedings of the Twenty-Sixth Conference on Uncertainty in Artificial Intelligence, pages 733–742. AUAI Press, 2010.

[64] J. Zhou, J. Chen, and J. Ye. Clustered multi-task learning via alternating structure optimization. In Advances in neural information processing systems, pages 702–710, 2011.

Jian Liang received his B.S. degree in automation from the Huazhong University of Science and Technology, Wuhan, China, in 2012. He is currently working toward his Ph.D. degree in the Department of Automation at Tsinghua University, Beijing. His research interests lie in the areas of multi-task learning and time-series data mining. He won the Best Short Paper Award at the 2016 IEEE International Conference on Healthcare Informatics (ICHI).

Ziqi Liu is currently a Ph.D. student at Xian Jiaotong University under advisor Professor Qinghua Zheng. His research interests lie in scalable machine learning and nonparametric modeling. Major awards that he has received include the WSDM16 Best Research Paper Award.

Jiayu Zhou is currently an Assistant Professor in the Department of Computer Science and Engineering at Michigan State University. He received his Ph.D. degree in computer science from Arizona State University in 2014. He has broad research interests in the fields of large-scale machine learning and data mining as well as biomedical informatics. He has served as a technical program committee member for premier conferences such as NIPS, ICML, and SIGKDD. His papers have received the Best Student Paper Award at the 2014 IEEE International Conference on Data Mining (ICDM), the Best Student Paper Award at the 2016 International Symposium on Biomedical Imaging (ISBI) and the Best Paper Award at IEEE Big Data 2016.

Xiaoqian Jiang is an assistant professor in the Department of Biomedical Informatics at the University of California, San Diego. He received his Ph.D. in computer science from Carnegie Mellon University. He is an associate editor of BMC Medical Informatics and Decision Making and serves as a member of the editorial board of the Journal of the American Medical Informatics Association. He works primarily in the fields of health data privacy and predictive models in biomedicine. Dr. Jiang was a recipient of the NIH K99/R00 award, and he won the Distinguished Paper Award from the American Medical Informatics Association Clinical Research Informatics (CRI) Summit in 2012 and 2013.

Changshui Zhang received his B.S. degree from Peking University, Beijing, China, in 1986 and his Ph.D. degree from Tsinghua University, Beijing, China, in 1992. He is currently a Professor in the Department of Automation at Tsinghua University. He is an member of the editorial board of Pattern Recognition and an IEEE Fellow. His research interests include artificial intelligence, image processing, pattern recognition, machine learning and evolutionary computation.

Fei Wang is an Assistant Professor in the Division of Health Informatics of the Department of Healthcare Policy and Research at Cornell University. His major research interests lie in data analytics and its applications in health informatics. His papers have received over 3,700 citations, with an H-index of 33. He won the Best Student Paper Award at ICDM 2015 and received a Best Research Paper nomination at ICDM 2010 and the Marco Romani Best Paper nomination at AMIA TBI 2014, and his papers were selected as Best Paper finalists at SDM 2011 and 2015. Dr. Wang is an action editor of the journal Data Mining and Knowledge Discovery, an associate editor of the Journal of Health Informatics Research and Smart Health, and a member of the editorial boards of Pattern Recognition and the International Journal of Big Data and Analytics in Healthcare. Dr. Wang is also the vice chair of the KDD working group at AMIA.
Supplemental Materials: Model-Protected Multi-Task Learning

APPENDIX A

Wishart Distribution

Definition 8 (Gupta and Nagar [28]). A $d \times d$ random symmetric positive definite matrix $E$ is said to have a Wishart distribution $E \sim W_d(\nu, V)$ if its probability density function is

$$p(E) = \frac{\left|E\right|^{(\nu-d-1)/2} \exp(-\text{tr}(V^{-1}E))/2}{\Gamma_d(\nu/2)} 2^{\nu/2} |V|^{1/2},$$

where $\nu > d - 1$ and $V$ is a $d \times d$ positive definite matrix.

APPENDIX B

Model-Decomposed MP-MTL Methods

In this section, we consider the extension of our MP-MTL framework for MTL methods using the decomposed parameter/model matrix. Specifically, we focus on the following problem, where the trace norm is used for knowledge sharing across tasks and the $\|\cdot\|_1$ norm (sum of the $\ell_1$ norm for vectors) is used for entry-wise outlier detection, as described in Algorithm 4.

$$\begin{align*}
\min_W & \sum_{i=1}^{m} L_i(X_i, w_i, y_i) + \lambda_1 \|P\|_1 + \lambda_2 \|Q\|_1 \\
\text{s.t.} & \quad W = P + Q,
\end{align*}$$

(24)

where $P, Q \in \mathbb{R}^{d \times m}$.

We note that in Algorithm 4, the role of $P$ is the same as the role of $W$ in Algorithm 2, and the additional procedures introduced to update $Q$ are still STL algorithms. As such, we have the result in Corollary 2.

Corollary 2. Algorithm 4 is an $(\epsilon, \delta)$-iterative MP-MTL algorithm.

Remark 3. Based on Algorithm 4, this will result in a similar procedure and identical theoretical results with respect to privacy by replacing the trace norm with the $\ell_2,1$ norm to force group sparsity in $P$ or by replacing the $\|\cdot\|_1$ norm with the $\ell_1,2$ norm (sum of the $\ell_2$ norm of column vectors) or $\|\cdot\|_F^2$ (square of the Frobenius norm).

APPENDIX C

MP-MTL Framework with Secure Multi-Party Computation

Pathak et al. [47] considered the demand for secure multi-party computation (SMC): protecting data instances from leaking to the curator and leaking between tasks during joint learning. However, by Proposition 3, the method of Pathak et al. [47] may introduce excess noise to protect both the data instances and the models simultaneously. To avoid unnecessary noise, we consider a divide-and-conquer strategy to ensure privacy for a single data instance and the model separately. Specifically, in each iteration of the iterative MP-MTL algorithms, we perform private sharing after introducing the perturbation to the parameter matrix to protect a single data instance, as described in Algorithm 5, where a noise vector is added in Step 5 to the model vector based on sensitivity of replacing a single data instance.

The results in Proposition 4 show that we can simultaneously protect a single data instance and the model using such a divide-and-conquer strategy. Because it is not necessary to protect all the data instances in each task using data-protected algorithms, the perturbation for data-instance protection can be reduced.

Proposition 4. Use Lemma 4 and Theorem 1. Algorithm 5 is an $(\epsilon_{mp}, \delta_{mp})$-iterative MP-MTL algorithm and an $(\epsilon_{dp}, \delta_{dp})$-iterative DP-MTL algorithm.

Algorithm 4 Model-Protected Low-Rank and SParse (MP-LR-SP) Estimator

Input: Datasets $(X_i, y_i) = \{(X_i, y_i)\ldots\{X_m, y_m\})$, where $\forall i \in [m]$, $X_i \in \mathbb{R}^{n_t \times d}$ and $y_i \in \mathbb{R}^{n_t \times 1}$. Privacy loss $\epsilon, \delta \geq 0$. Number of iterations $T$. Step size $\eta$. Regularization parameter $\lambda_1, \lambda_2 > 0$. Norm clipping parameter $K > 0$.

Output: $\hat{W}^{(1:T)}$.

1. For $t = 1, \ldots, T$, set $\epsilon_t$ such that $t \leq \epsilon$, where $\epsilon$ is defined in (7).
2. Let $P^{(0)} = Q^{(0)} = \tilde{Q}^{(0)} = W^{(0)}$.
3. for $t = 1 : T$ do
4. Norm clipping: $\tilde{P}^{(t-1)} = P^{(t-1)}/\max(1, \|P^{(t-1)}\|_2)$ for all $i \in [m]$. Let $P^{(t)} = \tilde{P}^{(t)}$.
5. Compute sensitivity: $s^{(t-1)} = 2$ for all $i \in [m]$.
6. $\Sigma^{(t)} = \tilde{\Sigma}^{(t-)} + E$, where $E \sim W_d(d+1, \text{max}(s^{(t-1)}, \eta \lambda^{(t-1)}))$ is a sample of the Wishart distribution.
7. Perform SVD decomposition: $U \Sigma^{(t)} U^T = \sigma^{(t)}$.
8. Let $S^{\sigma \lambda_1,i} = \text{a diagonal matrix and let } S^{\sigma \lambda_1}\{i, i\} = \max(0, 1 - \eta \lambda_1/\sqrt{X_{ii}})$ for $i = 1, \ldots, m$.
9. for $i \in [m], \text{let } \hat{P}^{(t)} = \tilde{U} S^{\sigma \lambda_1,i} \tilde{U}^T$ for all $i \in [m]$.
10. Let $Q^{(t)} = \hat{Q}^{(t)}$.
11. Let $q^{(t)} = \text{sign}(q^{(t-}) - \eta \lambda_2)$ for all $i \in [m], \text{where } \circ \text{ denotes the entry-wise product}.
12. Let $\tilde{W}^{(t)} = \hat{P}^{(t)} + Q^{(t)}$.
13. Let $z^{(t)} = \beta^{(t)}(\tilde{P}^{(t)}) - \hat{P}^{(t-1)}$ for all $i \in [m]$.
14. Let $z^{(t)} = q^{(t)} + \hat{Q}^{(t)} - \hat{Q}^{(t-1)}$ for all $i \in [m]$.
15. $\beta^{(t)} = \eta\lambda_1 \frac{\partial L_i(X_i, z^{(t)}) + \partial L_i(X_i, z^{(t)})}{\partial q^{(t)}}$ for all $i \in [m]$.
16. $\hat{q}^{(t)} = z^{(t)} - \eta\lambda_2 \frac{\partial L_i(X_i, z^{(t)}) + \partial L_i(X_i, z^{(t)})}{\partial q^{(t)}}$ for all $i \in [m]$.
17. end for

APPENDIX D

Results of Utility Analyses Under Other Two Settings

Here we consider the other two settings of $\{\epsilon_t\}$.

D.1 Setting No.1

In this setting, we have

$$\epsilon = \sum_{t=1}^{T} \epsilon_t.$$ 

Theorem 7 (Low rank - Convexity - Setting No.1). Consider Algorithm 2. For an index $k \leq q$ that satisfies the definition in Lemma 2 for all $t \in [T]$, $\eta = 1/L$, $\lambda = \Theta(K\sqrt{m})$, assume $\epsilon_t \leq 4K^2d(\log d)/q^2$ for $t \in [T]$.

No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then setting

$$T = \Theta\left(\frac{(a/2 - 1)^2 + 1 + 1}{kd \log d}\phi(a)\right)$$

for $E = f(1/d) \sum_{i=1}^{T} W^{(t)} - f(W_\ast)$, we have with high probability,

$$E = O(K^2L \left[\frac{kd \log d}{(a/2 - 1)^2 + 1 + 1}\right]^{\phi(a)}),$$

(25)

where

$$\phi(a) = \begin{cases} 1/(\alpha + 1), & \alpha > 2; \\ 1/3, & -1 < \alpha < 2; \\ 1/(2 - \alpha), & \alpha < -1. \end{cases}$$

(26)
Algorithm 5 MP-MTL framework with Secure Multi-party Computation (SMC)

Input: Datasets $(X^m, y^m) = \{(X_i, y_1), \ldots, (X_i, y_m)\}$, where $V i \in [m]$, $X_i \in \mathbb{R}^{n_{i,d}}$, and $y_i \in \mathbb{R}^{n_{i,1}}$. Privacy loss for model protection $\epsilon_{\text{mp}}, \delta_{\text{mp}} \geq 0$. Privacy loss for single data instance protection $\epsilon_{\text{dp}} \geq 0$. Number of iterations $T$. Shared information matrices $M(0)$. Initial models of tasks $W(0)$.

Output: $W^{(t+1)}$.

1. For $t = 1, \ldots, T$, set $m_{\text{cp}}$ such that $\epsilon_{\text{mp}} \leq m_{\text{cp}}$, where $m_{\text{cp}}$ is defined in (7), taking $\epsilon_{\text{mp}}, \epsilon_{\text{dp}} \leq m_{\text{cp}}$, $\delta_{\text{mp}} \geq 0$.
2. For $t = 1, \ldots, T$, set $\epsilon_{\text{dp},t}$ such that $\epsilon_{\text{dp}} \leq \epsilon_{\text{dp},t}, \epsilon_{\text{dp}} \leq \delta_{\text{dp}}$.
3. For $t = 1 : T$

4. Compute the sensitivity vector $\tilde{s}^{(t-1)} = [s_1^{(t-1)}, \ldots, s_m^{(t-1)}]^T$, which is defined for all $i \in [m],$

   $\tilde{s}_i^{(t-1)} = \max_{(w_i^{(t-1)})} \|w_i^{(t-1)} - (w_i^{(t-1)})\|_2$

where $(w_i^{(t-1)})$ is assumed to be generated using $D_i$, which differ with $D_i$ in a single data instance.

5. $w_i^{(t-1)} = w_i^{(t-1)} + b_i$, where $b_i$ is a sample with the density function of

   $p(b_i) \propto \exp\left(-\frac{\tilde{s}_i^{(t-1)}}{\epsilon_{\text{dp},t}} \|b_i\|_2\right)$

for all $i \in [m]$.

6. Compute the sensitivity vector $s_i^{(t-1)} = [s_1^{(t-1)}, \ldots, s_m^{(t-1)}]^T$, which is defined for all $i \in [m],$

   $s_i^{(t-1)} = \max_{(w_i^{(t)})} \|w_i^{(t)}\|_2$.

where $(w_i^{(t)})$ is assumed to be generated arbitrarily.

7. $\Sigma^{(t)} = \tilde{W}^{(t-1)}(\tilde{W}^{(t-1)})^T$ (or $\Sigma^{(t)} = (\tilde{W}^{(t-1)})^T\tilde{W}^{(t-1)}$).

8. $\Sigma^{(t)} = \Sigma^{(t)} + E$, where $E$ is a random variable $\sim W_{d+1, \sqrt{\epsilon_{\text{dp},t}}} \log Q$.

9. Perform an arbitrary mapping $f : \Sigma^{(t)} \rightarrow M(0)$.

10. $w_i^{(t)} = \mathbb{A}(\Sigma^{(t)}, M(0), w_{i-1}^{(t-1)}, X_i, y_i)$ for all $i \in [m]$, where $w_i^{(t-1)}$ are the initialization.

11. Set the input for the next iteration: $W^{(t)} = \tilde{W}^{(t)}$.

12. end for

Use acceleration: If we set $\beta_t = (t-1)/(t+2)$ for $t \in [m]$, then setting

   $T = \Theta\left(\frac{\epsilon_{\text{dp},t}}{k d \log d}\right)^{\phi(\alpha)/2}$

for $\mathcal{E} = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

   $\mathcal{E} = O\left(K^2L \left[\frac{k d \log d}{(\alpha/2)^2 |\alpha| + 1} \right]^{\phi(\alpha)}\right), \quad (27)$

where

   $\phi(\alpha) = \begin{cases} 2/(\alpha + 1), & \alpha > 4; \\ 2/5, & -1 < \alpha < 4; \\ 2/(4 -\alpha), & \alpha < -1. \end{cases}$

(28)

Theorem 8 (Group sparse - Convexity - Setting No.1). Consider Algorithm 3. For an index $k \leq d$ that suffices the definition in Lemma 3 for all $t \in [T], \eta = 1/L, \lambda = \Theta(LKd\sqrt{m})$, assume $\epsilon_t \leq k^2 \log(d)/4Kd(d-k)m$ for $t \in [T]$. No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then setting

   $T = \Theta\left(\frac{(\alpha/2 - 2)^2 |\alpha| + 1}{k d \log d}\right)^{\phi(\alpha)}$

for $\mathcal{E} = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

   $\mathcal{E} = O\left(K^2L \left[\frac{k d \log d}{(\alpha/2 - 2)^2 |\alpha| + 1} \right]^{\phi(\alpha)}\right), \quad (29)$

where $\phi(\alpha)$ is defined in (26).

Use acceleration: If we set $\beta_t = (t-1)/(t+2)$ for $t \in [m]$, then setting

   $T = \Theta\left(\frac{(\alpha/2 - 2)^2 |\alpha| + 1}{k d \log d}\right)^{\phi(\alpha)/2}$

for $\mathcal{E} = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

   $\mathcal{E} = O\left(K^2L \left[\frac{k d \log d}{(\alpha/2 - 2)^2 |\alpha| + 1} \right]^{\phi(\alpha)}\right), \quad (30)$

where $\phi(\alpha)$ is defined in (28).

Now we further assume that $m_f(W)$ is $\mu$-strongly convex and has $L$-Lipschitz-continuous gradient, where $\mu < L$. We set $\epsilon_t = \Theta(Q^{-1})$ for $Q > 0$ and $t \in [T]$ for this case.

Theorem 9 (Low rank - Strong convexity - Setting No.1). Consider Algorithm 2. For an index $k \leq q$ that suffices the definition in Lemma 2 for all $t \in [T]$, $\eta = 1/L, \lambda = \Theta(LKd\sqrt{m})$, assume $\epsilon_t \leq 4Kk^d d \log d/q^2$ for all $t \in [T]$. No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then denoting $\mathcal{E}_0 = 1 - \mu/L$ and setting

   $T = \Theta\left(\frac{k d \log d}{(\alpha/2 - 2)^2 |\alpha| + 1} \right)^{\phi(\alpha)}$

for $\mathcal{E} = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

   $\mathcal{E} = O\left(K \left[\frac{k d \log d}{(\sqrt{Q/\alpha} - 1)^2 |\alpha| + 1} \right]^{\phi(\alpha)}\right), \quad (31)$

where $\phi(\alpha)$ is defined in (19).

Use acceleration: If we set $\beta_t = (1 - \sqrt{\mu/L})/(1 + \sqrt{\mu/L})$ for $t \in [m]$, then denoting $\mathcal{E}_0 = 1 - \mu/L$ and setting

   $T = \Theta\left(\frac{k d \log d}{(\sqrt{Q/\alpha} - 1)^2 |\alpha| + 1} \right)^{\phi(\alpha)}$

for $\mathcal{E} = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

   $\mathcal{E} = O\left(K \left[\frac{k d \log d}{(\sqrt{Q/\alpha} - 1)^2 |\alpha| + 1} \right]^{\phi(\alpha)}\right), \quad (32)$

where $\phi(\alpha)$ is defined in (19).

Theorem 10 (Group sparse - Strong convexity - Setting No.1). Consider Algorithm 3. For an index $k \leq d$ that suffices the definition in Lemma 3 for all $t \in [T], \eta = 1/L, \lambda = \Theta(LKd\sqrt{m})$, assume $\epsilon_t \leq k^2 \log(d)/4Kd(d-k)m$ for $t \in [T]$. No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then denoting $\mathcal{E}_0 = 1 - \mu/L$ and setting

   $T = \Theta\left(\frac{(\alpha/2 - 2)^2 |\alpha| + 1}{k d \log d}\right)^{\phi(\alpha)}$

for $\mathcal{E} = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

   $\mathcal{E} = O\left(K \left[\frac{k d \log d}{(\sqrt{Q/\alpha} - 1)^2 |\alpha| + 1} \right]^{\phi(\alpha)}\right), \quad (33)$

where $\phi(\alpha)$ is defined in (19).
Use acceleration: If we set $\beta_t = (1 - \sqrt{\mu/L}/(1 + \sqrt{\mu/L})$ for $t \in [m]$, then denoting $Q_0 = 1 - \sqrt{\mu/L}$ and setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,

$$E = O \left( K \left[ k \log d \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right]^{\log_{1/\psi(Q, Q_0)} Q_0'}, \right)$$

where $\psi(\cdot, \cdot)$ is defined in (19).

Then we optimize the utility bounds with respect to the respective budget allocation strategies.

Theorem 11 (Budget allocation - Setting No.1). Consider Algorithm 2 and Algorithm 3.

For convex $f$, use Theorem 7 and Theorem 8.

(1) No acceleration: Both the bounds in (25) and (29) achieve their respective minimums w.r.t. $\alpha$ at $\alpha = 0$. Meanwhile, $\phi(\alpha) = 1/3$.

(2) Accelerated: Both the bounds in (27) and (30) achieve their respective minimums w.r.t. $\alpha$ at $\alpha = 2/3$. Meanwhile, $\phi(\alpha) = 2/5$.

For strongly convex $f$, use Theorem 9 and Theorem 10.

(1) No acceleration: Both the bounds in (31) and (33) achieve their respective minimums w.r.t. $Q$ at $Q = Q_0^{2/3}$. Meanwhile, $\log_{1/\psi(Q, Q_0)} Q_0 = 1/2$.

(2) Accelerated: Both the bounds in (32) and (34) achieve their respective minimums w.r.t. $Q$ at $Q = (Q_0')^{2/3}$. Meanwhile, $\log_{1/\psi(Q, Q_0')} Q_0 = 1$.

D.2 Setting No.2

In this setting, we have

$$\epsilon = \sum_{t=1}^T \frac{\left(\epsilon_t^* - 1\epsilon_t^* \right)}{\left(\epsilon_t^* + 1\right)} + \sum_{t=1}^T 2\epsilon_t^2 \log \left(\frac{1}{\delta} \right).$$

Theorem 12 (Low rank - Convexity - Setting No.2). Consider Algorithm 2. For an index $k \leq q$ that satisfies the definition in Lemma 2 for all $t \in [T]$, $\eta = 1/L$, $\lambda = \Theta(LK\sqrt{\psi})$, assume $\epsilon_t \leq K^2d(\log d)/q^2$ for $t \in [T]$. No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,

$$E = O \left( K^2L \left[ k \log d \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right]^{\log_{1/\psi(Q, Q_0)} Q_0'}, \right)$$

where $\phi(\alpha) = \frac{2/(2\alpha + 1)}{2/5 \sqrt{2\alpha + 1}}$, $\alpha > 1/2$, $1/2 < \alpha < 2$, $1/2 - 1/2 = 2\alpha + 1$, $1/2 - 1/2 = 2\alpha + 1$.

Use acceleration: If we set $\beta_t = (t - 1)/(t + 2)$ for $t \in [m]$, then setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,

$$E = O \left( K^2L \left[ k \log d \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right]^{\log_{1/\psi(Q, Q_0)} Q_0'}, \right)$$

where $\psi(\cdot, \cdot)$ is defined in (19).

Theorem 13 (Group sparse - Convexity - Setting No.2). Consider Algorithm 3. For an index $k \leq d$ that satisfies the definition in Lemma 3 for all $t \in [T]$, $\eta = 1/L$, $\lambda = \Theta(LKd\sqrt{m})$, assume $\epsilon_t \leq K^2d(\log d)/4Kd(d - k)^2$ for $t \in [T]$.

No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,

$$E = O \left( K^2L \left[ k \log d \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right]^{\log_{1/\psi(Q, Q_0)} Q_0'}, \right)$$

where $\phi(\alpha) = \frac{4/(2\alpha + 1)}{4/9 \sqrt{2\alpha + 1}}$, $\alpha > 4$, $1/2 < \alpha < 4$, $2/(4 - \alpha)$, $\alpha > 1/2$.

Theorem 14 (Low rank - Strong convexity - Setting No.2). Consider Algorithm 2. For an index $k \leq q$ that satisfies the definition in Lemma 2 for all $t \in [T]$, $\eta = 1/L$, $\lambda = \Theta(LK\sqrt{\psi})$, assume $\epsilon_t \leq 4K^2d(\log d)/q^2$ for $t \in [T]$. No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then denoting $Q_0 = 1 - \mu/L$ and setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,

$$E = O \left( K \left[ k \log d \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right]^{\log_{1/\psi(Q, Q_0)} Q_0'}, \right)$$

where $\psi(\cdot, \cdot)$ is defined in (19).

Use acceleration: If we set $\beta_t = (1 - \sqrt{\mu/L})/(1 + \sqrt{\mu/L})$ for $t \in [m]$, then denoting $Q_0 = 1 - \mu/L$ and setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,

$$E = O \left( K \left[ k \log d \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right]^{\log_{1/\psi(Q, Q_0)} Q_0'}, \right)$$

where $\psi(\cdot, \cdot)$ is defined in (19).

Theorem 15 (Group sparse - Strong convexity - Setting No.2). Consider Algorithm 3. For an index $k \leq d$ that satisfies the definition in Lemma 3 for all $t \in [T]$, $\eta = 1/L$, $\lambda = \Theta(LKd\sqrt{m})$, assume $\epsilon_t \leq K^2d(\log d)/4Kd(d - k)^2m$ for $t \in [T]$. No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then setting

$$T = \Theta \left( \log_{1/\psi(Q, Q_0)} \left( \frac{\left(\sqrt{Q_0'/\sqrt{Q_0'}} - 1\right)^2 \left|1 - Q_0'\psi|\psi Q_0 \right|}{k \log d} \right) \right)$$

for $E = f(W^{(T)}) - f(W_\ast)$, we have with high probability,
No acceleration: If we set $\beta_t = 0$ for $t \in [m]$, then denoting $Q_0 = 1 - \mu/L$ and setting

$$T = \Theta \left( \log_{\psi}(Q_0 Q_0^*) \left[ \frac{(Q_0 / \sqrt{Q} - 1)^2 \sqrt{1 - Q^2} K m \epsilon}{k \log d \sqrt{\log(1/\delta) + 2 \epsilon}} \right] \right)$$

for $E = \frac{1}{\psi} \| \tilde{W}^{(T)} - W_* \|_F$, we have with high probability,

$$\mathcal{E} = O \left( K \left[ \frac{k \log d \sqrt{\log(1/\delta) + 2 \epsilon}}{(Q_0 / \sqrt{Q} - 1)^2 \sqrt{1 - Q^2} K m \epsilon} \right] \log_{\psi}(Q_0 Q_0^*) Q_0^* \right),$$

where $\psi(\cdot, \cdot)$ is defined in (19).

Use acceleration: If we set $\beta_t = (1 - \sqrt{\mu/L})/(1 + \sqrt{\mu/L})$ for $t \in [m]$, then denoting $Q_0 = 1 - \sqrt{\mu/L}$ and setting

$$T = \Theta \left( \log_{\psi}(Q_0 Q_0^*) \left[ \frac{(\sqrt{Q_0^*} / \sqrt{Q} - 1)^2 \sqrt{1 - Q^2} K m \epsilon}{k \log d \sqrt{\log(1/\delta) + 2 \epsilon}} \right] \right)$$

for $E = f(\tilde{W}^{(T)}) - f(W_*)$, we have with high probability,

$$\mathcal{E} = O \left( K \left[ \frac{k \log d \sqrt{\log(1/\delta) + 2 \epsilon}}{(\sqrt{Q_0^*} / \sqrt{Q} - 1)^2 \sqrt{1 - Q^2} K m \epsilon} \right] \log_{\psi}(Q_0 Q_0^*) Q_0^* \right),$$

where $\psi(\cdot, \cdot)$ is defined in (19).

Then we optimize the utility bounds with respect to the respective budget allocation strategies.

**Theorem 16** (Budget allocation - Setting No.2). Consider Algorithm 2 and Algorithm 3.

For convex $f$, use Theorem 12 and Theorem 13.

1. No acceleration: Both the bounds in (35) and (39) achieve their respective minimums w.r.t. $\alpha$ at $\alpha = 0$. Meanwhile, $\phi(\alpha) = 2/5$.

2. Accelerated: Both the bounds in (37) and (40) achieve their respective minimums w.r.t. $\alpha$ at $\alpha = 2/5$. Meanwhile, $\phi(\alpha) = 4/9$.

For strongly convex $f$, use Theorem 14 and Theorem 15.

1. No acceleration: Both the bounds in (41) and (43) achieve their respective minimums w.r.t. $Q$ at $Q = Q_0^*$. Meanwhile, $\log_{\psi}(Q_0 Q_0^*) Q_0^* = 1/2$.

2. Accelerated: Both the bounds in (42) and (44) achieve their respective minimums w.r.t. $Q$ at $Q = (Q_0^*)^{1/5}$. Meanwhile, $\log_{\psi}(Q_0 Q_0^*) Q_0^* = 1$.

**APPENDIX E**

**Detailed Privacy-Accuracy Tradeoff for Baseline Methods on Synthetic Datasets**

In Fig. 9, the detailed performances of both of DP-MTRL and DP-AGGR are shown. Note that we have tuned the regularization parameters for both DP-MTRL and DP-AGGR for acceptable accuracies. Our Algorithm 2 outperforms DP-MTRL and DP-AGGR. In Fig. 9 (a), DP-MTRL outperforms the STL method and our Algorithm 3 when $\epsilon$ is large, because it suits the true model matrix, in which the relatedness among tasks is modeled by a graph. However, the true model matrix is not group-sparse, hence our Algorithm 3 underperforms comparing with Algorithm 2 and DP-MTRL when $\epsilon$ is large. By contrast, in Fig. 9 (b), the true model matrix is group-sparse and is not suitable for DP-MTRL, hence DP-MTRL underperforms comparing with the STL method even when $\epsilon$ is large. Fig. 9 (c) is used to show that the accuracy of DP-AGGR grows with $\epsilon$ under the same setting as in Fig. 9 (b). As we discussed, DP-AGGR only performs model-averaging, which is not suitable for the true model matrices in both settings of Fig. 9 (a) and (b), hence the accuracies of DP-AGGR are much worse than those of the respective STL methods.

**APPENDIX F**

**Detailed Privacy-Accuracy Tradeoff for DP-AGGR on Real-World Datasets**

In Fig. 10, the detailed performances of DP-AGGR are shown. Because the dimension is large and the number of tasks is not sufficient, the accuracy of DP-AGGR barely grows with $\epsilon$; other private-preserving methods, such as DP-MTRL and our algorithms, grow slowly with $\epsilon$ as well.

**APPENDIX G**

**Varying Training-Data Percentage**

Since the MTL behavior may change when the training-data percentage (the size of the training data divided by the size of the entire dataset) changes, we evaluated the methods on both real-world datasets at different training-data percentages.
Here, we present the results mostly for our low-rank algorithm (denoted by MP-MTL-LR) because it always outperforms our group-sparse algorithm (MP-MTL-GS) in the above experiments. The results corresponding to School Data are shown in Fig. 11; the results corresponding to LSOA II Data are shown in Fig. 12. From those plots, we observe that on both real-world datasets, our MP-MTL method behaves similarly at different training-data percentages and outperforms DP-MTRL and DP-AGGR, especially when $\epsilon$ is small.

**APPENDIX H**

**LEMMA 4 (Post-Processing immunity. Proposition 2.1 in Dwork et al. [20]).** Let algorithm $A_1(B_1) : D \rightarrow$
\( \theta_1 \in C_1 \) be an \((\epsilon, \delta)\) - differential privacy algorithm, and let \( f : C_1 \rightarrow C_2 \) be an arbitrary mapping. Then, algorithm \( A_2(B_2) : D \rightarrow \theta_2 \in C_2 \) is still \((\epsilon, \delta)\) - differentially private, i.e., for any set \( S \subseteq C \)

\[ P(\theta_2 \in S | B_2 = D) \leq e^{k \epsilon} P(\theta_2 \in S | B_2 = D') + e^{k \epsilon} \delta. \]

- **Group privacy.** This property guarantees the graceful increment of the privacy budget when more output variables need differentially private protection.

**Lemma 5** (Group privacy. Lemma 2.2 in [?]). Let algorithm \( A(B) : D \rightarrow \theta \in C \) be an \((\epsilon, \delta)\) - differential privacy algorithm. Then, considering two neighboring datasets \( D \) and \( D' \) that differ in \( k \) entries, the algorithm satisfies for any set \( S \subseteq C \)

\[ P(\theta \in S | B = D) \leq e^{k \epsilon} P(\theta \in S | B = D') + e^{k \epsilon} \delta. \]

- **Combination.** This property guarantees the linear incrementing of the privacy budget when the dataset \( D \) is repeatedly used.

**Lemma 6** (Combination. Theorem 3.16 in Dwork et al. [20]). Let algorithm \( A_i : D_i \rightarrow \theta_i \in C_i \) be an \((\epsilon_i, \delta_i)\) - differential privacy algorithm for all \( i \in [k] \). Then, \( A_{\oplus}(D) : D \rightarrow (\theta_1, \theta_2, \ldots, \theta_k) \in \otimes_{i=1}^k C_i \) is a \((\sum_i \epsilon_i, \sum_i \delta_i)\) - differentially private algorithm.

- **Adaptive composition.** This property guarantees privacy when an iterative algorithm is adopted on different datasets that may nevertheless contain information relating to the same individual.

**Lemma 7** (Adaptive composition. Directly taken Theorem 3.5 in Kairouz et al. [35]). Let algorithm \( A_i(B_i) : D_i \rightarrow \theta_i \in C_i \) be an \((\epsilon_i, \delta_i)\) - differential privacy algorithm, and for \( t = 2, \ldots, T \), let \( A_i(B_i) : (D_1, \theta_1), (D_2, \theta_2), \ldots, (D_{t-1}, \theta_{t-1}) \rightarrow \theta_t \in C_t \) be \((\epsilon_t, \delta_t)\) - differentially private for all given \((\theta_1, \theta_2, \ldots, \theta_{t-1}) \in \otimes_{i=1}^{t-1} C_i \). Then, for all neighboring datasets \( D_t \) and \( D'_t \) that differ in a single entry relating to the same individual and for any set \( S \subseteq \otimes_{t=1}^T C_t \)

\[ P((\theta_1, \ldots, \theta_T) \in S | \bigcap_{t=1}^T (B_t = (D_t, \theta_{t-1}, 1))) \leq e^{\epsilon_T} P((\theta_1, \ldots, \theta_T) \in S | \bigcap_{t=1}^T (B_t = (D'_t, \theta_{t-1}, 1))) \] (45)

\[ + 1 - (1 - \delta) \prod_{t=1}^T (1 - \delta_t), \]

where

\[ \theta_{1:t-1} = \begin{cases} 0, & t = 1 \\ \theta_1, \theta_2, \ldots, \theta_{t-1}, & t \geq 2, \end{cases} \]

and

\[ \epsilon = \min \left \{ \sum_{t=1}^T \epsilon_t + \left ( e^{\epsilon_t - 1} - e^{\epsilon_t + 1} \right ) + \sum_{t=1}^T 2 \epsilon_t^2 \log \left ( \frac{1}{\delta} \right ), \sum_{t=1}^T \left ( e^{\epsilon_t - 1} - e^{\epsilon_t + 1} \right ) + \sum_{t=1}^T 2 \epsilon_t^2 \log \left ( e + \frac{\sqrt{T} \epsilon_t^2}{\delta} \right ) \right \}. \]

**APPENDIX I**

**LEMMAS FOR PRIVACY GUARANTEES**

The following lemma shows that STL algorithms do not increase the privacy budget when they are concatenated with an MTL algorithm.

**Lemma 8.** For an \((\epsilon, \delta)\) - non-iterative MP-MTL algorithm \( A_{\text{mp}} : (W \in \mathbb{R}^{d \times m}, D^m) \rightarrow W \in \mathbb{R}^{d \times m} \) and any STL algorithm \( A_{\text{st}} : (W, D^m) \rightarrow \tilde{W} \in \mathbb{R}^{d \times m} \), an algorithm \( A_{\text{mp+st}} : (W \in \mathbb{R}^{d \times m}, D^m) \rightarrow \tilde{W} \in \mathbb{R}^{d \times m} \) that first uses \( A_{\text{mp}} \) before applying \( A_{\text{st}} \) is still an \((\epsilon, \delta)\) - non-iterative MP-MTL algorithm. Moreover, an algorithm \( A_{\text{mp+st}} \) that first uses a deterministic STL algorithm before applying an \((\epsilon, \delta)\) - non-iterative MP-MTL algorithm is also an \((\epsilon, \delta)\) - non-iterative MP-MTL algorithm.

The following result shows that adopting a series of Non-iterative MP-MTL algorithms defined in Definition 5 iteratively, we can develop an Iterative MP-MTL algorithm, as described in Algorithm 6.

**Algorithm 6 Iterative MP-MTL build by Non-iterative MP-MTL**

**Input:** Datasets \((X_m^i, y_m^i) = \{(X_1^i, y_1^i), \ldots, (X_m^i, y_m^i)\}, \) where \( v_i \in [m], X_i \in \mathbb{R}^{n_i \times d}, y_i \in \mathbb{R}^{n_i \times 1} \). Number of iterations \( T \). Privacy loss \( \{\epsilon_t, \delta_t\}, t = 1, \ldots, T, \delta \geq 0 \). Initial models of tasks \( W^{(0)} \).

**Output:** \( \hat{W}^{(1:T)} \).

1: for \( t = 1 : T \) do
2: \( W^{(t)} = A_{\text{mp}}(W^{(t-1)}, X_m^t, y_m^t), \) where \( A_{\text{mp}} \) denotes an \((\epsilon_t, \delta_t)\)-Non-iterative MP-MTL algorithm.
3: \( W^{(1:T)}(i) = A_{\text{st}}(W^{(1:t)}, X_i^i, y_i^i), \) for \( i = 1, \ldots, m \), where \( A_{\text{st}}(i) \) denotes a deterministic STL algorithm for the \( i \)-th task.
4: end for

**Lemma 9.** Use Lemmas 7 and 8. Algorithm 6 is an \((\epsilon, 1 - (1 - \delta) \prod_{t=1}^T (1 - \delta_t))\) - iterative MP-MTL algorithm, where \( \epsilon \) is defined in Lemma 7.

**APPENDIX J**

**LEMMAS FOR UTILITY ANALYSIS**

**Lemma 10.** For a integer \( T \geq 1 \), a constant \( \alpha \in \mathbb{R} \), by Euler-Maclaurin formula [?], we have

\[ \sum_{t=1}^T t^\alpha = \left \{ \begin{array}{ll} O(t^{\alpha+1}/(\alpha+1)), & \alpha > -1; \\ O(t/(-\alpha-1)), & \alpha < -1. \end{array} \right. \]

Proof. This is the direct result of EulerMaclaurin formula in Lemma 7.

**Lemma 11.** For a integer \( T \geq 1 \) and a constant \( Q > 0 \), we have

\[ \sum_{t=1}^T Q^{-t} \leq \left \{ \begin{array}{ll} \frac{1}{Q^T}, & Q > 1; \\ \frac{1}{Q^T}, & Q < 1. \end{array} \right. \]

Proof. Because \( \sum_{t=1}^T Q^{-t} = Q^{-1} - Q^{-T} \), we complete the proof.

**Lemma 12.** For constants \( c_1, c_2 > 0 \), a constant \( c_0 > 0 \), a integer \( T \geq 1 \), a mapping \( a : T \rightarrow s(t) > 0 \), a mapping \( S_1 : T \rightarrow S_1(T) > 0 \) and a mapping \( S_2 : T \rightarrow S_2(T) > 0 \), then if \( \sum_{t=1}^T c_0 s(t) \geq c_1 \) and \( \sum_{t=1}^T s(t) \leq S_1(T) \), we have

\[ \frac{1}{c_0} \leq S_1(T)/c_1. \]

On the other hand, if \( \sqrt{\sum_{t=1}^T c_0^2 s(t)^2} \geq c_2 \) and \( \sum_{t=1}^T s(t)^2 \leq S_2(T) \), we have

\[ \frac{1}{c_0} \leq \sqrt{S_2(T)/c_2}. \]

Proof. If \( \sum_{t=1}^T c_0 s(t) \geq c_1, 1/c_0 \leq \sum_{t=1}^T s(t)/c_1 \leq S_1(T)/c_1. \)

On the other hand, if \( \sqrt{\sum_{t=1}^T c_0^2 s(t)^2} \geq c_2, 1/c_0 \leq \sqrt{\sum_{t=1}^T s(t)^2}/c_2 \leq \sqrt{S_2(T)/c_2}. \)
Lemma 13. Consider Algorithm 2. For an index $k \leq d$ that suffices the definition in Lemma 2 for all $t \in [T]$, $\eta = 1/L$, $\lambda = \Theta(LKd/\sqrt{m})$, set $\epsilon_t \leq 4Kk^2d/d_k^2$ for $t \in [T]$. Assume in each iteration, $E$ is the defined Wishart random matrix. We have with probability at least $1 - d^{-c}$ for some constant $c > 1$ that

$$
\epsilon_t = \frac{1}{2\eta} \left\| \tilde{W}^{(t)} - C \right\|_F^2 + \lambda \left\| \tilde{W}^{(t)} \right\|_* - \left\{ \min \frac{1}{2\eta} \left\| W - C \right\|_F^2 + \lambda \right\| W \right\|_* \right\} = O\left( \frac{K^2 \sqrt{mk} \log d}{\eta \epsilon_t} \right).
$$

Proof. First, using Lemma 1 of Jiang et al. [34], we have in the $t$-th step, with probability at least $1 - d^{-c}$ for some constant $c > 1$,

$$
\sigma_1(E) = O\left( (\log \log d) \sigma_1 \left( \frac{\max \{ t^{-1}, 1 \} }{2\epsilon_t} \right) \right) = O(\log \log d) K/\epsilon_t.
$$

We also have $\sigma_1(C) \leq \| C \|_F \leq \sqrt{m} \max_i \| C_i^* \|_2 \leq K \sqrt{m}$, where $C_i$ is the $i$-th column of $C$.

As such, by Lemma 2, in the $t$-th iteration, for $\epsilon_t \leq 4Kk^2d/d_k^2$, where $q = \min \{ d, m \}$, we have

$$
\epsilon_t = \frac{1}{2\eta} \left\| \tilde{W}^{(t)} - C \right\|_F^2 + \lambda \left\| \tilde{W}^{(t)} \right\|_* - \left\{ \min \frac{1}{2\eta} \left\| W - C \right\|_F^2 + \lambda \right\| W \right\|_* \right\} 
\leq \frac{1}{\eta} \left( \frac{\sigma_1^2(C)}{\eta \lambda} + \sigma_1(C) \right) \left[ \frac{\sigma_1(E)}{\eta \lambda} \right] 
+ (r_{c,k} - k) I(r_{c,k} > k) \sqrt{\sigma_1(E)} + \left( \frac{k(k - 1)}{2\eta \lambda} + 2k \right) \sigma_1(E)
\leq \frac{1}{\eta} \left( \frac{K^2 m}{\eta \lambda} + K \sqrt{m} \right) \left[ \frac{\sigma_1(E)}{\eta \lambda} \right] 
+ q \sqrt{\sigma_1(E)} + \left( \frac{k(k - 1)}{2\eta \lambda} + 2k \right) \sigma_1(E)
\leq O\left( \frac{1}{\eta} \left( \frac{K^2 m}{\eta \lambda} + K \sqrt{m} \right) \left( \frac{k^2}{\eta \lambda} + 2k \right) d(\log d) K/\epsilon_t \right).
$$

Further setting $\eta = 1/L$ and $\lambda = \Theta(LKd/\sqrt{m})$, assuming $\epsilon_t \leq k^2 \log(d)/4Kd(d - k)^2$, we have

$$
\epsilon_t = O\left( \frac{1}{\eta} \left( \frac{K^2 m}{\eta \lambda} + K \sqrt{m} \right) \left( \frac{k^2}{\eta \lambda} + 2k \right) d(\log d) K/\epsilon_t \right) = O\left( \frac{Kk \log d}{\eta \epsilon_t} \right).
$$

Lemma 15. For matrices $W_1, W_2 \in W \subset \mathbb{R}^{d \times m}$, we have

$$
\| W_1 - W_2 \|_F = O(\sqrt{m}).
$$

Proof. Because $W_1, W_2 \in W$, $\max_{i \in [m]} \| w_{i,1} \|_2 \leq K$. Therefore

$$
\| W_1 - W_2 \|_F \leq 2\| W_1 \|_F \leq 2\sqrt{m} \max_{i \in [m]} \| w_{i,1} \|_2 \leq 2K \sqrt{m}.
$$

Lemma 16. For constants $\epsilon, \delta > 0$, a integer $T \geq 1$, a series constants $\epsilon_t > 0$, for $t \in [T]$, then if

$$
\epsilon = \sum_{t=1}^{T} \left( \epsilon_t^* - 1 \right) \epsilon_t + \sqrt{\sum_{t=1}^{T} 2\epsilon_t^2 \log \left( \frac{1}{\delta} \right)},
$$

we have

$$
\sqrt{\sum_{t=1}^{T} \epsilon_t^2} \geq \frac{\sqrt{2} \epsilon}{2 \sqrt{\log(1/\delta) + 2\epsilon}}.
$$

On the other hand, if

$$
\epsilon = \sum_{t=1}^{T} \left( \epsilon_t^* - 1 \right) \epsilon_t + \sqrt{\sum_{t=1}^{T} 2\epsilon_t^2 \log \left( e + \sqrt{\sum_{t=1}^{T} \epsilon_t^2 \delta} \right)},
$$

we have

$$
\sqrt{\sum_{t=1}^{T} \epsilon_t^2} \geq \max \left\{ \frac{\epsilon}{2}, \frac{\sqrt{2} \epsilon}{2 \sqrt{\log(e + \epsilon/\sqrt{2} \delta) + 2\epsilon}} \right\}.
$$

Proof. If $\epsilon = \sum_{t=1}^{T} \left( \epsilon_t^* - 1 \right) \epsilon_t + \sqrt{\sum_{t=1}^{T} 2\epsilon_t^2 \log \left( \frac{1}{\delta} \right)},$
Because \((e^x - 1)/(e^x + 1) \leq x\) for \(x \geq 0\), then
\[
\epsilon \leq \sum_{t=1}^{T} \epsilon_t^2 + \sqrt{\sum_{t=1}^{T} 2\epsilon_t^2 \log \left(\frac{1}{\delta} \right)}.
\]
Solving the inequality with respect to \(\sqrt{\sum_{t=1}^{T} \epsilon_t^2}\), we get
\[
\sqrt{\sum_{t=1}^{T} \epsilon_t^2} \geq \frac{\sqrt{2\epsilon}}{\sqrt{\log(e + \epsilon/\sqrt{\delta}) + 2\epsilon + \sqrt{\log(1/\delta)}}} \geq \frac{\sqrt{2\epsilon}}{2\sqrt{\log(1/\delta)} + 2\epsilon}.
\]
If we have
\[
\epsilon = \sum_{t=1}^{T} \frac{(e^{\epsilon_t} - 1)\epsilon_t}{(e^{\epsilon_t} + 1)} + \sqrt{T} \sqrt{2} \log \left(\frac{\epsilon + \sqrt{T} \epsilon_t}{\sqrt{\epsilon_t}}\right),
\]
where the second inequality is because \(\log(x + 1) \leq x + 1\) for \(x \geq 0\).

As such,
\[
\sqrt{\sum_{t=1}^{T} \epsilon_t^2} \geq \sqrt{\frac{\epsilon}{1 + \sqrt{2}/(e\delta)}}.
\]

On the other hand, by (49), it also holds that \(\sqrt{2\epsilon} \sqrt{\sum_{t=1}^{T} \epsilon_t^2} \leq \epsilon\). Then we have
\[
\epsilon \leq \sum_{t=1}^{T} \epsilon_t^2 + \sqrt{\sum_{t=1}^{T} 2\epsilon_t^2 \log \left(e + \sqrt{T} \epsilon_t^2 \right)} \leq \sum_{t=1}^{T} \epsilon_t^2 + \sqrt{\sum_{t=1}^{T} 2\epsilon_t^2 \log \left(e + \frac{\epsilon}{\sqrt{2}\delta}\right)}.
\]

Solving the inequality with respect to \(\sqrt{\sum_{t=1}^{T} \epsilon_t^2}\), we also get
\[
\sqrt{\sum_{t=1}^{T} \epsilon_t^2} \geq \frac{\sqrt{2\epsilon}}{\sqrt{\log(e + \epsilon/\sqrt{\delta}) + 2\epsilon + \sqrt{\log(1/\delta)}}} \geq \frac{\sqrt{2\epsilon}}{2\sqrt{\log(e + \epsilon/\sqrt{\delta})} + 2\epsilon}.
\]
If \( \sum_{t=1}^{T} \epsilon_t^2 \geq c_2 \), we have

\[
T \sum_{t=1}^{T} Q_0^{-t} \sqrt{\epsilon_t} = \begin{cases} 
O \left( \frac{\kappa Q^{-T}}{c_2(Q_0/\sqrt{\epsilon})^{2} \sqrt{1-Q^2}} \right), & 0 < Q < Q_0^2; \\
O \left( \frac{\kappa Q^{-T}}{c_2(Q_0/\sqrt{\epsilon})^{2} \sqrt{1-Q^2}} \right), & Q_0^2 < Q < 1; \\
O \left( \frac{\kappa Q^{-T}}{c_2(Q_0/\sqrt{\epsilon})^{2} \sqrt{Q^2-1}} \right), & Q > 1,
\end{cases}
\]

and

\[
T \sum_{t=1}^{T} \sqrt{\epsilon_t} Q_0^{-t} = \begin{cases} 
O \left( \frac{\kappa Q^{-T}}{c_2(\sqrt{\epsilon}/\sqrt{Q})^{2} \sqrt{1-Q^2}} \right), & 0 < Q < Q_0^2; \\
O \left( \frac{\kappa Q^{-T}}{c_2(\sqrt{\epsilon}/\sqrt{Q})^{2} \sqrt{1-Q^2}} \right), & Q_0^2 < Q < 1; \\
O \left( \frac{\kappa Q^{-T}}{c_2(\sqrt{\epsilon}/\sqrt{Q})^{2} \sqrt{Q^2-1}} \right), & Q > 1.
\end{cases}
\]

Proof. If \( \sum_{t=1}^{T} \epsilon_t = \sum_{t=1}^{T} c_0 Q^{-t} \geq c_1 \), we have

\[
T \sum_{t=1}^{T} Q_0^{-t} \sqrt{\epsilon_t} = O \left( \sum_{t=1}^{T} Q_0^{-t} \sqrt{\epsilon_0 Q^{-t}} \right) = O \left( \sum_{t=1}^{T} \left( Q_0/\sqrt{\epsilon} \right)^{-t} \sqrt{\frac{K}{\epsilon_0}} \right).
\]

Using Lemma 12, we have

\[
T \sum_{t=1}^{T} \sqrt{\epsilon_t} = O \left( \sum_{t=1}^{T} \left( Q_0/\sqrt{\epsilon} \right)^{-t} \sqrt{\frac{K}{c_1 \sum_{t=1}^{T} Q^{-t}}} \right).
\]

Then using Lemma 11, if \( Q < Q_0^2 \), i.e., \( Q_0/\sqrt{\epsilon} > 1 \), we have

\[
T \sum_{t=1}^{T} \sqrt{\epsilon_t} = O \left( \frac{1}{Q_0/\sqrt{\epsilon} - 1} \sqrt{\frac{K}{c_1} \sum_{t=1}^{T} Q^{-t}} \right) = O \left( \sqrt{\frac{K Q^{-T}}{c_1 (Q_0/\sqrt{\epsilon})^{2} (1-Q)}} \right).
\]

Results under other conditions can be proved similarly.

Lemma 19. For constants \( L, c_3, c_4 > 0 \), a integer \( T \geq 1 \), matrices \( \mathbf{W}^{(0)}, \mathbf{W}_1 \in \mathcal{W} \subseteq \mathbb{R}^{d \times m} \), if it holds for a series of positive constants \( \{ \epsilon_t \} \) that \( \sum_{t=1}^{T} \sqrt{\epsilon_t} = O(\sqrt{\epsilon_4 T^{c_3}}) \), setting \( T = \Theta((K^2 L/m/c_4)^{1/c_3}) \), we have

\[
\mathcal{E} = \frac{L}{m T^2} \left[ K \sqrt{m} + \frac{1}{\sqrt{T}} \sum_{t=1}^{T} \sqrt{\epsilon_t} \right]^2 = O \left( K^2 L \left[ \frac{c_4}{K^2 L m} \right]^{1/c_3} \right).
\]

Proof. First, because \( \epsilon_t > 0 \) for \( t \in [T] \), we have

\[
\sqrt{\sum_{t=1}^{T} \epsilon_t} \leq \sum_{t=1}^{T} \sqrt{\epsilon_t}.
\]

Then combining Lemma 15, it suffices that

\[
\mathcal{E} = O \left( \frac{L}{m T^2} \left[ K \sqrt{m} + \frac{1}{\sqrt{T}} \sum_{t=1}^{T} \sqrt{\epsilon_t} \right]^2 \right) = O \left( \left[ K \sqrt{\frac{T}{L} + \frac{1}{m L} \sum_{t=1}^{T} \sqrt{\epsilon_t}} \right]^2 \right) = O \left( \left[ K \sqrt{\frac{T}{L} + \frac{1}{m L} \sqrt{c_4 T^{c_3}}} \right]^2 \right).
\]

Then setting \( T = \Theta((K^2 L/m/c_4)^{1/c_3}) \), we complete the proof.

Lemma 20. For constants \( L, c_3, c_4 > 0 \), a integer \( T \geq 1 \), matrices \( \mathbf{W}^{(0)}, \mathbf{W}_1 \in \mathcal{W} \subseteq \mathbb{R}^{d \times m} \), if it holds for a series of positive constants \( \{ \epsilon_t \} \) that \( \sum_{t=1}^{T} \epsilon_t = O(\sqrt{\epsilon_4 T^{c_3}}) \), setting \( T = \Theta((K^2 L/m/c_4)^{1/c_3}) \), we have

\[
\mathcal{E} = \frac{2 L}{m (T+1)^2} \left( \| \mathbf{W}^{(0)} - \mathbf{W}_1 \|_F + 2 \sum_{t=1}^{T} \sqrt{\epsilon_t} \right) + O \left( K^2 L \left[ \frac{c_4}{K^2 L m} \right]^{2/c_3} \right).
\]

Proof. First, because \( \epsilon_t > 0 \) for \( t \in [T] \), we have

\[
\sqrt{\sum_{t=1}^{T} \epsilon_t} \leq \sum_{t=1}^{T} \sqrt{\epsilon_t} = \sum_{t=1}^{T} t \sqrt{\epsilon_t}.
\]

Then combining Lemma 15, it suffices that

\[
\mathcal{E} = O \left( \frac{L}{m T^2} \left[ K \sqrt{m} + \frac{1}{\sqrt{T}} \sum_{t=1}^{T} \sqrt{\epsilon_t} \right]^2 \right) = O \left( K \sqrt{\frac{T}{L} + \frac{1}{m L} \sqrt{c_4 T^{c_3}}} \right) + O \left( K^2 L \left[ \frac{c_4}{K^2 L m} \right]^{2/c_3} \right).
\]

Then setting \( T = \Theta((K^2 L/m/c_4)^{1/c_3}) \), we complete the proof.

Lemma 21. For constants \( L, c_6 > 0 \), a constant \( c_5 \in (0,1) \), a constant \( Q_0 \in (0,1) \), a integer \( T \geq 1 \), matrices \( \mathbf{W}^{(0)}, \mathbf{W}_1 \in \mathcal{W} \subseteq \mathbb{R}^{d \times m} \), if it holds for a series of positive constants \( \{ \epsilon_t \} \) that \( \sum_{t=1}^{T} \epsilon_t = O(\sqrt{c_6}) \), setting \( T = \Theta((K^2 L/m/c_6)^{1/c_5}) \), we have

\[
\mathcal{E} = \frac{Q_0^T}{\sqrt{m}} \left( \| \mathbf{W}^{(0)} - \mathbf{W}_1 \|_F + 2 \sum_{t=1}^{T} \epsilon_t \right) = O \left( K \left[ \frac{c_6}{K^2 L m} \right]^{\log_{c_5} Q_0} \right).
\]

Proof. Using Lemma 15, it suffices that

\[
\mathcal{E} = O \left( \frac{L}{m T^2} \left[ K \sqrt{m} + \frac{1}{\sqrt{T}} \sum_{t=1}^{T} \sqrt{\epsilon_t} \right]^2 \right) = O \left( \left[ K \sqrt{\frac{T}{L} + \frac{1}{m L} \sum_{t=1}^{T} \sqrt{\epsilon_t}} \right]^2 \right) = O \left( \left[ K \sqrt{\frac{T}{L} + \frac{1}{m L} \sqrt{c_4 T^{c_3}}} \right]^2 \right).
\]

Then setting \( T = \Theta((K^2 L/m/c_6)) \), we complete the proof.

Lemma 22. For constants \( L, \mu, c_6 > 0 \), a constant \( c_5 \in (0,1) \), a constant \( Q_0 \in (0,1) \), a integer \( T \geq 1 \), matrices \( \mathbf{W}^{(0)}, \mathbf{W}_1 \in \mathcal{W} \subseteq \mathbb{R}^{d \times m} \), if it holds for a series of positive constants \( \{ \epsilon_t \} \) that
\[
\sum_{t=1}^{T} \sqrt{\varepsilon_t} Q_0^{-t} = O(\sqrt{c_0 c_5^{-T}}), \text{ setting } T = \Theta((K^2 L m/c_4)^{1/c_3}).
\]

Therefore, all the procedures can be decoupled to independent.

### Proof
First, because \(\varepsilon_t > 0\) for \(t \in [T]\), we have
\[
\sum_{t=1}^{T} \varepsilon_t Q_0^{-t} < \sum_{t=1}^{T} \varepsilon_t Q_0^{-t}.
\]

Then it suffices that
\[
\mathcal{E} = O\left( \frac{Q_0^T}{m} \left[ K \sqrt{L m} + \sqrt{\frac{T}{\mu}} \sum_{t=1}^{T} \varepsilon_t Q_0^{-t} \right]^2 \right)
= O\left( Q_0^T \left[ K \sqrt{L} + \sqrt{\frac{T}{m \mu}} \sum_{t=1}^{T} \varepsilon_t Q_0^{-t} \right]^2 \right)
= O\left( Q_0^T \left[ K \sqrt{L} + \sqrt{\frac{T}{m \mu}} c_5^{-T} \right]^2 \right).
\]

Then setting \(T = \Theta(\log_{1/c_5}(K^2 \mu m/c_6))\), we complete the proof. \(\square\)

### Appendix K
PROOF OF RESULTS IN THE MAIN TEXT

#### K.1 Proof of Lemma 1

Proof. Under the setting of single-task learning, each task is learned independently, and thus, we have for \(i = 1, \ldots, m\), for any set \(S_i\),
\[
\mathbb{P}(\hat{w}_{[-i]} \in S_i | B = (w_{[-i]}, D_{[-i]}, w_i, D_i)) = \mathbb{P}(\hat{w}_{[-i]} \in S_i | B = (w_{[-i]}, D_{[-i]})).
\]

As such, we have for \(i = 1, \ldots, m\),
\[
\mathbb{P}(\hat{w}_{[-i]} \in S_i | B = (w_{[-i]}, D_{[-i]}, w_i, D_i)) = \frac{\mathbb{P}(\hat{w}_{[-i]} \in S_i | B = (w_{[-i]}, D_{[-i]}))}{\mathbb{P}(\hat{w}_{[-i]} \in S_i | B = (w_{[-i]}, D_{[-i]}))} = 1 \leq \varepsilon_0. \quad \square
\]

#### K.2 Proof of Proposition 1

Proof. First, for Algorithm 2, denoting \(\Sigma_0 = \mathbf{\Sigma}^{(t)}\), the \(j\)-th diagonal element of \(S_{\eta, j}\) is
\[
\max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0 + E)}} \right) \geq \max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_d(E)}} \right) \to 1.
\]

where \(\sigma_d(E)\) is the \(d\)-th largest singular value, i.e., the smallest singular value, of \(E\). As such, when \(\sigma_d(E) = C \lambda^2\) for sufficiently large \(C > 0\), \(\max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_d(E)}} \right) \to 1.

Then \(w_{[-i]}^{(t-1)} = U S_{\eta, j} U^T w_{[-i]}^{(t-1)} = U U^T w_{[-i]}^{(t-1)} = w_i^{(t-1)}\).

Therefore, all the procedures can be decoupled to independently run for each task, thus Algorithm 2 degrades to an STL algorithm with no random perturbation.

Similarly, for Algorithm 3, for all \(j \in [m]\), the \(j\)-th diagonal element of \(S_{\eta, j}\) is
\[
\max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\Sigma_{jj, 0} + E_{jj}}} \right) \quad \text{and}
= \max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\Sigma_{jj, 0} + E_{jj}}} \right).
\]

where the equality is because \(\Sigma_0\) is semi-positive definite and \(E\) is positive definite.

As such, when \(\min_j E_{jj} = C \lambda^2\) for sufficiently large \(C > 0\), \(\min_j \left[ \max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\Sigma_{jj, 0} + E_{jj}}} \right) \right] \to 1.\)

Then \(\hat{w}_i^{(t-1)} = S_{\eta, i} \hat{w}_i^{(t-1)} = w_i^{(t-1)}\). Therefore, all the procedures can be decoupled to independently run for each task, thus Algorithm 3 degrades to an STL algorithm with no random perturbation.

### K.3 Proof of Theorem 1

Proof. For simplicity, we omit the symbol \(B\) used to denote the input in the conditional events in some equations.

First, we show that for all \(t \in [T]\), the mapping \(W^{(t-1)} \rightarrow \mathbf{\Sigma}^{(t)}\) is an \((\varepsilon_t, 0)\)-differentially private algorithm.

**Case 1.** For \(\mathbf{\Sigma}^{(t)} = \mathbf{\Sigma}^{(t)} + E = W^{(t-1)}(W^{(t-1)})^T + E\), we follow the proof of Theorem 4 of Jiang et al. [34].

For all \(i \in [m]\), consider two adjacent parameter matrices \(W_i^{(t-1)}\) and \((W_i')^{(t-1)}\) that differ only in the \(i\)-th column such that \(W_i^{(t-1)} = [w_i^{(t-1)} \ldots w_i^{(t-1)} \ldots w_i^{(m)}]\) and \((W_i')^{(t-1)} = [w_i^{(t-1)} \ldots w_i^{(t-1)} \ldots w_i^{(m)}]\).

Now, let
\[
\mathbf{\Sigma}^{(t)} = W^{(t-1)}(W^{(t-1)})^T = \sum_{j=1}^{m} w_j^{(t-1)}(w_j^{(t-1)})^T
\]
\[
\mathbf{\Sigma}^{(t)} = \sum_{j \neq i} w_j^{(t-1)}(w_j^{(t-1)})^T + (w_i^{(t-1)})(w_i^{(t-1)})^T
\]
\[
\Delta = \mathbf{\Sigma}^{(t)} - (\mathbf{\Sigma}^{(t)})
= w_i^{(t-1)}(w_i^{(t-1)})^T - (w_i^{(t-1)})(w_i^{(t-1)})^T.
\]

Then, we have for the conditional densities
\[
\frac{p(\mathbf{\Sigma}^{(t)} | W^{(t-1)})}{p(\mathbf{\Sigma}^{(t)} | W^{(t-1)})} = \frac{p(\mathbf{\Sigma}^{(t)} | W^{(t-1)}(W^{(t-1)})^T + E_1)}{p(\mathbf{\Sigma}^{(t)} | (W^{(t-1)})(W^{(t-1)})^T + E_2)}.
\]

Because \(E_1, E_2 \sim W_0(\max_j s_j^{(t-1)} I_0, D, D + 1)\), letting \(V = \max_j s_j^{(t-1)} I_0 / 2s_{\varepsilon}/2s_{\varepsilon}\),
\[
\frac{p(\mathbf{\Sigma}^{(t)} | W^{(t-1)}(W^{(t-1)})^T + E_1)}{p(\mathbf{\Sigma}^{(t)} | (W^{(t-1)})(W^{(t-1)})^T + E_2)} = \exp[-\text{tr}(V^{-1}(\mathbf{\Sigma}^{(t)} - W^{(t-1)}(W^{(t-1)})^T)/2]
= \exp[-\text{tr}(V^{-1}(\mathbf{\Sigma}^{(t)} - (W^{(t-1)})(W^{(t-1)})^T)/2]
\]
\[
= \exp[\text{tr}(V^{-1}(\mathbf{\Sigma}^{(t)} - W^{(t-1)}(W^{(t-1)})^T)/2]
= \exp[\text{tr}(V^{-1}(\mathbf{\Sigma}^{(t)} - (W^{(t-1)})(W^{(t-1)})^T)/2]
\]
\[
= \exp[\text{tr}(V^{-1}(\mathbf{\Sigma}^{(t)} - W^{(t-1)}(W^{(t-1)})^T)/2]
= \exp[\text{tr}(V^{-1}(\mathbf{\Sigma}^{(t)} - (W^{(t-1)})(W^{(t-1)})^T)/2]
\]
\[
= \exp[-\text{tr}(w_i^{(t-1)}(w_i^{(t-1)})^T - (w_i^{(t-1)})(w_i^{(t-1)})^T)/(2s_{\varepsilon})]
= \exp[-\text{tr}(w_i^{(t-1)}(w_i^{(t-1)})^T - (w_i^{(t-1)})(w_i^{(t-1)})^T)/(2s_{\varepsilon})]
\]
\[
= \exp[-\text{tr}(w_i^{(t-1)}(w_i^{(t-1)})^T - (w_i^{(t-1)})(w_i^{(t-1)})^T)/(2s_{\varepsilon})]
\]
\[
\leq \exp[-\text{tr}(w_i^{(t-1)}(w_i^{(t-1)})^T)/(2s_{\varepsilon})] \leq \exp(\varepsilon_t).
\]
As such, we have
\[
\frac{p(\Sigma(t) | W^{(t-1)})}{p(\Sigma(t) | W(t-1)^{(t-1)})} \leq \exp(\epsilon_t).
\]

**Case 2.** Consider \( \Sigma(t) = \tilde{\Sigma}(t) + E = (W^{(t-1)})^TW^{(t-1)} + E. \)

For all \( i \in [m], \) consider two adjacent parameter matrices \( W^{(t-1)} \) and \( (W')^{(t-1)} \) that differ only in the i-th column such that \( W^{(t-1)} = (w_1^{(t-1)}, \ldots, w_i^{(t-1)}, \ldots, w_m^{(t-1)}) \) and \( (W')^{(t-1)} = (w_1^{(t-1)}, \ldots, (w')_i^{(t-1)}, \ldots, w_m^{(t-1)}). \) Let
\[
\Sigma(t) = (W^{(t-1)})^TW^{(t-1)},
\]
\[\tilde{\Sigma}(t) = ((W')^{(t-1)})^TW^{(t-1)}, \]
where the i-th diagonal element of \( \Delta = \|w_i^{(t-1)} - (w')_i^{(t-1)}\|^2_2 \) and the other diagonal elements of \( \Delta \) are zeros.

Then, we have
\[
\frac{p(\Sigma(t) | W^{(t-1)})}{p(\Sigma(t) | W(t-1)^{(t-1)})} = \frac{p(\Sigma(t) = (W^{(t-1)})^TW^{(t-1)} + E_i)}{p(\Sigma(t) = ((W')^{(t-1)})^TW^{(t-1)} + E_i)} \leq \exp(\epsilon_t).
\]

Because \( E_1, E_2 \sim W_0 (\text{diag}(s^{(t-1)}/2\epsilon), m + 1), \) letting \( V = \text{diag}(s^{(t-1)}/2\epsilon_i) \),
\[
\frac{p(\Sigma(t) = (W^{(t-1)})^TW^{(t-1)} + E_i)}{p(\Sigma(t) = ((W')^{(t-1)})^TW^{(t-1)} + E_i)} = \exp(-\tr(V^{-1}(\Sigma(t) - (W^{(t-1)})^TW^{(t-1)}))/2)
\]
\[= \exp(\tr(V^{-1}(\Sigma(t) - ((W')^{(t-1)})^TW^{(t-1)}))/2)
\]
\[= \exp(2s^{(t-1)}(2\epsilon_i)/2s^{(t-1)})) \leq \exp(\epsilon_t).
\]

As such, we also have
\[
\frac{p(\Sigma(t) | W^{(t-1)})}{p(\Sigma(t) | W(t-1)^{(t-1)})} \leq \exp(\epsilon_t).
\]

Next, given \( t \in [T], \Sigma(t) \rightarrow M(t) \) (when \( t = 1, \Sigma(1) = \emptyset \) and the mapping \( f : \Sigma(t) \rightarrow M(t) \) does not touch any unperturbed sensitive information, using the Post-Processing immunity Lemma (Lemma 4) for the mapping \( f' : \Sigma^{(t)} \rightarrow M(t), \) the algorithm \( \Sigma(t) \rightarrow M(t) \) is still an \((\epsilon_t, 0)\)-differentially private algorithm.

Then, because \( \bar{w}_i(t) \rightarrow A_{t,i} \Sigma_i(t), \) \( \bar{w}_i(t-1), \) \( X_i, y_i \) is an STL algorithm for the \( i \)-th task, for \( i = 1, \ldots, m, \) the mapping \( \Sigma(t) \rightarrow M(t) \), \( X_i, y_i \rightarrow (\bar{w}_i(t)) \) thus does not touch any unperturbed sensitive information for the \( i \)-th task. As such, applying the Post-Processing immunity Lemma again for the mapping \( f'' : \Sigma^{(t)} \rightarrow M(t), \) \( X_i, y_i \rightarrow (\bar{w}_i(t)) \) (when \( t = 1, \bar{w}_i(t) \rightarrow \emptyset \) ), we have for any set \( S_i \subseteq C_{t,i} \)
\[
\Pr(\theta_{t,i} \in S_{i,t} | W(t-1), \Sigma(t), \bar{w}_i(t), D_m) \leq \epsilon_t \Pr(\theta_{t,i} \in S_{i,t} | (W(t-1), \Sigma(t), \bar{w}_i(t), (D')_m),
\]
where \( W(t-1) \) and \( (W')^{(t-1)} \) differ only in the \( i \)-th column and \( D_m \) and \( (D')_m \) differ only in the \( i \)-th task.

Now, again, for \( t = 1, \ldots, T, \) we take the \( t \)-th dataset \( \mathcal{D}_t = \{ (\bar{w}_i^{(1)}, D_1), \ldots, (\bar{w}_m^{(1)}, D_m) \} \). Given that \( W(t) = \bar{W}(t) \) for all \( t \in [T], \) we have for any set \( S_{i,t} \subseteq C_{t,i} \)
\[
\Pr(\theta_{t,i} \in S_{i,t} | \mathcal{D}_t, \theta_{1:t-1}) \leq \epsilon_t \Pr(\theta_{t,i} \in S_{i,t} | \mathcal{D}_t', \theta_{1:t-1}),
\]
where \( \mathcal{D}_t \) and \( \mathcal{D}_t' \) are two adjacent datasets that differ in a single entry, the \( i \)-th data instance \( (\bar{w}_i^{(1)}, D_i = (X_i, y_i)), \)

This renders the algorithm in the \( t \)-th iteration an \((\epsilon_t, 0)\)-differentially private algorithm.

Now, again by the Adaptive composition Lemma (Lemma 7), for all \( i \in [m] \) and for any set \( S' \subseteq C_{t,i} \), we have
\[
\Pr((\theta_{t,i}, \ldots, \theta_{T,i}) \in S' | \bigcap_{t=1}^{T} (B_t = (\mathcal{D}_t, \theta_{1:t-1}))) \leq \epsilon' \Pr((\theta_{t,i}, \ldots, \theta_{T,i}) \in S' | \bigcap_{t=1}^{T} (B_t = (\mathcal{D}_t', \theta_{1:t-1}))) + \delta,
\]
where for all \( t \in [T], B_t \) denotes the input for the \( t \)-th iteration.

Finally, taking \( \theta_t = (\theta_{t,1}, \ldots, \theta_{t,m}) \) for all \( t \in [T], \) we have for any set \( S \subseteq \mathbb{R}^{d \times (m-1) + 1} \)
\[
\Pr((\bar{w}_0^{1:t-1}, \ldots, \bar{w}_m^{1:t-1}) \in S | \bigcap_{t=1}^{T} (B_t = (\mathcal{D}_t, \theta_{1:t-1}))) \leq \epsilon' \Pr((\bar{w}_0^{1:t-1}, \ldots, \bar{w}_m^{1:t-1}) \in S | \bigcap_{t=1}^{T} (B_t = (\mathcal{D}_t', \theta_{1:t-1}))) + \delta.
\]

**K.4 Proof of Corollary 1**

**Proof.** For simplicity, we omit the symbol \( B \) used to denote the input in the conditional events in some equations.

Using Theorem 1, we only need to show that Algorithm 2 complies with our MP-ML framework in Algorithm 1.

Consider the t-th iteration for all \( t \in [T] \). Because of the norm clipping, for \( i = 1, \ldots, m, \) the \( 2 \)-norm of any parameter vector is less than \( K \). Then, we have for \( i = 1, \ldots, m \)
\[
s_i(t) = \max_{\bar{w}_i^{(t)}} \|w_i^{(t)}\|_2 - \|\bar{w}_i^{(t)}\|_2 \leq \max_{\bar{w}_i^{(t)}} \|\bar{w}_i^{(t)}\|_2 + \|\bar{w}_i^{(t)}\|_2 = 2K.
\]

Because the norm clipping is a deterministic STL algorithm and because the mapping \( \bar{w}_i(t) \rightarrow \Sigma(t) \) an \((\epsilon_t, 0)\)-differentially private algorithm, we have for any set \( S \subseteq \mathbb{R}^{d \times d} \)
\[
\Pr(\Sigma(t) \in S | \bar{w}_i^{(t)}, \bar{w}_i^{(t)}) = \Pr(\Sigma(t) \in S | \bar{w}_i^{(t)}, \bar{w}_i^{(t)}) \leq \epsilon' \Pr(\Sigma(t) \in S | \bar{w}_i^{(t)}, \bar{w}_i^{(t)}) = \epsilon' \Pr(\Sigma(t) \in S | \bar{w}_i^{(t)}, \bar{w}_i^{(t)})
\]

which renders the mapping \( \bar{w}_i(t) \rightarrow \Sigma(t) \) as an \((\epsilon_t, 0)\)-differentially private algorithm as well.

Let \( M(t) = US \Sigma(U^T \bar{w}_i(t), \ bar{w}_i(t)) \). As such, the 7-th step to the 9-th step can be treated as the process of first performing a mapping \( f : \Sigma^{(t)} \rightarrow M(t) \) and then applying an STL algorithm:
\[
\bar{w}_i(t) = U S \Sigma(U^T \bar{w}_i(t), \ bar{w}_i(t)) = \text{for all } i \in [m].
\]

(50)
Now, because (50), the 10-th step and the 11-th step are all STL algorithms, they can be treated as a entire STL algorithm performing the mapping: \((M^{(t)}, w_{i}^{(0:t−1)}, x_{i}, y_{i}) \rightarrow \left(\hat{w}_{i}^{(t)}, \hat{w}_{i}^{(t)}\right)\).

As such, in all the iterations, Algorithm 2 complies with Algorithm 1. Thus, the result of Theorem 1 can be applied to Algorithm 2.

Similarly, using Theorem 1, we only need to show that Algorithm 3 complies with our MP-MTL framework in Algorithm 1.

The proof for the sensitivity is the same.

Now, let \(M^{(t)} = S_{0}\lambda\). As such, the 7-th step can be treated as a mapping \(f : \Sigma^{(t)} \rightarrow M^{(t)}\).

Then, because the 8-th step, the 9-th step and the 10-th step are all STL algorithms, they can be treated as a entire STL algorithm performing the mapping: \((M^{(t)}, w_{i}^{(0:t−1)}, x_{i}, y_{i}) \rightarrow \left(\hat{w}_{i}^{(t)}, \hat{w}_{i}^{(t)}\right)\).

Therefore, in all the iterations, Algorithm 3 complies with Algorithm 1, and thus, the result of Theorem 1 can be applied to Algorithm 3.

\[\square\]

**K.5 Proof of Lemma 2**

Proof. We invoke the results of Schmidt et al. [49] to bound the empirical optimization error.

In the \(t\)-th step, a standard proximal operator (see Ji and Ye [32]) optimizes the following problem:

\[
\min_{W} \frac{1}{2\eta} \|W - C\|^2_F + \lambda \|W\|_*,
\]

where \(C = \hat{W}^{(t−1)}\). By Theorem 3.1 of Ji and Ye [32], denote the solution of the problem by \(\hat{W}^{(t)} = U_{0}\Sigma_{0}^{(t)}U_{0}^T\). Let \(U_{0}A_{0}U_{0}^T = CC^T\) be the SVD decomposition of \(CC^T\), \(\Sigma_{0}^{(t)}\) is also a diagonal matrix and \(\Sigma_{0}^{(t)}\) is \(\max\{0, 1 - \eta \lambda \sqrt{\lambda} \} \) for \(i = 1, \ldots, \min\{d, m\}\).

By Algorithm 2, \(W^{(t)} = US_{\eta}U^T\).

Then we analyse the bound of \(\frac{1}{2\eta} \|\hat{W}^{(t)} - C\|^2_F + \lambda \|\hat{W}^{(t)}\|_*\).

First, we have

\[
\|\hat{W}^{(t)} - C\|^2_F + \|\hat{W}^{(t)} - C\|^2_F = \text{tr}(\hat{W}^{(t)} - C)^T(\hat{W}^{(t)} - C) - \text{tr}(\hat{W}^{(t)} - C)^T(\hat{W}^{(t)} - C))
\]

\[
= \text{tr}(\hat{W}^{(t)} - C)^T(\hat{W}^{(t)} - C) - 2\text{tr}(\hat{W}^{(t)} - C)^T(C - \hat{W}^{(t)}))
\]

\[
+ \text{tr}(\hat{W}^{(t)} - C)^T(C - \hat{W}^{(t)}))
\]

\[
\leq \sigma_1(\hat{W}^{(t)} - C)\|\hat{W}^{(t)} - C\|_* + \sigma_1(\hat{W}^{(t)} - C)\|\hat{W}^{(t)} - C\|_*
\]

\[
(51)
\]

where \(\sigma_1(\cdot)\) denotes the largest singular value of the enclosed matrix.

Denote \(T = US_{\eta}U^T, T_0 = U_{0}\Sigma_{0}U_{0}^T\). Since \(U\) is decomposed from a symmetric matrix, we have

\[
\sigma_1(\hat{W}^{(t)} - C) = \sigma_1(TC - C) \leq \sigma_1(C)\sigma_1(T - I)
\]

\[
= \sigma_1(C)\sigma_1(U\Sigma_{\eta}U^T - UT^T)
\]

\[
= \sigma_1(C)\sigma_1(U(\Sigma_{\eta} - I)U^T).
\]

Since \(\Sigma_{\eta} - I\) is a diagonal matrix, whose \(i\)-th diagonal element is \(\max\{0, 1 - \eta \lambda \sqrt{\lambda} \} \cdot \eta \lambda \) for \(i = 1, \ldots, \min\{d, m\}\), so \(\sigma_1(U(\Sigma_{\eta} - I)U^T) \leq 1\) and

\[
\sigma_1(\hat{W}^{(t)} - C) \leq \sigma_1(C).
\]

Similarly,

\[
\sigma_1(\hat{W}^{(t)} - C) \leq \sigma_1(C). \quad (53)
\]

On the other hand,

\[
\|\hat{W}^{(t)} - \hat{W}^{(t)}\|_* = \|TC - T_0C\|
\]

\[
= \sum_{j=1}^{d} \sigma_j(T)u_ju_j^T - \sum_{j=1}^{d} \sigma_j(T_0)u_ju_j^T \|C\|_*
\]

\[
= \sum_{j=1}^{d} (\sigma_j(T) - \sigma_j(T_0))u_ju_j^T C
\]

\[
- \sum_{j=1}^{d} \sigma_j(T_0)u_ju_j^T C
\]

\[
= \sum_{j=1}^{d} \sigma_j(T_0)(u_ju_j^T - u_ju_ju_j^T) C
\]

\[
+ \sum_{j=1}^{d} (\sigma_j(T) - \sigma_j(T_0))u_ju_j^T C
\]

\[
\leq \sum_{j=1}^{d} \sigma_j(T_0)(u_ju_j^T - u_ju_ju_j^T) C
\]

\[
+ \sum_{j=1}^{d} (\sigma_j(T) - \sigma_j(T_0))u_ju_j^T C
\]

\[
(54)
\]

where \(u_j\) and \(u_ju_j^T\) are the \(j\)-th column of \(U\) and \(U_0\), respectively.

Let \(r_c = \text{rank}(C) \leq \min\{d, m\}\) be the rank of \(C\). Then we have

\[
\left\| \sum_{j=1}^{d} (\sigma_j(T) - \sigma_j(T_0))u_ju_j^T C \right\|_*
\]

\[
\leq \sum_{j=1}^{d} \left( \sigma_j(T) - \sigma_j(T_0) \right) \sigma_j(C) \leq \sigma_1(C) \sum_{j=1}^{d} \left( \sigma_j(T) - \sigma_j(T_0) \right).
\]

\[
(55)
\]

Denote \(\Sigma_0 = \Sigma^{(t)} = CC^T\). Then we have for \(j \in [r_c],\)

\[
\left| \sigma_j(T) - \sigma_j(T_0) \right| = \max\left(0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0 + E)}} \right) - \max\left(0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0)}} \right)
\]

\[
\leq \max\left(0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j(E)}} \right) - \max\left(0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0)}} \right).
\]

**Case 1:** \(\eta \lambda > \sqrt{\sigma_j(\Sigma_0)}\). Then

\[
\left| \sigma_j(T) - \sigma_j(T_0) \right| = \max\left(0, 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j(E)}} \right) \leq 1 - \frac{\eta \lambda}{\sqrt{\eta \lambda^2 + \sigma_j(E)}}
\]

\[
\leq 1 - \frac{\eta \lambda}{\eta \lambda + \sqrt{\sigma_j(E)}} = \frac{\sqrt{\sigma_j(E)}}{\eta \lambda + \sqrt{\sigma_j(E)}} \leq \frac{\sqrt{\sigma_j(E)}}{\eta \lambda}
\]
Case 2: \( \eta \lambda \leq \sqrt{\sigma_j(\Sigma_0)} \). Then
\[
|\sigma_j(T) - \sigma_j(T_0)| = 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j(\Sigma)}} - 1 + \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0)}} = \eta \lambda \frac{\sqrt{\sigma_j(\Sigma_0) + \sigma_j(\Sigma)}}{\sqrt{\sigma_j(\Sigma_0)}} \left[ \eta \lambda + \sqrt{\sigma_j(\Sigma_0) + \sigma_j(\Sigma_0) + \sigma_j(\Sigma_0)} \right] \leq \frac{\eta \lambda}{\sqrt{\eta^2 \lambda^2 + 0 + \eta^2 \lambda^2}} \sqrt{\eta^2 \lambda^2 + 0} = \eta \lambda, \]
Suppose that there exists an index \( k \leq d \) such that \( \sigma_k^2(C) = \sigma_k^2(\Sigma_0) > \eta^2 \lambda^2, \sigma_{k+1}^2(C) = \sigma_{k+1}^2(\Sigma_0) \leq \eta^2 \lambda^2 \), then \( \sigma_j(T_0) > 0 \) for \( j \leq k, k \leq r, \) and
\[
\sum_{j=1}^{k} |\sigma_j(T) - \sigma_j(T_0)| \leq k \sigma_1(\Sigma) \frac{\sigma(T)}{\eta \lambda} (56)
\]
For another part of (54),
\[
\left| \sum_{j=1}^{d} \sigma_j(T_0)(u_j, u_j^T - u_{j,0}u_{j,0}^T) \right| = \left| \sum_{j=1}^{k} \sigma_j(T_0)(u_j, u_j^T - u_{j,0}u_{j,0}^T) \right| \leq \sigma_1(C) \left| \sum_{j=1}^{k} \sigma_j(T_0)(u_j, u_j^T - u_{j,0}u_{j,0}^T) \right| (57)
\]
Denote \( U_j = \sum_{j=1}^{j} u_j^T u_j^T, U_{j,0} = 0 \). Then \( u_j u_j = U_j - U_{j-1,0}u_{j,0} = U_{j,0} - U_{j-1,0} \) for \( j \in [d] \). Then we have
\[
\left| \sum_{j=1}^{k} \sigma_j(T_0)(u_j, u_j^T - u_{j,0}u_{j,0}^T) \right| = \left| \sum_{j=1}^{k} \sigma_j(T_0)(U_j - U_{j,0} - (U_{j-1} - U_{j-1,0})) \right| = \left| \sum_{j=1}^{k} \sigma_j(T_0)(U_j - U_{j,0}) + \sigma_k(T_0)(U_k - U_{k,0}) \right| \leq \left| \sum_{j=1}^{k} \sigma_j(T_0)(U_j - U_{j,0}) \right| + \sigma_k(T_0)(U_k - U_{k,0}) \leq \left| \sum_{j=1}^{k} \sigma_j(T_0)(U_j - U_{j,0}) \right| + \sigma_k(T_0)(U_k - U_{k,0}) \leq \sum_{j=1}^{k} \sigma_j(T_0)(U_j - U_{j,0} || U_j - U_{j,0} || \leq \sigma_k(T_0)(U_k - U_{k,0}) (60)
\]
We assume \( 2\min(\sigma_j(\Sigma_0) - \sigma_j+1(\Sigma_0) \) for all \( j \in [k] \), and apply the Theorem 6 of Jiang et al. [34]. Then for \( j \in [k] \),
\[
\|U_j - U_{j,0}\| \leq \min(2j, k) \|U_j - U_{j,0}\|_2 \leq 2\min(2j, k) \sigma_j(\Sigma) \leq 2\sigma_j(\Sigma).
\]
Since \( j \in [k-1] \),
\[
\sigma_j(T_0) - \sigma_j+1(T_0) = 1 - \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) - \sigma_j+1(\Sigma_0)}} = \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j+1(\Sigma_0) - 1}} \leq \frac{\eta \lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j+1(\Sigma_0) - 1}} \leq \frac{2\lambda}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j+1(\Sigma_0) - 1}} \leq \frac{2\lambda}{\eta \lambda} (58)
\]
therefore,
\[
\left| \sum_{j=1}^{k} \sigma_j(T_0)(u_j, u_j^T - u_{j,0}u_{j,0}^T) \right| \leq \sum_{j=1}^{k} \frac{2\eta \lambda \min(2j, k) \sigma_j(\Sigma)}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j(\Sigma_0) - 1}} + \frac{2\eta \lambda \sigma_j(\Sigma)}{\sqrt{\sigma_j(\Sigma_0) + \sigma_j(\Sigma_0) - 1}} \leq \frac{k}{\eta \lambda} \sigma_1(\Sigma) \leq \frac{2k}{\eta \lambda} \sigma_1(\Sigma) \leq \frac{2k}{\eta \lambda} \sigma_1(\Sigma) (59)
\]
On the other hand,
\[
\left| \sum_{j=1}^{k} \sigma_j(T_0)(u_j, u_j^T - u_{j,0}u_{j,0}^T) \right| \leq \sigma_k(T_0) = 1 - \frac{\eta \lambda}{\sqrt{\sigma_k(\Sigma_0)}} \leq 1 - \frac{\sqrt{\sigma_k+1(\Sigma_0)}}{\sqrt{\sigma_k(\Sigma_0)}} \leq \frac{2\lambda}{\eta \lambda} \sigma_1(\Sigma)
\]
Proof. In the \( t \)-th step, a standard proximal operator (see Liu et al. [39]) optimizes the following problem:
\[
\min \frac{1}{2\eta} \|W - C\|_F^2 + \lambda \|W\|_2^2,
\]
where \( C = \bar{W}^{(t-1)} \). By Theorem 5 of Liu et al. [39], denote the solution of the problem \( \bar{W}_{0,0}^{(t)} = S_{\lambda,0,0} \). Let \( S_0 \) be a diagonal matrix containing the diagonal elements of \( C \), and let \( \bar{S}_0 \) be a diagonal matrix and subject to \( \bar{S}_{i,0} = \Sigma_{t,0} \) for \( i = 1, \ldots, \min(d, m) \). \( S_{\lambda,0,0} \) is also a diagonal matrix and \( \lambda_{\lambda,0,0} = \max\{0, 1 - \eta \lambda/\Sigma_{t,0} \} \) for \( i = 1, \ldots, \min(d, m) \).

K.6 Proof of Lemma 3

Proof. In the \( t \)-th step, a standard proximal operator (see Liu et al. [39]) optimizes the following problem:
\[
\min \frac{1}{2\eta} \|W - C\|_F^2 + \lambda \|W\|_2^2,
\]
where \( C = \bar{W}^{(t-1)} \). By Theorem 5 of Liu et al. [39], denote the solution of the problem \( \bar{W}_{0,0}^{(t)} = S_{\lambda,0,0} \). Let \( S_0 \) be a diagonal matrix containing the diagonal elements of \( C \), and let \( \bar{S}_0 \) be a diagonal matrix and subject to \( \bar{S}_{i,0} = \Sigma_{t,0} \) for \( i = 1, \ldots, \min(d, m) \). \( S_{\lambda,0,0} \) is also a diagonal matrix and \( \lambda_{\lambda,0,0} = \max\{0, 1 - \eta \lambda/\Sigma_{t,0} \} \) for \( i = 1, \ldots, \min(d, m) \).
By Algorithm 2, $\mathbf{W}^{(t)} = \mathbf{U} \Sigma_0 \lambda \mathbf{U}^T \mathbf{C}$.

Then we analyse the bound of $\frac{1}{2\eta} \|\mathbf{W}^{(t)} - \mathbf{C}\|_F^2 + \lambda \|\mathbf{W}^{(t)}\|_{2.1}$.

First, similarly as in (51), we have

$$
\|\mathbf{W}^{(t)} - \mathbf{C}\|_F^2 = \text{tr}((\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)})(\mathbf{W}^{(t)} - \mathbf{C})^T) + \text{tr}((\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)})(\mathbf{W}_0^{(t)} - \mathbf{C})^T) = \sum_{j=1}^d (\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)})^T (\mathbf{W}^{(t)} - \mathbf{C})^T + \sum_{j=1}^d (\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)})^T (\mathbf{W}_0^{(t)} - \mathbf{C})^T \leq \|\mathbf{W}^{(t)} - \mathbf{C}\|_{2.1} \|\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)}\|_{2.1} + \|\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)}\|_{2.1} \|\mathbf{W}_0^{(t)} - \mathbf{C}\|_{2.1},
$$

(61)

where $(\cdot)^j$ denotes the $j$-th row vector of the enclosed matrix.

Denote $\mathbf{T} = S_{\eta \lambda} \mathbf{T}_0 = S_{\eta \lambda} \mathbf{0}$. Denote the indices of non-zero rows of $\mathbf{C}$ by $I_c = \{j : \mathbf{C}^j \neq \mathbf{0}\}$ and let $r_{c,s} = |I_c| \leq d$.

We have

$$
\|\mathbf{W}^{(t)} - \mathbf{C}\|_{2.1} = \left\| (\mathbf{T} - \mathbf{I}) \mathbf{C} \right\|_{2.1} = \sum_{j \in I_c} \left\| (\mathbf{T} - \mathbf{I}) \mathbf{C}_j \right\|_{2.1} = \sum_{j \in I_c} \sum_{i=1}^m \| (\mathbf{T} - \mathbf{I})_{ijj} \mathbf{C}_j \|_2^2 \leq \sum_{j \in I_c} \max_{i \in [d]} \| \mathbf{C}_j \|_2 \| (\mathbf{T} - \mathbf{I})_{ijj} \| \leq \left( \sum_{j \in I_c} \max_{i \in [d]} \| \mathbf{C}_j \|_2 \right) \sum_{j \in I_c} \| (\mathbf{T} - \mathbf{I})_{ijj} \| \| \mathbf{C}_j \|_2.
$$

(62)

Similarly,

$$
\|\mathbf{W}_0^{(t)} - \mathbf{C}\|_{2.1} \leq \sum_{j \in I_c} \max_{i \in [d]} \| \mathbf{C}_j \|_2 \| (\mathbf{I} - \mathbf{I})_{ijj} \| \| \mathbf{C}_j \|_2.
$$

(63)

On the other hand,

$$
\|\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)}\|_{2.1} = \|S_{\eta \lambda} \mathbf{C} - S_{\eta \lambda} \mathbf{0} \mathbf{C}\|_{2.1} = \max_{j \in [d]} \|S_{\eta \lambda} \mathbf{C} - S_{\eta \lambda} \mathbf{0} \mathbf{C}\|_2 \leq \max_{j \in [d]} \| \mathbf{C}_j \|_2 \sum_{j \in I_c} \|S_{\eta \lambda} \mathbf{C} - S_{\eta \lambda} \mathbf{0} \mathbf{C}\|_2.
$$

(64)

Denote $\Sigma_0 = \Sigma^{(t)} = \mathbf{C} \mathbf{C}^T$. Then we have for $j \in I_c$,

$$
|S_{\eta \lambda} \mathbf{C}_j - S_{\eta \lambda} \mathbf{0} \mathbf{C}_j| = \max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\Sigma_{jj} + |E_{jj}|}} \right) = \max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\Sigma_{jj} + |E_{jj}|}} \right).
$$

Case 1: $\eta \lambda > \sqrt{\Sigma_{jj} + |E_{jj}|}$. Then

$$
|S_{\eta \lambda} \mathbf{C}_j - S_{\eta \lambda} \mathbf{0} \mathbf{C}_j| = \max \left( 0, 1 - \frac{\eta \lambda}{\sqrt{\Sigma_{jj} + |E_{jj}|}} \right) \leq 1 = \frac{\eta \lambda}{\eta \lambda + \sqrt{|E_{jj}|}} \leq \frac{\sqrt{|E_{jj}|}}{\eta \lambda}.
$$

Case 2: $\eta \lambda \leq \sqrt{\Sigma_{jj} + |E_{jj}|}$. Then

$$
\left| S_{\eta \lambda} \mathbf{C}_j - S_{\eta \lambda} \mathbf{0} \mathbf{C}_j \right| = \frac{\eta \lambda}{\sqrt{\Sigma_{jj} + |E_{jj}|}} \leq \frac{\sqrt{|E_{jj}|}}{\eta \lambda}.
$$

(65)

Combining (61), (62), (63), (64) and (65), it follows that

$$
\|\mathbf{W}^{(t)} - \mathbf{C}\|_F^2 - \|\mathbf{W}^{(t)} - \mathbf{C}\|_F^2 \leq 2r_{c,s} \left( \max_{j \in [d]} \| \mathbf{C}^j \|_2^2 \right)^2 \left( \frac{k}{2\eta^2 \lambda^2} \right) \max_{j \in [d]} \| \mathbf{E}^j \|_2 + \frac{k}{\eta^2 \lambda^2} \max_{j \in [d]} \| \mathbf{E}^j \|_2.
$$

(66)

On the other hand,

$$
\|\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)}\|_{2.1} \leq \|\mathbf{W}^{(t)} - \mathbf{C}\|_{2.1} \leq \|\mathbf{W}^{(t)} - \mathbf{W}_0^{(t)}\|_{2.1}.
$$
K.7 Proof of Theorem 2

Proof. First, consider the case with no acceleration. We first use Proposition 1 of Schmidt et al. [49] by regarding procedures from Step 5 to Step 9 as approximation for the proximal operator in (8). Note that the norm clipping only bounds the parameter space and does not affect the results of Schmidt et al. [49]. Then for $\epsilon_t$ defined in Lemma 13 for $t \in [T]$, we have

$$E = \frac{2L}{m(T + 1)^2} \left( \| \hat{W}^{(0)} - W_* \|_F \right) + 2 \sum_{t=1}^{T} \left( \frac{2\epsilon_t}{T} \right)^2 + \sqrt{2} \sum_{t=1}^{T} \epsilon_t^2 \log \left( \epsilon_t + \frac{1}{2} \right) + 2 \epsilon_t^2 \sqrt{\epsilon_t^2 + \frac{1}{2}}$$

Meanwhile, by Lemma 13, we have

$$\epsilon_t = O \left( \frac{\kappa}{\epsilon_t} \right),$$

where $\kappa = k^2 \frac{\sqrt{ld \log d}}{\eta}$.

On the other hand, because

$$\epsilon = \sum_{t=1}^{T} \frac{(e^{\alpha t} - 1)\epsilon_t}{e^{\alpha t} + 1} + \sum_{t=1}^{T} 2\epsilon_t^2 \log \left( e + \frac{\sqrt{\epsilon_t^2 + \frac{1}{2}}}{\epsilon_t} \right),$$

then by Lemma 16, we have

$$\sum_{t=1}^{T} \epsilon_t^2 \leq \frac{\sqrt{2\epsilon}}{2 \log(e + \sqrt{2\epsilon})} = \frac{\epsilon}{\sqrt{\epsilon} + 2\epsilon}$$

Then by Lemma 17, we have

$$\sum_{t=1}^{T} \sqrt{\epsilon_t} = \begin{cases} O \left( \frac{k^{T+1/2}}{c_2(\alpha/2-1)\sqrt{2\alpha+1}} \right), & \alpha > 2; \\ O \left( \frac{k^{T/2}}{c_2(\alpha/2-1)\sqrt{2\alpha+1}} \right), & -1/2 < \alpha < 2; \\ O \left( \frac{k^{T-2-\alpha}}{c_2(\alpha/2-1)\sqrt{2\alpha-1}} \right), & \alpha < -1/2. \end{cases}$$

Because $\hat{W}^{(0)}$ is the result of the norm clipping, we have $\hat{W}^{(0)} \in W$.

Finally, taking $c_3 = \phi(\alpha)$ defined in (13) and $c_4 = \frac{2\epsilon(\alpha/2-1)^2}{c_2^2(\alpha/2-1)^2} \sqrt{2\alpha+1}$ under the assumption that $W_* \in W$, using Lemma 19, we have the results for the case with no acceleration.

For the accelerated case, we use Proposition 2 of Schmidt et al. [49] to have

$$E = \frac{2L}{m(T + 1)^2} \left( \| \hat{W}^{(0)} - W_* \|_F \right) + 2 \sum_{t=1}^{T} \left( \frac{2\epsilon_t}{T} \right)^2 + \sqrt{2} \sum_{t=1}^{T} \epsilon_t^2 \log \left( \epsilon_t + \frac{1}{2} \right) + 2 \epsilon_t^2 \sqrt{\epsilon_t^2 + \frac{1}{2}}$$

Then one can prove similarly combining Lemma 13, Lemma 16, Lemma 17 and Lemma 20.

K.8 Proof of Theorem 3

Proof. First, consider the case with no acceleration. We use Proposition 1 of Schmidt et al. [49] and prove similarly as in Appendix K.7, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 19.

For the accelerated case, we use Proposition 2 of Schmidt et al. [49] and prove similarly as in Appendix K.7, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 20.

K.9 Proof of Theorem 4

Proof. First, consider the case with no acceleration. We use Proposition 3 of Schmidt et al. [49] to have

$$E = \frac{Q_0^T}{m} \left( \| \hat{W}^{(0)} - W_* \|_F + 2 \sum_{t=1}^{T} \sum_{W} \sum_{D} \sum_{\mathcal{F}} \sum_{t=1}^{T} \sqrt{2\epsilon_t^2 + \frac{1}{2}} \right)$$

Then one can prove similarly as in Appendix K.7, using the assumption that $\hat{W}^{(0)} - W_* = O(K^2Lm)$, combining Lemma 13, Lemma 16, Lemma 17 and Lemma 21.

For the accelerated case, we use Proposition 4 of Schmidt et al. [49] to have

$$E = \frac{Q^T}{m} \left( \| \hat{W}^{(0)} - f(W_*) \|_F + 2 \sum_{t=1}^{T} \sum_{W} \sum_{D} \sum_{\mathcal{F}} \sum_{t=1}^{T} \sqrt{2\epsilon_t^2 + \frac{1}{2}} \right)$$

Then one can prove similarly as in Appendix K.7, using the assumption that $\hat{W}^{(0)} - f(W_*) = O(K^2Lm)$, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 22.

K.10 Proof of Theorem 5

Proof. First, consider the case with no acceleration. We use Proposition 3 of Schmidt et al. [49] and prove similarly as in Appendix K.9, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 21.

For the accelerated case, we use Proposition 4 of Schmidt et al. [49] and prove similarly as in Appendix K.9, using the assumption that $\hat{W}^{(0)} - f(W_*) = O(K^2Lm)$, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 22.

K.11 Proof of Theorem 6

Proof. Consider the bound in (12), whose logarithm is

$$\phi(\alpha) \log \left( \frac{kd \log d}{\sqrt{2\epsilon}} \right) + \sqrt{\epsilon} \log(e + \sqrt{2\epsilon}) + 2\epsilon$$

By Assumption 1, the first term dominates. Then we should firstly maximize $\phi(\alpha)$, which results in that $\phi(\alpha) = 2/5$ and $-1/2 < \alpha < 2$. Then since $\phi(\alpha)$ is now fixed, we maximize $(\alpha/2 - 1)^2 \sqrt{2\alpha + 1}$, which results in $\alpha = 0$. Results under other settings can be proved similarly.

K.12 Proof of Proposition 2

Proof. First, consider the method of Pathak et al. [47].

By Definition 7, an $(\epsilon, \delta)$-iterative DP-MTL algorithm with $T = 1$ should suffice for any set $S \subseteq \mathbb{R}^{d \times (m-1)}$ and all $i \in [m]$ that

$$\mathbb{P}(w^{(1)}_i) \in S \mid (W^{(0)}, D^m)$$

$$\leq \epsilon \mathbb{P}(w^{(1)}_i) \in S \mid (W^{(0)}, (D')^m) + \delta.$$
\(W^{(0)}\) and \((W')^{(0)}\), respectively. As such, we have for any set \(S \subseteq \mathbb{R}^{d \times (m-1)}\), all \(i \in [m]\) and \(\delta = 0\) that
\[
P(W^{(1)}_{[i]} \in S | W^{(0)}, D^m) 
\leq e^\epsilon P(W^{(1)}_{[i]} \in S | (W')^{(0)}, (D')^m) + \delta,
\]
which shows that the method of Pathak et al. [47] is an \((\epsilon, \delta)\)-iterative DP-MTL algorithm with \(T = 1\) and \(\delta = 0\).

Then we consider the method of Gupta et al. [29]. Assume a constant \(\delta \geq 0\) and the number of iterations \(T\) is given.

Taking \(T_0 = m, t = i\) for \(i \in [m]\), \(\delta_t = w_i, D^m = D^m, \epsilon\) for the \(\epsilon\) given in the method of Gupta et al. [29], using Theorem 1 of Gupta et al. [29], for \(t \in [T]\), we have in the \(t\)-th each iteration, for any set \(S \subseteq \mathbb{R}^{d \times (m-1)}\) and all \(i \in [m]\),
\[
P\left(W^{(t)} \in S | D^m\right) 
\leq e^\epsilon P\left(W^{(t)} \in S | (D')^m\right) + \delta,
\]
which suggests that for any set \(S \subseteq \mathbb{R}^{d \times (m-1)}\) and all \(i \in [m]\),
\[
P\left(W^{(t)}_{[i]} \in S | D^m\right) 
\leq e^\epsilon P\left(W^{(t)}_{[i]} \in S | (D')^m\right) + \delta,
\]
which is an \((\epsilon, \delta)\)-iterative DP-MTL algorithm.

### K.13 Proof of Proposition 3

Proof. Given an \((\epsilon, \delta)\)-iterative DP-MTL algorithm \(A(B)\), by Definition 7, we have for any set \(S \subseteq \mathbb{R}^{d \times (m-1)}\) that
\[
P\left(W^{(T)}_{[i]} \in S | \bigcap_{t=1}^{T} B_t = (W_t^{(t-1)}, D^m, \theta_{1:t-1})\right) 
\leq \exp(\epsilon) P\left(W^{(T)}_{[i]} \in S | \bigcap_{t=1}^{T} B_t = ((W')^{(t-1)}, (D')^m, \theta_{1:t-1})\right) + \delta.
\]

Furthermore, following the proof of the Group privacy (Lemma 5), shown by ?], for protecting the entire dataset, \(n\) data instances, of the \(i\)-th task, we construct a series of datasets, \(D_{(0)}^m, D_{(1)}^m, \ldots, D_{(n)}^m\), and let \(D_{(0)}^m = (D^m, D_{(n)}^m = (D')^m\) such that for \(j = 0, \ldots, n-1, D_{(j)}^m\) and \(D_{(j+1)}^m\) are two neighboring datasets that differ in one data instance. Let a series of model matrices, \(W_{(0)}, \ldots, W_{(n)}\), where \(W_{(0)} = W, W_{(n)} = W'\), be the input model matrices in those settings. Let a series of output objects \(\theta_{(0:1:t-1}, \ldots, \theta_{(n:1:t-1)}\), where \(\theta_{(0:1:t-1)} = \theta_{1:t-1}, \ldots, \theta_{(n:1:t-1)} = \theta_{1:t-1}\), be the output objects in those settings.

Then, we have
\[
P\left(W_{[i]}^{(T)} \in S | \bigcap_{t=1}^{T} B_t = (W_{(0)}^{(t-1)}, D_{(0)}^m, \theta_{(0:1:t-1)}^{(t-1)})\right) 
\leq \exp(n\epsilon) P\left(W_{[i]}^{(T)} \in S | \bigcap_{t=1}^{T} B_t = (W_{(1)}^{(t-1)}, D_{(1)}^m, \theta_{(1:1:t-1)}^{(t-1)})\right) + \delta
\]
\[
\vdots
\]
\[
\leq \exp(ne) P\left(W_{[i]}^{(T)} \in S | \bigcap_{t=1}^{T} B_t = (W_{(n)}^{(t-1)}, D_{(n)}^m, \theta_{(n:1:t-1)}^{(t-1)})\right) + n \exp(n\epsilon) \delta,
\]
which renders \(A\) as an \((ne, n \exp(n\epsilon) \delta)\)-iterative MP-MTL algorithm.

### APPENDIX L

**PROOF OF THE RESULTS IN APPENDIX B AND APPENDIX C**

#### L.1 Proof of Corollary 2

Proof. For simplicity, we omit the symbol \(B\) to denote the input in the conditional events in some equations.

Use Corollary 1 and Theorem 1. Given \(t \in [T]\), the algorithm \((P^{(t-1)}, \Sigma^{(1:t-1)}) \rightarrow (M^{(t)}, \Sigma^{(t)})\) is an \((\epsilon_t, 0)\)-differentially private algorithm, where \(M^{(t)} = US_n A^{(t)}\).

Now, for all \(i \in [m]\), applying the Post-Processing immunity (Lemma 4) for the mapping \(f : (M^{(t)}, P^{(t)}) \rightarrow P^{(t)}\), which does not touch any unperturbed sensitive information of the \(i\)-th task, we have for any set \(S \subseteq \mathbb{R}^{d \times (m-1)}\) that
\[
P\left(P^{(t)}_{[i]} \in S | P^{(t)}, \Sigma^{(1:t-1)}\right) 
\leq e^\epsilon P\left(P^{(t)}_{[i]} \in S | (P')^{(t)}, \Sigma^{(1:t-1)}\right),
\]
where \(P^{(t-1)}\) and \((P')^{(t-1)}\) differ only in the \(i\)-th column.
Then, because in the $t$-th iteration the mapping $\tilde{Q}^{(t-1)} \rightarrow \tilde{Q}^{(t-1)}$ is a deterministic STL algorithm, we have for any set $S \subseteq \mathbb{R}^{d \times (m-1)}$
that
\[
\mathbb{P}(\tilde{q}_{[t]}^{(t-1)} \in S | \tilde{Q}^{(t-1)})
= \mathbb{P}(\tilde{q}^{(t-1)}_{[t-1]} \in S | q_{[t]}^{(t-1)}, q^{(t-1)})
= \mathbb{P}(\tilde{q}^{(t-1)}_{[t-1]} \in S | q_{[t-1]}, q^{(t-1)})
= \mathbb{P}(q_{[t-1]}^{(t-1)} \in S | (Q^{(t-1)}) + 0,
\]
where $Q^{(t-1)}$ and $\tilde{Q}^{(t-1)}$ differ only in the $i$-th column.

Then applying Combination Lemma (Lemma 6), we have for any set $S \subseteq \mathbb{R}^{d \times (m-1)} \times \mathbb{R}^{d \times (m-1)}$
\[
\mathbb{P}((\tilde{p}^{(t)}_{[t]}, \tilde{q}^{(t)}_{[t-1]})) \in S | \mathbb{P}^{(t)}, \mathbb{S}^{(t-1)}, Q^{(t-1)}
\leq \epsilon_d \mathbb{P}((\tilde{p}^{(t)}_{[t]}, \tilde{q}^{(t)}_{[t-1]})) \in S | (P^{(t)}, \mathbb{S}^{(t-1)}, (Q^{(t-1)}) + 0,
\]
where $\mathbb{P}^{(t)}$ and $\mathbb{Q}^{(t)}$ differ only in the entire dataset of the $t$-th task.

Now, using Theorem 1, for $t = 1, \ldots, T$, we can take the $t$-th dataset $D_t = ((p_{1:t-1}, q_{[t]}^{(t-1)}), D_t), \ldots, (p_m^{(t-1)}, q_m^{(t-1)/D_m})$ and denote $\theta_t = (q_{[t]}^{(t-1)}, q_{[t]}^{(t-1)}, \mathbb{S}^{(t-1)}, \mathbb{S}^{(t-1)}, \mathbb{Q}^{(t-1)}, \mathbb{Q}^{(t-1)}, \mathbb{D}^{(t-1)}, \mathbb{D}^{(t-1)}) \subseteq C_t$. Given the fact that $\mathbb{P}^{(t)} \equiv \mathbb{P}^{(t)}$ and $\mathbb{Q}^{(t)} = \mathbb{Q}^{(t)}$ for all $t \in [T]$, we have for any set $S_t \subseteq C_t$ as
\[
\mathbb{P}(\theta_t \in S_t | \tilde{D}_t, \theta_{t-1})
\leq \epsilon_d \mathbb{P}(\theta_t \in S_t | \tilde{D}_t, \theta_{t-1}, )
\]
where $\tilde{D}_t$ and $\tilde{D}_t'$ are two adjacent datasets that differ in a single entry, the $i$-th “data instance” $(p_i, q_i^{(t-1)}, D_t = (X_t, Y_t))$, and
\[
\theta_{1:t-1} = \left\{ \emptyset, \theta_{1,1}, \ldots, \theta_{1,m}, \ldots, \theta_{t-1,1}, \ldots, \theta_{t-1,m} \right\},
\]
where $\mathcal{T} = \emptyset$ and $\theta_{1,1} = \emptyset$.

This renders the algorithm in the $t$-th iteration as an $(\epsilon_t, 0)$-differentially private algorithm.

Then, again by the Adaptive composition Lemma (Lemma 7), for all $t \in [m]$ and for any set $S_t \subseteq \mathcal{S}_t$, we have
\[
\mathbb{P}(\theta_{1:t-1} \in S_t | \tilde{D}_t, \theta_{1:t-1})
\leq \epsilon_d \mathbb{P}(\theta_{1:t-1} \in S_t | \tilde{D}_t, \theta_{1:t-1})
\]
where for all $t \in [T]$, $B_t$ denotes the input for the $t$-th iteration. Finally, for all $t \in [T]$, taking $\theta_t = (\theta_{1,1}, \ldots, \theta_{1,m})$ and given the fact that $\tilde{W}^{(t)} = \tilde{W}^{(t)} + \tilde{Q}^{(t)}$, we have for any set $S \subseteq \mathbb{R}^{d \times (m-1)} \times \mathbb{R}^{d \times (m-1)}$
\[
\mathbb{P}(\tilde{w}^{(1:T)}_{[t]} \in S_t | \tilde{B}_t = (W^{(t-1)} + \mathbb{D}^{(t-1)}, \theta_{1:t-1}))
\leq \epsilon_d \mathbb{P}(\tilde{w}^{(1:T)}_{[t]} \in S_t | \tilde{B}_t = (W^{(t-1)} + \mathbb{D}^{(t-1)}, \theta_{1:t-1}))
\]

where $(W^{(t-1)})$ are associated with the setting in which the $i$-th task has been replaced.

\textbf{L.2 Proof of Proposition 4}

\textit{Proof.} For simplicity, we omit the symbol $B$ used to denote the input in the conditional events in some equations.

First, the procedure from the 4-th step to the 5-th step is a standard output perturbation of Chaudhuri et al. [15]; thus, we have for all $t \in [m]$, for all neighboring datasets $D^{(m)}$ and $(D^{(m)})$ that differ in a single data instance of the $i$-th task, and for any $S \subseteq \mathbb{R}^{d}$
\[
P(w_{1:t-2}^{(t-1)} \in S | w_{1:t-2}^{(t-1)}), D^{(m)}, (D^{(m)})^{(t-1)},
\]
where $w_{1:t-2}^{(t-1)} = \emptyset$ when $t = 1$.

Then, because the mapping $(\tilde{W}^{(t-1)}, \mathbb{S}^{(t-1)} \rightarrow \theta_t = (\mathbb{S}^{(t-1)}), (D^{(m)}), \tilde{W}^{(t-1)}) \subseteq C_t$ does not touch any unperturbed sensitive information of $(X_t, Y_t, w_{1:t-1}^{(t-1)})$, the Post-Processing immunity Lemma (Lemma 4) can be applied such that we have for any set $S' \subseteq C_t$
\[
P(\theta_t \in S' | \tilde{W}^{(1:t-1)}, D^{(m)}, (D^{(m)})^{(t-1)},
\]

which means that
\[
P(\theta_t \in S' | D^{(m)}, \theta_{1:t-1})
\leq \epsilon_d \mathbb{P}(\theta_t \in S' | (D^{(m)})^{(t-1)}, \theta_{1:t-1}),
\]
where
\[
\theta_{1:t-1} = \left\{ \emptyset, \theta_{1,1}, \ldots, \theta_{1,m}, \ldots, \theta_{t-1,1}, \ldots, \theta_{t-1,m} \right\},
\]
where $\mathcal{T} = \emptyset$ and $\theta_{1,1} = \emptyset$.

Then, by the Adaptive composition Lemma (Lemma 7), we have for any set $S_t \subseteq \mathcal{S}_t$, we can apply such that we have for any set $S_t \subseteq \mathbb{R}^{d \times (m-1)} \times \mathbb{R}^{d \times (m-1)}$
\[
P(\theta_{1:T} \in S_t | \tilde{B}_t = (D^{(m)}, \theta_{1:t-1}))
\leq \epsilon_d \mathbb{P}(\theta_{1:T} \in S_t | (D^{(m)})^{(t-1)}, \theta_{1:t-1}) + \delta_d.
\]

Because the mapping $(\theta_t, D_{[t]} \\; w_{1:t-2}^{(t-1)} \rightarrow w_{1:t-2}^{(t-1)})$ does not touch any unperturbed sensitive information of $(X_t, Y_t, w_{1:t-1}^{(t-1)})$ for all $t \in [T]$ $(W^{(t-1)})$ is actually not used in the mapping), the Post-Processing immunity Lemma (Lemma 4) can be applied such that we have for any set $S_0 \subseteq \mathbb{R}^{d \times (m-1)} \times \mathbb{R}^{d \times (m-1)}$
\[
P(\tilde{w}^{(1:T)}_{[t]} \in S_0 | \tilde{B}_t = (D^{(m)}, \theta_{1:t-1}, W^{(t-1)}))
\leq \epsilon_d \mathbb{P}(\tilde{w}^{(1:T)}_{[t]} \in S_0 | (D^{(m)}, \theta_{1:t-1}, W^{(t-1)})) + \delta_d.
\]

where $(W^{(t-1)})$ is associated with the setting in which a single data instance of the $i$-th task has been replaced.

Therefore, Algorithm 5 is an $(\epsilon_d, \delta_d)$-iterative DP-MLT algorithm.
Next, for the conditional density of $\Sigma^{(t)}$ given $W^{(t-1)}$, we have
\[
p(\Sigma^{(t)} \mid W^{(t-1)}) = \int_{\tilde{W}^{(t-1)}} p(\Sigma^{(t)} \mid W^{(t-1)}, \tilde{W}^{(t-1)}) \, d\tilde{W}^{(t-1)}
\]
\[
p(W^{(t-1)} \mid W^{(t-1)}, \tilde{W}^{(t-1)}) = \int_{\tilde{W}^{(t-1)}} p(W^{(t-1)} \mid \tilde{W}^{(t-1)}) p(\tilde{W}^{(t-1)} \mid W^{(t-1)}) d\tilde{W}^{(t-1)}
\]
\[
p(W^{(t-1)} \mid W^{(t-1)}, \tilde{W}^{(t-1)}) = \int_{\tilde{W}^{(t-1)}} p(\Sigma^{(t)} \mid \tilde{W}^{(t-1)}) \prod_{t=1}^{m} p(\tilde{w}^{(t-1)} \mid w^{(t-1)}) \, d\tilde{W}^{(t-1)}.
\]

Because, for all $i \in [m]$ and some constant $c = \frac{\tilde{i}}{d p_s}$, we have
\[
p(\tilde{w}_i^{(t-1)} \mid w_i^{(t-1)}) \propto \exp\left(-c\|\tilde{w}_i^{(t-1)} - w_i^{(t-1)}\|_2^2\right),
\]
given $(W^j)^{(t-1)}$ such that for some $i \in [m]$, $(\tilde{w}_i^{(t-1)}) \neq w_i^{(t-1)}$, letting $(\tilde{w}_i^{(t-1)}) = \tilde{w}_i^{(t-1)} - w_i^{(t-1)} + (w_i^{(t-1)})$, we have
\[
\|\tilde{w}_i^{(t-1)} - (w_i^{(t-1)})\|_2 = \|\tilde{w}_i^{(t-1)} - w_i^{(t-1)}\|_2
\]
\[
= p(\tilde{w}_i^{(t-1)} \mid \tilde{w}_i^{(t-1)}) = p(\tilde{w}_i^{(t-1)} \mid w_i^{(t-1)}),
\]
and $d(\tilde{w}_i^{(t-1)}) = d\tilde{w}_i^{(t-1)}$.

Furthermore, based on the proof of Theorem 1 in Section K.3, we know that for neighboring matrices $W^{(t-1)}$ and $(\tilde{W}^{(t-1)})$ that differ in the $i$-th column, we have
\[
p(\Sigma^{(t)} \mid \tilde{W}^{(t-1)}) \leq \exp(\text{emp}_i) p(\Sigma^{(t)} \mid (\tilde{W}^{(t-1)})).
\]

Therefore, for all $i \in [m]$, given $(W^j)^{(t-1)}$ such that $(\tilde{w}_i^{(t-1)}) \neq w_i^{(t-1)}$, under the choice for $(\tilde{w}_i^{(t-1)})$, we have
\[
p(\Sigma^{(t)} \mid W^{(t-1)}) = \int_{W^{(t-1)}} p(\Sigma^{(t)} \mid \tilde{W}^{(t-1)}) \prod_{j=1}^{m} p(\tilde{w}_j^{(t-1)} \mid w_j^{(t-1)}) \, d\tilde{W}^{(t-1)}
\]
\[
\leq \int_{(W^j)^{(t-1)}} e^{\text{emp}_i} p(\Sigma^{(t)} \mid (\tilde{W}^{(t-1)})) p((\tilde{w}_i^{(t-1)} \mid (w_i^{(t-1)})) \prod_{j \in [m], j \neq i} p(\tilde{w}_j^{(t-1)} \mid w_j^{(t-1)}) \, d(\tilde{w}_i^{(t-1)})
\]
\[
= \int_{(W^j)^{(t-1)}} \exp(\text{emp}_i) p(\Sigma^{(t)} \mid (\tilde{W}^{(t-1)})) \, d(\tilde{w}_i^{(t-1)})
\]
\[
= \exp(\text{emp}_i) p(\Sigma^{(t)} \mid (\tilde{W}^{(t-1)})),
\]
which renders the mapping $W^{(t-1)} \rightarrow \Sigma^{(t)}$ as an (emp, $\delta$mp) - differentially private algorithm.

Then, according to the proof of Theorem 1 in Section K.3, Algorithm 5 is an (emp, $\delta$mp) - iterative MP-MLT algorithm.

**APPENDIX M**

**PROOF OF RESULTS IN APPENDIX D.1**

**M.1 Proof of Theorem 7**

*Proof.* First, consider the case with no acceleration. We first use Proposition 1 of Schmidt et al. [49] by regarding procedures from Step 5 to Step 9 as approximation for the proximal operator in (8). Note that the norm clipping only bounds the parameter space and does not affect the results of Schmidt et al. [49]. Then for $\epsilon$, defined in Lemma 13 for $i \in \{T\}$, we have
\[
\mathcal{E} = \frac{2L}{m(T + 1)^2} \left(\|\tilde{W}^{(0)} - W_{\ast}\|_F + 2 \sum_{t=1}^{T} \sqrt{2\epsilon_t} + \sqrt{\sum_{t=1}^{T} \epsilon_t^2} \right)^2.
\]

Meanwhile, by Lemma 13, we have
\[
\epsilon_t = O\left(\frac{\kappa}{\epsilon_t}\right),
\]
where $\kappa = \frac{\kappa^2}{\sqrt{m} d L \log d}$.

On the other hand, let
\[
c_1 = \epsilon = \sum_{t=1}^{T} \epsilon_t,
\]
then by Lemma 17, we have
\[
\sum_{t=1}^{T} \sqrt{\epsilon_t} = \begin{cases} 0 & \alpha > 2; \\ O\left(\frac{\kappa^2 \epsilon_t}{c_1 \sqrt{c_1}}\right) & -1 < \alpha < 2; \\ O\left(\frac{\kappa^2 \epsilon_t}{c_1 \sqrt{c_1}}\right) & \alpha < -1,
\end{cases}
\]

Because $\tilde{W}^{(0)}$ is the result of the norm clipping, we have $\tilde{W}^{(0)} \in W$.

Finally, taking $c_3 = \phi(\alpha)$ defined in (13) and $c_4 = \frac{\epsilon}{c_2 (\alpha^2/2 - 1)^{(\alpha + 1)}}$, under the assumption that $W_{\ast} \in W$, using Lemma 19, we have the results for the case with no acceleration.

For the accelerated case, we use Proposition 2 of Schmidt et al. [49] to have
\[
\mathcal{E} = \frac{2L}{m(T + 1)^2} \left(\|\tilde{W}^{(0)} - W_{\ast}\|_F + 2 \sum_{t=1}^{T} \sqrt{2\epsilon_t} + \sqrt{\sum_{t=1}^{T} \epsilon_t^2} \right)^2.
\]

Then one can prove similarly combining Lemma 13, Lemma 16, Lemma 17 and Lemma 20.

**M.2 Proof of Theorem 8**

*Proof.* First, consider the case with no acceleration. We use Proposition 1 of Schmidt et al. [49] and prove similarly as in Appendix M.1, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 19.

For the accelerated case, we use Proposition 2 of Schmidt et al. [49] and prove similarly as in Appendix M.1, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 20.

**M.3 Proof of Theorem 9**

*Proof.* First, consider the case with no acceleration. We use Proposition 3 of Schmidt et al. [49] to have
\[
\mathcal{E} = \frac{Q_0 T}{\sqrt{m}} \left(\|\tilde{W}^{(0)} - W_{\ast}\|_F + 2 \sum_{t=1}^{T} Q_0 \epsilon_t \sqrt{2\epsilon_t} \right)^2.
\]

Then one can prove similarly as in Appendix M.1, combining Lemma 13, Lemma 16, Lemma 17 and Lemma 21.
For the accelerated case, we use Proposition 4 of Schmidt et al. [49] to have
\[
\varepsilon = \frac{\langle Q, 0 \rangle^T}{m} \left( \sqrt{2(f(W^{0})) - f(W_{\ast})} + 2 \sqrt{\sum_{t=1}^{T} \varepsilon_t(Q_0)^{-1}} \right) + \sum_{t=1}^{T} \varepsilon_t(Q_0)^{-1}.
\]

Then one can prove similarly as in Appendix M.1, using the assumption that \(f(W^{0}) - f(W_{\ast}) = O(K^2 L m)\), combining Lemma 13, Lemma 16, Lemma 17 and Lemma 22.

\[\Box\]

M.4 Proof of Theorem 10

Proof. First, consider the case with no acceleration. We use Proposition 3 of Schmidt et al. [49] and prove similarly as in Appendix K.9, combining Lemma 14, Lemma 16, Lemma 17 and Lemma 21.

For the accelerated case, we use Proposition 4 of Schmidt et al. [49] and prove similarly as in Appendix K.9, using the assumption that \(f(\hat{W}^{0}) - f(\hat{W}_{\ast}) = O(K^2 L m)\), combining Lemma 14, Lemma 16, Lemma 17 and Lemma 22.

\[\Box\]

M.5 Proof of Theorem 11

Proof. Consider the bound in (25). First, by Assumption 1, \(\varepsilon\) is minimized by maximizing \(\phi(\alpha)\) and \((\alpha/2 - 1)^2 |\alpha + 1|\), which are maximized simultaneously when \(\alpha = 0\). Results under other settings can be proved similarly.

APPENDIX N

PROOF OF RESULTS IN APPENDIX D.2

Proof. Results in this settings are the corollaries of Theorem 2, Theorem 3, Theorem 4, Theorem 5 and Theorem 6, respectively, replacing the term \(\sqrt{\log(e + \epsilon/\delta)}\) with the term \(\sqrt{\log(1/\delta)}\) by Lemma 16.

\[\Box\]

APPENDIX O

PROOF OF RESULTS IN APPENDIX I

O.1 Proof of Lemma 8

Proof. For simplicity, we omit the symbol \(B\) in the conditional events.

Because \(\hat{W} = A_{\text{AMP}}(W, X^m, y^m)\) is an \((\epsilon, \delta)\)-non-iterative MP-MTL algorithm, by Definition 5, we have for \(i \in [m]\) and for any set \(S' \subseteq \mathbb{R}^{d_x (m-1)}\),
\[
P(\hat{w}_{[-i]} \in S' \mid w_{[-i]}, D_{[-i]}, w_i, D_i) 
\leq e^{\delta} P(\hat{w}_{[-i]} \in S_1 \mid w_{[-i]}, D_{[-i]}, w_i', D_i') + \delta.
\]

In the following, we follow the proof of Theorem B.1 of Dwork et al. [20].

For any \(C_1 \subseteq \mathbb{R}^{d_x (m-1)}\), define
\[
\mu(C_1) = P(\hat{w}_{[-i]} \in C_1 \mid w_{[-i]}, D_{[-i]}, w_i, D_i) - e^{\delta} P(\hat{w}_{[-i]} \in C_1 \mid w_{[-i]}, D_{[-i]}, w_i', D_i') \geq \mu(C_1) \leq \delta
\]
and then, \(\mu\) is a measure on \(C_1\) and \(\mu(C_1) \leq \delta\) by (68). As a result, we have for all \(s_1 \in C_1\),
\[
P(\hat{w}_{[-i]} \in s_1 \mid w_{[-i]}, D_{[-i]}, w_i, D_i) 
\leq e^{\delta} P(\hat{w}_{[-i]} \in s_1 \mid w_{[-i]}, D_{[-i]}, w_i', D_i') + \mu(ds_1).
\]

As such, for any set \(S \subseteq \mathbb{R}^{d_x (m-1)} \times \mathbb{R}^{d_x (m-1)}\) and \(S_1\), which denotes the projection of \(S\) onto \(C_1\),
\[
P((\hat{w}_{[-i]}', \hat{w}_{[-i]}) \in S \mid w_{[-i]}, D_{[-i]}, w_i, D_i) 
\leq \int_{S_1} P((\hat{w}_{[-i]}, s_1) \in S \mid \hat{w}_{[-i]}, w_{[-i]}, D_{[-i]}, w_i, D_i) \mu(ds_1) 
\leq \int_{S_1} P((\hat{w}_{[-i]}, s_1) \in S \mid \hat{w}_{[-i]}, w_{[-i]}, D_{[-i]}, w_i, D_i) 
\left[ e^{\delta} P(\hat{w}_{[-i]} \in s_1 \mid w_{[-i]}, D_{[-i]}, w_i', D_i') + \mu(ds_1) \right] 
= \int_{S_1} P((\hat{w}_{[-i]}, s_1) \in S \mid \hat{w}_{[-i]}, w_{[-i]}, D_{[-i]}, w_i', D_i') + \mu(S_1)
= \int_{S_1} P((\hat{w}_{[-i]}, s_1) \in S \mid \hat{w}_{[-i]}, w_{[-i]}, D_{[-i]}, w_i', D_i') + \mu(S_1)
\leq e^{\delta} P((\hat{w}_{[-i]}, \hat{w}_{[-i]}) \in S \mid w_{[-i]}, D_{[-i]}, w_i', D_i') + \delta.
\]

The second equality uses the independence of the learning process for \(w_{[-i]}\) given \((\hat{w}_{[-i]}, D_{[-i]})\).

The procedure is similar to proving that the algorithm \(A_{\text{STL}+\text{mp}}\) that first uses a deterministic STL algorithm \(A_{\text{st}}\) before applying \(\text{Amp}\) is also an \((\epsilon, \delta)\) - non-iterative MP-MTL algorithm.

For a deterministic STL algorithm \(\hat{W} = A_{\text{st}}(W, X^m, y^m)\), for \(i \in [m]\), by the independence of the learning process for \(\hat{w}_{[-i]}\) given \((w_{[-i]}, D_{[-i]})\), we have
\[
p(w_{[-i]} \mid w_{[-i]}, D_{[-i]}, w_i, D_i) = p(w_{[-i]} \mid w_{[-i]}, D_{[-i]}, w_i', D_i').
\]

Because the STL algorithm is deterministic, when the input is given, it is reasonable to assume that the output is given. As such, we also have for \(i \in [m]\),
\[
p(\cdot \mid w_i, D_i) = p(\cdot \mid \hat{w}_i, D_i)
\]
\[
p(\cdot \mid w_{[-i]}, D_{[-i]}) = p(\cdot \mid \hat{w}_{[-i]}, D_{[-i]}).
\]

Then, for an \((\epsilon, \delta)\)-non-iterative MP-MTL algorithm \(\hat{W} = A_{\text{AMP}}(W, X^m, y^m)\), by Definition 5, we have for \(i \in [m]\) and for any set \(S' \subseteq \mathbb{R}^{d_x (m-1)}\),
\[
P((\hat{w}_{[-i]}', \hat{w}_{[-i]}) \in S' \mid \hat{w}_{[-i]}, D_{[-i]}, w_i, D_i) 
\leq e^{\delta} P((\hat{w}_{[-i]}, \hat{w}_{[-i]}) \in S' \mid \hat{w}_{[-i]}, D_{[-i]}, w_i', D_i') + \delta,
\]

where \(\hat{w}_i'\) can be replaced with \(w_i'\) because Definition 5 allows replacing \(\hat{w}_i\) with any different model.
As such,

\[
P((\tilde{w}_{[-1]}, \tilde{w}_{[-1]})) \in S | w_{[-1]}, D_{[-1]}, w_i, D_i)
\]

\[
\leq \int_{S_1} \mathbb{P}(w_{[-1], s_1}) \in S | \tilde{w}_{[-1], w_{[-1]}, D_{[-1]}, w_i, D_i)
\]

\[
P(w_{[-1]} \in d_{s_1} | w_{[-1]}, D_{[-1]}, w_i, D_i)
\]

\[
= \int_{S_1} \mathbb{P}(w_{[-1], s_1}) \in S | \tilde{w}_{[-1], D_{[-1]}, w_i, D_i)
\]

\[
P(w_{[-1]} \in d_{s_1} | w_{[-1]}, D_{[-1]}, D_i)
\]

\[
\leq \int_{S_1} \left( \epsilon P((\tilde{w}_{[-1], s_1}) \in S | \tilde{w}_{[-1], D_{[-1]}, w_{i}', D_i')
\]

\[
+ \delta \right) \bigwedge \mathbb{P}(w_{[-1]} \in d_{s_1} | w_{[-1]}, D_{[-1], w_{i}, D_i}))
\]

\[
\leq \int_{S_1} \left( \epsilon P((\tilde{w}_{[-1], s_1}) \in S | \tilde{w}_{[-1], D_{[-1]}, w_{i}', D_i')
\]

\[
+ \delta \right) \bigwedge \mathbb{P}(w_{[-1]} \in d_{s_1} | w_{[-1]}, D_{[-1], w_{i}, D_i}))
\]

\[
= \epsilon P((\tilde{w}_{[-1], s_1}) \in S | \tilde{w}_{[-1], D_{[-1]}, w_{i}', D_i')
\]

\[
+ \delta
\]

The second inequality uses (71), the first equality uses (70), and the second equality uses (69).

\[\square\]

### O.2 Proof of Lemma 9

**Proof.** For simplicity, we omit the symbol \( S \) to denote the input in the conditional events in some equations.

First, because for all \( t \in [T] \), \( \tilde{W}^{(i)} = A_{\text{mp}}(W^{(-1)}, X^m, y^m) \) is an \((\epsilon_i, \delta_i)\)-non-iterative MP-MTL algorithm and because for all \( i \in [m] \), \( w^{(i)} = A_{\text{stl}}(\tilde{w}^{(i)}, x, y) \) is a deterministic STL algorithm for the \( i \)-th task, then by the proof of Lemma 8, we have that the mapping \((X^m, y^m, W^{(t-1)}) \rightarrow (\tilde{W}^{(i)}, W^{(i)}) \) is an \((\epsilon_i, \delta_i)\)-non-iterative MP-MTL algorithm for all \( t \in [T] \). In other words, for all \( i \in [m] \), we have for any set \( S \subseteq \mathbb{R}^{d \times (m-1)} \times \mathbb{R}^{d \times (m-1)} \) that

\[
P((w^{(i)}_{[-1]}, w^{(i)}_{[-1]})) \in S | w_{[-1]}, D_{[-1], w_i^{(t-1)}, D_i})
\]

\[
\leq \epsilon P((w^{(i)}_{[-1]}, w^{(i)}_{[-1]})) \in S | w_{[-1]}, D_{[-1], (w_i^{(t-1)}, D_i')}
\]

\[
+ \delta_i
\]

(72)

Then, for \( t = 1, \ldots, T \), take the \( t \)-th dataset \( \tilde{D}_t = \{(w^{(t-1)}_{[-1]}, D_{1} = (x_1, y_1)), \ldots, (w^{(t-1)}_{[-1]}, D_{m} = (x_m, y_m))\} \), i.e., treat \((w^{(t-1)}_{[-1]}, D_{i} = (x_i, y_i))\) as the \( i \)-th data instance of the dataset \( D_i \) for all \( i \in [m] \). For all \( t \in [T] \) and for all \( t \in [T] \), take the \( t \)-th output \( \theta_{t, i} = (\tilde{w}^{(i)}_{[-1]}, \tilde{w}^{(i)}_{[-1]}) \). By (72), we have for all \( t \in [T] \) for all \( i \in [m] \), and for any set \( S_t \subseteq \mathbb{R}^{d \times (m-1)} \times \mathbb{R}^{d \times (m-1)} \) that

\[
P(\theta_{t, i} \in S_t | \tilde{D}_t) \leq \epsilon \mathbb{P}(\theta_{t, i} \in S_t | \tilde{D}_t') + \delta_i
\]

where \( \tilde{D}_t \) and \( \tilde{D}_t' \) are two adjacent datasets that differ in a single entry, the \( i \)-th data instance \((w^{(t-1)}_{[-1]}, D_{i} = (x_i, y_i))\), which renders the algorithm in the \( t \)-th iteration an \((\epsilon_t, \delta_t)\)-differentially private algorithm. As such, by the *Adaptive composition* Lemma