Federated Learning with Sparsification-Amplified Privacy and Adaptive Optimization

Rui Hu, Yanmin Gong* and Yuanxiong Guo
The University of Texas at San Antonio
{rui.hu, yanmin.gong, yuanxiong.guo}@utsa.edu

Abstract
Federated learning (FL) enables distributed agents to collaboratively learn a centralized model without sharing their raw data with each other. However, data locality does not provide sufficient privacy protection, and it is desirable to facilitate FL with rigorous differential privacy (DP) guarantee. Existing DP mechanisms would introduce random noise with magnitude proportional to the model size, which can be quite large in deep neural networks. In this paper, we propose a new FL framework with sparsification-amplified privacy. Our approach integrates random sparsification with gradient perturbation on each agent to amplify privacy guarantee. Since sparsification would increase the number of communication rounds required to achieve a certain target accuracy, which is unfavorable for DP guarantee, we further introduce acceleration techniques to help reduce the privacy cost.

We rigorously analyze the convergence of our approach and utilize Renyi DP to tightly account the end-to-end DP guarantee. Extensive experiments on benchmark datasets validate that our approach outperforms previous differentially-private FL approaches in both privacy guarantee and communication efficiency.

1 Introduction
Federated learning (FL) is a new distributed learning paradigm that enables multiple agents to collaboratively learn a shared model under the orchestration of the cloud without sharing their local data [McMahan et al., 2017]. By keeping data locally, FL is advantageous in privacy and communication efficiency compared with traditional centralized learning paradigm. However, recent inference attacks [Fredrikson et al., 2015; Shokri et al., 2017] show that the local model updates shared between agents could also lead to privacy leakage, and it is desirable to protect the shared local model updates with rigorous privacy guarantee.

To address this issue, several privacy-preserving frameworks have been proposed, among which differential privacy (DP) [Dwork and Roth, 2014] has become the de-facto standard due to its rigorous privacy guarantee and effectiveness in data analysis tasks [Abadi et al., 2016; Hu et al., 2020; Huang et al., 2019; Guo and Gong, 2018; Gong et al., 2016]. General DP mechanisms, such as Gaussian or Laplacian mechanism, rely on the injection of carefully calibrated noise to the output of an algorithm directly. This poses new challenges to achieving DP in FL because the added noise is proportional to the model size which can be very large with modern deep learning neural networks (e.g., millions of model parameter), resulting in significantly degraded model accuracy. Under the local DP setting where the cloud is not fully trusted, the challenges become more prominent as all the local updates shared with the cloud need to be protected.

Existing works on differentially-private machine learning either consider centralized DP [Abadi et al., 2016], or rely on costly techniques such as secure multi-party computation [Truex et al., 2019] and shuffling via anonymous channels [Liu et al., 2020; Erlingsson et al., 2019] to remove the requirement of a trusted cloud and improve the model accuracy in local DP. How to better balance the model accuracy and privacy protection in FL efficiently remains largely unknown.

In this paper, we propose a novel differentially-private FL scheme, called Fed-SPA, to provide strong privacy guarantee in the local DP setting while maintaining high model accuracy. In light of the observation that local model updates in FL are largely sparse, we design a sparsification-coded DP mechanism that integrates gradient perturbation with random sparsification to amplify the privacy guarantee with little sacrifice on the model accuracy. Random sparsification transforms a large vector into a sparse one by keeping only a random subset of coordinates while setting other coordinates to zeros. As we will show in this paper, random sparsification not only introduces randomness to the scheme, but also reduces the sensitivity of the shared model updates with respect to raw data, thus resulting in smaller privacy loss at every communication round. Furthermore, as sparsification can slow down the convergence speed of learning algorithms and increase the total number of communication rounds, we propose to further reduce the end-to-end privacy loss by using convergence acceleration techniques to offset the negative impact of sparsification. We provide theoretical analysis to demonstrate the convergence of our scheme and rigorous privacy guarantee.

The main contributions of this paper are summarized be-
• We propose to use sparsification for privacy amplification in FL while also improving communication efficiency. Previous works that consider both communication efficiency and DP treat them as two separate goals and solve them in an uncoordinated manner. Unlike previous approaches, we focus on the interplay of those two goals and aim to kill two birds with one stone in this paper, i.e., use sparsification as a tool to improve DP and achieve communication efficiency at the same time. We theoretically analyze the impacts of sparsification on the utility-privacy trade-off and design a sparsification-coded DP mechanism for FL that provides stronger privacy guarantee with the same amount of random noise.

• To further improve the utility-privacy trade-off, we integrate the sparsification-coded DP mechanisms with convergence acceleration techniques, which can reduce the number of required communication rounds and ensure faster convergence. Specifically, we adapt an acceleration strategy similar to that of Adam optimizer to the FL setting and design an adaptive aggregation strategy on the cloud to reduce the number of communication rounds. The resulting scheme called Fed-SPA provides a better utility-privacy trade-off than the state-of-art differentially private FL methods.

• We empirically evaluate our scheme on several benchmark datasets. The experiment results show that Fed-SPA significantly boosts the model accuracy, and at the same time saves more than 80% of the bandwidth cost compared to the state-of-art approaches under the same DP guarantee.

It is worth noting that our scheme aims to improve the utility-privacy trade-off while achieving communication efficiency. This distinguishes our paper from previous studies on communication efficient and differentially-private distributed learning that focus on ensuring privacy protection and achieving communication efficiency at the same time. For example, cpSGD [Agarwal et al., 2018] is a modified distributed SGD scheme which is private and communication-efficient via gradient quantization and binomial mechanism. However, since quantization does not provide any privacy amplification effects as sparsification, the utility-privacy trade-off is not improved in that approach.

2 Preliminaries

DP is a rigorous notion of privacy that has become the de-facto standard for measuring privacy risk. In the context of FL, DP ensures that the exchanged model updates are nearly the same regardless of the usage of a data sample. In this paper, we consider a relaxed DP definition called Rényi differential privacy (RDP), which is strictly stronger than $(\epsilon, \delta)$-DP for $\delta > 0$ and allows tighter composition analysis.

**Definition 1** ($(\alpha, \rho)$-RDP). Given a real number $\alpha \in (1, +\infty)$ and privacy parameter $\rho \geq 0$, a randomized mechanism $\mathcal{M}$ satisfies $(\alpha, \rho)$-RDP if for any two neighboring datasets $D, D'$ that differs in one record, the Rényi $\alpha$-divergence between $\mathcal{M}(D)$ and $\mathcal{M}(D')$ satisfies

$$D_\alpha[\mathcal{M}(D)\|\mathcal{M}(D')] := \frac{1}{\alpha - 1}\log \mathbb{E} \left[ \left( \frac{\mathcal{M}(D)}{\mathcal{M}(D')} \right)^\alpha \right] \leq \rho,$$

where the expectation is taken over the output of $\mathcal{M}(D')$.

**Lemma 1** (RDP Composition [Mironov, 2017]). If $\mathcal{M}_3$ satisfies $(\alpha, \rho_1)$-RDP and $\mathcal{M}_2$ satisfies $(\alpha, \rho_2)$-RDP then their composition $\mathcal{M}_1 \circ \mathcal{M}_2$ satisfies $(\alpha, \rho_1 + \rho_2)$-RDP.

**Lemma 2** (Gaussian Mechanism [Mironov, 2017]). Let $h : D \rightarrow \mathbb{R}^d$ be a vector-valued function over datasets. The Gaussian mechanism $\mathcal{M} = h(D) + b$ with $b \sim N(0, \sigma^2 I_d)$ satisfies $(\alpha, \alpha \phi(h)/2\sigma^2)$-RDP, where $\phi(h)$ is the $L_2$ sensitivity of $h$ defined by $\phi(h) = \sup_{D, D'} \| h(D) - h(D') \|_2$ with $D, D'$ being two neighboring datasets in $\mathcal{D}$.

3 Fed-SPA: Federated Learning with Sparsification-Amplified Privacy and Adaptive Optimization

**Notation.** We use $[n]$ to denote the set of integers $\{1, 2, \ldots, n\}$ with any positive integer $n$, and $[i]$ to denote the $j$-th coordinate of a vector. Let $\|\cdot\|$ be the $\ell_2$ vector norm.

3.1 Problem Formulation

A typical FL system consists of $n$ agents and a central server (e.g., the cloud). Each agent $i \in [n]$ has a local dataset with $m$ data samples, and all agents collaboratively train a global model $\theta$ on the collection of their local datasets under the orchestration of the central server. The agents in FL aim to find the optimal global model $\theta$ by solving the following empirical risk minimization problem while keeping their data locally:

$$\min_{\theta \in \mathbb{R}^d} f(\theta) := \frac{1}{n} \sum_{i=1}^{n} f_i(\theta),$$

where $f_i(\theta) = \mathbb{E}_{z \sim D_i} [l_i(\theta; z)]$ represents the loss function of $i$-th agent (possibly non-convex), $D_i$ is the data distribution of $i$-th agent, and $z$ represents a data sampled from $D_i$. For $i \neq j$, the data distributions $D_i$ and $D_j$ may be very different.

**Threat Model.** Before elaborating the proposed solutions, we first define the following threat model considered in this paper. The adversary considered here can be the “honest-but-curious” aggregation server or agents in the system. The aggregation server will honestly follow the designed training protocol but are curious about agents’ private data and may infer it from the shared messages. Furthermore, some agents can collude with the aggregation server or each other to infer private information about a specific victim agent. Besides, the adversary could also be the passive outside attacker. These attackers can eavesdrop all shared messages in the execution of the training protocol but will not actively inject false messages into or interrupt message transmissions.

3.2 Classic FL Algorithm: Federated Averaging

As the most widely-used algorithm in the FL setting, Federated Averaging (FedAvg) [McMahan et al., 2017] solves (1) by selecting and distributing the current global model to a
subset of agents, running multiple steps of SGD in parallel on
the selected agents, and then aggregating the model updates
from those agents to improve the global model iteratively.
Specifically, FedAvg involves $T$ communication rounds, and
each round consists of four stages: First, at the beginning of
round $t \in \{0, \ldots, T-1\}$, the server selects a subset of agents
$\mathcal{W} \subseteq \{n\}$ to participate and sends them the latest global model
$\theta_t$. Second, each agent $i \in \mathcal{W}$ initializes its local model $\theta_i^{t,0}$
to be the global model $\theta_t$ and then performs $\tau$ iterations of SGD on its local dataset as follows:

$$
\theta_i^{t,s+1} = \theta_i^{t,s} - \eta_i g_i^{t,s}, \quad s = 0, 1, \ldots, \tau - 1
$$

where $\eta_i$ is the local learning rate. Here, $g_i^{t,s} := (1/B) \sum_{z \in \xi_i^{t,s}} \nabla f_i(\theta_i^{t,s}, z)$ represents the stochastic gradient computed on a mini-batch $\xi_i^{t,s}$ of $B$ samples, which is unbi-
ased estimate of $\nabla f_i(\theta_i^{t,s})$. Third, each agent $i \in \mathcal{W}$ uploads the final local model update $\theta_i^{t,\tau} - \theta_t$ to the server. Fourth,
the server aggregates the local model updates from all particip-
ating agents and improves the global model as

$$
\theta_{t+1} = \theta_t + \frac{1}{|\mathcal{W}|} \sum_{i \in \mathcal{W}} (\theta_i^{t,\tau} - \theta_t).
$$

The same procedure repeats for the next round.

**Privacy and Communication Drawbacks.** Although Fe-
dAvg avoids the direct information leakage by keeping data
locally, the intermediate updates exchanged during the col-
laboration process such as $\theta_i^{t,\tau} - \theta_t$ and $\theta_t$ could still leak private information about the local data as demonstrated in recent advanced attacks such as model inversion attacks [Fredrikson et al., 2015] and membership attacks [Shokri et al., 2017]. Furthermore, in FedAvg, agents need to repeatedly upload local model updates (i.e., $\theta_i^{t,\tau} - \theta_t$) of large size (e.g., millions of model parameters for modern deep neural network models) to the server and download the newly-updated global model (i.e., $\theta_t$) from the server in order to learn an ac-
curate global model (e.g., $\approx 1000$ rounds for running CNN on
MINIST dataset or $\approx 4000$ for LSTM on Shakespeare dataset
to reach 99% accuracy [McMahan et al., 2017]). Since the privacy loss is proportional to the model dimension and the number of communication rounds, the size of added DP noise could be very large in order to provide a strong local DP guarantee, which will degrade the model accuracy heavily. Besides, as the bandwidth between the server and agents could be rather limited in practice (e.g., wireless connection between the cloud and smartphones), especially for uplink transmis-
sions, the overall communication cost could be very high. The above drawbacks motivate us to develop a new privacy-preserving and communication-efficient FL scheme.

### 3.3 Proposed Fed-SPA Algorithm

In this subsection, we present Fed-SPA, our proposed FL
scheme with the goal of improving user privacy protection
and also communication efficiency while maintaining high
model accuracy. To ensure easy integration into existing
packages/systems, Fed-SPA follows the same overall struc-
ture of FedAvg but differs in the following two key aspects:

1) local models are updated at each agent using a variant
of SGD, where the gradients are perturbed by our proposed
sparsification-coded DP mechanism; and 2) the global model
is updated adaptively instead of simple averaging to acceler-
ate convergence at the server. The entire process of Fed-SPA
is summarized in Algorithm 1.

**User-Side Sparsification-Coded DP Mechanism.** To
address privacy and communication aspects simultaneously, we
choose to use a sparsification-coded DP mechanism, which inte-
grates Gaussian mechanism and sparsification to reduce the
privacy loss of each local iteration and the size of transmitted
local model updates at each communication round. Spe-
cifically, we use the $\text{rand}_k$ sparsifier to reduce the message size
by a factor of $d/k$, which is defined as follows:

**Definition 2** ($\text{rand}_k$ Sparsifier). For parameter $k \in [d]$, the
operator $\text{rand}_k : \mathbb{R}^d \times \Omega_k \rightarrow \mathbb{R}^d$ is defined for a vector
$\mathbf{x} \in \mathbb{R}^d$ as

$$
[\text{rand}_k(\mathbf{x}, \omega)]_j = \left\{ \begin{array}{ll}
|\mathbf{x}|_j, & \text{if } j \in \omega, \\
0, & \text{otherwise,}
\end{array} \right.
$$

where $\Omega_k = \{1, \ldots, k\}$ denotes the set of all $k$-element subsets
of $[d]$. We omit the second argument whenever it is chosen
uniformly at random, i.e., $\omega \sim_{\text{unif}} \Omega_k$.

With the $\text{rand}_k$ sparsifier, our sparsification-coded DP mechanism works as follows: at communication round $t$, each selected agent $i \in \mathcal{W}$ first generates its own sparsifier $\text{rand}_k(\cdot)$ by randomly sampling a set of $k$ active coordinates $\omega_i^t$ before performing $\tau$ SGD updates, and then, at $s$-th local
iteration, perturbs and sparsifies the stochastic gradient using
Gaussian noise and the generated sparsifier $\text{rand}_k(\cdot)$. We use
the same sparsifier (with active set $\omega_i^t$) across all local itera-
tions of communication round $t$ on agent $i$ so that the trans-
mitted model update $(\theta_i^{t,\tau} - \theta_t)$ is still a sparse vector (which
has active coordinates $\omega_i^t$), preserving the communication efficiency
benefit of sparsification. Let $p = k/d$ represent the compression ratio, the update rule at each agent is:

$$
\theta_i^{t,s+1} = \theta_i^{t,s} - \eta_i S_i^t(g_i^{t,s} + b_i^{t,s}),
$$

where $S_i^t(\cdot) := (1/p) \text{rand}_k(\cdot)$ is a scaled variant
of $\text{rand}_k(\cdot)$, and $b_i^{t,s}$ is the noise sampled from the Gaussian
distribution $\mathcal{N}(0, \sigma^2 I_d)$. We use the scaled sparsifier $S_i^t(\cdot)$ so
that the sparsified noisy gradient is an unbiased estimate of
the true gradient.

**Server-Side Adaptive Update.** The sparsification-coded
DP mechanism will inevitably slow down the convergence
speed due to the increased variance of the stochastic gradient
used in each iteration, and the privacy loss of each agent
increases proportionally with the number of iterations accord-
ing to the composition property of DP in Lemma 1. To im-
prove the privacy, we speed up the convergence by updating
the model in an adaptive manner similar as Adam [Kingma
and Ba, 2014] on the server. The adaptive optimizer like
Adam can be modified by adding noise to their gradients
to provide better DP guarantee, in terms of reducing the itera-
tions needed to achieve a target model accuracy [Yu et al.,
2018]. However, there are two main constraints unique to
deploying the adaptive optimizer on each agent in the FL setting. First, it is often the case that each agent participates only once or several times intermittently during the entire training process, and hence, replacing SGD with an adaptive optimizer at each agent during the local update stage will perform poorly due to the stale historical information such as the momentum in Adam. Second, maintaining the historical information on resource-constrained agents (e.g., smartphones) is costly for computation and storage resources.

To address the above issues, in Fed-SPA, the server, rather than the agents, will carry out the adaptive update without any additional communication. The server maintains two momentum vectors $v_t, u_t \in \mathbb{R}^d$ which get updated at each round. Specifically, at round $t$, after $\tau$ local iterations, each agent $i \in \mathcal{W}$ uploads its model update $\Delta_i^t := \theta_i^{t,\tau} - \theta_t$ to the server to improve the global model as follows:

$$
\begin{align*}
    u_t &= \beta_1 u_{t-1} + (1 - \beta_1) \sum_{i \in \mathcal{W}} \Delta_i^t / |\mathcal{W}|, \\
    v_t &= \beta_2 v_{t-1} + (1 - \beta_2) u_t^2, \\
    \theta_{t+1} &= \theta_t + \eta_g u_t / (\sqrt{v_t} + \kappa),
\end{align*}
$$

where $\beta_1, \beta_2 \in (0, 1)$ are momentum parameters, $\eta_g$ is the global learning rate, and $\kappa$ controls the degree of adaptivity. Note that the math operations in (6) are element-wise.

## 4 Main Theoretical Results

In this section, we give the formal privacy guarantee and rigorous convergence analysis of Fed-SPA. Before stating our results, we make the following assumptions:

**Assumption 1** (Smoothness). The local objective function $f_i$ is $L$-smooth, i.e., for any $i \in [n]$ and $x, y \in \mathbb{R}^d$, we have $f_i(y) \leq f_i(x) + \langle \nabla f_i(x), y - x \rangle + (L/2) \|y - x\|^2$.

**Assumption 2** (Bounded Variance). Let $g_i$ be the stochastic gradient over the mini-batch sampled from the distribution $D_i$. The function $f_i$ has a bounded local variance i.e., $\mathbb{E} \|g_i - \nabla f_i(x)\|^2 \leq \zeta_i^2$ for all $x \in \mathbb{R}^d, j \in [d]$ and $i \in [n]$. Moreover, the global variance is bounded, i.e., $\left(1/n\right) \sum_{i=1}^n \mathbb{E} \|g_i - \nabla f(x)\|^2 \leq \zeta_G^2$ for all $x \in \mathbb{R}^d, j \in [d]$ and $i \in [n]$. We also denote $\zeta_i^2 := : \sum_{j=1}^d \zeta_{ij}^2$ and $\zeta_G^2 := \sum_{d=1}^d \zeta_{g,j}^2$ for convenience.

**Assumption 3** (Bounded Gradient). The loss function $l_i(x, z)$ has $G/\sqrt{d}$-bounded gradients, i.e., for any data sample $x \in D_i$, we have $\|\nabla l_i(x, z)\| \leq G/\sqrt{d}$ for all $x \in \mathbb{R}^d, j \in [d]$ and $i \in [n]$.

Assumption 1 is standard and implies that the global loss function $f$ is also $L$-smooth. Assumption 2 and Assumption 3 are fairly standard in non-convex optimization literature [Reddi et al., 2020; Kingma and Ba, 2014]. Assumption 3 characterizes the sensitivity of each coordinate of gradient $\nabla l(x, z)$ and implies $\mathbb{E} \|\nabla l_i(x, z)\|^2 \leq G^2$, which can be enforced by the gradient clipping technique.

### 4.1 Privacy Analysis

In this subsection, we discuss how the sparsification in our sparsification-coded DP mechanism amplifies the privacy and provide the end-to-end privacy guarantee of Fed-SPA.

## 1. Privacy Analysis

In our sparsification-coded DP mechanism, the randomness of the sparsifier does not provide any DP guarantee by itself, but it amplifies the privacy guarantee provided by additive Gaussian noises. To analyze the end-to-end privacy, we first need to analyze the sensitivity of the sparsified gradient in Line 9, Algorithm 1. With the randomness of the active coordinate set $\omega$ is chosen independently of data and does not leak privacy, and only the values of active coordinates $\{x_j, j \in \omega\}$ contain private data information and need to be protected. Therefore, in our sparsification-coded DP mechanism, only values of active coordinates of the gradient are actually perturbed by the Gaussian noise. More precisely, let $\omega_i^t$ denote the active coordinate set for participating agent $i$ at round $t$, the sparsified noisy gradient at each local iteration can be represented as $S_i^t(g_i^{t,s} + b_i^{t,n}) = [g_i^{t,s} + b_i^{t,n}]_\omega^{t} / p = [g_i^{t,s}]_\omega^{t} / p + [b_i^{t,n}]_\omega^{t} / p$, where $p$ we observe that the amount of added noise is proportional to $k$, the number of active coordinates, and is reduced by a factor of $\sqrt{d/k}$ compared with the standard Gaussian mechanism.

In the following, we analyze the sensitivity of $[g_i^{t,s}]_\omega^{t}$ and then compute the privacy guarantee after adding noise $[b_i^{t,n}]_\omega^{t}$.

For agent $i$, given any two neighboring datasets $\xi_i^{t,s}$ and $\xi_i^{t,s'}$ that have the same size $B$ but differ in one data sample (e.g., $z \in \xi_i^{t,s}$ and $\hat{z} \in \xi_i^{t,s'}$). The local privacy sensitivity of $[g_i^{t,s}]_\omega^{t}$ can be denoted as $\phi_{i}^{2} = \max \| [g_i^{t,s}]_\omega^{t} - \nabla f_i(\hat{\theta}_i^{t,s}, z) \|_\omega^{t}$, and $\phi_{i}^{2}$ is upper-bounded by $2pG^2 / B^2$ following Assumption 3. We observe that the sensitivity of $[g_i^{t,s}]_\omega^{t}$ is proportional to the compression ratio $p$, reducing the privacy loss according to Lemma 2.
in Theorem 1 and provide the proof in Appendix E. Given a fixed value of \( \delta \), \( \epsilon \) is computed numerically by searching an optimal \( \alpha \) that minimizes \( \epsilon \). We observe that the noise magnitude \( \sigma \) is proportional to \( p \), which implies that sparsification, i.e., when \( p < 1 \), can reduce the magnitude of Gaussian noise and hence improve the model accuracy.

**Theorem 1 (Privacy Guarantee).** Suppose the mini-batch \( \xi_i \) is sampled without replacement at each iteration. Let \( q := B/n \) be the data sampling rate. Let \( I_i \) represent the number of rounds agent \( i \) participates during the training. Under Assumption 3, if \( \sigma^2 = \sigma^2 B^2/2pG^2 \geq 0.7 \), Fed-SPA achieves \((\epsilon, \delta)\)-DP for agent \( i \) where

\[
\epsilon = \frac{7q^2I_t \alpha \epsilon p G^2}{B^2 \sigma^2} + \frac{\log(1/\delta)}{\alpha - 1},
\]

for any \( \alpha \leq (2/3)\sigma^2 \log (1/\alpha(q + 1/\sigma^2)) + 1 \) and \( \delta \in (0, 1) \).

### 4.2 Convergence Analysis

In this subsection, we present the convergence results of Fed-SPA for general loss functions satisfying Assumptions 1-3. For ease of illustration, we assume full participation, i.e., \(|\mathcal{W}| = n\), and \( \beta_i = 0 \), though our analysis can be easily extended to \( \beta_i > 0 \) and partial participation (i.e., \(|\mathcal{W}| < n\), see Appendix H for details). As \( f(\cdot) \) may be non-convex, we study the gradient of the global model \( \theta_t \) as \( t \) increases. We give the result in Theorem 2 and the proof in the full version.

**Theorem 2 (Convergence Result).** Let Assumptions 1-3 hold, and \( L, G, \zeta_t, \zeta_g \) be as defined therein. Suppose the local learning rate satisfies \( \eta_l \leq \min\{1/8Lr, (1/8\tau) \min\{\kappa \sqrt{d}/G, (\kappa \sqrt{d}/G \eta_l L)^{1/2}\}\} \). Let \( \zeta_{dp}^2 = (G^2 + \zeta_t^2)/p + p \sigma^2 \), then the iterates of Algorithm 1 satisfy:

\[
\frac{1}{T} \sum_{t=0}^{T-1} E\|\nabla f(\theta_t)\|^2 = O\left((\sqrt{\beta_d \eta_l \tau G}/\sqrt{d} + \kappa)(\Xi + \Xi')\right)
\]

with

\[
\Xi = \frac{f(\theta_0) - f^*}{\eta_l \eta_r \tau T} + \frac{5n^2 \rho^2 L^2}{2 \kappa} (\zeta_{dp} + 6\tau \zeta_g^2),
\]

\[
\Xi' = \frac{\eta_r L_2}{2} + \frac{G}{\sqrt{d}} \left[ \frac{4n \rho^2 \zeta_{dp}^2}{\sqrt{d}} + \frac{20n^2 \rho^2 L^2}{\kappa^2} (\zeta_{dp}^2 + 6\tau \zeta_g^2) \right],
\]

where \( f^* \) is the optimal objective value.

We restate the above result for a specific choice of \( \eta_l, \eta_g \), and \( \kappa \) in Lemma 3 to highlight the dependence on \( \tau \) and \( T \). Note that when \( T \) is sufficiently large compared to \( \tau \), \( O(1/\sqrt{\tau T}) \) is the dominant term in Lemma 3. Therefore, Fed-SPA converges at a rate of \( O(1/\sqrt{\tau T}) \), which matches the best known rate for the general non-convex setting of our interest [Reddi et al., 2020]. We also note that both sparsification and Gaussian noise will slow down the convergence. However, a small compression ratio \( p \) can reduce the amount of added noise (i.e., the term \( p \sigma^2 \)) by a factor of \( 1/p \), which implies the privacy amplification effect of sparsification.

**Lemma 3.** Choose the local learning rate \( \eta_l = \Theta(1/Lr \sqrt{T}) \) that satisfies the condition in Theorem 2. Suppose \( \eta_g = \Theta(\sqrt{n/\tau}) \) and \( \kappa = G/\sqrt{d} \), then the iterates of Algorithm 1 satisfy

\[
\frac{1}{T} \sum_{t=0}^{T-1} E\|\nabla f(\theta_t)\|^2 = O \left( \left( \frac{f(\theta_0) - f^*}{\sqrt{\tau T}} + \frac{2c_{dp} L}{G^2 \sqrt{n/\tau}} \frac{(c_{dp}^2 + 6\tau \zeta_g^2)}{G T} \right)^2 \right),
\]

when \( T \) is sufficiently large.

## 5 Experimental Evaluation

The goal of this section is to evaluate the performance of Fed-SPA on several benchmark datasets. We aim at evaluating the performance of Fed-SPA with different levels of compression and comparing them with the performance of the following three schemes: 1) FedAvg: the classic FL algorithm; 2) DP-Fed: this baseline follows the algorithm of FedAvg except that the stochastic gradient is perturbed by adding Gaussian noise \( \mathcal{N}(0, \sigma^2 I_d) \); 3) cpSGD [Agarwal et al., 2018]: this baseline follows the algorithm of classic distributed SGD except that the stochastic gradient is quantized into some discrete domain and then perturbed using Binomial mechanism.

### 5.1 Experimental Setup

We explore two widely-used benchmark datasets in FL: MNIST [LeCun et al., 1998] and CIFAR-10 [Krizhevsky et al., 2009]. The MNIST dataset consists of 10 classes of 28 x 28 handwritten digit images. There are 60K training examples and 10K testing examples, which are partitioned among 100 agents, each containing 600 training and 100 testing examples. The CIFAR-10 dataset consists of 10 classes of 32 x 32 images. There are 50K training examples and 10K testing examples in the dataset, which are partitioned into 100 agents, each containing 500 training and 100 testing examples. We use a CNN model for the MNIST dataset, which has two 5 x 5 convolutional layers (the first with 10 filters, the second with 20 filters, each followed with 2 x 2 max pooling and ReLu activation), a fully connected layer with 50 units and ReLu activation, and a final softmax output layer. For the CIFAR-10 dataset, we use a CNN model that consists of three 3 x 3 convolution layers (the first with 64 filters, the second with 128 filters, the third with 256 filters, each followed with 2 x 2 max pooling and ReLu activation), two fully connected layers (the first with 128 units, the second with 256 units, each followed with ReLu activation), and a final softmax output layer.

We set the privacy failure probability \( \delta = 10^{-3} \) and the sampling ratio of agents \( r = |\mathcal{W}|/n = 0.1 \) for all experiments by default. Since cpSGD follows the classic distributed SGD scheme, we have \( \tau = 1 \) and \( r = 1.0 \) for cpSGD. We tune the hyperparameters using grid-search. We set the number of local iterations \( \tau = 300 \) for MNIST and \( \tau = 50 \) for CIFAR-10. The details of other hyperparameter settings are given in the full version. The per-coordinate sensitivity \( G/\sqrt{d} \) is selected during an initialization round for each scheme by taking the median value over \( N \) absolute values.
Table 1: Summary of results on MNIST dataset.

| Compression ratio | Algorithm     | Performance |
|-------------------|---------------|-------------|
|                   |               | Accuracy (%) | Cost (MB) | ε   |
| p = 0.05          | Fed-SPA       | 92.65        | 0.0197    | 1.0 |
|                   | cpSGD         | diverge      | -         | -   |
| p = 0.1           | Fed-SPA       | 92.16        | 0.0393    | 1.0 |
|                   | cpSGD         | diverge      | -         | -   |
| p = 0.4           | Fed-SPA       | 94.84        | 0.1572    | 1.0 |
|                   | cpSGD         | 87.32        | 1.5720    | 3.63|
| p = 1.0           | Fed-SPA       | 94.70        | 0.3931    | 1.0 |
|                   | cpSGD         | 88.48        | 3.9310    | 2.26|
|                   | DP-Fed        | 91.41        | 0.3931    | 1.0 |
|                   | FedAvg        | 96.87        | 0.3931    | -   |

Table 2: Summary of results on CIFAR-10 dataset.

5.2 Experimental Results

Table 1 shows the best accuracy over 45 communication rounds for each scheme on the MNIST dataset, and Table 2 represents the best accuracy over 200 rounds for each scheme on the CIFAR-10 dataset. Assume each value of the model parameter is represented by a 32-bit floating number. The Compression ratio for Fed-SPA is calculated as $p = k/d$. For cpSGD, $p = \log_2(m + b)/32$, where $b$ implies the $b$-bit quantization and $m$ is the parameter for the Binomial distribution Bin($m, 0.5$). For FedAvg and DP-Fed, we have $p = 1.0$. Cost is the average bandwidth consumption calculated as $p \times d \times 32 \times T \times r$, where $r$ is the sampling probability of devices and $T$ is the communication rounds. Note that since how to analyze Binomial mechanism in cpSGD using RDP is still unknown, we account the privacy loss $\epsilon$ of cpSGD using the standard subsampling amplification [Balle et al., 2018] and advanced composition [Dwork et al., 2010].

Without compression, i.e., when $p = 1.0$, Fed-SPA outperforms cpSGD and DP-Fed on both datasets as the server in Fed-SPA updates the global model adaptively to speed up the convergence, and its best accuracy to achieve $(1.0, 10^{-3})$-DP is close to the best accuracy of FedAvg under the same communication cost. Note that since the Binomial noise used in cpSGD is not as concentrated as the Gaussian noise used in Fed-SPA and DP-Fed, the model accuracy of cpSGD degrades heavily, and hence to achieve a target accuracy, the privacy loss of cpSGD is very large. As the compression ratio $p$ decreases, the performance of Fed-SPA on both datasets does not degrade much, compared with cpSGD which cannot achieve a reasonable privacy guarantee when $p \leq 0.1$. More importantly, Fed-SPA for MNIST achieves a higher accuracy than DP-Fed under the same privacy cost, while saving 86% communication cost when $p = 0.05$. The reason is that decreasing $p$ also lowers the sensitivity of the sparsified gradient which has a direct impact on the noise magnitude to achieve a target privacy guarantee, as explain in Section 4.1. We observe a similar trend for CIFAR-10 from Table 2: Fed-SPA performs better when the compression ratio is small, e.g., when $p \leq 0.4$, as the sensitivity in this case is small.

Then, we show the privacy-accuracy trade-off of Fed-SPA for both datasets with different levels of compression in Figure 1. As we mentioned above, a small compression ratio results in a smaller sensitivity, and hence less Gaussian noise will be added to the model. On the other hand, the compression ratio cannot be arbitrarily small as it will increase the variance of gradient as explained in Section 4.2. Therefore, we should find an optimal $p$ that is small enough to reduce the size of additive Gaussian noise but large enough to avoid large compression error. For both datasets, we can observe that when the privacy budget $\epsilon$ is limited (e.g., $\epsilon < 1.0$), a small enough $p$ (e.g., $p = 0.8$ for MNIST and $p = 0.2$ for CIFAR-10) achieves higher accuracy as it reduces the size of Gaussian noise. As $\epsilon$ increases, the size of Gaussian noise decreases, and hence Fed-SPA with larger $p$ performs better due to the smaller compression error.

6 Conclusion

This paper has proposed Fed-SPA, a new FL scheme based on sparsification-coded DP mechanism and server-side adaptive update, to improve privacy-accuracy trade-off and achieve communication efficiency at the same time. We have provided rigorous convergence and privacy analysis of Fed-SPA. Extensive experiments based on benchmark datasets have been conducted to verify the effectiveness of the proposed scheme and numerically show the trade-off between privacy guarantee and model accuracy. For future work, we plan to investigate the interplay of privacy protection with other communication-efficient techniques in FL.

Acknowledgements

The work of R. Hu and Y. Gong was supported by the U.S. National Science Foundation under grants US CNS-2029685 and CNS-1850523. The work of Y. Guo was supported by the U.S. National Science Foundation under grant US CNS-2029685.
References

[Abadi et al., 2016] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 308–318. ACM, 2016.

[Agarwal et al., 2018] Naman Agarwal, Ananda Theertha Suresh, Felix Xinnan X Yu, Sanjiv Kumar, and Brendan McMahan. cpgsd: Communication-efficient and differentially-private distributed sgd. In Advances in Neural Information Processing Systems, pages 7564–7575, 2018.

[Balle et al., 2018] Borja Balle, Gilles Barthe, and Marco Gaboardi. Privacy amplification by subsampling: Tight analyses via couplings and divergences. In Advances in Neural Information Processing Systems, pages 6277–6287, 2018.

[Dwork and Roth, 2014] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4):211–407, 2014.

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

[Erlingsson et al., 2019] ´Ulfar Erlingsson, Vitaly Feldman, Ilya Mironov, Ananth Raghunathan, Kunal Talwar, and Abhradeep Thakurta. Amplification by shuffling: From local to central differential privacy via anonymity. In Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 2468–2479. SIAM, 2019.

[Fredriksson et al., 2015] Matt Fredriksson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 1322–1333, 2015.

[Gong et al., 2016] Yanmin Gong, Yuguang Fang, and Yuanxiong Guo. Private data analytics on biomedical sensing data via distributed computation. IEEE/ACM transactions on computational biology and bioinformatics, 13(3):431–444, 2016.

[Guo and Gong, 2018] Yuanxiong Guo and Yanmin Gong. Practical collaborative learning for crowdsensing in the internet of things with differential privacy. In 2018 IEEE Conference on Communications and Network Security (CNS), pages 1–9. IEEE, 2018.

[Hu et al., 2020] Rui Hu, Yuanxiong Guo, Hongning Li, Qingqi Pei, and Yanmin Gong. Personalized federated learning with differential privacy. IEEE Internet of Things Journal, 2020.

[Huang et al., 2019] Zonghao Huang, Rui Hu, Yuanxiong Guo, Eric Chan-Tin, and Yanmin Gong. DP-ADMM: ADMM-based distributed learning with differential privacy. IEEE Transactions on Information Forensics and Security, 15:1002–1012, 2019.

[Kingma and Ba, 2014] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980, 2014.

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

[LeCun et al., 1998] Yann LeCun, Léon Bottou, Yoshua Bengio, Patrick Haffner, et al. Gradient-based learning applied to document recognition. Proceedings of the IEEE, 86(11):2278–2324, 1998.

[Liu et al., 2020] Ruixuan Liu, Yang Cao, Hong Chen, Ruoyang Guo, and Masatoshi Yoshikawa. FLAME: Differentially private federated learning in the shuffle model. arXiv preprint arXiv:2009.08063, 2020.

[McMahan et al., 2017] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and Statistics, pages 1273–1282, 2017.

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

[Reddi et al., 2020] Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečný, Sanjiv Kumar, and H Brendan McMahan. Adaptive federated optimization. arXiv preprint arXiv:2003.00295, 2020.

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

[Truex et al., 2019] Stacey Truex, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig, Rui Zhang, and Yi Zhou. A hybrid approach to privacy-preserving federated learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, pages 1–11, 2019.

[Wang et al., 2019a] Lingxiao Wang, Bargav Jayaraman, David Evans, and Quanquan Gu. Efficient privacy-preserving nonconvex optimization. arXiv preprint arXiv:1910.13659, 2019.

[Wang et al., 2019b] Yu-Xiang Wang, Borja Balle, and Shiva Prasad Kasiviswanathan. Subsampled rényi differential privacy and analytical moments accountant. In The 22nd International Conference on Artificial Intelligence and Statistics, pages 1226–1235. PMLR, 2019.

[Yu et al., 2018] Da Yu, Huishuai Zhang, and Wei Chen. Improve the gradient perturbation approach for differentially private optimization. NeurIPS 2018 Workshop, 2018.
A Experiments
A.1 Hyperparameter settings
We tune the hyperparameters using grid-search and choose the following optimal values: for MNIST, we use batch size $B = 10$, number of local iterations $\tau = 300$ and local learning rate $\eta_l = 0.01$; for CIFAR-10, we use batch size $B = 50$, number of local iterations $\tau = 50$ and local learning rate $\eta_l = 0.1$. For Fed-SPA, we set $\beta_1 = 0.9$, $\beta_2 = 0.99$ and $\kappa = 10^{-3}$ for both datasets, and the global learning rate for MNIST and CIFAR-10 are $\eta_g = 0.01$ and $\eta_g = 0.005$, respectively. Note that we let both local and global learning rates decay at a rate of $1/\sqrt{T}$.

B Additional Lemmas of RDP
Lemma 4 (RDP to DP conversion [Wang et al., 2019b]). If $M$ satisfies $(\alpha, \rho)$-RDP, then it also satisfies $(\rho + \frac{\log(1/\delta)}{\alpha - 1}, \delta)$-DP.

Lemma 5 (RDP for Subsampling Mechanism [Wang et al., 2019b; Wang et al., 2019a]). For a Gaussian mechanism $M$ and any $m$-datapoints dataset $D$, define $M \circ SUBSAMPLING$ as 1) subsample without replacement $B$ datapoints from the dataset (denote $q = B/m$ as the sampling ratio); and 2) apply $M$ on the subsampled dataset as input. Then if $M$ satisfies $(\alpha, \rho(\alpha))$-RDP with respect to the subsampled dataset for all integers $\alpha \geq 2$, then the new randomized mechanism $M \circ SUBSAMPLING$ satisfies $(\alpha, \rho'(\alpha))$-RDP with respect to $D$, where

$$\rho'(\alpha) \leq \frac{1}{\alpha - 1} \log \left(1 + \frac{q^2(\alpha)}{2} \min \{4(\rho'^2(2) - 1), 2\rho'^2(2)\} + \sum_{j=3}^{\alpha} q^2(\alpha) 2e^{(j-1)\rho(j)} \right).$$

If $\sigma^2 = \phi^2(h) \geq 0.7$ and $\alpha \leq (2/3)\sigma^2 \log \left(1/q\alpha(1 + \sigma^2)^2 \right) + 1$, $M \circ SUBSAMPLING$ satisfies $(\alpha, 3.5q^2\phi^2(h)\alpha/\sigma^2)$-RDP.

C Useful inequalities
Lemma 6. For arbitrary set of $n$ vectors $\{\alpha_i\}_{i=1}^n, \alpha_i \in \mathbb{R}^d$,

$$\left\| \sum_{i=1}^n \alpha_i \right\|^2 \leq n \sum_{i=1}^n \left\| \alpha_i \right\|^2. \tag{7}$$

Lemma 7. For given two vectors $\alpha, \beta \in \mathbb{R}^d$,

$$\left\| \alpha + \beta \right\|^2 \leq (1 + \alpha)\left\| \alpha \right\|^2 + (1 + \alpha^{-1})\left\| \beta \right\|^2, \forall \alpha > 0. \tag{8}$$

This inequality also holds for the sum of two matrices, $\mathbf{A}, \mathbf{B} \in \mathbb{R}^{n \times d}$ in Frobenius norm.

D Proof of Lemma 8
Lemma 8 (Unbiased Sparsification). Given a vector $x \in \mathbb{R}^d$, parameter $k \in [d]$, and sparsifier $S^k(x) := (d/k) \text{rand}_k(x)$. Let $p := k/d \in (0, 1]$ be the compression ratio, it holds that

$$\mathbb{E}_\omega[S^k(x)] = x, \quad \mathbb{E}_\omega||S^k(x) - x||^2 = \left(\frac{1}{p} - 1\right)||x||^2.$$ 

Proof. By applying the expectation over the active set $\omega$, we have

$$\mathbb{E}_\omega[S^k(x)] = \frac{d}{k} \left[\frac{k}{d}[x]_1, \ldots, \frac{k}{d}[x]_d\right] = x,$$

and

$$\mathbb{E}_\omega||S^k(x) - x||^2 = \sum_{j=1}^d \left(\frac{k}{d} [x]_j - \frac{d}{k} [x]_j\right)^2 + \left(1 - \frac{k}{d}\right) [x]_j^2\right) = \left(\frac{1}{p} - 1\right)||x||^2.$$
E  Proof of Theorem 1

Proof. Let \( \omega_i^t \) denote the active coordinate set for participating agent \( i \) at round \( t \). The sparsified noisy gradient at each local iteration can be represented as

\[
S_i^t(g_i^{t,s} + b_i^{t,s}) = \frac{[g_i^{t,s} + b_i^{t,s}]}{p} = \frac{[g_i^{t,s}]_{\omega_i^t} + [b_i^{t,s}]_{\omega_i^t}}{p},
\]

where we can observe that due to the use of sparsification, Gaussian noises are only added to the values of active coordinates in \( \omega_i^t \) in Fed-SPA. Therefore, we need to analyze the privacy loss of \( [g_i^{t,s}]_{\omega_i^t} \) after adding noise \( [b_i^{t,s}]_{\omega_i^t} \). For agent \( i \), given any two neighboring mini-batch \( \xi_i^{t,s} \) and \( \xi_i^{t,s} \) that have the same size \( B \) but differ only in one data sample (e.g., \( z \) and \( \hat{z} \)). Let \( \phi_{\omega_i^t} \) be the \( L \)-sensitivity of \( [g_i^{t,s}]_{\omega_i^t} \), then we have

\[
\phi_{\omega_i^t}^2 = \max \left\| [g_i^{t,s}]_{\omega_i^t} - \left[ \nabla f_i(\theta_i^{t,s}, \xi_i^{t,s}) \right]_{\omega_i^t} \right\|^2
= \max \left\| \frac{1}{B} \left[ \nabla l(\theta_i^{t,s}, z) - \nabla l(\theta_i^{t,s}, \hat{z}) \right]_{\omega_i^t} \right\|^2
\leq \frac{2pG^2}{B^2},
\]

where the last inequality comes from Assumption 3. Given that the noise added to each coordinate of \( [g_i^{t,s}]_{\omega_i^t} \) is drawn from the Gaussian distribution \( \mathcal{N}(0, \sigma^2) \), each local iteration of Algorithm 1 achieves \((\alpha, \alpha pG^2/B^2\sigma^2)\)-RDP for the sub-sampled mini-batch \( \xi_i^{t,s} \) by Lemma 2.

By the sub-sampling amplification property of RDP in Lemma 5, each local iteration of Algorithm 1 achieves \((\alpha, 7q^2\rho_i(\alpha))\)-RDP for agent \( i \)'s local dataset \( D_i \) if \( \sigma^2 = \sigma^2 B^2 / 2pG^2 \geq 0.7 \) and \( \alpha \leq (2/3)\sigma^2 \log \left(1/q \alpha (1 + \sigma^2)\right) + 1 \). After \( T \) communication rounds, agent \( i \) will perform \( I_i \tau \) iterations of SGD. By Lemma 1, Fed-SPA satisfies \((\alpha, 7q I_i \tau \rho_i(\alpha))\)-RDP for agent \( i \) across \( T \) communication rounds. Therefore, Theorem 1 follows by Lemma 4.

For clarity of presentation, Theorem 1 relies on the amplification by sub-sampling result of [Wang et al., 2019b] which has a simple closed-form. A tighter and more general result (without restriction on the values of \( \sigma, q, m, p \)) can be readily obtained by using the results of [Wang et al., 2019b].

F  Proof of Theorem 2

Proof. We note that both the moment and model update on the server are element-wise as following: \( \forall j \in [d], \)

\[
\begin{align*}
[u_t]_j &= \beta_1[u_{t-1}]_j + (1 - \beta_1)[\Delta_t]_j, \\
[v_t]_j &= \beta_2[v_{t-1}]_j + (1 - \beta_2)[u_t]^2, \\
[\theta_{t+1}]_j &= [\theta_t]_j + \eta_g \frac{[u_t]_j}{\sqrt{[v_t]_j + \kappa}}.
\end{align*}
\]

By the \( L \)-smoothness of function \( f \), we have

\[
\begin{align*}
E_t[f(\theta_{t+1}) - f(\theta_t)] &\leq E_t \left( \nabla f(\theta_t), \theta_{t+1} - \theta_t \right) + \frac{L}{2} E_t \left\| \theta_{t+1} - \theta_t \right\|_2^2 \\
&= \eta_g E_t \left( \nabla f(\theta_t), \frac{u_t}{\sqrt{v_t + \kappa}} \right) + \frac{L \eta_g}{2} \sum_{j=1}^d E_t \left\| \frac{[u_t]_j}{\sqrt{[v_t]_j + \kappa}} \right\|_2^2 \\
&= \eta_g E_t \left( \nabla f(\theta_t), \frac{u_t}{\sqrt{\beta_2 v_{t-1} + \kappa}} \right) + \eta_g E_t \left( \nabla f(\theta_t), \frac{u_t}{\sqrt{\beta_2 v_{t-1} + \kappa}} \right) \\
&\quad + \frac{L \eta_g}{2} \sum_{j=1}^d E_t \left( \frac{[u_t]_j^2}{(\sqrt{[v_t]_j + \kappa})^2} \right)
\end{align*}
\]

where the expectation is taken over randomness at round \( t \).
Bounding $T_2$. We observe the following about $T_2$:

\[ T_2 = E_t \left[ \sum_{j=1}^{d} |\nabla f(\theta_t)|_j \times \left[ \left( \frac{|u_t|_j}{\sqrt{|v_{t-1}|_j + \kappa}} \right) - \frac{|u_t|_j}{\sqrt{v_{t-1}|_j + \kappa}} \right] \right] \]

\[ = E_t \left[ \sum_{j=1}^{d} |\nabla f(\theta_t)|_j \times |u_t|_j \times \left[ \frac{\sqrt{v_{t-1}|_j} - \sqrt{|v_{t}|_j}}{(\sqrt{|v_{t}|_j + \kappa})(\sqrt{v_{t-1}|_j + \kappa})} \right] \right] \]

\[ = E_t \left[ \sum_{j=1}^{d} |\nabla f(\theta_t)|_j \times |u_t|_j \times \left[ \frac{-(1 - \beta_2)|u_t|_j^2}{(\sqrt{|v_{t}|_j + \kappa})(\sqrt{v_{t-1}|_j + \kappa})(\sqrt{v_{t-1}|_j + \sqrt{|v_{t}|_j}})} \right] \right] \]

Given that $-(1 - \beta_2)|u_t|_j^2 = (\sqrt{v_{t-1}|_j} - \sqrt{|v_{t}|_j})(\sqrt{v_{t-1}|_j + \sqrt{|v_{t}|_j}})$. Moreover, we have that

\[ T_2 \leq (1 - \beta_2)E_t \left[ \sum_{j=1}^{d} \left( |\nabla f(\theta_t)|_j \times \sqrt{\left( \sqrt{|v_{t}|_j - \beta_2 v_{t-1}|_j} \right)(\sqrt{v_{t-1}|_j + \sqrt{|v_{t}|_j}})} \right) \right] \]

\[ \times \left[ \frac{|u_t|_j^2}{(\sqrt{|v_{t}|_j + \kappa})(\sqrt{v_{t-1}|_j + \kappa})(\sqrt{v_{t-1}|_j + \sqrt{|v_{t}|_j}})} \right] \]

\[ \leq \sqrt{1 - \beta_2}E_t \left[ \sum_{j=1}^{d} \left( |\nabla f(\theta_t)|_j \times \sqrt{\left( \sqrt{|v_{t}|_j - \beta_2 v_{t-1}|_j} \right) \times \left[ \frac{|u_t|_j^2}{\sqrt{|v_{t}|_j + \kappa}(\sqrt{v_{t-1}|_j + \kappa})} \right]} \right) \right] \]

\[ \leq \sqrt{1 - \beta_2}E_t \left[ \sum_{j=1}^{d} \frac{G}{\kappa \sqrt{d}} \left[ \frac{|u_t|_j^2}{\sqrt{|v_{t}|_j + \kappa}} \right] \right] \]

using the fact that $|v_{t-1}|_j$ is increasing in $t$ and $(\sqrt{|v_{t}|_j} - \beta_2 v_{t-1}|_j)/(\sqrt{v_{t-1}|_j + \sqrt{|v_{t}|_j}}) \leq 1$. Next, using the fact that $||\nabla f(\theta)|_j| \leq G/\sqrt{d}$ and $|v_{t-1}|_j \geq \tau^2$ since $|v_{t-1}|_j \geq \tau^2$ and $v_{t-1}|_j$ is increasing in $t$, one yields

\[ T_2 \leq \sqrt{1 - \beta_2}E_t \left[ \sum_{j=1}^{d} \frac{G}{\kappa \sqrt{d}} \left[ \frac{|u_t|_j^2}{\sqrt{|v_{t}|_j + \kappa}} \right] \right] \]

For expository purpose, we assume $\beta_1 = 0$, so $u_t = \Delta_t$ and hence

\[ T_2 \leq \sqrt{1 - \beta_2}E_t \left[ \sum_{j=1}^{d} \frac{G}{\kappa \sqrt{d}} \left[ \frac{\Delta_t^2}{\sqrt{|v_{t}|_j + \kappa}} \right] \right] . \]  \(10\)

Bounding $T_1$. Note that

\[ T_1 = \sum_{j=1}^{d} \left( |\nabla f(\theta_t)|_j \times E_t \left[ \frac{|u_t|_j}{\sqrt{v_{t-1}|_j + \kappa}} \right] \right) \]

\[ = \sum_{j=1}^{d} \left( \frac{|\nabla f(\theta_t)|_j}{\sqrt{v_{t-1}|_j + \kappa}} \times E_t \left[ |u_t|_j - \eta \tau |\nabla f(\theta_t)|_j + \eta \tau |\nabla f(\theta_t)|_j \right] \right) \]

\[ = -\eta \tau \sum_{j=1}^{d} \frac{|\nabla f(\theta_t)|_j^2}{\sqrt{v_{t-1}|_j + \kappa}} + \frac{1}{\sqrt{v_{t-1}|_j + \kappa}} \left( \frac{\nabla f(\theta_t)}{\sqrt{v_{t-1}|_j + \kappa}} \times E_t \left[ u_t + \eta \tau |\nabla f(\theta_t)|_j \right] \right) . \]  \(11\)
Summing over \( t = 0 \) to \( T-1 \) and using telescoping sum, one can get

\[
\mathbb{E}[f(\theta_T) - f(\theta_0)] \leq \frac{-\eta T}{4} \sum_{t=0}^{T-1} \sum_{j=1}^{d} \frac{[\nabla f(\theta_t)]_{ij}^2}{\sqrt{\beta_2 v_{t-1,j} + \kappa}} + \frac{5\eta \eta_s^3 \tau^2 L^2}{2\kappa} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 + 6\tau \zeta_t^2 \right)
\]

Summing over \( t = 0 \) to \( T-1 \) and using telescoping sum, one can get

\[
\mathbb{E}_t [f(\theta_{t+1}) - f(\theta_t)] \leq \frac{-\eta T}{4} \sum_{t=0}^{T-1} \sum_{j=1}^{d} \frac{[\nabla f(\theta_t)]_{ij}^2}{\sqrt{\beta_2 v_{t-1,j} + \kappa}} + \frac{5\eta \eta_s^3 \tau^2 L^2}{2\kappa} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 + 6\tau \zeta_t^2 \right)
\]
Using Lemma 11 and the same idea in Lemma 11 to bound \( \sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{(\Delta t)^2}{(\sqrt{V_t})^2 + \kappa} \right] \), we finally obtain that

\[
\mathbb{E}[f(\theta_T) - f(\theta_0)] \leq -\frac{\eta_1 \eta_0^2}{4} + \sum_{t=0}^{T-1} \sum_{j=1}^{d} \frac{\|\nabla f(\theta_t)\|^2}{\beta_2(V_{t-1})} + \kappa + \frac{5\eta_1 \eta_2 \tau^2 L^2 T}{2\kappa} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 + 6\tau \zeta_t^2 \right)
\]

\[
+ \left( \frac{G \eta_0 \sqrt{1 - \beta_2}}{\sqrt{d}} + \frac{\eta_2 L}{2} \right) \left[ \frac{4\eta_0^2 \tau T}{n\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 \right) \right]
\]

\[
+ \frac{20\eta_0^4 \tau^3 L^2 T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 + 6\tau \zeta_t^2 \right)
\]

Based on the condition of \( \eta_t \) in Theorem 2, we have

\[
\left( G \sqrt{1 - \beta_2} + \frac{\eta_0 L}{2} \right) \frac{4\eta_0 \tau}{\kappa^2} \leq \frac{1}{8(\sqrt{\beta_2} \eta_t G / \sqrt{d} + \kappa)}
\]

We also observe that

\[
\sqrt{\beta_2 |\nu_{t-1}|_j + \kappa \leq \sqrt{\beta_2} \eta_t G / \sqrt{d} + \kappa,
\]

so rearranging (14) and dividing both sides by \( T \) yields

\[
\frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E} \| \nabla f(\theta_t) \|^2 \leq \frac{8(\sqrt{\beta_2} \eta_t G / \sqrt{d} + \kappa)}{\eta_t \eta_0^2} (f(\theta_0) - f^*) + \frac{8(\sqrt{\beta_2} \eta_t G / \sqrt{d} + \kappa)}{\eta_t \eta_0^2} \frac{5\eta_1 \eta_2 \tau^2 L^2}{2\kappa} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 + 6\tau \zeta_t^2 \right)
\]

\[
+ \frac{8(\sqrt{\beta_2} \eta_t G / \sqrt{d} + \kappa)}{\eta_t \eta_0^2} \left( G \sqrt{d} + \frac{\eta_0 L}{2} \right) \left[ \frac{4\eta_0^2 \tau T}{n\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 \right) \right]
\]

\[
+ \frac{20\eta_0^4 \tau^3 L^2 T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_t^2) + p\sigma^2 + 6\tau \zeta_t^2 \right)
\],

where we use the fact that \( f(\theta_T) \geq f^* \).

Note that in the above convergence analysis, we use \( \beta_1 = 0 \) just for expository purposes though our analysis can be directly extended to \( \beta_1 > 0 \). Specifically, if \( \beta_1 > 0 \), \( u_t = \beta_1 u_{t-1} + (1 - \beta_1) \Delta_t = (1 - \beta_1) \sum_{h=1}^{t} \beta_1^{t-h} \Delta_h \) which only makes the expectation and variance of \( u_t \) different. Assume \( \mathbb{E}[\Delta_h] = \mathbb{E}[\Delta_t] \), then we have \( \mathbb{E}[u_t] = (1 - \beta_1) \Delta_t \) and \( \sum_{t=1}^{T} ||u_t||^2 \leq \sum_{t=1}^{T} ||\Delta_t||^2 / (1 - \beta_1)^2 \). Then all the proof steps in Appendix F follow directly by substituting the above new expectation and variance bounds into \( T_1 \) and \( T_2 \).

\[\square\]

### G Intermediate Results

**Lemma 9** (Bounded Sparsified Noisy Gradient). The sparsified noisy gradient in Fed-SPA is unbiased and has a bounded variance, i.e., \( \mathbb{E}[S_t^i(g_{t,s}^i + b_{t,s}^i)] = \nabla f_i(\theta_i^{1,s}) \) and \( \mathbb{E}[||S_t^i(g_{t,s}^i + b_{t,s}^i)||^2] \leq (G^2 + \zeta_i^2) / p + p\sigma^2 \).

**Proof.** By the unbiasedness property of the sparsification in Lemma 8, we have

\[
\mathbb{E}[S_t^i(g_{t,s}^i + b_{t,s}^i)] = \mathbb{E}_{\omega_t^i} [g_{t,s}^i] + \mathbb{E}_{b_t^i} [b_{t,s}^i] = \nabla f_i(\theta_i^{1,s}),
\]

where the expectation \( \mathbb{E}[\cdot] \) is taken over the random variables \( \omega_t^i, \xi_t^i, b_t^i, \) and \( b_{t,s}^i \). Here, we use the fact that \( \omega_t^i, \xi_t^i \) and \( b_t^i \) are
independent with each other. Then, applying the expectation \(\mathbb{E}[:\cdot:]\) on the norm of the sparsified noisy gradient, one yields

\[
\mathbb{E}\|S_i^t(g_i^{t,s} + b_i^{t,s})\|^2 = \mathbb{E}\|S_i^t(g_i^{t,s})\|^2 + \mathbb{E}\|b_i^{t,s}\|^2
\]

\[
= \mathbb{E}\|S_i^t(g_i^{t,s}) - \nabla f_i(\theta_i^{t,s})\|^2 + \|\nabla f_i(\theta_i^{t,s})\|^2 + \mathbb{E}_\omega \sum_{j \in \omega_i} \mathbb{E}_\omega_1 \|b_i^{t,s}_j\|^2
\]

\[
= \mathbb{E}\|S_i^t(g_i^{t,s}) - g_i^{t,s} + g_i^{t,s} - \nabla f_i(\theta_i^{t,s})\|^2 + \|\nabla f_i(\theta_i^{t,s})\|^2 + \frac{k}{d} \sum_{j \in [d]} \sigma^2
\]

\[
= \mathbb{E}\|S_i^t(g_i^{t,s}) - g_i^{t,s}\|^2 + \mathbb{E}\|g_i^{t,s} - \nabla f_i(\theta_i^{t,s})\|^2 + \|\nabla f_i(\theta_i^{t,s})\|^2 + p \mathbb{E}\|f_i(\theta_i^{t,s})\|^2
\]

\[
\leq \left(\frac{1}{p} - 1\right) \mathbb{E}\|f_i(\theta_i^{t,s})\|^2 + \zeta_i^2 + \|\nabla f_i(\theta_i^{t,s})\|^2 + p \mathbb{E}\|f_i(\theta_i^{t,s})\|^2
\]

\[
\leq \frac{1}{p} \zeta_i^2 + \frac{1}{p} \|\nabla f_i(\theta_i^{t,s})\|^2 + p \mathbb{E}\|f_i(\theta_i^{t,s})\|^2
\]

\[
\leq \frac{1}{p} (G^2 + \zeta_i^2) + p \mathbb{E}\|f_i(\theta_i^{t,s})\|^2,
\]

using the fact that \(\mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - \mathbb{E}[X]^2\), Lemma 8 and Assumption 3.

\(\Box\)

**Lemma 10.** The distance between the global model and the local model is bounded as follows: when \(s \in [0, \tau]\),

\[
\frac{1}{n} \sum_{i=1}^{n} \mathbb{E}\|\theta_i^{t,s} - \theta_i\|^2 \leq 57\eta_i^2 \left(\frac{1}{p} (G^2 + \zeta_i^2) + p \mathbb{E}\|f_i(\theta_i)\|^2 + 6 \tau \zeta_i^2\right) + 30 \tau^2 \eta_i^2 \mathbb{E}\|f_i(\theta_i)\|^2,
\]

(15)

if the local learning rate satisfies \(\eta_i \leq 1/8 L \tau\).

**Proof.** The result trivially holds for \(s = 0\) since \(\theta_i^{t,0} = \theta_i\) for all \(i \in [n]\). We observe that for any \(s \in (0, \tau]\),

\[
\mathbb{E}\|\theta_i^{t,s} - \theta_i\|^2 = \mathbb{E}\|\theta_i^{t,s-1} - \eta_i S_i^t(g_i^{t,s-1} + b_i^{t,s}) - \theta_i\|^2
\]

\[
= \mathbb{E}\|\theta_i^{t,s-1} - \theta_i - \eta_i S_i^t(g_i^{t,s-1} + b_i^{t,s}) + \eta_i \nabla f_i(\theta_i^{t,s-1}) - \eta_i \nabla f_i(\theta_i)\|^2
\]

\[
= \mathbb{E}\|\theta_i^{t,s-1} - \theta_i - \eta_i \nabla f_i(\theta_i^{t,s-1}) + \eta_i \nabla f_i(\theta_i) - \eta_i \nabla f_i(\theta_i)\|^2
\]

\[
+ \eta_i^2 \mathbb{E}\|S_i^t(g_i^{t,s-1} + b_i^{t,s}) - \nabla f_i(\theta_i^{t,s-1})\|^2
\]

\[
\leq (1 + \alpha) \mathbb{E}\|\theta_i^{t,s-1} - \theta_i\|^2 + (1 + \alpha^{-1}) \eta_i^2 \mathbb{E}\|\nabla f_i(\theta_i^{t,s-1}) - \nabla f_i(\theta_i)\|^2 + \mathbb{E}\|\nabla f_i(\theta_i^{t,s-1}) - \nabla f_i(\theta_i)\|^2
\]

\[
+ \eta_i^2 \left(\mathbb{E}\|S_i^t(g_i^{t,s-1} + b_i^{t,s})\|^2 - \mathbb{E}\|\nabla f_i(\theta_i^{t,s-1})\|^2\right)
\]

\[
\leq \left(1 + \frac{1}{2 \tau - 1}\right) \mathbb{E}\|\theta_i^{t,s-1} - \theta_i\|^2 + 6 \tau \eta_i^2 \mathbb{E}\|\nabla f_i(\theta_i^{t,s-1}) - \nabla f_i(\theta_i)\|^2 + 6 \tau \eta_i^2 \mathbb{E}\|\nabla f_i(\theta_i)\|^2
\]

\[
+ 6 \tau \eta_i^2 \mathbb{E}\|\nabla f_i(\theta_i)\|^2 + \eta_i^2 \left(\frac{1}{p} (G^2 + \zeta_i^2) + p \mathbb{E}\|f_i(\theta_i)\|^2\right)
\]

\[
\leq \left(1 + \frac{1}{2 \tau - 1}\right) \mathbb{E}\|\theta_i^{t,s-1} - \theta_i\|^2 + 6 \tau L \eta_i^2 \mathbb{E}\|\theta_i^{t,s-1} - \theta_i\|^2 + 6 \tau \eta_i^2 \mathbb{E}\|\nabla f_i(\theta_i)\|^2
\]

\[
+ \eta_i^2 \left(\frac{1}{p} (G^2 + \zeta_i^2) + p \mathbb{E}\|f_i(\theta_i)\|^2\right)
\]

\[
= \left(1 + \frac{1}{2 \tau - 1} + 6 \tau L^2 \eta_i^2\right) \mathbb{E}\|\theta_i^{t,s-1} - \theta_i\|^2 + 6 \tau \eta_i^2 \mathbb{E}\|\nabla f_i(\theta_i)\|^2 + \eta_i^2 \left(\frac{1}{p} (G^2 + \zeta_i^2) + p \mathbb{E}\|f_i(\theta_i)\|^2\right),
\]
where the third equality uses the fact that \( \mathbb{E} [S_i^\alpha(i, \theta_i^{s-1} + b_i^{s, t})] = \nabla f_i(\theta_i^{s-1}) \), the first inequality results from (8), the second inequality comes from choosing \( \alpha = 1/(2\tau - 1) \), (7) and Lemma 9, and last inequality uses the \( L \)-smoothness of function \( f_i \) and Assumption 2.

Taking the average over the agent \( i \) and choosing the learning rate \( \eta_i \leq 1/8L\tau \), we obtain that

\[
\frac{1}{n} \sum_{i=1}^{n} \mathbb{E} \left\| \theta_i^{t,s} - \theta_i \right\|^2 \leq \left( 1 + \frac{1}{2\tau - 1} \right) \left( 1 + \frac{1}{\tau - 1} \right) \left[ 6\tau \eta_i^2 \mathbb{E} \left\| \nabla f(\theta_i) \right\|^2 + \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 + 6\tau \zeta_g^2 \right] \left( 1 + \frac{1}{\tau - 1} \right) + 6\tau \eta_i^2 \mathbb{E} \left\| \nabla f(\theta_i) \right\|^2 + \eta_i^2 \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 + 6\tau \zeta_g^2 \right) \left( 1 + \frac{1}{\tau - 1} \right) \left[ \left( 1 + \frac{1}{\tau - 1} \right)^\tau - 1 \right] (10)
\]

where we use the fact that \( 1/(2\tau - 1) \leq 1/(\tau - 1) \) and \( 6\tau L^2 \eta_i^2 \leq 1/(\tau - 1) \). Unrolling the recursion, one yields

\[
\frac{1}{n} \sum_{i=1}^{n} \mathbb{E} \left\| \theta_i^{t,s} - \theta_i \right\|^2 \leq \sum_{h=0}^{T-1} \left( 1 + \frac{1}{\tau - 1} \right)^h \left[ 6\tau \eta_i^2 \mathbb{E} \left\| \nabla f(\theta_i) \right\|^2 + \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 + 6\tau \zeta_g^2 \right] \left( 1 + \frac{1}{\tau - 1} \right) \left[ \left( 1 + \frac{1}{\tau - 1} \right)^\tau - 1 \right] (11)
\]

where we use the fact that \( (1 + 1/(\tau - 1))^\tau \leq 5 \) for \( \tau > 1 \). \( \square \)

**Lemma 11.** The following upper bound holds for Algorithm 1:

\[
\sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{[\Delta t]_j^2}{(\sqrt{[\nu_t]_j} + \kappa)^2} \right] \leq \sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{[\Delta t]_j^2}{[\nu_t]_j + \kappa} \right] \leq \sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{[\Delta t]_j^2}{\kappa^2} \right] \leq \frac{1}{\kappa^2} \sum_{t=0}^{T-1} \mathbb{E} \left\| \Delta_t + \eta_t \nabla f(\theta_t) - \eta_t \nabla f(\theta_t) \right\|^2 \leq \frac{2}{\kappa^2} \sum_{t=0}^{T-1} \mathbb{E} \left\| \Delta_t + \eta_t \nabla f(\theta_t) \right\|^2 \leq \frac{4\eta_t^2 \tau T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 \right) + \frac{20\eta_t^4 \tau^3 L^2 T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 + 6\tau \zeta_g^2 \right)
\]

**Proof.** We bound the desired quantity in the following manner:

\[
\sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{[\Delta t]_j^2}{(\sqrt{[\nu_t]_j} + \kappa)^2} \right] \leq \sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{[\Delta t]_j^2}{[\nu_t]_j + \kappa} \right] \leq \sum_{t=0}^{T-1} \sum_{j=1}^{d} \mathbb{E} \left[ \frac{[\Delta t]_j^2}{\kappa^2} \right] \leq \frac{1}{\kappa^2} \sum_{t=0}^{T-1} \mathbb{E} \left\| \Delta_t + \eta_t \nabla f(\theta_t) - \eta_t \nabla f(\theta_t) \right\|^2 \leq \frac{2}{\kappa^2} \sum_{t=0}^{T-1} \mathbb{E} \left\| \Delta_t + \eta_t \nabla f(\theta_t) \right\|^2 \leq \frac{4\eta_t^2 \tau T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 \right) + \frac{20\eta_t^4 \tau^3 L^2 T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 + 6\tau \zeta_g^2 \right) + \frac{2}{\kappa^2} \sum_{t=0}^{T-1} \mathbb{E} \left\| \Delta_t + \eta_t \nabla f(\theta_t) \right\|^2 \leq \frac{4\eta_t^2 \tau T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 \right) + \frac{20\eta_t^4 \tau^3 L^2 T}{\kappa^2} \left( \frac{1}{p} (G^2 + \zeta_i^2) + p \sigma^2 + 6\tau \zeta_g^2 \right). \quad (17)
\]
Then, we bound $T_4$ as follows

$$T_4 = 2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{n} \sum_{i=1}^{n} \sum_{\tau_i=0}^{\tau-1} \eta \left( -S^{(t,s)}_i (g^{(t,s)}_i + b^{(t,s)}_i) + \nabla f_i (\theta^{(t,s)}_i) - \nabla f_i (\theta^{(t,s)}_i) + \nabla f_i (\theta_i) + \nabla f (\theta_i) \right) \right|^2 \right]$$

$$= 2\eta_1^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{n} \sum_{i=1}^{n} \sum_{s=0}^{\tau-1} \eta \left( -S^{(t,s)}_i (g^{(t,s)}_i + b^{(t,s)}_i) + \nabla f_i (\theta^{(t,s)}_i) - \nabla f_i (\theta^{(t,s)}_i) + \nabla f_i (\theta_i) + \nabla f (\theta_i) \right) \right|^2 \right]$$

$$\leq 4\eta_1^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{n} \sum_{i=1}^{n} \sum_{s=0}^{\tau-1} S^{(t,s)}_i (g^{(t,s)}_i + b^{(t,s)}_i) - \nabla f_i (\theta^{(t,s)}_i) \right|^2 \right] + 4\eta_2^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{n} \sum_{i=1}^{n} \sum_{s=0}^{\tau-1} \nabla f_i (\theta^{(t,s)}_i) - \nabla f_i (\theta_i) \right|^2 \right]$$

$$\leq 4\eta_1^2 \sum_{t=0}^{T-1} \sum_{i=1}^{n} \sum_{s=0}^{\tau-1} \mathbb{E} \left[ \left| S^{(t,s)}_i (g^{(t,s)}_i + b^{(t,s)}_i) - \nabla f_i (\theta^{(t,s)}_i) \right|^2 \right] + 4\eta_2^2 \sum_{t=0}^{T-1} \sum_{i=1}^{n} \sum_{s=0}^{\tau-1} \mathbb{E} \left[ \left| \nabla f_i (\theta^{(t,s)}_i) - \nabla f_i (\theta_i) \right|^2 \right]$$

where the first inequality results from (7), the second inequality uses the independence of unbiased stochastic gradients $\{g^{(t,s)}_i, i \in [n], s \in [0, \tau]\}$ and (7), and the last inequality comes from Lemma 10. The result follows by plugging $T_1$ into (17).

### H Partial Participation

For the partial participation when $|W| < n$, the main changed in the proof is the upper bound of $T_4$. The rest of the proof is similar to that of Theorem 2, so we focus on bounding $T_4$ with partial participation here. Assume $W$ is sampled uniformly for all subsets of $[n]$ with size $r$ at each round. In this case, we have

$$T_4 = \frac{2}{\kappa^2} \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{|W|} \sum_{i \in W} \sum_{s=0}^{\tau-1} \eta \left( -S^{(t,s)}_i (g^{(t,s)}_i + b^{(t,s)}_i) + \nabla f_i (\theta^{(t,s)}_i) - \nabla f_i (\theta^{(t,s)}_i) + \nabla f_i (\theta_i) + \nabla f (\theta_i) \right) \right|^2 \right]$$

$$\leq 6\eta_1^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{r} \sum_{i \in W} \sum_{s=0}^{\tau-1} S^{(t,s)}_i (g^{(t,s)}_i + b^{(t,s)}_i) - \nabla f_i (\theta^{(t,s)}_i) \right|^2 \right] + 6\eta_2^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{r} \sum_{i \in W} \sum_{s=0}^{\tau-1} \nabla f_i (\theta^{(t,s)}_i) - \nabla f_i (\theta_i) \right|^2 \right]$$

$$+ 6\eta_1^2 \sum_{t=0}^{T-1} \sum_{i \in W} \sum_{s=0}^{\tau-1} \mathbb{E} \left[ \nabla f_i (\theta_i) - r \nabla f (\theta_i) \right]^2$$

$$\leq 6\eta_1^2 \sum_{t=0}^{T-1} \sum_{i \in W} \sum_{s=0}^{\tau-1} \mathbb{E} \left[ \nabla f_i (\theta_i) - r \nabla f (\theta_i) \right]^2$$

$$\leq 6T \eta_1^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{p} (G^2 + \zeta^2) + pd\sigma^2 \right| \right] + 3T \eta_1^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \nabla f (\theta_i) \right| \right]^2$$

$$+ \frac{6\eta_2^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \frac{1}{p} (G^2 + \zeta^2) + pd\sigma^2 + 6\tau_2^2 \right| \right] + \frac{6\eta_2^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \nabla f (\theta_i) \right| \right]^2}{k^2}}$$

$$+ \frac{6\eta_2^2 \sum_{t=0}^{T-1} \mathbb{E} \left[ \left| \nabla f (\theta_i) \right| \right]^2}{k^2}.$$
where the first inequality results from (7), the second inequality uses the independence of unbiased stochastic gradients \( \{g^{t,s}_i, i \in \mathcal{W}, s \in [0, \tau) \} \) and (7), and the last inequality comes from Lemma 10.