

A Novel Privacy Enhancement Scheme with Dynamic Quantization for Federated Learning

Yifan Wang, *Student Member, IEEE*, Xianghui Cao, *Senior Member, IEEE*,
Shi Jin, *Fellow, IEEE*, and Mo-Yuen Chow, *Fellow, IEEE*

Abstract—Federated learning (FL) has been widely regarded as a promising paradigm for privacy preservation of raw data in machine learning. Although data privacy in FL is locally protected to some extent, it is still a desideratum to enhance privacy and alleviate communication overhead caused by repetitively transmitting model parameters. Typically, these challenges are addressed separately, or jointly via a unified scheme that consists of noise-injected privacy mechanism and communication compression, which may lead to model corruption due to the introduced composite noise. In this work, we propose a novel model-splitting privacy-preserving FL (MSP-FL) scheme to achieve private FL with precise accuracy guarantee. Based upon MSP-FL, we further propose a model-splitting privacy-preserving FL with dynamic quantization (MSPDQ-FL) to mitigate the communication overhead, which incorporates a shrinking quantization interval to reduce the quantization error. We provide privacy and convergence analysis for both MSP-FL and MSPDQ-FL under non-i.i.d. dataset, partial clients participation and finite quantization level. Numerical results are presented to validate the superiority of the proposed schemes.

Index Terms—Federated learning, privacy preservation, model splitting, dynamic quantization, accuracy guarantee.

I. INTRODUCTION

EMPOWERED by immense amount of data, deep learning has become a breakthrough for a broad range of applications, adequately unleashing the power of data [1]. Deep learning is usually implemented in a centralized manner, where a powerful server has access to the entire data, risking leakage of privacy-sensitive data. Meanwhile, the communication overhead substantially increases, owing to the collection of massive raw data at the server. In response to these challenges, federated learning (FL) has emerged as a viable paradigm to prevent data leakage and reduce communication overhead [2]. FL enables the independent training of distributed client models on local dataset, orchestrated by the central server [3].

Typically, FL is designed by a decentralized parameter-server framework with a powerful server mastering the aggregation process, yet it is still desired to enhance the privacy of clients. Specifically, although data are not explicitly shared among clients, data privacy is still at risk of being divulged as adversaries are potentially able to reconstruct raw data

of a target client based on the exchanged model parameters [4]. There are many methods deal with extracting sensitive information from trained models, e.g., model-inversion attack, membership-inference attack and model-rebuild attack [5]–[7].

To cope with the privacy concern, some approaches in [8], [9] enhanced the privacy in FL by homomorphic encryption and splitting learning, however, resulted in severe computational burden and poor learning efficiency, respectively. An intuitive consideration involves integrating artificial noise into FL, namely differential private (DP)-based FL, known for its verifiable privacy guarantee [10]. In accordance with DP technique, local differential privacy (LDP) framework is widely adopted, wherein each local model parameter is perturbed by Laplacian or Gaussian noise before uploading [11], [12]. Especially, the authors in [13] were the first to theoretically analyze the convergence property of DP-based FL. To mitigate the adverse impact of DP noise, the authors in [14] proposed a novel DP perturbation mechanism employing amplitude-varying noise. Alternatively, in the context of average consensus, temporally or spatially correlated noise-based methods were devised for privacy preservation while maintaining accuracy [15]–[17]. For instance, a state decomposition method in [16] was proposed by decomposing each local state into two substates. However, such an approach is inapplicable to preserve privacy in decentralized FL by directly decomposing the model parameter according to certain public decomposition rule.

Regarding communication overhead, it becomes more urgent in privacy-preserving FL owing to the sacrifice of communication resource for privacy enhancement [13]. In order to compress the communication, prior works usually turn to reducing the volume of transmitted model updates via sparsification or quantization [18]–[20], aggregating with partially received information [21] and event-triggered communication [22]. In this paper, we mainly focus on tools from quantization theory to tackle communication overhead under finite communication bandwidth. It is worth noting that some recent works proposed attractive designs for quantization to further improve the communication efficiency [23], [24].

The aforementioned studies separately considered privacy concern and communication overhead in FL. Yet the privacy enhancement brought by LDP actually sacrifices the convergence accuracy of the model parameter, and in turn requires more communication cost for the interactions between the server and clients. Thereby, it naturally emerges a necessity to consider both challenges of privacy enhancement and communication compression for FL. Recently, a handful of studies

Y. Wang and X. Cao are with the School of Automation, Southeast University, Nanjing 210096, China (e-mail: {evan,xhcao}@seu.edu.cn).

S. Jin is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: jinshi@seu.edu.cn).

M.-Y. Chow is with the UM-SJTU Joint Institute Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: moyuen.chow@sjtu.edu.cn).

This work has been submitted to the IEEE for possible publication. Copyright may be transferred without notice, after which this version may no longer be accessible.

have jointly tackled privacy enhancement and communication efficiency in FL. The authors in [25] were the first to provide trade-off analysis on privacy, convergence and communication for convex loss functions. Later, in [26], a unified FL framework was proposed by exploiting general communication compression scheme and LDP mechanism for nonconvex optimization setting, together with concrete analysis on trade-offs among privacy, utility and communication. To avoid injecting excessive noise, noise from subtractive dithered quantization (SDQ) was utilized together with a low-power and dedicated privacy-preserving noise to build up LDP mechanism, hence, obtaining a less distorted model via such a joint design [27]. Nonetheless, these studies inevitably introduced persistent noise either from the LDP mechanism or lossy compression, compromising the model accuracy more or less. To the best of our knowledge, it still remains an open problem how to realize both privacy guarantee and communication efficiency in FL with exact model accuracy and provable convergence.

Driven by the aforementioned considerations, this paper emphasizes the necessity to simultaneously design privacy enhancement and compressed communication in FL. Concretely, instead of using LDP mechanism to enhance privacy, we firstly develop the state decomposition approach in FL coined model-splitting privacy-preserving FL (MSP-FL). Under MSP-FL, each local model parameter is split into two types of submodel parameters, wherein one of the submodel parameters is appointed as the visible submodel and the others are invisible. At each selected client, only the visible submodel parameter is uploaded to the channel. Note that, to avoid the observability of the remaining invisible submodel parameters, the number of invisible local submodel parameters is kept privately at each client. To proceed, on the basis of MSP-FL, we propose a model-splitting privacy-preserving with dynamic quantization FL (MSPDQ-FL), which is equipped with dynamic quantization intervals in channels to further reduce the volume of transmitted submodels. Given that MSP-FL ensures precise convergence accuracy if the number of communication rounds after each learning round is sufficiently large, hence, the privacy and quantization mechanisms can be independently designed in MSPDQ-FL. This is exactly one of the major differences between our work and [26], [27]. The main contributions of this paper are summarized as follows:

- We propose an MSP-FL for privacy enhancement in FL. In contrast to traditional LDP-based FL, MSP-FL can achieve exact model accuracy in expectation via correlated noise and specific interaction protocol designs for submodels. Meanwhile, a new privacy notion is used to measure the privacy degree due to the incompletely randomized characteristic of model splitting mechanism.
- To further reduce the communication overhead, we present a novel scheme coined MSPDQ-FL. By assigning dynamic quantization intervals, MSPDQ-FL asymptotically reduces the quantization errors during the transmissions.
- We rigorously analyze the convergence performance of both MSP-FL and MSPDQ-FL. The results theoretically prove that the model parameter errors stemming from

privacy enhancement and quantization can be eliminated, as long as the number of communication rounds K_t following each learning round t exceed a lower bound.

- From the perspective of differential privacy, we explore the sufficient condition of model splitting rule for differential privacy noise. In addition, we prove that the proposed quantization scheme achieves at least $(0, \delta)$ -differential privacy under provable convergence accuracy.

Organization: Section II introduces the system model and threat model. Section III presents MSP-FL along with theoretical analysis of privacy and convergence properties. Section IV further extends MSP-FL to MSPDQ-FL by incorporating dynamic quantization. Discussions are presented in Section V. Numerical results are shown in Section VI. Finally, Section VII concludes the paper.

Notations: Throughout this paper, we introduce the following conventions: Sets are represented by upper calligraphy letters; vectors are represented by bold lowercase letters; matrices are denoted by bold uppercase letters; scalars are written as regular lowercase or uppercase letters. $\mathbb{R}^d$, $^*\mathbb{R}^d$ and $\mathbb{R}^{n \times d}$ denote the sets of real vectors of dimension d , hyperreal vectors of dimension d , and real matrices of dimension $n \times d$, respectively. The identity matrix and the vector of ones are represented by $\mathbf{I}$ and $\mathbf{1}$ with proper dimensions, respectively. The superscript $\top$ denotes the transpose of a vector or matrix. Let $\text{col}(w_1, \dots, w_n)$ be a column vector of $\{w_i \in \mathbb{R} | i = 1, \dots, n\}$. $[i]$ is the index number of i in a set or sequence. For a matrix $\mathbf{U}$, $\lambda_{k, \mathbf{U}}$ denotes the k -th largest eigenvalue of $\mathbf{U}$, and $\lambda_{\min, \mathbf{U}}$ is the smallest one. Denote by $\|\cdot\|$ the Euclidean norm (or Frobenius norm) of a vector (or a matrix). The stochastic expectation is denoted by $\mathbb{E}\{\cdot\}$.

II. PRELIMINARIES

This section reviews a basic framework of FL and presents the considered problem together with threat model.

A. System Model

In FL, a server and a set of clients $\mathcal{N} = \{1, \dots, N\}$ collaboratively train a model, parameterized by $\mathbf{w} \in \mathbb{R}^d$, by solving the following decentralized learning problem

$$\min_{\mathbf{w} \in \mathbb{R}^d} F(\mathbf{w}) \triangleq \sum_{i=1}^N p_i F_i(\mathbf{w}), \quad (1)$$

where $F_i(\mathbf{w})$ is the local loss function of i -th client which evaluates the fitness between the global model parameter¹ $\mathbf{w}$ and the local dataset $\mathcal{D}_i$. $p_i = |\mathcal{D}_i| / \sum_{i=1}^N |\mathcal{D}_i|$, where $|\mathcal{D}_i|$ denotes the size of $\mathcal{D}_i$. Therewith, one can conclude that the global loss function $F(\mathbf{w})$ evaluates how well the global model fits the overall data of all the clients. Given a mini-batch sample ζ_i with data size s_i , the local loss function can be further represented as $F_i(\mathbf{w}, \zeta^i) = \frac{1}{s_i} \sum_{j=1}^{s_i} f_i(\mathbf{w}, \zeta^{i,j})$, where $f_i(\mathbf{w}, \zeta^{i,j})$ is the local loss function with respect to the j -th selected data sample in ζ^i . If the mini-batch sample is the whole local dataset, i.e., $s_i = |\mathcal{D}_i|$, it has $F_i(\mathbf{w}, \zeta^i) = F_i(\mathbf{w})$.

¹In the remaining paper, the ‘model parameter’ is called ‘model’ for brevity.

For the learning problem in (1), we make the following assumptions that are commonly employed in the context of distributed learning [18], [22], [27], [28].

Assumption 1. (*Assumptions on loss functions and gradients*)

1) (*Convexity*) Each loss function F_i is μ -strongly convex, i.e., for all $\mathbf{v}$ and $\mathbf{w}$, it has $F_i(\mathbf{v}) - F_i(\mathbf{w}) - \nabla F_i(\mathbf{w})^\top (\mathbf{v} - \mathbf{w}) \geq \frac{\mu}{2} \|\mathbf{v} - \mathbf{w}\|^2$.

2) (*Smoothness*) Each loss function F_i is L -Lipschitz smooth, i.e., for all $\mathbf{v}$ and $\mathbf{w}$, it has $F_i(\mathbf{v}) - F_i(\mathbf{w}) - \nabla F_i(\mathbf{w})^\top (\mathbf{v} - \mathbf{w}) \leq \frac{L}{2} \|\mathbf{v} - \mathbf{w}\|^2$.

3) (*Bounded variance of stochastic gradients*) For each client, the variance of the stochastic gradient on any mini-batch data is bounded by a positive constant σ_i , i.e., $\mathbb{E} \{ \|\nabla F_i(\mathbf{w}_t^i, \xi^i) - \nabla F_i(\mathbf{w}_t^i)\|^2 \} \leq \sigma_i, \forall i \in \mathcal{N}$ and $\forall t$.

4) (*Uniformly bounded stochastic gradients*) There exists a positive constant $G > 0$, such that the expected squared norm of the stochastic gradients are uniformly bounded, i.e., $\mathbb{E} \{ \|\nabla F_i(\mathbf{w}_t^i, \xi^i)\|^2 \} \leq G, \forall i \in \mathcal{N}$ and $\forall t$.

In this work, we consider a general FL system model that follows FedAvg with only partial clients participating in model uploading after each learning round and with non-i.i.d. data distribution² [29]. Specifically, the server and clients execute the following procedures at each learning round t :

(1) **Server broadcasts global model to partial clients.** The server randomly selects a set of clients, denoted as $\mathcal{S}_t$ with $|\mathcal{S}_t| = M$, and broadcasts the latest global model $\mathbf{w}_{t-1}$ to the selected clients.

(2) **Clients update local models.** Based on the received global model, each client $i \in \mathcal{S}_t$ updates its local model by iteratively running the mini-batch stochastic gradient descent (SGD) method as follows:

$$\mathbf{w}_{t,0}^i = \mathbf{w}_{t-1}, \quad (2a)$$

$$\mathbf{w}_{t,e+1}^i = \mathbf{w}_{t,e}^i - \eta_t \nabla F_i(\mathbf{w}_{t,e}^i, \xi_e^i), \forall e \in \{0, \dots, E-1\}, \quad (2b)$$

$$\mathbf{w}_t^i = \mathbf{w}_{t,E}^i, \quad (2c)$$

where E is the number of SGD updates during each learning round. η_t is a time-varying learning rate to be designed. $\mathbf{w}_t^i$ is the updated local model for upload.

(3) **Clients upload local models for global aggregation.** Clients in $\mathcal{S}_t$ upload local models to the server. Then, the server generates a new global model by average aggregation. The learning process terminates after a total of T rounds.

B. Threat Model

We assume that there exists a trusted authority in the considered FL scenario besides the clients and the central server, where the trusted authority provides trusted and limited information exchanges among legitimate clients. Meanwhile, adversaries are considered as follows:

Honest-but-curious adversaries follow the stipulated protocol without falsifying the shared information. Meanwhile,

adversaries attempt at least two classes of attacks: i) *data-oriented attacks*—such as model inversion, membership inference, and gradient/parameter-leakage (e.g., iDLG)—which aim to reconstruct an individual example or test its presence in a client's dataset and can even recover labels or images from a single step [5], [7]; ii) *model-oriented attacks*—such as model and functionality stealing attacks which try to infer a client's local model parameters or create a knock-off model that should be indistinguishable to the adversary [30], [31]. Both types of attacks pose a direct and substantial threat to model privacy. We denote them as a set $\mathcal{A}_h \triangleq \mathcal{A}_c \cup \mathcal{A}_s$, where $\mathcal{A}_c$ denotes the set of honest-but-curious clients and $\mathcal{A}_s$ denotes the server. Note that the information is shared with each other in $\mathcal{A}_h$.

The considered threat model that consists of both honest-but-curious server and clients is commonly seen in the field of FL [32]. Meanwhile, such a threat model exist in many practical scenarios that are in the form of non-cooperative game problem [33], [34]. For instance, in the problem of grid-to-vehicle energy exchange between a smart grid and plug-in electric vehicle groups (PEVG), each PEVG aims to maximize the benefit from consumed energy or minimize the cost, while the grid aims to maximize the revenue by selling energy surplus to PEVGs. Therefore, the curious grid tends to control the nature of energy consumption of PEVGs. Most PEVGs tend to protect their own privacy and are curious about others' privacy information including energy consumption in order to maximize their own utility. However, some PEVGs might collaboratively share inferred information with the grid, one possibility being that they are stakeholders in the market (e.g., an energy trading center and its affiliated units). In extreme cases, e.g., when all clients are compromised, the honest-but-curious server may share inferences with all clients. Regarding the implementation of privacy inference sharing, it can be directly achieved through the existing communication channels between the server and (honest-but-curious) clients. For privacy inference sharing among (honest-but-curious) clients, the server can support the sharing by acting as a relay.

In some other works, external eavesdroppers are also considered as a type of adversaries, which wiretap all transmitted data and attempt to estimate local models by certain estimating algorithm. Usually, eavesdroppers are more disruptive than honest-but-curious adversaries, because they can estimate local models by certain algorithms with the accumulated information. However, owing to the existence of the honest-but-curious server, external eavesdroppers actually access less information than honest-but-curious adversaries. Hence, we mainly consider the privacy preservation in FL against adversaries in the set $\mathcal{A}_h$ in this paper.

III. MSP-FL: MODEL-SPLITTING PRIVACY-PRESERVING FEDERATED LEARNING

In this section, we first present MSP-FL, and then provide analysis of its privacy and convergence properties.

A. The Proposed Privacy-preserving Scheme: MSP-FL

To simultaneously make provision for privacy enhancement and learning accuracy, the key idea of MSP-FL which is

²The degree of non-i.i.d., namely heterogeneity, is quantified as $\Gamma = F^* - \sum_{i=1}^N p_i F_i^*$, where F^* and F_i^* denote the minimum values of global loss function and local loss function, respectively [28].

inspired by [16], is stochastically splitting each local model into two types of submodels, i.e., a visible and invisible submodels, and uploading the visible ones to the server. Compared to FedAvg, MSP-FL brings about subsequent K_t communication rounds between the server and clients after each learning round t instead of one round communication.

The overall illustration of MSP-FL is depicted in Fig. 1. Concrete details about model splitting mechanism³ are stated as follows: Let's denote the index of an arbitrarily selected client as i . At each learning round t , once entirely finishing training its local model $\mathbf{w}_t^i$ as described in (2), it splits $\mathbf{w}_t^i$ into $m_i + 1$ submodels where $m_i \geq 1$ is unknown to any client $j \in \{S_t \setminus i\}$ and the server, and randomly assigns initial values for submodels. Without loss of generality, we denote one of submodels as $\mathbf{w}_t^{i,\alpha} \in \mathbb{R}^d$, and the others as $\mathbf{w}_t^{i,\beta_n} \in \mathbb{R}^d$, $n \in \{1, \dots, m_i\}$. The criteria for randomly selecting initial values of submodels is: The initial value of $\mathbf{w}_t^{i,\alpha}$, denoted by $\mathbf{w}_t^{i,\alpha}[0]$ is randomly drawn from a uniform distribution over the interval $[\varepsilon \mathbf{w}_t^i, (2 - \varepsilon) \mathbf{w}_t^i]$ where $\varepsilon \in [0, 1)$ is a splitting factor. Initial values of other submodels, denoted by $\mathbf{w}_t^{i,\beta_n}[0]$, $n \in \{1, \dots, m_i\}$, are not required to be selected in this manner but satisfy $\sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[0] = (1 + m_i) \mathbf{w}_t^{i,\alpha}[0]$. After such a model splitting procedure, client i uploads $\mathbf{w}_t^{i,\alpha}[0]$ to the server, while $\mathbf{w}_t^{i,\beta_n}[0]$, $n \in \{1, \dots, m_i\}$, are kept private and only interact internally with $\mathbf{w}_t^{i,\alpha}[0]$. It is precisely for this fact that we refer to $\mathbf{w}_t^{i,\alpha}$ as the visible submodel and $\mathbf{w}_t^{i,\beta_n}$, $n \in \{1, \dots, m_i\}$, as invisible submodels for any $i \in S_t$. The reason for such a selection is discussed in Remark 1. In the subsequent communication rounds between the server and the selected clients after the learning round t , the i -th client downloads the latest global model from the server, which is an average aggregation of visible submodels (i.e., $\frac{1}{M} \sum_{i \in S_t} \mathbf{w}_t^{i,\alpha}[k]$), to update the current local submodels.

In such a manner, one can see that only the visible part, which acts the role of the original local model, is exposed to the server or an eavesdropper either in the uplink or downlink channels, though the invisible part internally interacts with it.

Under the proposed MSP-FL, the updating rule of the selected i -th client after t -th learning round is given as follows:

$$\mathbf{w}_t^{i,\alpha}[k+1] = \mathbf{w}_t^{i,\alpha}[k] + \epsilon \left(\mathbf{w}_t[k] - \mathbf{w}_t^{i,\alpha}[k] \right) + \sum_{n=1}^{m_i} a_{i,\alpha\beta_n}[k] \left(\mathbf{w}_t^{i,\beta_n}[k] - \mathbf{w}_t^{i,\alpha}[k] \right), \quad (3a)$$

$$\mathbf{w}_t^{i,\beta_n}[k+1] = \mathbf{w}_t^{i,\beta_n}[k] + a_{i,\alpha\beta_n}[k] \left(\mathbf{w}_t^{i,\alpha}[k] - \mathbf{w}_t^{i,\beta_n}[k] \right), \quad n = 1, 2, \dots, m_i, \quad (3b)$$

where ϵ is a design parameter. $a_{i,\alpha\beta_n}[k]$ is a weight between the visible submodel and the n -th invisible submodel of client

³Model splitting in our work differs from the split learning explored in other research such as [35]. In our proposed model splitting, the model parameters are randomly partitioned into submodel parameters, while preserving the dimensionality during aggregation. In contrast, split learning aims to divide the machine learning model (e.g., a deep neural network) into at least two submodels, typically involving a few layers of the entire network, resulting in dimensionality reduction. As such, each client only trains a submodel that consists of a subset of layers, while the remaining layers are trained at the server. In the remaining paper, the 'submodel parameter' is called 'submodel' for brevity, which actually differs from 'submodel' in split learning.

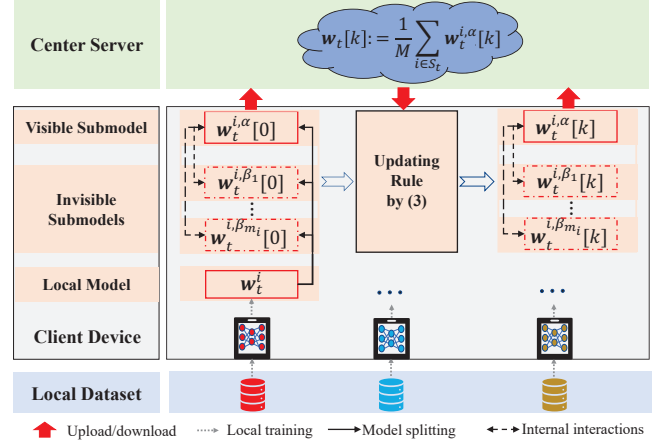


Fig. 1. Illustration of MSP-FL

i . $\mathbf{w}_t[k]$ is the global model at the k -th communication round. Correspondingly, the current $(k+1)$ -th aggregation at the server side is given by

$$\mathbf{w}_t[k+1] = \frac{1}{M} \sum_{i \in S_t} \mathbf{w}_t^{i,\alpha}[k+1]. \quad (4)$$

From (3) and (4), one can observe that

$$\begin{aligned} & \sum_{i \in S_t} \left(\mathbf{w}_t^{i,\alpha}[k+1] + \sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[k+1] \right) \\ &= \sum_{i \in S_t} \left(\mathbf{w}_t^{i,\alpha}[k] + \sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[k] + \epsilon \left(\mathbf{w}_t[k] - \mathbf{w}_t^{i,\alpha}[k] \right) \right). \end{aligned} \quad (5)$$

Clearly, by substituting (4) into (5), the sum of visible part and invisible part over the selected clients is time-invariant with respect to k after the current learning round. Meanwhile, this together with the asymptotic convergence result, that is, it guarantees to reach average consensus under dynamics (3) with appropriate step sizes and weights, yields $\lim_{k \rightarrow \infty} \mathbf{w}_t^{i,\alpha}[k] = \lim_{k \rightarrow \infty} \mathbf{w}_t^{i,\beta_n}[k], \forall i \in S_t, n \in \{1, \dots, m_i\}$. That is to say, privacy-utility trade-off can be avoided via dedicated designs for injected noises and interaction protocol as in (3) for submodels. However, in practical settings of FL, both the visible and invisible parts are unable to achieve completely consensus state due to the restricted communication resources. Thereby, following a finite and variable number of communication rounds denoted by K_t that depends on t , the global model is determined as an aggregated value of the last communication round, i.e.,

$$\mathbf{w}_t = \frac{1}{M} \sum_{i \in S_t} \mathbf{w}_t^{i,\alpha}[K_t]. \quad (6)$$

Additionally, the clients selection scheme in this work is in line with [28], [36]. Specifically, the clients contained in S_t are randomly selected with replacement for M times according to the independent distribution probabilities $p_1, \dots, p_N$. Then, it has the following lemma about unbiased sampling scheme.

Lemma 1. *Under the above random clients selection scheme, the partial aggregation after t -th learning round as shown in*

(6) is an unbiased estimation of the full aggregation $\tilde{\mathbf{w}}_t = \sum_{i=1}^N p_i \mathbf{w}_t^{i,\alpha}[K_t]$ with regard to any $\mathcal{S}_t$, i.e., $\mathbb{E}\{\mathbf{w}_t\} = \tilde{\mathbf{w}}_t$.

Proof. The proof of Lemma 1 follows the line of proof of Lemma 4 in [28]. Denote a fixed sequence as $\{\mathbf{w}_t^{i_j,\alpha}[K_t] | i = 1, \dots, N\}$, and a multiset $\mathcal{S}_t = \{i_1, \dots, i_M\} \subset \mathcal{N}$ is sampled at sampling time t where each sample $\mathbf{w}_t^{i_j,\alpha}[K_t]$ is selected with probability q_i . Meanwhile, we require each sampling distribution to be identical. Then, we have the following observation:

$$\begin{aligned} \mathbb{E}\left\{\frac{1}{M} \sum_{j \in \mathcal{S}_t} \mathbf{w}_t^{j,\alpha}[K_t]\right\} &= \mathbb{E}\left\{\frac{1}{M} \sum_{j=1}^M \mathbf{w}_t^{i_j,\alpha}[K_t]\right\} \\ &= \mathbb{E}\left\{\mathbf{w}_t^{i_j,\alpha}[K_t]\right\}, \quad \forall i_j \in \mathcal{S}_t, \end{aligned} \quad (7)$$

where the last equality is obtained by the identical sampling distribution. Moreover, recalling that $\mathbb{E}\{\mathbf{w}_t^{i_j,\alpha}[K_t]\} = \sum_{i=1}^N q_i \mathbf{w}_t^{i,\alpha}[K_t]$. By selecting the probability q_i as p_i , we complete the proof. $\square$

Remark 1. Note that, after the entire training process at each learning round t , the initial value of each visible submodel, i.e., $\mathbf{w}_t^{i,\alpha}[0]$, is randomly drawn from the uniform distribution over the interval $[\varepsilon \mathbf{w}_t^i, (1 + m_i - \varepsilon) \mathbf{w}_t^i]$. The reason is that, as such, it follows with two key properties that are shown in Lemma 8: (1) unbiased stochastic splitting; (2) bounded aggregation error of visible submodels. For those invisible submodels, we can also randomly select their initial values in a similar criterion as long as the condition $\sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[0] = (1 + m_i) \mathbf{w}_t^i - \mathbf{w}_t^{i,\alpha}[0]$ still holds.

B. The Property of Privacy Preservation

In this subsection, we will present analysis of MSP-FL for its privacy guarantee in the presence of adversaries.

For the sake of subsequent analysis, some notations are given as follows. Let us rewrite the term $\epsilon(\mathbf{w}_t[k] - \mathbf{w}_t^{i,\alpha}[k])$ in (3a) as $\epsilon \sum_{j \in \mathcal{S}_t} \alpha_j[k] (\mathbf{w}_t^{j,\alpha}[k] - \mathbf{w}_t^{i,\alpha}[k])$, where $\alpha_j[k] = \frac{1}{M}$ for all $j \in \mathcal{S}_t$ and $k \in \{0, 1, \dots, K_t - 1\}$. Denote the information set accessible to $\mathcal{A}_h$ at the k -th communication round after the t -th learning round as $\mathcal{I}_t^{\mathcal{A}_h}[k] = \{\mathcal{I}_t^j[k], \mathcal{I}_t^{\mathcal{A}_s}[k] | j \in \mathcal{A}_c\}$, where $\mathcal{I}_t^j[k] = \{\mathbf{w}_t^{j,\alpha}[k], \mathbf{w}_t^{j,\beta_n}[k], \alpha_j[k], a_{j,\alpha\beta_n}[k], \mathbf{w}_t[k] | n \in \{1, \dots, m_j\}\}$ and $\mathcal{I}_t^{\mathcal{A}_s}[k] = \{\mathbf{w}_t^{i,\alpha}[k] | i \in \mathcal{S}_t\}$.

To see the performance of privacy preservation, we first show the nondeterminacy of local models.

Lemma 2. Under MSP-FL, for any $i \in \mathcal{S}_t$, if m_i is inaccessible to $\mathcal{A}_h$, then the local model $\mathbf{w}_t^i$ is indeterminate to any adversary in $\mathcal{A}_h$ in an asymptotic sense.

Proof. Let $\mathbf{z}_t^i[k] = \mathbf{w}_t^{i,\alpha}[k] + \sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[k]$. By (3a) and (3b), one has

$$\mathbf{z}_t^i[k+1] = \mathbf{z}_t^i[k] + \epsilon(\mathbf{w}_t[k] - \mathbf{w}_t^{i,\alpha}[k]).$$

By summing the above equation for all k together, we have

$$\mathbf{z}_t^i[0] = \lim_{k \rightarrow \infty} \left[\mathbf{z}_t^i[k] - \epsilon \sum_{k=1}^{k-1} (\mathbf{w}_t[k_1] - \mathbf{w}_t^{i,\alpha}[k_1]) \right]. \quad (8)$$

One can observe that any adversary in $\mathcal{A}_h$ can not exactly infer the value of $\lim_{k \rightarrow \infty} \mathbf{z}_t^i[k]$, due to the unknown number

of local invisible submodels. Consequently, $\mathbf{w}_t^i$ is not uniquely estimated by any adversary in $\mathcal{A}_h$ by $\mathbf{z}_t^i[0]$ from (8). $\square$

Remark 2. For any $i \in \mathcal{S}_t$, if m_i is fixed and known to $\mathcal{A}_h$, then MSP-FL degrades to a direct application of the state decomposition mechanism in [16]. In this circumstance, $\mathbf{w}_t^i$ is uniquely determined by the adversary set $\mathcal{A}_h$ by (8) in an asymptotic sense because $\lim_{k \rightarrow \infty} \mathbf{z}_t^i[k] = \lim_{k \rightarrow \infty} (1 + m_i) \mathbf{w}_t^{i,\alpha}[k]$. Even though $k = K_t < \infty$ in FL resulting in an incomplete consensus among local submodels, an adversary can still derive a sufficiently approximate range of $\mathbf{w}_t^i$ from an estimated $\mathbf{z}_t^i[K_t]$. The observation reveals that direct application of the state decomposition mechanism in [16] is unserviceable to preserve the privacy in FL. An intuitive explanation is that, in a decentralized network, it can be deemed that any legitimate client j of client i is directly connected to $\mathcal{A}_h$, resulting in the term $\mathbf{w}_t[k_1] - \mathbf{w}_t^{i,\alpha}[k_1]$ in (8) losing its capability to help preserve the initial value $\mathbf{z}_t^i[0]$. Once the convergence value of $\lim_{k \rightarrow \infty} \mathbf{z}_t^i[k]$ or its approximate range can be easily obtained, then $\mathbf{z}_t^i[0]$ is estimated with some probability. In our work, we show that one of the cruxes to alter the determinacy of local model in such a decentralized network by (8) is to hide the local splitting rule, specifically, to simply hide the number of local invisible submodels. This is one of the differences between this work and others following the line of state decomposition mechanism, e.g., [16].

Now, we show the indistinguishability of the information set accessible to adversaries in $\mathcal{A}_h$. Define $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$ as the union of information set until the time instant $k = K_t$ after the t -th learning round. For any feasible $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$, denote $\mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$ as the set of all feasible local models $\mathbf{w}_t^i$ at client i that a set of initial submodels $\{\mathbf{w}_t^{l,\alpha}[0], \mathbf{w}_t^{l,\beta_n}[0] | l \in \mathcal{S}_t, n \in \{1, \dots, m_l\}\}$ and a set of weight sequences $\{a_{l,\alpha\beta_n}[k], \alpha_l[k] | l \in \mathcal{S}_t, n \in \{1, \dots, m_l\}, k \in \{0, 1, \dots, K_t - 1\}\}$ exist such that the set of sequences $\{a_{j,\alpha\beta_n}[k_1], \alpha_j[k_1], \mathbf{w}_t^{j,\alpha}[k_2], \mathbf{w}_t^{j,\beta_n}[k_2] | j \in \mathcal{A}_c, i \in \mathcal{S}_t, n \in \{1, \dots, m_j\}, k_1 \in \{0, 1, \dots, K_t - 1\}, k_2 \in \{0, 1, \dots, K_t\}\}$ generated by MSP-FL is the same as that in the adversary information set $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$.

The intrinsic meaning of set $\mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$ is that it comprises all possible current local models of client i that yields the same $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$. Meanwhile, we define the diameter of $\mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$ as

$$\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)) = \sup_{\{\mathbf{w}_t^i, \bar{\mathbf{w}}_t^i\} \in \mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)} \|\mathbf{w}_t^i - \bar{\mathbf{w}}_t^i\|. \quad (9)$$

In light of (9), we introduce the considered model-oriented privacy notion to evaluate the privacy degree of MSP-FL. Similar privacy notions can be found in literatures [37]–[41].

Definition 1. The privacy of the local model of client i after t -th learning round is said to be insensitive to any adversary in $\mathcal{A}_h$ if $\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)) = \infty$ for any feasible $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$.

The privacy notion in Definition 1 is extended from the concept of ℓ -diversity [37]. It measures the diversity of sensitive information of a selected client i (i.e., the local model $\mathbf{w}_t^i$ as well as its associated data), which is represented by the diameter of the set $\mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$. In FL, we treat the

continuous-valued model parameter vector $\mathbf{w}_t^i$, for $i \in \mathcal{S}_t$ after any learning round t , as the sensitive information and measure its diversity by $\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t))$.

Remark 3. The proposed model splitting mechanism is still in line with noise-adding approaches, wherein the added noise for assigning initial values of submodels are spatially correlated and zero-sum. A distinctive design is the subsequent multiple rounds of interaction between local submodels and the server as described in (3a) and (3b). This process enables the asymptotic elimination of spatially correlated noise, thereby avoiding the trade-off between learning accuracy and privacy. However, regarding the dynamics of this interaction protocol, there is no stochasticity. Moreover, we do not require any specific statistic model for the noise resulting from model splitting. These features render probability-based privacy definitions, e.g., differential privacy, unsuitable for evaluating the privacy preservation provided by our proposed method, and necessitate the introduction of the privacy notion in Definition 1 which indicates the indistinguishability in a definite sense between any two adjacent model parameters $\forall i \in \mathcal{S}_t$.

Remark 4. Under Definition 1, an extreme situation of privacy leakage is that $\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)) = 0$, implying that an adversary is able to uniquely determine a model parameter $\mathbf{w}_t^i$ via its accessible information set at learning round t . Such an extreme situation of privacy leakage is possible if the rules of model splitting and interactions among local submodels are known to an adversary, e.g., the hidden splitting number m_i is disclosed.

In the literature on privacy-preserving federated learning, there are various privacy definitions, wherein differential privacy stands as the prominent position. Preliminaries of standard data-oriented differential privacy and model-oriented differential privacy are given below.

Definition 2. (Adjacent datasets [10]) Two datasets at client i denoted as $\mathcal{D}_i^{(1)} = \{\mathcal{D}_{i,j}^{(1)}\}_{j=1}^n$ and $\mathcal{D}_i^{(2)} = \{\mathcal{D}_{i,j}^{(2)}\}_{j=1}^n$ are said to be adjacent if there exists some $j_0 \in \{1, 2, \dots, n\}$ such that $\mathcal{D}_{i,j}^{(1)} = \mathcal{D}_{i,j}^{(2)}$ for any $j \neq j_0$ and $\mathcal{D}_{i,j_0}^{(1)} \neq \mathcal{D}_{i,j_0}^{(2)}$.

Definition 3. (data-oriented ϵ_{DP} -differential privacy [10]) Given $\epsilon_{DP} > 0$, a randomized mechanism $\mathcal{M} : \mathcal{X} \rightarrow \mathcal{R}$ with domain $\mathcal{X}$ and range $\mathcal{R}$ satisfies ϵ_{DP} -differential privacy, if for any observation $\mathcal{S} \subseteq \mathcal{R}$ and for any pair of adjacent datasets $\mathcal{D}_i^{(1)}$ and $\mathcal{D}_i^{(2)} \in \mathcal{X}$, it has

$$\Pr(\mathcal{M}(\mathcal{D}_i^{(1)}) \in \mathcal{S}) \leq e^{\epsilon_{DP}} \Pr(\mathcal{M}(\mathcal{D}_i^{(2)}) \in \mathcal{S}). \quad (10)$$

Definition 4. (σ -adjacent model parameters⁴) Given $\sigma \in \mathbb{R}_+$, the model parameters x and y are σ -adjacent if, for some $i_0 \in \{1, 2, \dots, d\}$,

$$|x_i - y_i| \leq \begin{cases} \sigma, & \text{if } i = i_0 \\ 0, & \text{otherwise} \end{cases}$$

for $i \in \{1, 2, \dots, d\}$, where $x, y \in \mathbb{R}^d$.

⁴The concept of adjacent model parameters follows from σ -adjacency defined for state variables in dynamic systems [42].

Definition 5. (model-oriented ϵ_{DP} -differential privacy) Given $\epsilon_{DP} > 0$, a randomized mechanism $\mathcal{M} : \mathbb{R}^d \rightarrow \mathcal{R}$ with domain $\mathcal{X}$ and range $\mathcal{R}$ satisfies ϵ_{DP} -differential privacy, if for any observation $\mathcal{S} \subseteq \mathcal{R}$ and for any pair of σ -adjacent model parameters $\mathbf{w}_i^{(1)}$ and $\mathbf{w}_i^{(2)} \in \mathbb{R}^d$, it has

$$\Pr(\mathcal{M}(\mathbf{w}_i^{(1)}) \in \mathcal{S}) \leq e^{\epsilon_{DP}} \Pr(\mathcal{M}(\mathbf{w}_i^{(2)}) \in \mathcal{S}).$$

In what follows, we discuss the connections between the privacy notion in Definition 1 and differential privacy notion.

Remark 5. Compared to DP, Definition 1 gives only prerequisites while falling short of established privacy guarantees with probabilistic resolution. Even in earlier works that introduce this type of privacy notion, such as [16], [38], provable privacy guarantees akin to those in DP remain absent. The intrinsic meaning of DP is that an adversary cannot distinguish between any two adjacent inputs with certain probability based on the output of a randomized mechanism. In this regard, Definition 1 is similar to DP as it also evaluates the indistinguishability of the inputs (i.e., model parameters) of a privacy-preserving mechanism when the public information accessible to the adversary is always in an identical set $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$ (i.e., the resulting public information accessible to the adversary is always the same). Infinite diameter, i.e., $\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)) = \infty$, ensures that the indistinguishability of model privacy holds for any two adjacent model parameters $\mathbf{w}_t^{i,(1)}$ and $\mathbf{w}_t^{i,(2)}$ for $i \in \mathcal{S}_t$. Hence, to some extent, the concept of infinite diameter $\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)) = \infty$ in Definition 1 is similar to “any pair of adjacent datasets” in standard data-oriented DP notion. Major differences between these two privacy notions are:

- 1) Different privacy objects: The input of a randomized mechanism in differential privacy is dataset $\mathcal{D}$, while the privacy notion used in this paper defines the model parameters as the direct privacy object. Many methods including model-inversion and membership-inference attacks deal with extracting sensitive information from trained models. In certain neural networks with fully-connected layers, the input data to the network can be reconstructed uniquely from the network’s output [6]. Hence, model-oriented privacy notions like Definition 1 and Definition 5 are also of importance;
- 2) Probability of indistinguishability: In differential privacy, the outputs of a randomized mechanism over any two adjacent datasets are nearly statistically identical. While this event is in a definite sense as a condition of privacy preservation in Definition 1. Moreover, due to the ingenious design of model splitting mechanism in handling the injected noise, the privacy-utility trade-off is avoided. Therefore, there is no parameter similar to a privacy budget in this privacy notion.

Based on the above discussion, we know that a sufficient relationship whereby Definition 1 implies standard data-oriented differential privacy exists. The essential requirement is the existence of a “neighboring” mapping between the parameter solutions corresponding to different datasets (e.g., the modification of a single data sample leads to at most a change of Δ in the model parameters with probability 1).

In the sequel, we show that the privacy of any local model is protected against any honest-but-curious adversary in $\mathcal{A}_h$.

Theorem 1. *Under MSP-FL, for any $i \in \mathcal{S}_t$, if the number of invisible submodels (i.e., m_i) is inaccessible to $\mathcal{A}_h$, and there exists at least one legitimate client j that shares mutual trust with i via the trusted authority, then any adversary in $\mathcal{A}_h$ is unable to infer $\mathbf{w}_t^i$ with any guaranteed accuracy.*

Proof. Denote $\{\mathbf{w}_t^{l,\alpha}[0], \mathbf{w}_t^{l,\beta_n}[0], a_{l,\alpha\beta_n}[k], \alpha_l[k] | l \in \mathcal{S}_t, n \in \{1, \dots, m_l\}, k \in \{0, 1, \dots, K_t - 1\}\}$ as an arbitrary set consisting of sequences of weights and initial local submodels that satisfies $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$. According to the splitting rule, it has $(1+m_i)\mathbf{w}_t^i = \mathbf{w}_t^{i,\alpha}[0] + \sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[0], \forall i \in \mathcal{S}_t$. Meanwhile, let $\bar{\mathbf{w}}_t^i = \mathbf{w}_t^i + \mathbf{e}$ where $\mathbf{e} \in \mathbb{R}^d$ is an arbitrary hyperreal vector.

As one of the conditions of privacy preservation, we have proved in Lemma 2 that any adversary in $\mathcal{A}_h$ is unable to infer $\mathbf{w}_t^i$ by (8) based on the current accessible information. Then, to prove the privacy preservation for any selected client i against the set $\mathcal{A}_h$, it suffices to show the insensitivity or indistinguishability of information. That is, under any different local model $\bar{\mathbf{w}}_t^i$, there exists a set of sequences $\{\bar{\mathbf{w}}_t^{l,\alpha}[k_1], \bar{\mathbf{w}}_t^{l,\beta_n}[k_1], \bar{a}_{l,\alpha\beta_n}[k_2], \bar{\alpha}_l[k_2], | l \in \mathcal{S}_t, k_1 \in \{0, 1, \dots, K_t\}, k_2 \in \{0, 1, \dots, K_t - 1\}, n \in \{1, \dots, m_l\}\}$ such that $\bar{\mathbf{w}}_t^i \in \mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$. In other words, the information set $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$ accessible to honest-but-curious adversary set $\mathcal{A}_h$ is the same under any different $\bar{\mathbf{w}}_t^i$.

We show that if there exists at least one legitimate client $j \notin \mathcal{A}_h$ that cooperates with client i via the trusted authority, and by properly selecting initial values of submodels and weights, especially, $\{\bar{\mathbf{w}}_t^{i,\alpha}[0], \bar{\mathbf{w}}_t^{i,\beta_n}[0], \bar{a}_{i,\alpha\beta_n}[0], \bar{\alpha}_i[0] | n \in \{1, \dots, m_i\}\}$ and $\{\bar{\mathbf{w}}_t^{j,\alpha}[0], \bar{\mathbf{w}}_t^{j,\beta_n}[0], \bar{a}_{j,\alpha\beta_n}[0], \bar{\alpha}_j[0] | n \in \{1, \dots, m_j\}\}$, then it has $\bar{\mathbf{w}}_t^i \in \mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$. Specifically, initial values of local models and submodels are given by:

$$\begin{aligned} \bar{\mathbf{w}}_t^i &= \mathbf{w}_t^i + \mathbf{e}; \quad \bar{\mathbf{w}}_t^j = \mathbf{w}_t^j - \mathbf{e}, \\ \bar{\mathbf{w}}_t^{i,\alpha}[0] &= \mathbf{w}_t^{i,\alpha}[0]; \quad \bar{\mathbf{w}}_t^{i,\beta_n}[0] = \mathbf{w}_t^{i,\beta_n}[0], n \in \{1, \dots, m_i\} \setminus p, \\ \bar{\mathbf{w}}_t^{j,\alpha}[0] &= \mathbf{w}_t^{j,\alpha}[0]; \quad \bar{\mathbf{w}}_t^{j,\beta_n}[0] = \mathbf{w}_t^{j,\beta_n}[0], n \in \{1, \dots, m_j\} \setminus q, \\ \bar{\mathbf{w}}_t^{i,\beta_p}[0] &= (1+m_i)\bar{\mathbf{w}}_t^i - \bar{\mathbf{w}}_t^{i,\alpha}[0] - \sum_{n \in \{1, \dots, m_i\} \setminus p} \bar{\mathbf{w}}_t^{i,\beta_n}[0], \\ \bar{\mathbf{w}}_t^{j,\beta_q}[0] &= (1+m_j)\bar{\mathbf{w}}_t^j - \bar{\mathbf{w}}_t^{j,\alpha}[0] - \sum_{n \in \{1, \dots, m_j\} \setminus q} \bar{\mathbf{w}}_t^{j,\beta_n}[0], \\ \bar{\mathbf{w}}_t^l &= \mathbf{w}_t^l; \quad \bar{\mathbf{w}}_t^{l,\alpha}[0] = \mathbf{w}_t^{l,\alpha}[0]; \quad \bar{\mathbf{w}}_t^{l,\beta_n}[0] = \mathbf{w}_t^{l,\beta_n}[0], \\ &\quad \forall l \in \mathcal{S}_t \setminus \{i, j\}, n \in \{1, \dots, m_l\}, \end{aligned} \quad (11)$$

and the settings of weights are as follows:

$$\begin{aligned} \bar{a}_{i,\alpha\beta_p}[0] &= \frac{-(1+m_i)\mathbf{e} + a_{i,\alpha\beta_p}[0](\mathbf{w}_t^{i,\alpha}[0] - \mathbf{w}_t^{i,\beta_p}[0])}{\bar{\mathbf{w}}_t^{i,\alpha}[0] - \bar{\mathbf{w}}_t^{i,\beta_p}[0]}, \\ \bar{a}_{i,\alpha\beta_n}[0] &= a_{i,\alpha\beta_n}[0], \quad \forall n \in \{1, \dots, m_i\} \setminus p, \\ \bar{a}_{j,\alpha\beta_q}[0] &= \frac{(1+m_j)\mathbf{e} + a_{j,\alpha\beta_q}[0](\mathbf{w}_t^{j,\alpha}[0] - \mathbf{w}_t^{j,\beta_q}[0])}{\bar{\mathbf{w}}_t^{j,\alpha}[0] - \bar{\mathbf{w}}_t^{j,\beta_q}[0]}, \\ \bar{a}_{j,\alpha\beta_n}[0] &= a_{j,\alpha\beta_n}[0], \quad \forall n \in \{1, \dots, m_j\} \setminus q, \\ \bar{\alpha}_i[0] &= \frac{(1+m_i)\mathbf{e} + \epsilon\alpha_i(\mathbf{w}_t^{i,\alpha}[0] - \mathbf{w}_t^{i,\alpha}[0])}{\epsilon(\bar{\mathbf{w}}_t^{i,\alpha}[0] - \bar{\mathbf{w}}_t^{i,\alpha}[0])}, \\ \bar{\alpha}_j[0] &= \frac{-(1+m_j)\mathbf{e} + \epsilon\alpha_j(\mathbf{w}_t^{j,\alpha}[0] - \mathbf{w}_t^{j,\alpha}[0])}{\epsilon(\bar{\mathbf{w}}_t^{j,\alpha}[0] - \bar{\mathbf{w}}_t^{j,\alpha}[0])}, \end{aligned}$$

$$\begin{aligned} \bar{a}_{i,\alpha\beta_n}[k] &= a_{i,\alpha\beta_n}[k], \quad \forall n \in \{1, \dots, m_i\}, k \in \{1, \dots, K_t - 1\}, \\ \bar{a}_{j,\alpha\beta_n}[k] &= a_{j,\alpha\beta_n}[k], \quad \forall n \in \{1, \dots, m_j\}, k \in \{1, \dots, K_t - 1\}, \\ \bar{a}_{l,\alpha\beta_n}[k] &= a_{l,\alpha\beta_n}[k], \quad \forall l \in \mathcal{S}_t \setminus \{i, j\}, n \in \{1, \dots, m_l\}, \\ &\quad k \in \{0, \dots, K_t - 1\}, \\ \bar{\alpha}_i[k] &= \alpha_i[k] = \bar{\alpha}_j[k] = \alpha_j[k] = \frac{1}{M}, \quad k \in \{1, \dots, K_t - 1\}, \\ \bar{\alpha}_l[k] &= \alpha_l[k] = \frac{1}{M}, \quad \forall l \in \mathcal{S}_t \setminus \{i, j\}, k \in \{0, \dots, K_t - 1\}. \end{aligned} \quad (12)$$

Under (11) and (12), it can be verified with some calculations that the information set accessible to $\mathcal{A}_h$ is the same as $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$. Meanwhile, it implies that $\bar{\mathbf{w}}_t^i = \mathbf{w}_t^i + \mathbf{e} \in \mathcal{S}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t), i)$, which further yields

$$\text{Diam}(\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)) \geq \sup \|\bar{\mathbf{w}}_t^i - \mathbf{w}_t^i\| = \sup_{\mathbf{e} \in \mathbb{R}^d} \|\mathbf{e}\| = \infty.$$

By Definition 1, one has that the privacy of the local model of any client $i \in \mathcal{S}_t$ is insensitive to any honest-but-curious adversary in $\mathcal{A}_h$, if the difference between $\mathbf{w}_t^i$ and $\bar{\mathbf{w}}_t^i$ which is denoted by $\mathbf{e}$ can be transmitted via the trusted authority to j , and both initial visible submodels of client i and j are transmitted via the trusted authority to each other (i.e., the trust between client i and j is mutual via the trusted authority). Equipped with Lemma 2 which indicates the nondeterminacy of current local model under MSP-FL, the insensitivity of current information set accessible to $\mathcal{A}_h$ shows that the privacy of $\mathbf{w}_t^i, \forall i \in \mathcal{S}_t$, is preserved. $\square$

The key idea of the proof presented above can be interpreted as follows: Firstly, the first equation in (11) ensures that the sum of local models, denoted as $\sum_{i \in \mathcal{S}_t} \bar{\mathbf{w}}_t^i$, remains unchanged and equals to the original value $\sum_{i \in \mathcal{S}_t} \mathbf{w}_t^i$. Then, by maintaining the initial visible part invariant, any changes in local models are transferred to the initial invisible part, represented by $\bar{\mathbf{w}}_t^{i,\beta_p}[0]$ and $\bar{\mathbf{w}}_t^{j,\beta_q}[0]$. Simultaneously, the weight settings in (12) completely compensate for these changes from initial states. Consequently, the subsequent information set $\mathcal{I}_t^{\mathcal{A}_h}(0, K_t)$ accessible to $\mathcal{A}_h$ remains unchanged.

Remark 6. *It shall be pointed out that the coefficient of aggregation in (6) is still $1/M$, even though $\bar{\alpha}_i[0]$ and $\bar{\alpha}_j[0]$ are changed in the weight mechanism (12) for the local update of client i and j , respectively.*

Remark 7. *One can observe that the difference of local model at client i denoted by $\mathbf{e}$ together with $\mathbf{w}_t^{i,\alpha}[0]$ is transmitted via the trusted authority to legitimate client j to reconstruct a new set $\{\bar{\mathbf{w}}_t^{j,\alpha}[k], \bar{\mathbf{w}}_t^{j,\beta_n}[k], \bar{\alpha}_j[k], \bar{a}_{j,\alpha\beta_n}[k] | n \in \{1, \dots, m_j\}\}$. Nonetheless, it is impossible to leakage the information of local model, since the other transmitted information between clients and the server involves only visible part.*

C. The Sufficient Condition for Model Splitting Rule to Obtain Differential Privacy Noise

One may wonder how much noise resulting from model splitting rule is equivalent to differential privacy noise when assigning initial values for submodels? For clarity of exposition, we take Laplacian mechanism to achieve ϵ_{DP} -differential privacy for illustration. Let $\text{Laplace}(\mu, b)$ be a

Laplace distributed noise with location μ and scale b . Main result is presented in the following proposition. It shall be pointed out that, the discussed sufficient condition on the splitting rule does not conflict with the derivation of Lemma 8 (specifically, the equation (45)), because $\mathbb{E}_{SS}\{\mathbf{w}_t^{i,\alpha}[0]\} = \mathbf{w}_t^i$ still holds under the random selection scheme for $\mathbf{w}_t^{i,\alpha}[0]$ over $\text{Laplace}(\mathbf{w}_t^i, \Delta f/\epsilon_{DP})$. Similarly, the noise $\xi_{t,a}^i$ can be Gaussian noise to achieve (ϵ_{DP}, δ) -DP.

Proposition 1. *For any function $f : \mathbb{D} \rightarrow \mathbb{R}^d$ where $\mathbb{D}$ is a domain of datasets $\mathcal{D}$, if the initial value of $\mathbf{w}_t^{i,\alpha}[0]$ is randomly drawn as the distribution $\text{Laplace}(\mathbf{w}_t^i, \Delta f/\epsilon_{DP})$ where $\Delta f = \max_{\mathcal{D}_i^{(1)}, \mathcal{D}_i^{(2)}} \|f(\mathcal{D}_i^{(1)}) - f(\mathcal{D}_i^{(2)})\|_1$, then the injected noise $\xi_{t,a}^i$ resulting from stochastic splitting is equivalent to the random noise injected via data-oriented ϵ_{DP} -DP mechanism.*

Proof. Laplace mechanism is given as follows:

Definition 6. *For any function $f : \mathbb{D} \rightarrow \mathbb{R}^d$ where $\mathbb{D}$ is a domain of datasets $\mathcal{D}$, the Laplace mechanism defined as*

$$\mathcal{M}^{\text{Laplace}}(f(x), \epsilon_{DP}) = f(x) + [\varsigma_1, \dots, \varsigma_d]^\top, \quad (13)$$

is ϵ_{DP} -DP. In (13), $\varsigma_i \stackrel{i.i.d.}{\sim} \text{Laplace}(0, \Delta f/\epsilon_{DP})$, i.e., its probability density function at a realization $x \in \mathbb{R}$ is given by

$$\text{Laplace}(x|0, \Delta f/\epsilon_{DP}) = \frac{1}{2\Delta f/\epsilon_{DP}} \exp\left(-\frac{|x|}{\Delta f/\epsilon_{DP}}\right), \quad (14)$$

where $\Delta f \triangleq \max_{x,y \in \mathcal{D}} \|f(x) - f(y)\|_1$.

Recalling that the initial value of each visible submodel, i.e., $\mathbf{w}_t^{i,\alpha}[0]$, can be viewed as a noise-distorted variant of $\mathbf{w}_t^i$, hence, we rewrite $\mathbf{w}_t^{i,\alpha}[0]$ as

$$\mathbf{w}_t^{i,\alpha}[0] = \mathbf{w}_t^i + \xi_{t,a}^i, \quad (15)$$

wherein, the additive noise $\xi_{t,a}^i$ is determined by the splitting rule when assigning initial values for visible submodels. Obviously, the condition for the noise $\xi_{t,a}^i$ to satisfy the Laplace privacy-preserving noise as defined in Definition 4 is that

$$\mathbf{w}_t^{i,\alpha}[0] \sim \text{Laplace}(\mathbf{w}_t^i, \Delta f/\epsilon_{DP}). \quad (16)$$

That is, the initial value of $\mathbf{w}_t^{i,\alpha}[0]$ is randomly drawn as the Laplace distribution $\text{Laplace}(\mathbf{w}_t^i, \Delta f/\epsilon_{DP})$. It shall be pointed out that, this requirement on the splitting rule does not conflict with the derivation of Lemma 8 (specifically, the equation (45)), because $\mathbb{E}_{SS}\{\mathbf{w}_t^{i,\alpha}[0]\} = \mathbf{w}_t^i$ still holds under the random selection scheme for $\mathbf{w}_t^{i,\alpha}[0]$ over $\text{Laplace}(\mathbf{w}_t^i, \Delta f/\epsilon_{DP})$.

This completes the proof. $\square$

D. Convergence Analysis

To proceed, we analyze the convergence property of MSP-FL. For ease of presentation and analysis, the number of invisible local submodels is assumed to be $m_i = 1, \forall i \in \mathcal{S}_t$. Let $a_{\alpha\beta_1}^{\max} = \max\{a_{i,\alpha\beta_1}[k] | i \in \mathcal{S}_t, k \in \{0, \dots, K_t - 1\}\}$.

The following customary assumption is listed for analysis.

Assumption 2. (Uniformly bounded local models) *There exists a vector $\mathbf{w}_{\max} \in \mathbb{R}^d$ such that after multi steps of stochastic*

gradient descent, each local model is uniformly bounded, i.e., $\|\mathbf{w}_t^i\| \leq \|\mathbf{w}_{\max}\| \forall i \in \mathcal{N}$ and $t = 1, 2, \dots, T$.

Now we give the convergence result of MSP-FL.

Theorem 2. *Let $\vartheta = \max\{\frac{8L}{\mu}, E\} - 1, \epsilon \in (0, \frac{M}{M-1})$, $K_t = \lceil \log_{\lambda}^{2/\mu(\vartheta+t)} \rceil$ and $a_{\alpha\beta_1}^{\max} \in (0, \frac{\lambda_{\min, \mathbf{U}}}{1+\lambda_{\min, \mathbf{U}}})$ where $\mathbf{U}$ is defined in (39). Choose the diminishing learning rate as $\eta_t = \frac{2}{\mu(\vartheta+t)}$. Suppose that Assumptions 1-2 hold, then MSP-FL has the following convergence property:*

$$\mathbb{E}\{F(\bar{\mathbf{w}}_t)\} - F^* \leq \frac{8L}{\mu(\vartheta+t)} \left(\frac{2D_2}{\mu} + \frac{8L+\mu E}{2} \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\} \right) \quad (17)$$

where $D_2 = \frac{(2\epsilon^2-4\epsilon+8)}{3} C^2 \|\mathbf{w}_{\max}\|^2 + \sum_{i=1}^N p_i^2 \sigma_i + 6L\Gamma + 8(E-1)^2 G + \frac{4}{M} E^2 G$.

Proof. The proof is given in Appendix A. $\square$

In Theorem 2, we derive a bound on the objective value of the model learned via MSP-FL and that of the optimal model. The behavior of the bound in (17) implies the asymptotic convergence of MSP-FL with a rate of $\mathcal{O}(1/t)$. That is, as the number of learning rounds t progresses, the learned model converges to the optimal one with a difference decaying as $1/t$. The convergence rate is at the same order of FedAvg in [29] and FL with privacy and communication efficiency requirements in [26], [27], and it is better than the $\mathcal{O}(\log(t)/\sqrt{t})$ rate observed in [25]. One can observe from (17) that, for privacy enhancement considerations, the model splitting procedure indeed yields an additive term in D_2 . Specifically, D_2 contains several additive terms, wherein, the first term $\frac{(2\epsilon^2-4\epsilon+8)}{3} C^2 \|\mathbf{w}_{\max}\|^2$ is a derivative part resulting from privacy enhancement via model splitting mechanism, which is dictated by the splitting factor ϵ and the upper bound of model parameters. It is worth noting that $\epsilon \in [0, \frac{1+m_i}{2})$, and the splitting factor ϵ affects the selection of initial values of the visible submodels after local training process of each learning round. Therewith, it implies that, on one hand, a smaller splitting factor brings about a smaller impact of model splitting mechanism on the learning profile if the number of iterations in (3) is finite and fixed. On the other hand, a smaller splitting factor means that the initial random values selected for visible submodels are closer to the true model obtained at learning round t . $\sum_{i=1}^N p_i^2 \sigma_i$, $6L\Gamma$, $8(E-1)^2 G$ and $\frac{4}{M} E^2 G$ in D_2 reveal the impacts of stochastic gradients, heterogeneity of data distribution and model parameter, and partial clients participation on the learning profile, respectively. Detailed analysis about these terms can be found in the earlier research [28]. To further mitigate the impact of these heterogeneities, e.g., ‘client-drift’, please refer to methods including SCAFFOLD in [43].

IV. MODEL-SPLITTING PRIVACY-PRESERVING WITH DYNAMIC QUANTIZATION FEDERATED LEARNING

This section considers both privacy enhancement and quantization in FL, and proposes a scheme named MSPDQ-FL. Compared to vanilla FedAvg, MSP-FL results in totally

$\frac{\sum_{t=1}^T (K_t+1)}{T}$ times communication burden for privacy enhancement. To tackle this challenge, we utilize tools from quantization theory to reduce the usage of communication bandwidth. Simultaneously, the distortion induced by the compression of transmitted submodel is enforced to vanish as the dynamic quantization interval shrinks. Note that the dynamic quantization mechanism can be independently designed in such a joint scheme. The reason is that MSP-FL actually ensures exact convergence guarantee in expectation as long as the communication round K_t after each learning round t is larger than a dynamic lower bound, whereas, the communication round is independent of the design for quantization. The details of MSPDQ-FL are presented below.

A. The Proposed Scheme: MSPDQ-FL

For the split submodel $\mathbf{w}_t^{i,\alpha}[k]$ of the i -th client during the k -th communication round, it is assumed that any element of $\mathbf{w}_t^{i,\alpha}[k]$ is bounded in a closed interval, i.e., $w_t^{i,j,\alpha}[k] \in [w_{\min}^{i,\alpha}, w_{\max}^{i,\alpha}]$, $\forall j \in \{1, 2, \dots, d\}$, $\forall k$. Denote the quantization interval as $\mathcal{R}_i \triangleq [w_{\min}^{i,\alpha} \mathbf{1}, w_{\max}^{i,\alpha} \mathbf{1}]$. Given a quantization level l with the quantization bits $B = \lceil \log_2(l) \rceil$, the knobs uniformly spaced in the interval $\mathcal{R}_i$ are denoted as $\{c_0, c_1, \dots, c_{l-1}\}$, where $c_\tau = w_{\min}^{i,\alpha} + \tau \frac{w_{\max}^{i,\alpha} - w_{\min}^{i,\alpha}}{l-1}$, $\forall \tau = 0, 1, \dots, l-1$.

Suppose that the j -th element of submodel $\mathbf{w}_t^{i,\alpha}[k]$ is located in $[c_\tau, c_{\tau+1})$. Then, $w_t^{i,j,\alpha}[k]$ is quantized by the following stochastic quantizer:

$$\mathcal{Q}(w_t^{i,j,\alpha}[k]) = \begin{cases} \text{sign}(w_t^{i,j,\alpha}[k])c_\tau, & \text{w.p. } \frac{c_{\tau+1} - |w_t^{i,j,\alpha}[k]|}{c_{\tau+1} - c_\tau} \\ \text{sign}(w_t^{i,j,\alpha}[k])c_{\tau+1}, & \text{w.p. } \frac{|w_t^{i,j,\alpha}[k]| - c_\tau}{c_{\tau+1} - c_\tau} \end{cases} \quad (18)$$

where, for brevity, we denote $q_t^{i,j}[k] = \mathcal{Q}(w_t^{i,j,\alpha}[k])$ and $\mathbf{q}_t^i[k] = [q_t^{i,1}[k], q_t^{i,2}[k], \dots, q_t^{i,d}[k]]^\top$. ‘w.p.’ represents ‘with probability’. Additionally, one has the quantization error given by

$$\|\Delta_t^i[k]\| = \|\mathbf{q}_t^i[k] - \mathbf{w}_t^{i,\alpha}[k]\| \leq \frac{\sqrt{d}(w_{\max}^{i,\alpha} - w_{\min}^{i,\alpha})}{l-1}. \quad (19)$$

It can be observed from (19) that the quantization error is directly relevant to the magnitude of the quantization interval $[w_{\min}^{i,\alpha}, w_{\max}^{i,\alpha}]$, when the quantized level l is finite and fixed. In this work, our motivation that follows with [44] is to adaptively refine the quantization interval for such a stochastic quantizer as a dynamic one at each communication round, i.e., $\mathcal{R}_t^i[k]$. The magnitude of $\mathcal{R}_t^i[k]$ is designed to shrink as k goes. Specifically, given the current time instant as k , the quantization interval for the next communication round is determined by the current information as

$$\mathcal{R}_t^i[k+1] = \left[\mathbf{q}_t^i[k] - \frac{\pi_t a_{\alpha\beta_1}^{\max}[k]}{2} \mathbf{1}, \mathbf{q}_t^i[k] + \frac{\pi_t a_{\alpha\beta_1}^{\max}[k]}{2} \mathbf{1} \right], \quad (20)$$

where π_t is a parameter to be designed that governs the interval bounds during the communication rounds $k \in \{0, \dots, K_t\}$. $a_{\alpha\beta_1}^{\max}[k] \triangleq \max\{a_{i,\alpha\beta_1}[k] | i \in \mathcal{S}_t\}$ mainly controls the rate at which the dynamic quantization interval shrinks. As such, the variance of quantization error decays asymptotically as the

magnitude of quantization interval shrinks. We denote such stochastic dynamic quantizer as $\mathcal{Q}_k^i(\cdot)$.

Equipped with the aforementioned stochastic dynamic quantizer for model aggregation, the updating rule for submodels in MSPDQ-FL is written as follows:

$$\begin{aligned} \mathbf{w}_t^{i,\alpha}[k+1] &= \mathbf{w}_t^{i,\alpha}[k] + \epsilon(\mathbf{w}_t[k] - \mathbf{q}_t^i[k]) \\ &\quad + \sum_{n=1}^{m_i} a_{i,\alpha\beta_n}[k] \left(\mathbf{w}_t^{i,\beta_n}[k] - \mathbf{w}_t^{i,\alpha}[k] \right), \end{aligned} \quad (21a)$$

$$\mathbf{w}_t^{i,\beta_n}[k+1] = \mathbf{w}_t^{i,\beta_n}[k] + a_{i,\alpha\beta_n}[k] (\mathbf{w}_t^{i,\alpha}[k] - \mathbf{w}_t^{i,\beta_n}[k]), \quad n = 1, 2, \dots, m_i, \quad (21b)$$

where the aggregated model at the server is given by

$$\mathbf{w}_t[k+1] = \sum_{i \in \mathcal{S}_t} \frac{1}{M} \mathbf{q}_t^i[k+1]. \quad (22)$$

Detailed procedure of MSPDQ-FL is shown in Algorithm 1.

For the execution of MSPDQ-FL, we give the following initial settings: 1) $\mathbf{w}_t^{i,\alpha}[0] = \mathbf{q}_t^i[0] = c_\tau$ for some arbitrarily index $\tau \in \{0, \dots, l-1\}$; 2) Each initially split visible part submodel is randomly generated from a uniform distribution on the interval $[\varepsilon \mathbf{w}_t^i, (1+m_i-\varepsilon) \mathbf{w}_t^i]$ satisfying $\mathbf{w}_t^{i,\alpha}[0] + \sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[0] = (1+m_i) \mathbf{w}_t^i$ for all $i \in \mathcal{S}_t$ and $t = 1, 2, \dots, T$. Moreover, it requires that $\mathbf{w}_t^{i,\alpha}[0] = \mathbf{w}_t^{j,\alpha}[0]$, $\forall \{i, j\} \in \mathcal{S}_t$.⁵

Remark 8. The intuition of such a design for shrinking quantization interval is that, as the local updating rule in (21) proceeds after t -th learning round, client i becomes more certain about where the current submodel $\mathbf{w}_t^{i,\alpha}[k]$ is and the subsequent submodel $\mathbf{w}_t^{i,\alpha}[k+1]$ will be on the whole quantization interval. Based on the current information, it determines a shrinking quantization interval $\mathcal{R}_t^i[k+1]$ for the next communication round.

B. Privacy and Convergence Analysis

In this subsection, we present the analysis of MSPDQ-FL for its privacy preservation and convergence performance.

Proposition 2. Under MSPDQ-FL, for any $i \in \mathcal{S}_t$, any adversary in $\mathcal{A}_h$ is unable to infer $\mathbf{w}_t^i$ in the sense of expectation with any guaranteed accuracy, if the following conditions are satisfied: 1. At least one legitimate client j shares mutual trust with i via the trusted authority; 2. The number of invisible submodels m_i is inaccessible to adversaries in the set $\mathcal{A}_h$.

Proof. Note that the quantizer $\mathcal{Q}_k^i(\cdot)$ is unbiased as stated in Lemma 11, hence, the proof directly follows from the line of derivation in the proof of Theorem 1. $\square$

For ease of analysis, an additional assumption is listed below, and the number of invisible submodels of each selected client is assigned to be $m_i = 1 \forall i \in \mathcal{S}_t$, similarly as in Section III.C.

Assumption 3. (Adapted from Assumption 2 in [44]) Let $\pi_t = \frac{8(\epsilon + \tilde{\epsilon} + \tilde{\epsilon} \tilde{W}_{t,k}^{\max})}{1 - \lambda_2, \mathbf{U}}$ where $\tilde{\epsilon} = \max\{1, \epsilon\}$ and $\tilde{W}_{t,k}^{\max} =$

⁵The condition $\mathbf{w}_t^{i,\alpha}[0] = \mathbf{w}_t^{j,\alpha}[0]$, $\forall \{i, j\} \in \mathcal{S}_t$, can be achieved by the server to broadcast any uploaded $\mathbf{w}_t^{i,\alpha}[0]$ after each learning round.

Algorithm 1 MSPDQ-FL

```

1: Initialize global model  $\mathbf{w}_0, \epsilon \in (0, \frac{M}{M-1}), \tilde{\epsilon} = \max\{1, \epsilon\},$ 
    $\pi_t = \frac{8(\epsilon + \tilde{\epsilon} + \tilde{\epsilon}\tilde{W}_{t,k}^{\max})}{1 - \lambda_{2,U}}$  and  $a_{i,\alpha\beta_n}[k] = \frac{\gamma_i}{k+1} \quad \forall n \in$ 
    $\{1, 2, \dots, m_i\}$  and  $\gamma_i \in (0, \frac{\lambda_{\min,U}}{1 + \lambda_{\min,U}})$ ;
2: for  $t = 1, 2, \dots, T$  do
3:   Server selects  $M$  clients randomly with replacement
   by probabilities  $\{p_1, p_2, \dots, p_N\}$ , denoted by  $\mathcal{S}_t$ ;
4:   Server broadcasts  $\mathbf{w}_{t-1}$ ;
5:   for client  $i \in \mathcal{S}_t$  do in parallel
6:      $\mathbf{w}_{t,0}^i \leftarrow \mathbf{w}_{t-1}$ ;
7:      $K_t = \max \left\{ \left\lceil \log_{\lambda} \left( \frac{2}{\mu(\vartheta+t)} \right) \right\rceil, \left\lceil \frac{\mu(\vartheta+t)}{2} \right\rceil \right\};$ 
8:     Client updates local model as in (21);
9:   end for
10:  Each client  $i$  sets  $\mathbf{w}_t^i \leftarrow \mathbf{w}_{t,E}^i$ ;
11:  Each client  $i$  randomly splits  $\mathbf{w}_t^{i,\alpha}[0]$  from a uniform
  distribution on the interval  $[\epsilon \mathbf{w}_t^i, (1 + m_i - \epsilon) \mathbf{w}_t^i]$  with
   $\mathbf{w}_t^{i,\alpha}[0] + \sum_{n=1}^{m_i} \mathbf{w}_t^{i,\beta_n}[0] = (1 + m_i) \mathbf{w}_t^i[0]$ , and
   $\mathbf{w}_t^{i,\alpha}[0] = \mathbf{w}_t^{j,\alpha}[0], \forall \{i, j\} \in \mathcal{S}_t$ ;
12:  Each client  $i \in \mathcal{S}_t$  initializes
  

- Uniformly Divide  $[w_{\min}^{i,\alpha} \mathbf{1}, w_{\max}^{i,\alpha} \mathbf{1}]$  into  $l^d$  rectangular
    bins as  $w_{\min}^{i,\alpha} \mathbf{1} = \tau_1 \leq \dots \leq \tau_{l^d} \leq w_{\max}^{i,\alpha} \mathbf{1}$ ;
- Let  $\mathbf{w}_t^{i,\alpha}[0] = \mathbf{q}_t^{i,b}[0] = \tau_m$  for some  $m \in [0, l^d]$ . Compute  $\mathbf{q}_t^{i,b}[0]$  using the quantization scheme
     $\mathcal{Q}_0(\mathbf{w}_t^{i,\alpha}[0])$  over  $[w_{\min}^{i,\alpha} \mathbf{1}, w_{\max}^{i,\alpha} \mathbf{1}]$ ;
- A sequence of positive and non-increasing step sizes
     $\{a_{i,\alpha\beta_n}[k] | n = 1, 2, \dots, m_i\}$ ;


13:  Each client  $i \in \mathcal{S}_t$  uploads  $\mathbf{q}_t^{i,b}[0]$ ;
14:  Server receives  $\mathbf{q}_t^{i,b}[0]$  from clients, recovers  $\mathbf{q}_t^i[0]$ 
  from  $\mathbf{q}_t^{i,b}[0]$  over  $\mathcal{R}_t^i[0] = [w_{\min}^{i,\alpha} \mathbf{1}, w_{\max}^{i,\alpha} \mathbf{1}]$ , performs
  aggregation as (22) and broadcasts  $\mathbf{w}_t[0]$ ;
15:  for  $k = 0, 1, \dots, K_t - 1$  do
16:    for client  $i \in \mathcal{S}_t$  do in parallel
17:      Client  $i$  executes (21) to update  $\mathbf{w}_t^{i,\alpha}[k+1]$ ;
18:      Client  $i$  computes  $\mathbf{q}_t^{i,b}[k+1]$  and  $\mathbf{q}_t^{i,b}[k+1]$  by
       $\mathcal{Q}_{k+1}^i(\cdot)$  over (20);
19:      Client uploads  $\mathbf{q}_t^{i,b}[k+1]$ ;
20:    end for
21:    Server receives  $\mathbf{q}_t^{i,b}[k+1]$  from clients, recovers
     $\mathbf{q}_t^i[k+1]$  over  $\mathcal{R}_{t+1}^i(k+1)$ , performs aggregation
    as (22) and broadcasts  $\mathbf{w}_t[k+1]$ ;
22:  end for
23:  Server finds  $\mathbf{w}_t \leftarrow \mathbf{w}_t[K_t]$ ;
24: end for

```

$\max\{\|\mathbf{W}_t^{\alpha}[k_1] - \mathbf{W}_t^{\beta_1}[k_1]\| | k_1 \in \{0, \dots, k\}\}$. The number of bits B of the communication bandwidth satisfies

$$B \leq \log_2 \sqrt{M d \pi_t + 1}, \quad \forall t = 1, 2, \dots, T. \quad (23)$$

Our main result for the convergence analysis of MSPDQ-FL is stated as follows.

Theorem 3. Let ϑ, ϵ and η_t be defined in Theorem 2. In addition, let $K_t = \max\{\lceil \log_{\lambda}^{2/\mu(\vartheta+t)} \rceil, \lceil \frac{\mu(\vartheta+t)}{2} \rceil\}$ and the

diminishing step size $a_{i,\alpha\beta_1}[k]$ for all $i \in \mathcal{S}_t$ be designed as $\frac{\gamma_i}{k+1}$, where $\gamma_i \in (0, \frac{\lambda_{\min,U}}{1 + \lambda_{\min,U}})$. If Assumptions 1-3 hold, then the convergence property of MSPDQ-FL with fixed quantization level l satisfies

$$\mathbb{E}\{F(\bar{\mathbf{w}}_t)\} - F^* \leq \frac{8L}{\mu(\vartheta+t)} \left(\frac{2(D_2 + D_3)}{\mu} + \frac{8L + \mu E}{2} \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\} \right) \quad (24)$$

where $D_3 = \frac{d\gamma_{\max}^2 \tilde{\pi}^2}{4M(2^B - 1)^2}$, $\gamma_{\max} = \max\{\gamma_1, \dots, \gamma_N\}$ and $\tilde{\pi} = \frac{8(\epsilon + \tilde{\epsilon} + \tilde{\epsilon}\tilde{W}^{\max})}{1 - \lambda_{2,U}}$ with $\tilde{W}^{\max} = \max\{\tilde{W}_{t,k}^{\max} | t = 1, 2, \dots, T\}$.

Proof. The proof is given in Appendix B. $\square$

Remark 9. In the proofs of Theorem 2 and Theorem 3, Assumption 2 (namely, uniformly bounded local models) and Assumption 3 (including the condition of bounded difference between visible and invisible submodels) are used as part of sufficient conditions to guarantee the asymptotic convergence. Actually, both of these two conditions are reasonable since the communication resources are limited. Hence, it is impossible to transmit an infinitely large model or submodel.

In the above, one can see that, for both MSP-FL and MSPDQ-FL, $K_t + 1$ communication rounds are introduced after each t -th local training. Hence, in what follows, we study the communication complexity. As the communication complexity of MSP-FL follows similarly with that of MSPDQ-FL, we focus on the latter one. In the setting, the communication complexity is defined as the total number of uploads over the selected clients with the expected convergence accuracy ϱ .

Proposition 3. Given the conditions the same as those in Theorem 3, the communication complexity of MSPDQ-FL, denoted as $\mathbb{C}(\varrho)$, is upper bounded by

$$\mathbb{C}(\varrho) < M \lceil \mathbb{I}(\varrho) \rceil \left(1 + \mu\vartheta + \frac{\mu}{2} (1 + \lceil \mathbb{I}(\varrho) \rceil) \right), \quad (25)$$

where $\mathbb{I}(\varrho)$ is the learning round complexity given by $\mathbb{I}(\varrho) = \frac{\nu_2}{\varrho \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}} - \vartheta$, $\nu_2 = \max\left\{\frac{\rho^2(D_2 + D_3)}{\rho\mu - 1}, (\vartheta + 1) \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}\right\}$.

Proof. By (71), it has that

$$\begin{aligned} \frac{\mathbb{E}\{\|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2\}}{\mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}} &\leq \frac{\nu_2}{(\vartheta + t) \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}} \leq \varrho \\ \implies t &\geq \frac{\nu_2}{\varrho \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}} - \vartheta. \end{aligned} \quad (26)$$

Then, we conclude that the learning round complexity is $\mathbb{I}(\varrho) = \frac{\nu_2}{\varrho \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}} - \vartheta$. Building on the learning round complexity and recalling that, for each t , each client $i \in \mathcal{S}_t$ inherently engages in $K_t + 1$ communication rounds, hence, the total communication complexity $\mathbb{C}(\varrho)$ is given by

$$\mathbb{C}(\varrho) = \sum_{i \in \mathcal{N}} \text{Communication rounds of client } i = M \sum_{t=1}^{\lceil \mathbb{I}(\varrho) \rceil} (K_t + 1). \quad (27)$$

By substituting $K_t = \max\{\lceil \log_{\lambda}^{2/\mu(\vartheta+t)} \rceil, \lceil \frac{\mu(\vartheta+t)}{2} \rceil\}$ into (27), and using $K_t \leq \lceil \log_{\lambda}^{2/\mu(\vartheta+t)} \rceil + \frac{\mu(\vartheta+t)}{2}$ together with the basic inequality $\log(1+x) \leq x, \forall x > -1$, it has that

$$\begin{aligned} \mathbb{C}(\varrho) &= M \sum_{t=1}^{\lceil \mathbb{I}(\varrho) \rceil} (\lceil \mu(\vartheta+t) \rceil + 1) \\ &< M \lceil \mathbb{I}(\varrho) \rceil \left(1 + \mu\vartheta + \frac{\mu}{2} (1 + \lceil \mathbb{I}(\varrho) \rceil) \right). \end{aligned}$$

This completes the proof. $\square$

Here, we further investigate the privacy performance of MSPDQ-FL based on the preliminary results of the proposed quantizer presented in Lemma 10. Quantization introduces additional distortion into model parameters, even though the magnitude of distortion gradually weakens over time. That is, MSPDQ-FL achieves stronger privacy protection compared to MSP-FL. However, the composite privacy enhancement cannot be trivially analyzed in a probabilistic expression, because the partial dynamics of model splitting mechanism is not randomized and the privacy notion in this paper is not in a probabilistic expression. At this stage, we analyze the inherent privacy of the proposed quantizer by differential privacy notion.

Proposition 4. *Suppose that the difference between any two adjacent model parameters $\mathbf{w}_t^{i,\alpha,(1)}$ and $\mathbf{w}_t^{i,\alpha,(2)}$ is bounded by a positive constant C_4 , i.e., $\|\mathbf{w}_t^{i,\alpha,(1)} - \mathbf{w}_t^{i,\alpha,(2)}\|_1 \leq C_4$. If Assumption 3 holds, and the parameters of the proposed dynamic quantizer are set as in Lemma 10, then the proposed quantizer ensures at least $(0, \delta)$ -differential privacy with $\delta = \min \left\{ \frac{C_4(l-1)}{\pi_t a_{\alpha\beta_1}^{\max}[k]}, \frac{l-1}{2^B-1} \right\}$ for each element of the quantization input $w_t^{i,\alpha}[k] \forall i \in \mathcal{S}_t$.*

Proof. Since the quantization intervals are uniformly partitioned, we only need to analyze an arbitrary quantization interval between c_τ and $c_{\tau+1}$. According to the mechanism of stochastic quantization as in (18), one has that the quantized value of an element in $\mathbf{w}_t^{i,\alpha}[k]$ has different distributions. When $w_t^{i,j,\alpha}[k] \geq 0$,

$$\begin{cases} \Pr(\mathcal{Q}(w_t^{i,j,\alpha}[k]) = c_\tau \mid \mathbf{w}_t^{i,\alpha}) = \frac{c_{\tau+1} - |w_t^{i,j,\alpha}[k]|}{c_{\tau+1} - c_\tau} \\ \Pr(\mathcal{Q}(w_t^{i,j,\alpha}[k]) = c_{\tau+1} \mid \mathbf{w}_t^{i,\alpha}) = \frac{|w_t^{i,j,\alpha}[k]| - c_\tau}{c_{\tau+1} - c_\tau} \end{cases}, \quad (28)$$

and when $w_t^{i,j,\alpha}[k] < 0$,

$$\begin{cases} \Pr(\mathcal{Q}(w_t^{i,j,\alpha}[k]) = -c_\tau \mid \mathbf{w}_t^{i,\alpha}) = \frac{c_{\tau+1} - |w_t^{i,j,\alpha}[k]|}{c_{\tau+1} - c_\tau} \\ \Pr(\mathcal{Q}(w_t^{i,j,\alpha}[k]) = -c_{\tau+1} \mid \mathbf{w}_t^{i,\alpha}) = \frac{|w_t^{i,j,\alpha}[k]| - c_\tau}{c_{\tau+1} - c_\tau} \end{cases}. \quad (29)$$

Given that the quantization of each element is independent of that of other elements, we can consider the privacy of different elements separately. For simplicity of notation, we denote the j -th element of any two adjacent model parameters, $w_t^{i,j,\alpha,(1)}[k]$ and $w_t^{i,j,\alpha,(2)}[k]$, by $x_t^{i,j}$ and $y_t^{i,j}$, respectively. Since the difference between any two adjacent model parameters is bounded, it has $\|x_t^i - y_t^i\|_1 \leq C_4$ for some $C_4 > 0 \forall i \in \mathcal{N}$ and $\forall t \in \{1, 2, \dots, T\}$.

According to the definition of differential privacy, to prove that $(0, \delta)$ -differential privacy is achieved for some $\delta > 0$, i.e., $|\Pr(\mathcal{Q}(x_t^{i,j}) \in \mathcal{S} \mid x_t^{i,j}) - \Pr(\mathcal{Q}(y_t^{i,j}) \in \mathcal{S} \mid y_t^{i,j})| \leq \delta$ for all $\mathcal{S} \in \{\pm c_\tau, \pm c_{\tau+1}\}$ and all $x_t^{i,j}$ and $y_t^{i,j}$ with $\|x_t^i - y_t^i\|_1 \leq C_4$, the derivation can be divided into two cases: 1) $x_t^{i,j}$ and $y_t^{i,j}$ are of the same sign; 2) $x_t^{i,j}$ and $y_t^{i,j}$ are of different signs.

Case 1: Considering that both $x_t^{i,j}$ and $y_t^{i,j}$ are nonnegative. One has that

$$\begin{aligned} & \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| \Pr(\mathcal{Q}(x_t^{i,j}) = c_\tau) - \Pr(\mathcal{Q}(y_t^{i,j}) = c_\tau) \right| \\ &= \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| \frac{c_{\tau+1} - |x_t^{i,j}|}{c_{\tau+1} - c_\tau} - \frac{c_{\tau+1} - |y_t^{i,j}|}{c_{\tau+1} - c_\tau} \right| \\ &\leq \frac{|x_t^{i,j}| - |y_t^{i,j}|}{c_{\tau+1} - c_\tau} \\ &\leq \frac{C_4}{c_{\tau+1} - c_\tau}, \end{aligned} \quad (30)$$

and

$$\begin{aligned} & \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| \Pr(\mathcal{Q}(x_t^{i,j}) = c_{\tau+1}) - \Pr(\mathcal{Q}(y_t^{i,j}) = c_{\tau+1}) \right| \\ &= \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| \frac{|x_t^{i,j}| - c_\tau}{c_{\tau+1} - c_\tau} - \frac{|y_t^{i,j}| - c_\tau}{c_{\tau+1} - c_\tau} \right| \\ &\leq \frac{C_4}{c_{\tau+1} - c_\tau}. \end{aligned} \quad (31)$$

Similarly, one can obtain the same relation when both $x_t^{i,j}$ and $y_t^{i,j}$ are negative.

Case 2: Considering that $x_t^{i,j}$ and $y_t^{i,j}$ are of different signs. Assume $x_t^{i,j} \geq 0$ and $y_t^{i,j} < 0$. Based on the rule of stochastic quantization, one obtains that

$$\begin{aligned} & \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| \Pr(\mathcal{Q}(x_t^{i,j}) = -c_\tau) - \Pr(\mathcal{Q}(y_t^{i,j}) = -c_\tau) \right| \\ &= \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| 0 - \frac{c_{\tau+1} - |y_t^{i,j}|}{c_{\tau+1} - c_\tau} \right| \\ &\leq \frac{|\Delta_t^{i,j}[k]|}{c_{\tau+1} - c_\tau}, \end{aligned} \quad (32)$$

and

$$\begin{aligned} & \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| \Pr(\mathcal{Q}(x_t^{i,j}) = -c_{\tau+1}) - \Pr(\mathcal{Q}(y_t^{i,j}) = -c_{\tau+1}) \right| \\ &= \sup_{\|x_t^i - y_t^i\|_1 \leq C_4} \left| 0 - \frac{|y_t^{i,j}| - c_\tau}{c_{\tau+1} - c_\tau} \right| \\ &\leq \frac{|\Delta_t^{i,j}[k]|}{c_{\tau+1} - c_\tau}, \end{aligned} \quad (33)$$

where $\Delta_t^{i,j}[k]$ is the quantization error of j -th element. The same result can be obtained if $x_t^{i,j} < 0$ and $y_t^{i,j} \geq 0$.

Recalling that $c_{\tau+1} - c_\tau$ is determined by the dynamic quantization interval $\mathcal{R}_t^i[k+1] = \left[\mathbf{q}_t^i[k] - \frac{\pi_t a_{\alpha\beta_1}^{\max}[k]}{2} \mathbf{1}, \mathbf{q}_t^i[k] + \frac{\pi_t a_{\alpha\beta_1}^{\max}[k]}{2} \mathbf{1} \right]$, and there are l knobs located in the interval $\mathcal{R}_t^i[k]$. Hence, we have

$$c_{\tau+1} - c_\tau = \frac{\pi_t a_{\alpha\beta_1}^{\max}[k]}{l-1}, \quad (34)$$

where $a_{\alpha\beta_1}^{\max}[k] \triangleq \max\{a_{i,\alpha\beta_1}[k] \mid i \in \mathcal{S}_t\}$, and $a_{i,\alpha\beta_1}[k]$ is the diminishing step size (e.g., $a_{i,\alpha\beta_1}[k] = \frac{\gamma_i}{k+1}$ with $\gamma_i \in (0, \frac{\lambda_{\min, \mathbf{U}}}{1 + \lambda_{\min, \mathbf{U}}})$). Specific settings of parameters should satisfy the conditions as in Lemma 10 such that the quantization input is always located in the shrinking quantization interval.

Meanwhile, from Lemma 10, we have that the quantization error of each element in the model parameter vector is bounded by

$$|\Delta_t^{i,j}[k]| \leq \frac{\pi_t}{2^B - 1} a_{\alpha\beta_1}^{\max}[k], \quad (35)$$

where $B = \lceil \log_2(l) \rceil$.

Inserting (34) and (35) into (30)-(33) in Cases 1 and 2, we always have at least $(0, \delta)$ -differential privacy with $\delta = \min \left\{ \frac{C_4(l-1)}{\pi_t a_{\alpha\beta_1}^{\max}[k]}, \frac{l-1}{2^B-1} \right\}$ for each element of the quantization input $\mathbf{w}_t^{i,\alpha}[k]$ for each client $i \in \mathcal{S}_t$.

This completes the proof. $\square$

Remark 10. Regarding the tuning rule of the dynamic shrinking interval in $\mathcal{R}_t^i[k+1]$, two key parameters are involved, i.e., $a_{\alpha\beta_1}^{\max}[k]$ and $\widetilde{W}_{t,k}^{\max}$ in π_t . For the tuning rule of the decaying factor $a_{\alpha\beta_1}^{\max}[k]$, we can set $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{k+1}$ for all $i \in \mathcal{S}_t$ where $\gamma_{\max} \in (0, \frac{\lambda_{\min,U}}{1+\lambda_{\min,U}})$. For the tuning rule of $\widetilde{W}_{t,k}^{\max}$, we can iteratively compare the value of $\|\mathbf{W}_t^\alpha[k] - \mathbf{W}_t^{\beta_1}[k]\|$ with that of $\|\mathbf{W}_t^\alpha[k-1] - \mathbf{W}_t^{\beta_1}[k-1]\|$, and select the larger one as $\widetilde{W}_{t,k}^{\max}$, because $\|\mathbf{W}_t^\alpha[k-1] - \mathbf{W}_t^{\beta_1}[k-1]\|$ is the largest value up to the k -th communication round.

V. DISCUSSION

In this section, we give extended discussions on the strategy for nonconvex settings, and the impact of the scale of invisible submodels on the global model quality.

A. Extension to nonconvex settings

In nonconvex settings for FL, SGD is a widely used and efficient method. Under the Polyak-Łojasiewicz condition or general nonconvex assumption for objective functions, previous studies have established a rigorous theoretical foundation for SGD with almost sure convergence. For the linear speedup property of SGD variants, accelerated techniques, e.g., momentum methods [45], can be incorporated into SGD, which also increases the probability of optimization algorithms escaping from the local minimum. In our proposed algorithms (MSP-FL and MSPDQ-FL), SGD is still the primary method in the local training stage. Our designed modules for privacy enhancement and quantization lie in the communication process after the training stage. Consequently, the variants of our proposed algorithms in nonconvex settings can be naturally extended based on those strategies for nonconvex settings, e.g., momentum SGD and proximal approach [45], [46]. However, for the variants of our proposed algorithms in nonconvex settings, the analysis framework needs to be re-designed. Related literature usually uses the (average) expected squared gradient norm to characterize the convergence rate, because establishing the convergence rate for objective values, as in Theorems 2 and 3, is generally impossible.

B. Impact of the scale of invisible submodels

In the above, we consider the model splitting with $m_i = 1$ for all i for ease of convergence analysis. Here, we discuss the impact of the number of invisible submodels m_i for $i \in \mathcal{S}_t$ on the global model quality when $m_i \geq 2$. Denote $m =$

$\max\{m_i | i \in \mathcal{S}_t\}$, $\mathbf{A}_n[k] = \text{diag}(a_{i,\alpha\beta_n}[k] | i \in \mathcal{S}_t)$ for $n = 1, 2, \dots, m$, and $\hat{\mathbf{A}}[k] = \sum_{n=1}^m \mathbf{A}_n[k]$. We rewrite $\mathbf{P}[k]$ in (38) in the following formulation that is with $m \geq 2$:

$$\mathbf{P}[k] = \begin{bmatrix} \mathbf{U} - \hat{\mathbf{A}}[k] & \mathbf{A}_1[k] & \mathbf{A}_2[k] & \cdots & \mathbf{A}_m[k] \\ \mathbf{A}_1[k] & \mathbf{I} - \mathbf{A}_1[k] & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{A}_2[k] & \mathbf{0} & \mathbf{I} - \mathbf{A}_2[k] & \vdots & \vdots \\ \vdots & \vdots & \cdots & \ddots & \mathbf{0} \\ \mathbf{A}_m[k] & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{I} - \mathbf{A}_m[k] \end{bmatrix}. \quad (36)$$

Noting that m is the maximal number of local invisible submodels in the selected clients set $\mathcal{S}_t$, therewith some of diagonal entries in $\mathbf{A}_n[k]$, for $n = 2, 3, \dots, m$, are 0, i.e., $a_{i,\alpha\beta_n}[k] = 0$ for some $i \in \mathcal{S}_t$ and $n = 2, 3, \dots, m$.

By observing the state transition matrix $\mathbf{P}[k]$ in (36), we have that the conditions that suffice for the positive semi-definiteness of the matrix $\mathbf{P}[k]$ are $\epsilon \in (0, \frac{M}{M-1})$ and $\sum_{n=1}^m a_{\alpha\beta_n}^{\max} \in (0, \frac{\lambda_{\min,U}}{1+\lambda_{\min,U}})$, where $a_{\alpha\beta_n}^{\max} = \max\{a_{i,\alpha\beta_n} | i \in \mathcal{S}_t\}$. Clearly, if m_i is quite large, each non-zero $a_{i,\alpha\beta_n}$ for $n \in \{1, 2, \dots, m_i\}$ is assigned a small value for $i \in \mathcal{S}_t$. This, on one hand, leads to a slow rate for the update process in (3). On the other hand, given an irreducible stochastic matrix $\mathbf{P}[k]$ and a valid value for $a_{\alpha\beta_n}^{\max}$, $n = 1, 2, \dots, m$ that satisfies $\sum_{n=1}^m a_{\alpha\beta_n}^{\max} \in (0, \frac{\lambda_{\min,U}}{1+\lambda_{\min,U}})$, it is known that reducing diagonal elements (or equivalently increasing off-diagonal elements) can decrease the second largest eigenvalue of $\Phi(k, 0) \triangleq \mathbf{P}[k]\mathbf{P}[k-1] \dots \mathbf{P}[0]$, denoted by $\lambda_{2,\Phi(k,0)}$, as the number of invisible portions m increases. Consequently, the designed steps for the communication rounds K_t (e.g., $K_t = \lceil \log_{\lambda}^{2/\mu(\vartheta+t)} \rceil$ required in Theorem 2) may not be sufficient to suppress the accumulated model parameter errors due to model splitting where $\lambda \in (\lambda_{2,\Phi(k,0)}, 1)$. This leads to a significant degradation of the global model quality. The above provides a qualitative analysis of the impact of the number of invisible portions on the global model quality.

VI. NUMERICAL EXPERIMENTS

To validate the theoretical results, we present the simulations of the proposed MSP-FL and MSPDQ-FL. All the tests were conducted on the Ubuntu 18.04 operating system, with an Intel i7-10700 CPU running at 2.90 GHz and an Nvidia RTX3090 graphics card with 32 GB of video memory.

A. Experimental Setup

On the basis of python environment and pytorch platform, we build up a FL framework on image classification tasks. We train CNN models on the MNIST and CIFAR-10 datasets in a non-i.i.d fashion.

1) Models, Datasets and Parameters Settings:

- **MNIST Dataset:** The data, divided into 60000 training and 10000 test samples, is evenly distributed among $N = 100$ clients, from which $M = 20$ clients are selected to participate in aggregation. Major training parameters are: local mini-batch size $s_i = 10$, local epoch $E = 10$ and learning rate $\eta_t = \frac{1}{5(t+1)}$.

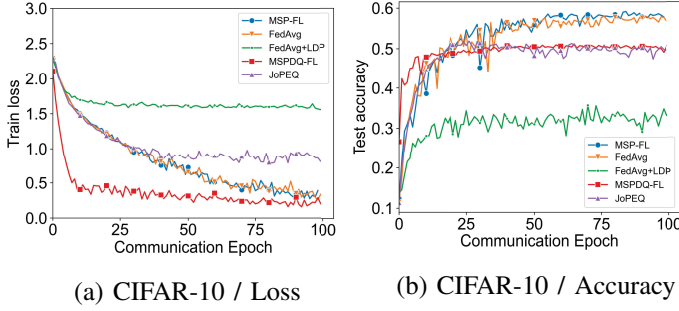


Fig. 2. Comparing the learning performance of MSP-FL, MSPDQ-FL and baselines on CIFAR-10 dataset.

- **CIFAR-10 Dataset:** The CIFAR-10 dataset has 50000 images for training and 10000 images for testing. The distribution of data samples is similar to the MNIST. Major training parameters are: local mini-batch size $s_i = 40$, local epoch $E = 5$ and learning rate $\eta_t = \frac{1}{10(t+1)}$.

2) **Baselines:** We compare MSP-FL and MSPDQ-FL with the following baselines:

- **FedAvg [29]:** Vanilla FL.
- **FedAvg+LDP [13]:** We deploy LDP technique into FedAvg as a baseline of MSP-FL to compare the testing accuracy.
- **JoPEQ:** We deploy JoPEQ from [27] as a baseline to compare the performance of MSPDQ-FL.

B. Numerical Results

1) **Learning performance of MSP-FL:** We begin by only focusing on evaluating the learning performance of MSP-FL and MSPDQ-FL in terms of training loss and testing accuracy under CIFAR-10 datasets. As a baseline, FedAvg+LDP is equipped with a privacy budget $\epsilon_{DP} = 10$. For MSP-FL, the communication round after each learning round is set as $K_t = 4$. While for MSPDQ-FL, the communication round is set as $K_t = 10$. The communication bits for MSPDQ and JoPEQ are both $B = 8$. We observe from Fig. 2 that MSP-FL achieves similar performance to FedAvg. Both MSP-FL and MSPDQ-FL show better performance than that of FedAvg+LDP or JoPEQ across all epochs under the CIFAR-10 dataset. It indicates that our proposed privacy-preserving mechanism in MSP-FL and MSPDQ-FL sacrifices less model precision during the aggregation process. If FedAvg+LDP combines with SDQ for communication efficiency with a carefully designed noise (i.e., JoPEQ), it presents a relatively poor learning performance compared to our proposed MSPDQ-FL. This is not surprising because the power of noise introduced by quantization in MSPDQ-FL significantly decreases compared to that in JoPEQ, as the quantization error asymptotically decays in the sense of expectation with the shrinking quantization interval.

2) **Learning performance and communication complexity of MSPDQ-FL:** In Fig. 3, we show the convergence performance of MSPDQ-FL under different K_t and B . Since the performance of MSP-FL under different K_t is similar to that of MSPDQ-FL, it is omitted. In the experiment, we notice that

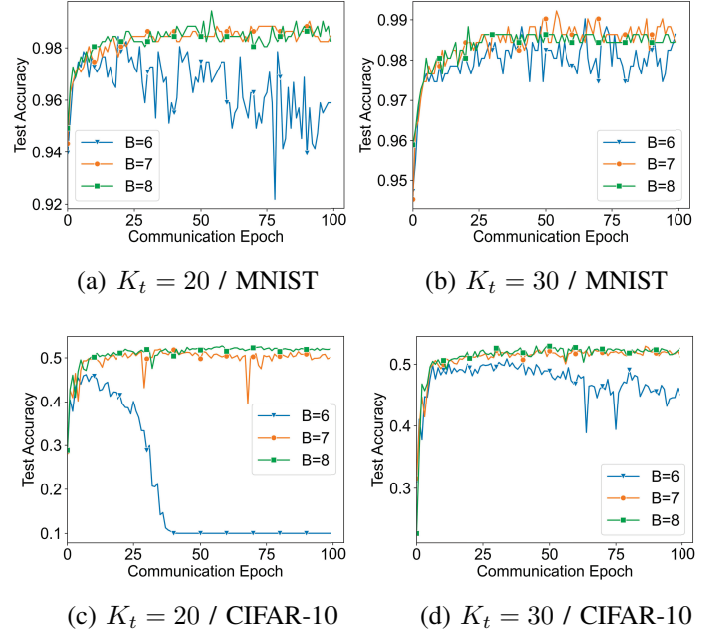


Fig. 3. Comparing the learning accuracy of MSPDQ-FL with different communication rounds and quantization bits.

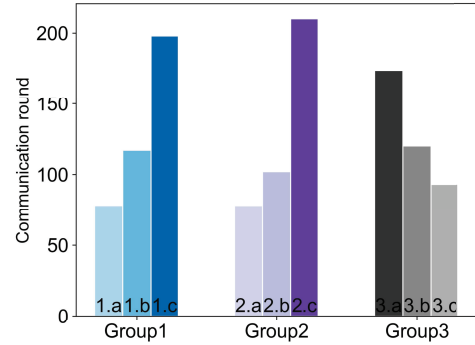
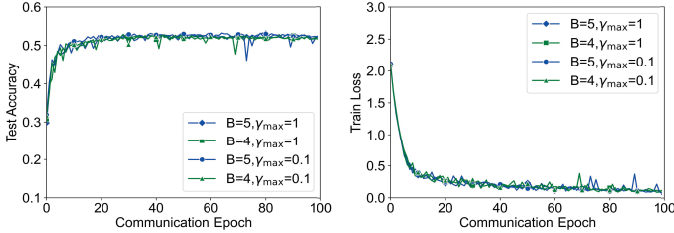


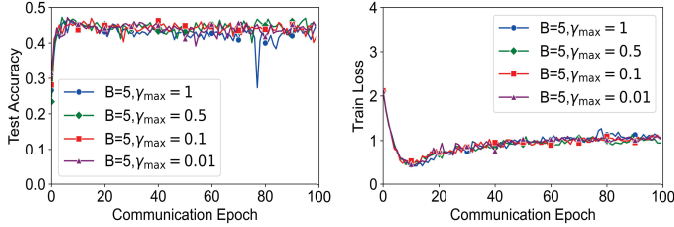
Fig. 4. The impact of different dominated coefficients on the communication complexity of MSPDQ-FL. Group 1 is dominated by prescribed learning error $\|\mathbf{w}_t - \mathbf{w}^*\|$, where the error ratio in 1.a, 1.b and 1.c is 4 : 3 : 2. Group 2 is dominated by communication bits B , where $B_{2.a} = 8$, $B_{2.b} = 7$ and $B_{2.c} = 6$. Group 3 is dominated by model-splitting coefficient ϵ , where $\epsilon_{3.a} = 0.3$, $\epsilon_{3.b} = 0.5$ and $\epsilon_{3.c} = 0.7$.

the value of K_t is mainly governed by a small strongly-convex coefficient μ as shown in Theorem 3 (e.g., set as 10^{-2}), hence, we set most K_t as constant. We observe in Fig. 3a and Fig. 3c that the test accuracy is normal in all cases during initial epochs. At around the 10th epoch, the test accuracy degrades under $B = 6$ in Fig. 3c, resulting from the fact that $K_t = 20$ is insufficient for the case under 6 bits as t increases. The explanation for such a fact is that, on one hand, it requires sufficient communication rounds for aggregation to reduce the error caused by model splitting; on the other hand, it needs a sufficiently large K_t to wait for the quantization interval to shrink into a small range, especially when the number of quantization bits is small.

In Fig. 4, we pick a few intuitively dominated coefficients to see their impacts on the communication complexity of



(a) $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{k+1} / \text{Accuracy}$ (b) $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{k+1} / \text{Loss}$



(c) $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{\sqrt{k+1}} / \text{Accuracy}$ (d) $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{\sqrt{k+1}} / \text{Loss}$

Fig. 5. Learning performance of MSPDQ-FL on CIFAR-10 dataset with $K_t = 20$ and different hyperparameters.

MSPDQ-FL. The results are reasonable and in accordance with the derived upper bound of communication complexity in Proposition 3.

In Fig. 5, we further investigate how sensitive the learning performance of MSPDQ-FL is to the major hyperparameters in shrinking quantization intervals. We set $\pi_t = \frac{8(\epsilon + \tilde{\epsilon} + \tilde{\epsilon} \tilde{W}_{t,k}^{\max})}{1 - \lambda_2, U}$, where $\tilde{W}_{t,k}^{\max} \triangleq \max\{\|\mathbf{W}_t^\alpha[k_1] - \mathbf{W}_t^{\beta_1}[k_1]\| \mid k_1 \in \{0, \dots, k\}\}$ iteratively finds its maximum value. The constant parameter $\gamma_{\max}$ in $a_{i,\alpha\beta_1}[k] \triangleq \frac{\gamma_{\max}}{k+1}$ is modified to show the impact of the dynamic quantization interval sizes on the learning performance. Moreover, considering the potential impact of the shrinking rate of the quantization intervals, we add a comparison result by setting $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{\sqrt{k+1}}$. Given a fixed rule for $a_{i,\alpha\beta_1}[k]$, we can observe from Fig. 5 that the parameter $\gamma_{\max}$, that influences the quantization interval sizes, has little impact on the learning performance in each subfigure. By comparing Fig. 5a with Fig. 5c or comparing Fig. 5b with Fig. 5d, one can see a decline of learning performance with the decaying factor $a_{i,\alpha\beta_1}[k] = \frac{\gamma_{\max}}{\sqrt{k+1}}$ for shrinking quantization intervals. This is because, under fixed quantization bits, quantization intervals $\mathcal{R}_t^i[k+1]$ with a slower decaying rate result in relatively larger quantization errors.

3) *Privacy leakage mitigation evaluation:* Here, we empirically verify the privacy guarantees of MSP-FL and MSPDQ-FL by assessing the defense performance against model inversion attacks. The attacks are implemented based on iDLG mechanism proposed in [5]. The setup including the image classification task, model architecture, dataset and attack parameters, follows the one in [5]. To evaluate the privacy leakage mitigation, mean squared error (MSE) is used to measure the discrepancy between the reconstructed images and truth label as the communication epoch progresses. Regarding

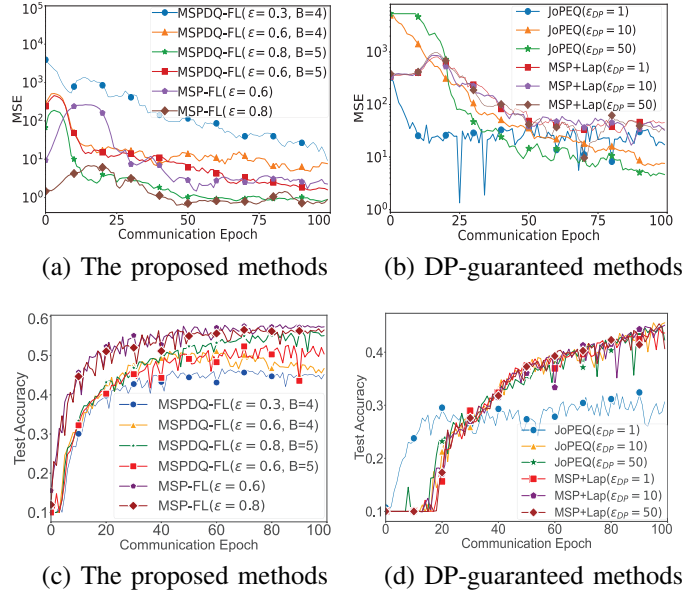


Fig. 6. MSE defense score and the corresponding learning accuracy under MSP-FL, MSPDQ-FL, MSP+Lap and JoPEQ.

the parameter setting, note that the initial values of submodels in the model splitting procedure are influenced by the splitting factor ϵ , hence we treat this factor as analogous to the privacy budget ϵ_{DP} in differential privacy although this has not yet been fully substantiated through rigorous theoretical analysis. Therewith, Fig. 6a presents the MSE defense score achieved by MSP-FL and MSPDQ-FL against iDLG under different splitting factors and quantization bits. As a comparison, Fig. 6b reports the MSE defense scores achieved by DP-based method (JoPEQ) under different privacy budgets ϵ_{DP} . The results indicate that, under the current parameter settings, our proposed methods provide a level of privacy protection comparable to that of DP-based method. Fig. 6a further demonstrates that, due to quantization noise, MSPDQ-FL brings stronger privacy protection than MSP-FL. As the number of quantization bits decreases, the MSE naturally increases. This is consistent with the existing conclusion, i.e., the quantization enhances privacy preservation.

Considering that the comparison between the proposed model splitting methods and the differential privacy method is somewhat unfair, even though our intention is only to demonstrate that the proposed methods provides a certain level of privacy protection rather than greater privacy strength than differential privacy methods, we supplement the MSE defense scores of MSP-FL under the splitting rule that guarantees differential privacy property for initial values of submodels in Fig. 6b. As discussed in Section III-C, there exists a splitting rule that ensures the noise injected into the initial submodel parameters follows a Laplace distribution. For simplicity, we denote the MSP-FL method with Laplace distribution for the injected noise as MSP+Lap. MSE scores of MSP+Lap in Fig. 6b demonstrate a matched privacy preservation level to DP-based method (JoPEQ). It is seen that the MSE scores of MSP+Lap exhibit consistency, and are slightly higher than

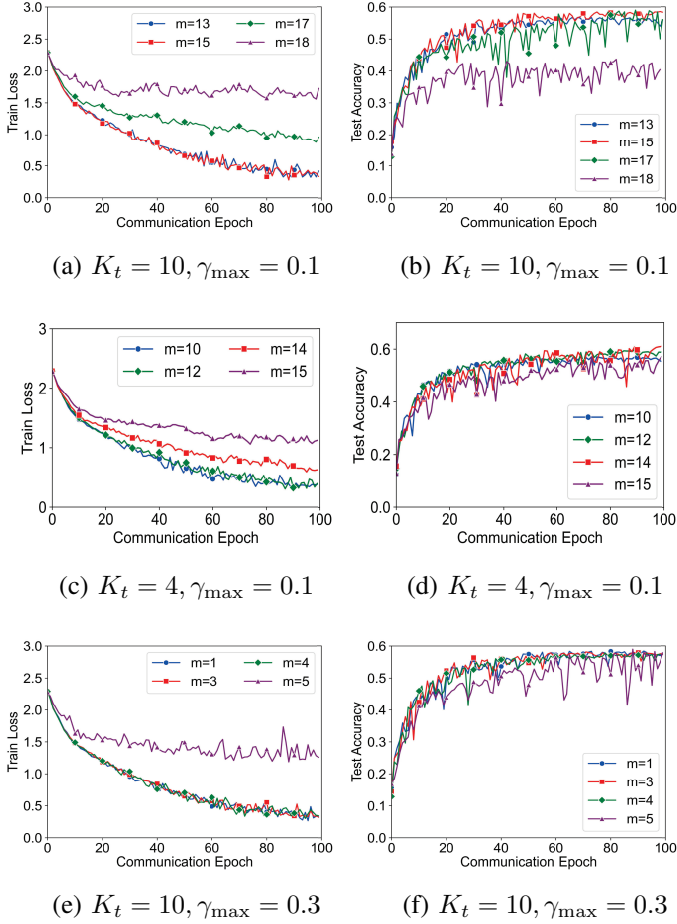


Fig. 7. Comparing the learning performance of MSP-FL on CIFAR-10 dataset with varying sizes of invisible submodels.

MSE scores of JoPEQ. Intuitively, this is because the Laplace noise injected via model splitting can be amplified by the discrepancies among local submodels during the dynamics as in (3a) and (3b).

We further test the learning accuracy of the abovementioned privacy-preserving methods under identical hyper-parameter settings to see the privacy-accuracy trade-off. The simulation results presented in Fig. 6a-6d, especially the blue curves (MSPDQ-FL with $\epsilon = 0.3$, $B = 4$ and JoPEQ with $\epsilon_{DP} = 1$), show that our proposed model splitting method does not suffer as severe learning accuracy degradation as traditional noise-adding methods while maintaining comparable privacy protection effects. For a fair comparison, the results in Fig. 6d show that MSP+Lap also achieves similar or better learning accuracy to JoPEQ across various ϵ_{DP} values. Notably, as illustrated in Fig. 6d, learning accuracy of MSP+Lap remains largely unaffected even when noise intensity increases to a privacy budget of $\epsilon_{DP} = 1$. This robustness stems from the zero-sum noise requirement in model splitting mechanism and the well-designed dynamics for the interaction of submodels, which mitigates the privacy-utility trade-off in the conventional noise-adding methods.

4) *Impact of the number of invisible submodels m_i* : Our subjective speculation for the impact is that, with the premise

of ensuring the learning accuracy, the value of m affects the least number of communication rounds K_t and the interaction weight $a_{i,\alpha\beta_n}[k]$ for all $i \in \mathcal{S}_t$, $n \in \{1, 2, \dots, m_i\}$. Given a fixed communication round K_t and the parameter $\gamma_{\max} \triangleq \max\{\gamma_1, \dots, \gamma_N\}$ (which is a key parameter in the formulation of interaction weights $a_{i,\alpha\beta_n}[k]$), Fig. 7a and Fig. 7b report the learning performance of MSP-FL with varying sizes of invisible submodels. As the proportion of invisible submodels increases, the results indicate an apparent reduction in learning performance when the maximal number of invisible submodels reaches a critical point at $m = 18$. That is, the global model quality is overly degraded if $m \geq 18$ under the current settings. Setting $K_t = 10$ and $\gamma_{\max} = 0.1$ as a benchmark, we further explore the impact of varying invisible submodel sizes m on the communication rounds K_t and interaction weight $a_{i,\alpha\beta_n}[k]$. We can observe from Fig. 7c and Fig. 7d that the maximal number of invisible submodels currently allowed is close to that in Fig. 7a and Fig. 7b with $K_t = 10$. This is because $K_t = 4$ is nearly the least number of communication rounds that suffices for the aggregation error to be suppressed. In Fig. 7e and Fig. 7f, we increase the key parameter $\gamma_{\max}$ in the interaction weight $a_{i,\alpha\beta_n}[k]$ for $i \in \mathcal{S}_t$ to 0.3, while keeping $K_t = 10$. In this case, the maximal number of invisible submodels allowed significantly decreases to $m = 4$. The result is consistent with the discussion in Section V-C. Similar results can be obtained for MSPDQ-FL with varying invisible submodel sizes.

VII. CONCLUSION

This paper introduced an MSPDQ algorithm to solve both of privacy and communication efficiency issues in FL. Due to the incompletely randomized property of model splitting method, a new privacy notion is used to evaluate the privacy degree. Model splitting method averts the privacy-utility tradeoff via dedicated designs for correlated noises and interaction protocol for submodels. Moreover, in contrast to LDP mechanism (e.g., JoPEQ), our proposed scheme not only saves communication bandwidth benefiting from dynamic quantization, but also reduces the total communication rounds under the same learning accuracy. The theoretical results showed that both the proposed MSP-FL and MSPDQ-FL preserve the privacy, and ensure the convergence to the optimal model in the sense of expectation with an $\mathcal{O}(1/t)$ rate. In addition, we explored sufficient conditions for the DP guarantee under model splitting mechanism, and proved that the proposed dynamic quantizer in MSPDQ-FL achieves at least $(0, \delta)$ -differential privacy. Future works include analyzing the tradeoff between the privacy level and communication cost, and extending the theoretical results without strong convexity and bounded gradients assumptions.

APPENDIX A PROOF OF THEOREM 2

A. Notations

The updating rule (3) is rewritten in a compact form as

$$\mathbf{W}_t[k+1] = \mathbf{P}[k]\mathbf{W}_t[k] \quad (37)$$

where

$$\mathbf{W}_t[k] = \begin{pmatrix} \mathbf{W}_t^{1,\alpha}[k]^\top \\ \vdots \\ \mathbf{W}_t^{2M}[k]^\top \end{pmatrix} = \begin{pmatrix} \text{col}(\mathbf{w}_t^{i,\alpha}[k]^\top | i \in \mathcal{S}_t) \\ \text{col}(\mathbf{w}_t^{i,\beta_1}[k]^\top | i \in \mathcal{S}_t) \end{pmatrix},$$

$$\mathbf{P}[k] = \begin{bmatrix} \mathbf{U} - \mathbf{A}[k] & \mathbf{A}[k] \\ \mathbf{A}[k] & \mathbf{I} - \mathbf{A}[k] \end{bmatrix}, \quad (38)$$

$$U_{ij} = \begin{cases} \frac{\epsilon}{M}, & \text{if } j \neq i, \\ 1 - \frac{\epsilon(M-1)}{M}, & \text{otherwise,} \end{cases} \quad (39)$$

$\mathbf{A}[k] = \text{diag}(a_{i,\alpha\beta_1}[k] | i \in \mathcal{S}_t)$. In the above definitions, with a slight abuse of notation, we use $\mathbf{W}_t^i[k]^\top$ to denote a row vector in the i -th row of matrix $\mathbf{W}_t[k]$.

The overall timeline is set according to the SGD iteration step instead of the communication round. For each $i \in \mathcal{S}_t$, the procedure in (37), that consists of a total of K_t communication rounds between the server and i , is viewed as an integrated communication step and denoted as $\text{Aggr}(\mathbf{w}_t^i)$. Then, after such an integrated communication step, we rewrite the last aggregation process in (6) as $\mathbf{w}_t = \sum_{i \in \mathcal{S}_t} \frac{1}{M} \text{Aggr}(\mathbf{w}_t^i)$. Let $\mathcal{I}_E = \{nE | n = 1, 2, \dots\}$ denote the set of timestamps on the overall timeline for such an integrated communication step. Then, the dynamics under MSP-FL can be written as

$$\mathbf{r}_{t+1}^i = \mathbf{w}_t^i - \eta_t \nabla F_i(\mathbf{w}_t^i, \zeta_t^i), \quad (40a)$$

$$\mathbf{u}_{t+1}^i = \begin{cases} \mathbf{r}_{t+1}^i, & \text{if } t+1 \notin \mathcal{I}_E, \\ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{r}_{t+1}^i, & \text{otherwise,} \end{cases} \quad (40b)$$

$$\mathbf{w}_{t+1}^i = \begin{cases} \mathbf{r}_{t+1}^i, & \text{if } t+1 \notin \mathcal{I}_E, \\ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i), & \text{otherwise,} \end{cases} \quad (40c)$$

where $\mathbf{r}_{t+1}^i$ records the result of one step SGD. Under partial clients selection, if $t+1 \in \mathcal{I}_E$, $\mathbf{u}_{t+1}^i$ denotes the local model after one round communication for aggregation, and $\mathbf{w}_{t+1}^i$ denotes that after the integrated communication step. In the dynamics (40), the randomness from stochastic gradients, random sampling of clients, stochastic splitting of model and stochastic quantization is represented by $\mathbb{E}_{SG}$, $\mathbb{E}_{RS}$, $\mathbb{E}_{SS}$ and $\mathbb{E}_{SQ}$, respectively. For the subsequent analysis, we additionally define $\bar{\mathbf{r}}_{t+1} = \sum_{i=1}^N p_i \mathbf{r}_{t+1}^i$, $\bar{\mathbf{u}}_{t+1} = \sum_{i=1}^N p_i \mathbf{u}_{t+1}^i$, $\bar{\mathbf{w}}_{t+1} = \sum_{i=1}^N p_i \mathbf{w}_{t+1}^i$, $\bar{\mathbf{g}}_t = \sum_{i=1}^N p_i \nabla F_i(\mathbf{w}_t^i)$ and $\mathbf{g}_t = \sum_{i=1}^N p_i \nabla F_i(\mathbf{w}_t^i, \zeta_t^i)$. Due to the unbiased property of the clients selection scheme for model aggregation shown in Lemma 1, we have the following results at $t+1 \in \mathcal{I}_E$:

$$\bar{\mathbf{u}}_{t+1} = \sum_{i=1}^N p_i \mathbf{u}_{t+1}^i = \mathbb{E} \left\{ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{r}_{t+1}^i \right\}, \quad (41)$$

$$\bar{\mathbf{w}}_{t+1} = \sum_{i=1}^N p_i \mathbf{w}_{t+1}^i = \mathbb{E} \left\{ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i) \right\}. \quad (42)$$

B. Supporting Lemmas

To present Theorem 3, it is crucial to display a few lemmas, where Lemmas 3-6 are established in [28].

Lemma 3. (Result of one step SGD) Suppose Assumptions 1.1-1.2 hold, and $\eta_t \leq \frac{1}{4L}$ for all t , then it has

$$\mathbb{E}_{SG} \{ \|\bar{\mathbf{r}}_{t+1} - \mathbf{w}^*\|^2 \} \leq (1 - \eta_t \mu) \mathbb{E}_{SG} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} + 6L\eta_t^2 \Gamma + \eta_t^2 \mathbb{E}_{SG} \{ \|\mathbf{g}_t - \bar{\mathbf{g}}_t\|^2 \} + 2\mathbb{E}_{SG} \left\{ \frac{1}{N} \sum_{i=1}^N \|\bar{\mathbf{w}}_t - \mathbf{w}_t^i\|^2 \right\}.$$

Lemma 4. (Bound on the variance of $\mathbf{g}_t$) Suppose Assumption 1.3 holds, it has $\mathbb{E}_{SG} \{ \|\mathbf{g}_t - \bar{\mathbf{g}}_t\|^2 \} \leq \sum_{i=1}^N p_i^2 \sigma_i$.

Lemma 5. (Bound on the divergence of $\mathbf{w}_t^i$) If Assumption 1.4 holds, η_t is non-increasing and satisfies $\eta_t \leq 2\eta_{t+E}$ for all $t \geq 0$, it has $\mathbb{E}_{SG} \left\{ \sum_{i=1}^N p_i \|\bar{\mathbf{w}}_t - \mathbf{w}_t^i\|^2 \right\} \leq 4\eta_t^2 (E-1)^2 G$.

Lemma 6. (Unbiased sampling and bound on the variance of $\bar{\mathbf{u}}_{t+1}$) If η_t is non-increasing and satisfies $\eta_t \leq 2\eta_{t+E}$ for all $t > 0$, then for $t+1 \in \mathcal{I}_E$, it has that

$$\mathbb{E}_{RS} \{ \bar{\mathbf{u}}_{t+1} \} = \bar{\mathbf{r}}_{t+1}, \quad (43a)$$

$$\mathbb{E}_{RS} \{ \|\bar{\mathbf{u}}_{t+1} - \bar{\mathbf{r}}_{t+1}\|^2 \} \leq \frac{4}{M} \eta_t^2 E^2 G. \quad (43b)$$

Lemma 7. If $\epsilon \in (0, \frac{M}{M-1})$ and $a_{\alpha\beta_1}^{\max} \in (0, \frac{\lambda_{\min, \mathbf{U}}}{1 + \lambda_{\min, \mathbf{U}}})$, then for some positive constant C and $\lambda \in (|\lambda_2, \Phi(k, 0)|, 1)$, it holds that $|\Phi(k, 0)_{ij} - \frac{1}{2M}| \leq C\lambda^{k+1}$ for all i, j and k , where $\Phi(k, 0) = \mathbf{P}[k]\mathbf{P}[k-1] \dots \mathbf{P}[0]$.

Proof. Explicit statement of Proposition 1 in [47]. $\square$

Lemma 8. (Unbiased stochastic splitting, and bounded error of aggregation with visible submodels) For $t+1 \in \mathcal{I}_E$, if Assumption 2 holds, $\epsilon \in (0, \frac{M}{M-1})$, $a_{\alpha\beta_1}^{\max} \in (0, \frac{\lambda_{\min, \mathbf{U}}}{1 + \lambda_{\min, \mathbf{U}}})$ and $K_t = \lceil \log \eta_t \rceil$, we have that $\mathbb{E} \{ \bar{\mathbf{w}}_{t+1} \} = \bar{\mathbf{u}}_{t+1}$ and $\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{u}}_{t+1}\|^2 \} \leq \eta_t^2 D_1$, where $D_1 = \frac{(2\epsilon - 4\epsilon + 8)}{3} C^2 \|\mathbf{w}_{\max}\|^2$.

Proof. Define the mean of the matrices $\mathbf{P}[k]$ as $\bar{\mathbf{P}}$. In terms of the independence of matrices $\mathbf{P}[k]$ for all k , it has that $\mathbb{E} \{ \Phi(k, 0) \} = \prod_{t=0}^k \mathbb{E} \{ \mathbf{P}[t] \} = \bar{\mathbf{P}}^{k+1}$. It is not hard to see that the matrix $\bar{\mathbf{P}}$ is doubly stochastic, then $\lim_{k \rightarrow \infty} \bar{\mathbf{P}}^k = \frac{1}{2M} \mathbf{1}\mathbf{1}^\top$. That is to say, $\Phi(k, 0)$ converges in expectation to $\frac{1}{2M} \mathbf{1}\mathbf{1}^\top$. Accordingly, it yields

$$\begin{aligned} \mathbb{E} \{ \text{Aggr}(\mathbf{r}_{t+1}^i) \} &= \mathbb{E} \left\{ \left(\sum_{j=1}^{2M} [\Phi(k, 0)]_{ij} \mathbf{w}_{t+1}^j[0] \right)^\top \right\} \\ &= \frac{1}{2M} \mathbb{E}_{SS} \{ \mathbf{W}_{t+1}[0]^\top \} \mathbf{1}, \end{aligned} \quad (44)$$

where the second equality is obtained for the independence of expectation between $\mathbb{E} \{ \Phi(k, 0) \}$ and $\mathbb{E}_{SS} \{ \mathbf{W}_{t+1}[0] \}$.

Note that, at $t+1 \in \mathcal{I}_E$, $\mathbf{w}_{t+1}^{i,\alpha}[0]$ is randomly drawn from a uniform distribution on the interval $[\epsilon \mathbf{w}_{t+1}^i, (2-\epsilon) \mathbf{w}_{t+1}^i]$ by the initial setting, where $\mathbf{w}_{t+1}^i$ is the local training model after multi-step SGD and represented by $\mathbf{r}_{t+1}^i$ as in (40a). Then, for any $i \in \mathcal{S}_{t+1}$, it has that

$$\mathbb{E}_{SS} \{ \mathbf{W}_{t+1}^{[i]}[0]^\top \} = \mathbb{E}_{SS} \{ \mathbf{W}_{t+1}^{[i+M]}[0]^\top \} = \mathbf{r}_{t+1}^i. \quad (45)$$

By plugging (44) and (45) into (42), it yields

$$\begin{aligned} \mathbb{E} \{ \bar{\mathbf{w}}_{t+1} \} &= \mathbb{E} \left\{ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i) \right\} \\ &= \mathbb{E} \left\{ \frac{1}{M} \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \sum_{j \in \mathcal{S}_{t+1}} \mathbf{r}_{t+1}^j \right\} \\ &\stackrel{(a)}{=} \mathbb{E} \left\{ \frac{1}{M} \sum_{i \in \mathcal{S}_{t+1}} \mathbf{u}_{t+1}^i \right\} \stackrel{(b)}{=} \bar{\mathbf{u}}_{t+1}, \end{aligned} \quad (46)$$

where the equality (a) follows from (40b). The equality (b) is obtained due to the fact of unbiased aggregation as in (41), i.e., $\bar{\mathbf{u}}_{t+1} = \sum_{i=1}^N p_i \mathbf{u}_{t+1}^i = \mathbb{E} \{ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{u}_{t+1}^i \}$.

$$\begin{aligned}
\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{u}}_{t+1}\|^2 \} &= \mathbb{E} \left\{ \left\| \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \sum_{j=1}^{2M} [\Phi(k, 0)]_{ij} \mathbf{w}_{t+1}^j [0]^\top - \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \sum_{j=1}^{2M} \frac{1}{2M} \mathbf{w}_{t+1}^j [0]^\top \right\|^2 \right\} \\
&= \frac{1}{M^2} \sum_{i \in \mathcal{S}_{t+1}} \mathbb{E} \left\{ \left\| \sum_{j=1}^{2M} \left([\Phi(k, 0)]_{ij} - \frac{1}{2M} \right) \mathbf{w}_{t+1}^j [0]^\top \right\|^2 \right\} \\
&\quad + \mathbb{E} \left\{ \sum_{\substack{h, i, j \in \mathcal{S}_{t+1} \\ h \neq i \neq j}} \left\langle \frac{1}{M} \sum_{j=1}^{2M} \left([\Phi(k, 0)]_{ij} - \frac{1}{2M} \right) \mathbf{w}_{t+1}^j [0]^\top, \frac{1}{M} \sum_{i=1}^{2M} \left([\Phi(k, 0)]_{hi} - \frac{1}{2M} \right) \mathbf{w}_{t+1}^i [0]^\top \right\rangle \right\} \\
&\leq \frac{1}{M^2} \sum_{i \in \mathcal{S}_{t+1}} \sum_{j=1}^{2M} \left\| [\Phi(k, 0)]_{ij} - \frac{1}{2M} \right\|^2 \mathbb{E}_{SS} \left\{ \|\mathbf{w}_{t+1}^j [0]\|^2 \right\} \leq \frac{(2\epsilon^2 - 4\epsilon + 8)}{3} C^2 \|\mathbf{w}_{\max}\|^2 \lambda^{2(k+1)}, \quad (49)
\end{aligned}$$

Let $\text{Aggr}^*(\cdot)$ denote the limit state of the integrated communication step $\text{Aggr}(\cdot)$ when $k \rightarrow \infty$. By (41) and (42), and resorting to the fact that $\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{r}_{t+1}^i = \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}^*(\mathbf{r}_{t+1}^i)$, it has

$$\begin{aligned}
&\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{u}}_{t+1}\|^2 \} \\
&= \mathbb{E} \left\{ \left\| \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i) - \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}^*(\mathbf{r}_{t+1}^i) \right\|^2 \right\}. \quad (47)
\end{aligned}$$

Meanwhile, when $k \rightarrow \infty$ the dynamics (37) achieves average consensus, which implies that

$$\text{Aggr}^*(\mathbf{r}_{t+1}^i) = \frac{1}{2M} \mathbf{W}_{t+1} [0]^\top \mathbf{1}. \quad (48)$$

By virtue of the Schur Compliment, the matrix $\mathbf{P}[k]$ in (37) is positive semidefinite with conditions $\epsilon \in (0, \frac{M}{M-1})$ and $a_{\alpha\beta_1}^{\max} \in (0, \frac{\lambda_{\min, \mathbf{U}}}{1 + \lambda_{\min, \mathbf{U}}})$. Then, with Assumption 2, inserting (48) into (47) leads to the result as shown in (49) at the top of the next page. Further, if the lower bound of communication rounds for update in (37) is a dynamic value, and designed as $k+1 = K_t = \lceil \log_{\lambda}^{\eta_t} \rceil$, we arrive at

$$\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{u}}_{t+1}\|^2 \} \leq \eta_t^2 D_1. \quad (50)$$

This completes the proof. $\square$

C. Proof of Theorem 2

Proof. To see the gap between $\mathbb{E} \{ F(\bar{\mathbf{w}}_t) \} - F^*$, we turn to analyze the variance of $\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*$. Notice that

$$\begin{aligned}
\|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 &= \underbrace{\|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{u}}_{t+1}\|^2}_{T_{01}} + \underbrace{\|\bar{\mathbf{u}}_{t+1} - \mathbf{w}^*\|^2}_{T_{02}} \\
&\quad + 2 \underbrace{\langle \bar{\mathbf{w}}_{t+1} - \bar{\mathbf{u}}_{t+1}, \bar{\mathbf{u}}_{t+1} - \mathbf{w}^* \rangle}_{T_{03}}. \quad (51)
\end{aligned}$$

If $t+1 \notin \mathcal{I}_E$, it has $\bar{\mathbf{w}}_{t+1} = \bar{\mathbf{u}}_{t+1} = \bar{\mathbf{r}}_{t+1}$. Then, both T_{01} and T_{03} vanish in expectation, leading to

$$\begin{aligned}
\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} &\leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} \\
&\quad + \eta_t^2 \left[\sum_{i=1}^N p_i^2 \sigma_i + 6L\Gamma + 8(E-1)^2 G \right], \quad (52)
\end{aligned}$$

where the inequality follows from Lemmas 3-5. Please refer to [28] for detailed proof.

If $t+1 \in \mathcal{I}_E$, $\mathbb{E}\{T_{01}\}$ is bounded as Lemma 8 presents. T_{02} can be rewritten as

$$\begin{aligned}
\|\bar{\mathbf{u}}_{t+1} - \mathbf{w}^*\|^2 &= \underbrace{\|\bar{\mathbf{u}}_{t+1} - \bar{\mathbf{r}}_{t+1}\|^2}_{T_{11}} + \underbrace{\|\bar{\mathbf{r}}_{t+1} - \mathbf{w}^*\|^2}_{T_{12}} \\
&\quad + 2 \underbrace{\langle \bar{\mathbf{u}}_{t+1} - \bar{\mathbf{r}}_{t+1}, \bar{\mathbf{r}}_{t+1} - \mathbf{w}^* \rangle}_{T_{13}}, \quad (53)
\end{aligned}$$

where $\mathbb{E}\{T_{12}\}$ can be bounded as in (52). $\mathbb{E}\{T_{13}\}$ vanishes due to the unbiased sampling, which is shown in Lemma 6. Inserting (43) and (52) into (53) gives rise to

$$\begin{aligned}
\mathbb{E}\{T_{02}\} &\leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} \\
&\quad + \eta_t^2 \left[\sum_{i=1}^N p_i^2 \sigma_i + 6L\Gamma + 8(E-1)^2 G + \frac{4}{M} E^2 G \right]. \quad (54)
\end{aligned}$$

With regard to T_{03} , it also vanishes in expectation since $\mathbb{E}\{\bar{\mathbf{w}}_{t+1}\} = \bar{\mathbf{u}}_{t+1}$. Now, by substituting (54) into (51) and invoking (50), it boils down to

$$\begin{aligned}
\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} &\leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} \\
&\quad + \eta_t^2 \left[D_1 + \sum_{i=1}^N p_i^2 \sigma_i + 6L\Gamma + 8(E-1)^2 G + \frac{4}{M} E^2 G \right]. \quad (55)
\end{aligned}$$

At this stage, one can observe from (52) and (55) that no matter whether $t+1 \in \mathcal{I}_E$ or not, it always holds that

$$\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} + \eta_t^2 D_2, \quad (56)$$

where $D_2 = D_1 + \sum_{i=1}^N p_i^2 \sigma_i + 6L\Gamma + 8(E-1)^2 G + \frac{4}{M} E^2 G$. Let $\rho > \frac{1}{\mu}$, $\vartheta \geq 0$ and design the learning rate η_t as $\frac{\rho}{\vartheta+t}$ such that $\eta_t < \min\{\frac{1}{\mu}, \frac{1}{4L}\}$ and $\eta_t \leq 2\eta_{t+E}$. As a standard technique, we will show that $\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq \frac{\nu_1}{\vartheta+t+1}$ via the mathematical induction method, where $\nu_1 = \max\left\{ \frac{\rho^2 D_2}{\rho\mu-1}, (\vartheta+1) \mathbb{E} \{ \|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2 \} \right\}$.

First, it comes naturally when $t=0$ from the definition of ν_1 . Then, we assume that the claim still holds true for some $t > 0$. Based on (56), it has

$$\begin{aligned}
\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} &\leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} + \eta_t^2 D_2 \\
&\leq \left(1 - \frac{\rho\mu}{\vartheta+t} \right) \frac{\nu_1}{\vartheta+t} + \frac{\rho^2 D_2}{(\vartheta+t)^2} \\
&= \frac{\vartheta+t-1}{(\vartheta+t)^2} \nu_1 + \frac{\rho^2 D_2}{(\vartheta+t)^2} - \frac{\rho\mu-1}{(\vartheta+t)^2} \nu_1 \\
&\leq \frac{(\vartheta+t-1)\nu_1}{(\vartheta+t)^2 - 1} \\
&= \frac{\nu_1}{\vartheta+t+1} \quad (57)
\end{aligned}$$

where the first equality follows by subtracting and adding $\frac{\nu_1}{(\vartheta+t)^2}$ on the right-hand side. The last inequality is derived from the definition of ν_1 . Evidently, these collaboratively affirm the claim that $\mathbb{E}\{\|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2\} \leq \frac{\nu_1}{\vartheta+t+1}$.

Next, let $\rho = \frac{2}{\mu}$ and $\vartheta = \max\{\frac{8L}{\mu}, E\} - 1$, and utilize the following inequalities, i.e., $\vartheta + 1 \leq \frac{8L}{\mu} + E$ and $\nu_1 \leq \frac{\rho^2 D_2}{\rho\mu-1} + (\vartheta+1)\mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\}$, then one can proceed to the relationship of $\mathbb{E}\{F(\bar{\mathbf{w}}_t)\} - F^*$ by the L -smoothness, i.e.,

$$\begin{aligned} & \mathbb{E}\{F(\bar{\mathbf{w}}_t)\} - F^* \\ & \leq \frac{L\nu_1}{2(\vartheta+t)} \\ & \leq \frac{8L}{\mu(\vartheta+t)} \left(\frac{2D_2}{\mu} + \frac{8L+\mu E}{2} \mathbb{E}\{\|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2\} \right). \end{aligned} \quad (58)$$

This ends the proof. $\square$

APPENDIX B PROOF OF THEOREM 3

A. Additional Notations

Some additional notations are given for the subsequent analysis. Similarly as in (40), we reformulate the dynamics under MSPDQ-FL and present it below. Unlike the reformulation of MSP-FL shown in (40), $\mathbf{v}_{t+1}^i$ and $\mathbf{w}_{t+1}^i$ denote sequences of integrated communication step with and without quantized submodels, respectively.

$$\mathbf{r}_{t+1}^i = \mathbf{w}_t^i - \eta_t \nabla F_i(\mathbf{w}_t^i, \zeta_t^i), \quad (59a)$$

$$\mathbf{u}_{t+1}^i = \begin{cases} \mathbf{r}_{t+1}^i, & \text{if } t+1 \notin \mathcal{I}_E, \\ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{r}_{t+1}^i, & \text{otherwise,} \end{cases} \quad (59b)$$

$$\mathbf{v}_{t+1}^i = \begin{cases} \mathbf{r}_{t+1}^i, & \text{if } t+1 \notin \mathcal{I}_E, \\ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i), & \text{otherwise,} \end{cases} \quad (59c)$$

$$\mathbf{w}_{t+1}^i = \begin{cases} \mathbf{r}_{t+1}^i, & \text{if } t+1 \notin \mathcal{I}_E, \\ \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{q}_{t+1}^i), & \text{otherwise.} \end{cases} \quad (59d)$$

Define $\mathbf{W}_{t+1}^\alpha[k] = \text{col}(\mathbf{w}_{t+1}^{i,\alpha}[k]^\top | i \in \mathcal{S}_{t+1})$ (doing likewise with $\mathbf{Q}_{t+1}[k]$ and $\Delta_{t+1}[k]$), $\mathbf{W}_{t+1}^{\beta_1}[k] = \text{col}(\mathbf{w}_{t+1}^{i,\beta_1}[k]^\top | i \in \mathcal{S}_{t+1})$, $\bar{\mathbf{W}}_{t+1}^\alpha[k] = \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{w}_{t+1}^{i,\alpha}[k]^\top$ and $\bar{\mathbf{q}}_{t+1}[k] = \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{q}_{t+1}^i[k]$.

B. Supporting Lemmas

Some other lemmas are provided for the remaining proof.

Lemma 9. Let $\epsilon \in (0, \frac{M}{M-1})$, and $\{a_{i,\alpha\beta_1}[k] | i \in \mathcal{S}_t\}$ be positive non-increasing sequences of step sizes. Under MSPDQ-FL, it has that

$$\begin{aligned} & \|\mathbf{W}_t^\alpha[k+1] - \mathbf{1}\bar{\mathbf{W}}_t^\alpha[k+1]\| \\ & \leq 2 \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} \|\Delta_t[l]\| + \widetilde{W}_t^{\max} \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}[l]. \end{aligned} \quad (60)$$

Proof. For the k -th communication round after the t -th learning round, let $\mathbf{X}_t[k] := \Theta \mathbf{W}_{t+1}^\alpha[k]$ denote the visible sub-

model deviation from the average state, where $\Theta = \mathbf{I} - \frac{1}{M} \mathbf{1}\mathbf{1}^\top$. To see its upper bound, we firstly arrange $\mathbf{X}_t[k+1]$ as follows:

$$\begin{aligned} \mathbf{X}_t[k+1] &= \mathbf{U} \mathbf{W}_t^\alpha[k] + (\mathbf{I} - \mathbf{U})(\mathbf{W}_t^\alpha[k] - \mathbf{Q}_t[k]) \\ & \quad + \mathbf{A}[k] (\mathbf{W}_t^{\beta_1}[k] - \mathbf{W}_t^\alpha[k]) - \mathbf{1}\bar{\mathbf{W}}_t^\alpha[k] \\ & \quad - \mathbf{1} \sum_{i \in \mathcal{S}_t} \frac{1}{M} a_{i,\alpha\beta_1}[k] (\mathbf{w}_t^{i,\beta_1}[k] - \mathbf{w}_t^{i,\alpha}[k])^\top \\ &= \mathbf{U} \Theta \mathbf{W}_t^\alpha[k] + (\mathbf{I} - \mathbf{U}) \Delta_t[k] \\ & \quad + \mathbf{A}[k] \Theta (\mathbf{W}_t^{\beta_1}[k] - \mathbf{W}_t^\alpha[k]). \end{aligned} \quad (61)$$

Notice that the matrix $\mathbf{U}$ is doubly stochastic under the condition $\epsilon \in (0, \frac{M}{M-1})$. Accordingly, taking Frobenius norm on both sides of (61) and building upon the facts that $\|\mathbf{U}\| < \lambda_{2,\mathbf{U}}$, $\|\mathbf{I} - \mathbf{U}\| \leq 2$ and $\|\Theta\| < 1$ yield

$$\begin{aligned} & \|\mathbf{X}_t[k+1]\| \\ & \leq \|\mathbf{U} \Theta \mathbf{W}_t^\alpha[k]\| + \|(\mathbf{I} - \mathbf{U}) \Delta_t[k]\| + \|\mathbf{A}[k] \Theta (\mathbf{W}_t^{\beta_1}[k] - \mathbf{W}_t^\alpha[k])\| \\ & \leq \lambda_{2,\mathbf{U}} \|\Theta \mathbf{W}_t^\alpha[k]\| + 2 \|\Delta_t[k]\| + a_{\alpha\beta_1}^{\max}[k] \|\mathbf{W}_t^{\beta_1}[k] - \mathbf{W}_t^\alpha[k]\| \\ & \leq \lambda_{2,\mathbf{U}}^{k+1} \|\mathbf{X}_t[0]\| + 2 \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} \|\Delta_t[l]\| + \widetilde{W}_t^{\max} \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}[l]. \end{aligned}$$

By recalling the initial setting of visible submodels after each learning round t , specifically, $\mathbf{w}_t^{i,\alpha}[0] = \mathbf{w}_t^{j,\alpha}[0] \forall \{i, j\} \in \mathcal{S}_t$, which implies that $\|\mathbf{X}_t[0]\| = 0$, then the above inequality further turns into (60). $\square$

Lemma 10. Let $\epsilon \in (0, \frac{M}{M-1})$ and $\tilde{\epsilon} = \max\{1, \epsilon\}$. For any $i \in \mathcal{S}_t$, define $a_{i,\alpha\beta_1}[k] = \frac{\gamma_i}{k+1}$ such that $a_{i,\alpha\beta_1}[k] \leq 2a_{i,\alpha\beta_1}[2k]$, where $\gamma_i > 0$. If Assumption 3 holds, then it has the following properties of MSPDQ-FL: $\mathbf{w}_t^{i,\alpha}[k+1] \in \mathcal{R}_t^i[k+1]$ and $\|\Delta_t^i[k]\| \leq \frac{\sqrt{d}\pi_t}{2^{B-1}} a_{\alpha\beta_1}^{\max}[k]$.

Proof. By subtracting $\mathbf{q}_t^i[k]$ on both sides of (21), it has that

$$\begin{aligned} & \|\mathbf{w}_t^{i,\alpha}[k+1] - \mathbf{q}_t^i[k]\| \\ & \leq \|\Delta_t^i[k]\| + \epsilon \left\| \sum_{j \in \mathcal{S}_t} \frac{1}{M} (\mathbf{q}_t^j[k] - \mathbf{q}_t^i[k]) \right\| \\ & \quad + a_{i,\alpha\beta_1}[k] \|\mathbf{w}_t^{i,\beta_1}[k] - \mathbf{w}_t^{i,\alpha}[k]\| \\ & \stackrel{(a)}{\leq} (1 + \epsilon) \|\Delta_t[k]\| + \epsilon \|\mathbf{W}_t^\alpha[k] - \mathbf{1}\bar{\mathbf{W}}_t^\alpha[k]\| \\ & \quad + a_{\alpha\beta_1}^{\max}[k] \|\mathbf{W}_t^{\beta_1}[k] - \mathbf{W}_t^\alpha[k]\| \\ & \stackrel{(b)}{\leq} (1 + \epsilon) \|\Delta_t[k]\| + 2\epsilon \sum_{l=0}^{k-1} \lambda_{2,\mathbf{U}}^{k-1-l} \|\Delta_t[l]\| \\ & \quad + \epsilon \widetilde{W}_t^{\max} \sum_{l=0}^{k-1} \lambda_{2,\mathbf{U}}^{k-1-l} a_{\alpha\beta_1}^{\max}[l] + \widetilde{W}_t^{\max} a_{\alpha\beta_1}^{\max}[k] \\ & \leq (\epsilon + \tilde{\epsilon}) \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} \|\Delta_t[l]\| + \tilde{\epsilon} \widetilde{W}_{t,k}^{\max} \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}[l] \end{aligned} \quad (62)$$

where the inequality (a) is obtained due to the inequality $\|\sum_{j \in \mathcal{S}_t} \frac{1}{M} (\mathbf{q}_t^j[k] - \mathbf{q}_t^i[k])\| \leq \|\mathbf{W}_t^\alpha[k] - \mathbf{1}\bar{\mathbf{W}}_t^\alpha[k]\| + \|\Delta_t[k]\|$. By combining with the upper bound of $\|\mathbf{W}_t^\alpha[k] - \mathbf{1}\bar{\mathbf{W}}_t^\alpha[k]\|$ in Lemma 9, we obtain the inequality (b).

It is clear that $\mathbf{w}_t^{i,\alpha}[0] \in \mathcal{R}_t^i[0]$ under initial settings as stated in Section IV.A. Suppose that $\mathbf{w}_t^{i,\alpha}[k] \in \mathcal{R}_t^i[k]$ holds for some $k > 0$. Then, for any $k_3 \in [0, k]$, it has that $\|\Delta_t^i[k_3]\| \leq \frac{\sqrt{d}\pi_t}{2^{B-1}} a_{\alpha\beta_1}^{\max}[k_3]$, $\forall i \in \mathcal{S}_t$, which together with Assumption 3 yields $\|\Delta_t[k_3]\| \leq a_{\alpha\beta_1}^{\max}[k_3]$. By substituting it into (62), we arrive at

□

$$\begin{aligned}
& \left\| \mathbf{w}_t^{i,\alpha}[k+1] - \mathbf{q}_t^i[k] \right\| \\
& \leq (\epsilon + \tilde{\epsilon}) \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}(l) + \tilde{\epsilon} \widetilde{W}_{t,k}^{\max} \sum_{l=0}^k \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}(l) \\
& \leq (\epsilon + \tilde{\epsilon} + \tilde{\epsilon} \widetilde{W}_{t,k}^{\max}) \left[\sum_{l=0}^{\lfloor \frac{k}{2} \rfloor} \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}[l] + \sum_{l=\lceil \frac{k}{2} \rceil}^k \lambda_{2,\mathbf{U}}^{k-l} a_{\alpha\beta_1}^{\max}[l] \right] \\
& \stackrel{(a)}{<} (\epsilon + \tilde{\epsilon} + \tilde{\epsilon} \widetilde{W}_{t,k}^{\max}) \frac{\gamma_{\max} \lambda_{2,\mathbf{U}}^{\lceil \frac{k}{2} \rceil} + a_{\alpha\beta_1}^{\max}[\lceil \frac{k}{2} \rceil]}{1 - \lambda_{2,\mathbf{U}}} \\
& \leq \frac{4\gamma_{\max}(\epsilon + \tilde{\epsilon} + \tilde{\epsilon} \widetilde{W}_{t,k}^{\max})}{(1 - \lambda_{2,\mathbf{U}})(k+1)} \\
& = \frac{\pi_t}{2} a_{\alpha\beta_1}^{\max}[k], \tag{63}
\end{aligned}$$

where the inequality (a) follows from the facts that $1 - \lambda_{2,\mathbf{U}} \in (0, 1)$ and $a_{\alpha\beta_1}^{\max}[0] = \gamma_{\max} > a_{\alpha\beta_1}^{\max}[k]$ for $k > 0$. The last inequality is obtained by $\lambda_{2,\mathbf{U}}^k \leq \frac{1}{\gamma_{\max}} a_{\alpha\beta_1}^{\max}[k]$ and $a_{\alpha\beta_1}^{\max}[\lceil \frac{k}{2} \rceil] \leq 2a_{\alpha\beta_1}^{\max}[k]$. Recalling that k can be an arbitrary number, therefore it always has that $\mathbf{w}_t^{i,\alpha}[k+1] \in \mathcal{R}_t^i[k+1]$ and the quantization error associated with the dynamic quantization interval is bounded by $\frac{\sqrt{d}\pi_t}{2^{B-1}} a_{\alpha\beta_1}^{\max}[k]$. □

Lemma 11. (Properties of stochastic quantization): *With the stochastic quantization as in (18), each split submodel of visible part is unbiasedly estimated if Assumption 3 holds, i.e., $\mathbb{E}_{SQ}\{\mathbf{q}_t^i[k]\} = \mathbf{w}_t^{i,\alpha}[k]$, and the associated quantization error is bounded by $\mathbb{E}_{SQ}\{\|\mathbf{q}_t^i[k] - \mathbf{w}_t^{i,\alpha}[k]\|^2\} \leq \frac{d\pi_t^2(a_{\alpha\beta_1}^{\max}[k-1])^2}{4(2^B-1)^2}$.*

Proof. Proof of Lemma 11 is trivial, and has been discussed in the existing literature. In Lemma 10, it shows that $\mathbf{w}_{t+1}^{i,\alpha}[k] \in \mathcal{R}_{t+1}^i[k]$ for all k after any $(t+1)$ -th learning round, thereby it is reasonable to assume that any element of $\mathbf{w}_{t+1}^{i,\alpha}[k]$, i.e., $w_{t+1}^{i,j,\alpha}[k]$, is located in the interval $[c_\tau, c_{\tau+1})$ for some $\tau \in \{0, \dots, l-1\}$. With some calculations, it has $\mathbb{E}_{SQ}\{q_{t+1}^{i,j}[k]\} = w_{t+1}^{i,j,\alpha}[k]$.

For $\mathbf{w}_{t+1}^{i,\alpha}[k] = [w_{t+1}^{i,1,\alpha}[k], \dots, w_{t+1}^{i,d,\alpha}[k]]^\top$, it is clear that $\mathbb{E}_{SQ}\{\mathbf{q}_{t+1}^i[k]\} = \mathbf{w}_{t+1}^{i,\alpha}[k]$.

The quantization error is given by

$$\begin{aligned}
& \mathbb{E}_{SQ}\left\{\left\|q_{t+1}^{i,j}[k] - w_{t+1}^{i,j,\alpha}[k]\right\|^2\right\} \\
& = (c_\tau - w_{t+1}^{i,j,\alpha}[k])^2 Pr\left\{q_{t+1}^{i,j}[k] = c_\tau\right\} \\
& \quad + (c_{\tau+1} - w_{t+1}^{i,j,\alpha}[k])^2 Pr\left\{q_{t+1}^{i,j}[k] = c_{\tau+1}\right\} \\
& \leq \left(\frac{c_{\tau+1} - c_\tau}{2}\right)^2 \leq \frac{\pi_t^2(a_{\alpha\beta_1}^{\max}[k-1])^2}{4(2^B-1)^2}
\end{aligned}$$

where the last inequality is obtained by substituting into the magnitude of dynamic interval at the k -th communication round, i.e., $c_{\tau+1} - c_\tau = \frac{\pi_t a_{\alpha\beta_1}^{\max}[k-1]}{l-1}$. Meanwhile, it has

$$\begin{aligned}
& \mathbb{E}_{SQ}\left\{\left\|\mathbf{q}_{t+1}^i[k] - \mathbf{w}_{t+1}^{i,\alpha}[k]\right\|^2\right\} \\
& = \sum_{j=1}^d \mathbb{E}_{SQ}\left\{\left\|q_{t+1}^{i,j}[k] - w_{t+1}^{i,j,\alpha}[k]\right\|^2\right\} \\
& \leq \frac{d\pi_t^2(a_{\alpha\beta_1}^{\max}[k-1])^2}{4(2^B-1)^2}.
\end{aligned}$$

Lemma 12. (Unbiased and variance bounded quantization): *Let Assumption 3 hold, under MSPDQ-FL, we have $\mathbb{E}_{SQ}\{\bar{\mathbf{w}}_{t+1}\} = \bar{\mathbf{v}}_{t+1}$ and $\mathbb{E}_{SQ}\{\|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{v}}_{t+1}\|^2\} \leq \frac{d\pi_{t+1}^2(a_{\alpha\beta_1}^{\max}[K_t-1])^2}{4M(2^B-1)^2}$.*

Proof. Due to the unbiasedness of partial model aggregation, it has $\bar{\mathbf{v}}_{t+1} = \mathbb{E}_{RS}\{\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i)\}$ and $\bar{\mathbf{w}}_{t+1} = \mathbb{E}_{RS}\{\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{q}_{t+1}^i)\}$ that are similar to (41) and (42). Meanwhile, noting that after K_t communication rounds, it has the following facts, i.e., $\text{Aggr}(\mathbf{q}_{t+1}^i) = \mathbf{q}_{t+1}^i[K_t]$ and $\text{Aggr}(\mathbf{r}_{t+1}^i) = \mathbf{w}_{t+1}^{i,\alpha}[K_t]$. Then, one has

$$\begin{aligned}
\mathbb{E}_{SQ}\{\bar{\mathbf{w}}_{t+1}\} & = \mathbb{E}_{SQ}\left\{\mathbb{E}_{RS}\left\{\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{q}_{t+1}^i[K_t]\right\}\right\} \\
& \stackrel{(a)}{=} \mathbb{E}_{RS}\left\{\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{w}_{t+1}^{i,\alpha}[K_t]\right\} \\
& = \mathbb{E}_{RS}\left\{\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \text{Aggr}(\mathbf{r}_{t+1}^i)\right\} = \bar{\mathbf{v}}_{t+1} \tag{64}
\end{aligned}$$

where the equality (a) is obtained in light of Lemma 11 and the independence between $\mathbb{E}_{RS}$ and $\mathbb{E}_{SQ}$.

Following the similar arguments as in (49), and using Lemma 11 lead to

$$\begin{aligned}
& \mathbb{E}_{SQ}\left\{\|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{v}}_{t+1}\|^2\right\} \\
& = \mathbb{E}_{SQ}\left\{\left\|\sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{q}_{t+1}^i[K_t] - \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M} \mathbf{w}_{t+1}^{i,\alpha}[K_t]\right\|^2\right\} \\
& = \sum_{i \in \mathcal{S}_{t+1}} \frac{1}{M^2} \mathbb{E}_{SQ}\left\{\|\Delta_{t+1}^i[K_t]\|^2\right\} \\
& \quad + \mathbb{E}_{SQ}\left\{\sum_{i,j \in \mathcal{S}_{t+1}, i \neq j} \left\langle \frac{1}{M} \Delta_{t+1}^i[K_t], \frac{1}{M} \Delta_{t+1}^j[K_t] \right\rangle\right\} \\
& \leq \frac{d\pi_{t+1}^2(a_{\alpha\beta_1}^{\max}[K_t-1])^2}{4M(2^B-1)^2} \tag{65}
\end{aligned}$$

where the inequality holds for $\mathbb{E}_{SQ}\{\Delta_{t+1}^i[k]\} = 0$, and $\Delta_{t+1}^i[k]$ and $\Delta_{t+1}^j[k]$ are independent for any k if $i \neq j$. □

C. Proof of Theorem 3

Proof. Similar to the proof of Theorem 2, we rewrite the expectation over $\|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2$ as

$$\begin{aligned}
\mathbb{E}\{\|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2\} & = 2\mathbb{E}\{\langle \bar{\mathbf{w}}_{t+1} - \bar{\mathbf{v}}_{t+1}, \bar{\mathbf{v}}_{t+1} - \mathbf{w}^* \rangle\} \\
& \quad + \mathbb{E}\{\|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{v}}_{t+1}\|^2\} + \mathbb{E}\{\|\bar{\mathbf{v}}_{t+1} - \mathbf{w}^*\|^2\} \tag{66}
\end{aligned}$$

If $t+1 \notin \mathcal{I}_E$, it has $\bar{\mathbf{w}}_{t+1} = \bar{\mathbf{v}}_{t+1}$, leading to

$$\begin{aligned}
\mathbb{E}\{\|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2\} & \leq (1 - \eta_t \mu) \mathbb{E}\{\|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2\} \\
& \quad + \eta_t^2 \left[\sum_{i=1}^N p_i^2 \sigma_i + 6L\Gamma + 8(E-1)^2 G \right], \tag{67}
\end{aligned}$$

which is exactly the result as in (52). If $t+1 \in \mathcal{I}_E$, it has

$$\begin{aligned}
& \mathbb{E}\{\|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2\} \\
& \stackrel{(a)}{=} \mathbb{E}_{SQ}\{\|\bar{\mathbf{w}}_{t+1} - \bar{\mathbf{v}}_{t+1}\|^2\} + \mathbb{E}\{\|\bar{\mathbf{v}}_{t+1} - \mathbf{w}^*\|^2\} \\
& \stackrel{(b)}{\leq} \frac{d\pi_{t+1}^2(a_{\alpha\beta_1}^{\max}[K_t-1])^2}{4M(2^B-1)^2} + \mathbb{E}\{\|\bar{\mathbf{v}}_{t+1} - \mathbf{w}^*\|^2\}, \tag{68}
\end{aligned}$$

where the equality (a) and the first term on the right-hand side of the inequality (b) follow from Lemma 12.

Note that $K_t = \max \left\{ \left\lceil \log_{\lambda}^{2/\mu(\vartheta+t)} \right\rceil, \left\lceil \frac{\mu(\vartheta+t)}{2} \right\rceil \right\}$ and $a_{\alpha\beta_1}^{\max}[K_t - 1] = \frac{\gamma_{\max}}{K_t}$. Via a simple calculation, we have $a_{\alpha\beta_1}^{\max}[K_t - 1] \leq \gamma_{\max}\eta_t$ and $\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq \eta_t^2 D_1$ which is obtained in the same way as that in (50). Next, by resorting to similar arguments used from (53) to (55), one can derive

$$\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} + \eta_t^2 D_2, \quad (69)$$

where D_2 is defined in (56). Plugging the inequality $a_{\alpha\beta_1}^{\max}[K_t - 1] \leq \gamma_{\max}\eta_t$ and (69) into (68) yields

$$\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} + \eta_t^2 \left(D_2 + \frac{d\gamma_{\max}^2 \tilde{\pi}^2}{4M(2^B - 1)^2} \right). \quad (70)$$

By (67) and (70), one can conclude that regardless of whether $t + 1 \in \mathcal{I}_E$ or $t + 1 \notin \mathcal{I}_E$, it always holds that

$$\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq (1 - \eta_t \mu) \mathbb{E} \{ \|\bar{\mathbf{w}}_t - \mathbf{w}^*\|^2 \} + \eta_t^2 (D_2 + D_3),$$

where, for brevity, let $D_3 = \frac{d\gamma_{\max}^2 \tilde{\pi}^2}{4M(2^B - 1)^2}$. By virtue of the mathematical induction method again and invoking similar arguments shown in Theorem 2 from (56) to (58), we derive

$$\mathbb{E} \{ \|\bar{\mathbf{w}}_{t+1} - \mathbf{w}^*\|^2 \} \leq \frac{\nu_2}{\vartheta + t + 1} \quad (71)$$

together with the result as shown in (24) by L -smoothness, i.e.,

$$\begin{aligned} & \mathbb{E} \{ F(\bar{\mathbf{w}}_t) \} - F^* \\ & \leq \frac{8L}{\mu(\vartheta + t)} \left(\frac{2(D_2 + D_3)}{\mu} + \frac{8L + \mu E}{2} \mathbb{E} \{ \|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2 \} \right), \end{aligned}$$

where $\nu_2 = \max \left\{ \frac{\rho^2(D_2 + D_3)}{\rho\mu - 1}, (\vartheta + 1) \mathbb{E} \{ \|\bar{\mathbf{w}}_0 - \mathbf{w}^*\|^2 \} \right\}$. $\square$

REFERENCES

- [1] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.
- [2] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and open problems in federated learning," *Foundations and Trends® in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.
- [3] T. Gafni, N. Shlezinger, K. Cohen, Y. C. Eldar, and H. V. Poor, "Federated learning: A signal processing perspective," *IEEE Signal Processing Magazine*, vol. 39, no. 3, pp. 14–41, 2022.
- [4] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in *Advances in Neural Information Processing Systems*, vol. 32, 2019.
- [5] B. Zhao, K. R. Mopuri, and H. Bilen, "Idlg: Improved deep leakage from gradients," *arXiv preprint arXiv:2001.02610*, 2020.
- [6] J. Geiping, H. Bauermeister, H. Dröge, and M. Moeller, "Inverting gradients-how easy is it to break privacy in federated learning?" *Advances in neural information processing systems*, vol. 33, pp. 16937–16947, 2020.
- [7] N. Haim, G. Vardi, G. Yehudai, O. Shamir, and M. Irani, "Reconstructing training data from trained neural networks," in *Advances in Neural Information Processing Systems*, vol. 35. Curran Associates, Inc., 2022, pp. 22911–22924.
- [8] J. Zhao, H. Zhu, F. Wang, R. Lu, Z. Liu, and H. Li, "Pvd-fl: A privacy-preserving and verifiable decentralized federated learning framework," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2059–2073, 2022.
- [9] C. Thapa, P. C. M. Arachchige, S. Camtepe, and L. Sun, "Splitfed: When federated learning meets split learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 8, 2022, pp. 8485–8493.
- [10] C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*. Foundations and Trends® in Theoretical Computer Science, 2014, vol. 9, no. 3–4.
- [11] S. Truex, L. Liu, K.-H. Chow, M. E. Gursoy, and W. Wei, "Ldp-fed: Federated learning with local differential privacy," in *Proceedings of the 3rd ACM International Workshop on Edge Systems, Analytics and Networking*, 2020, pp. 61–66.
- [12] K. Wei, J. Li, C. Ma, M. Ding, C. Chen, S. Jin, Z. Han, and H. V. Poor, "Low-latency federated learning over wireless channels with differential privacy," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 1, pp. 290–307, 2022.
- [13] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020.
- [14] X. Yuan, W. Ni, M. Ding, K. Wei, J. Li, and H. V. Poor, "Amplitude-varying perturbation for balancing privacy and utility in federated learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1884–1897, 2023.
- [15] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2017.
- [16] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4711–4716, 2019.
- [17] F. Ye, Z. Cheng, X. Cao, and M.-Y. Chow, "A random-weight privacy-preserving algorithm with error compensation for microgrid distributed energy management," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4352–4362, 2021.
- [18] N. Shlezinger, M. Chen, Y. C. Eldar, H. V. Poor, and S. Cui, "Uveqfed: Universal vector quantization for federated learning," *IEEE Transactions on Signal Processing*, vol. 69, pp. 500–514, 2021.
- [19] Y. Wang, L. Lin, and J. Chen, "Communication-efficient adaptive federated learning," in *Proceedings of the International Conference on Machine Learning*, vol. 162, 2022, pp. 22802–22838.
- [20] S. Wang, M. Chen, C. G. Brinton, C. Yin, W. Saad, and S. Cui, "Performance optimization for variable bitwidth federated learning in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 23, no. 3, pp. 2340–2356, 2024.
- [21] E. Rizk, S. Vlaski, and A. H. Sayed, "Federated learning under importance sampling," *IEEE Transactions on Signal Processing*, vol. 70, pp. 5381–5396, 2022.
- [22] X. He, X. Yi, Y. Zhao, K. H. Johansson, and V. Gupta, "Asymptotic analysis of federated learning under event-triggered communication," *IEEE Transactions on Signal Processing*, vol. 71, pp. 2654–2667, 2023.
- [23] A. Mahmoudi, J. H. da Cruz Júnior, H. S. Ghadikolaei, and C. Fischione, "A-lag: Adaptive lazily aggregated quantized gradient," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 1828–1833.
- [24] L. Chen, W. Liu, Y. Chen, and W. Wang, "Communication-efficient design for quantized decentralized federated learning," *IEEE Transactions on Signal Processing*, vol. 72, pp. 1175–1188, 2024.
- [25] A. Girgis, D. Data, S. Diggavi, P. Kairouz, and A. T. Suresh, "Shuffled model of differential privacy in federated learning," in *Proceedings of the International Conference on Artificial Intelligence and Statistics*, vol. 130, 2021, pp. 2521–2529.
- [26] Z. Li, H. Zhao, B. Li, and Y. Chi, "Soteriafl: A unified framework for private federated learning with communication compression," in *Advances in Neural Information Processing Systems*, vol. 35, 2022, pp. 4285–4300.
- [27] N. Lang, E. Sofer, T. Shaked, and N. Shlezinger, "Joint privacy enhancement and quantization in federated learning," *IEEE Transactions on Signal Processing*, vol. 71, pp. 295–310, 2023.
- [28] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, "On the convergence of fedavg on non-iid data," in *Proceedings of the International Conference on Learning Representations*, 2020.
- [29] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proceedings of the International Conference on Artificial Intelligence and Statistics*, vol. 54, 2017, pp. 1273–1282.
- [30] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 601–618.
- [31] T. Orekondy, B. Schiele, and M. Fritz, "Knockoff nets: Stealing functionality of black-box models," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4949–4958.
- [32] T. Nguyen and M. T. Thai, "Preserving privacy and security in federated learning," *IEEE/ACM Transactions on Networking*, vol. 32, no. 1, pp. 833–843, 2024.

- [33] K. Anoh, S. Maharjan, A. Ikpehai, Y. Zhang, and B. Adebisi, "Energy peer-to-peer trading in virtual microgrids in smart grids: A game-theoretic approach," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1264–1275, 2020.
- [34] S. Zhang and S. Zhang, "Efficient federated connected electric vehicle scheduling system: A noncooperative online incentive approach," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2025.
- [35] X. Liu, Y. Deng, and T. Mahmoodi, "Wireless distributed learning: A new hybrid split and federated learning approach," *IEEE Transactions on Wireless Communications*, vol. 22, no. 4, pp. 2650–2665, 2023.
- [36] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," in *Proceedings of the MLSys Conference*, vol. 2, 2020, pp. 429–450.
- [37] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *Proceedings of the International Conference on Data Engineering*, 2007, pp. 106–115.
- [38] Y. Lu and M. Zhu, "On privacy preserving data release of linear dynamic networks," *Automatica*, vol. 115, p. 108839, 2020.
- [39] X. Chen, L. Huang, K. Ding, S. Dey, and L. Shi, "Privacy-preserving push-sum average consensus via state decomposition," *IEEE Transactions on Automatic Control*, vol. 68, no. 12, pp. 7974–7981, 2023.
- [40] A. Xie, X. Wang, W. Yang, M. Cao, and X. Ren, "The least information set needed by privacy attackers," *IEEE Transactions on Automatic Control*, vol. 70, no. 3, pp. 1652–1666, 2025.
- [41] L. Pan, H. Shao, Y. Lu, M. Mesbahi, D. Li, and Y. Xi, "Privacy-preserving average consensus via matrix-weighted inter-agent coupling," *Automatica*, vol. 174, p. 112094, 2025.
- [42] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Transactions on Signal Processing*, vol. 68, pp. 4069–4082, 2020.
- [43] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "SCAFFOLD: Stochastic controlled averaging for federated learning," in *Proceedings of the 37th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, vol. 119. PMLR, 13–18 Jul 2020, pp. 5132–5143.
- [44] T. T. Doan, S. T. Maguluri, and J. Romberg, "Fast convergence rates of distributed subgradient methods with adaptive quantization," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2191–2205, 2021.
- [45] H. Yu, R. Jin, and S. Yang, "On the linear speedup analysis of communication efficient momentum sgd for distributed non-convex optimization," in *Proceedings of the International Conference on Machine Learning*, vol. 97, 2019, pp. 7184–7193.
- [46] J. Zhang, S. Ge, T.-H. Chang, and Z.-Q. Luo, "Decentralized non-convex learning with linearly coupled constraints: Algorithm designs and application to vertical learning problem," *IEEE Transactions on Signal Processing*, vol. 70, pp. 3312–3327, 2022.
- [47] V. S. Mai and E. H. Abed, "Distributed optimization over directed graphs with row stochasticity and constraint regularity," *Automatica*, vol. 102, pp. 94–104, 2019.