
Additively Homomorphical Encryption based Deep Neural Network for Asymmetrically Collaborative Machine Learning

Yifei Zhang

Chinese University of Hong Kong
yifeiacc@gmail.com

Hao Zhu

Australian National University
allenhaozhu@gmail.com

Abstract

The financial sector presents many opportunities to apply various machine learning techniques. Centralized machine learning creates a constraint which limits further applications in finance sectors. Data privacy is a fundamental challenge for a variety of finance and insurance applications that account on learning a model across different sections. In this paper, we define a new practical scheme of collaborative machine learning that one party owns data, but another party owns labels only, and term this **Asymmetrically Collaborative Machine Learning**. For this scheme, we propose a novel privacy-preserving architecture where two parties can collaboratively train a deep learning model efficiently while preserving the privacy of each party's data. More specifically, we decompose the forward propagation and backpropagation of the neural network into four different steps and propose a novel protocol to handle information leakage in these steps. Our extensive experiments on different datasets demonstrate not only stable training without accuracy loss, but also more than 100 times speedup compared with the state-of-the-art system.

1 Introduction

Machine learning makes use of algorithms to perform tasks such as prediction or classification. Classical machine learning approaches need centralizing the training data on one machine or in a cluster. Centralized machine learning is, by far, the most common architecture. However, it also stops further applications in finance sectors (e.g., insurance and bank) from employing machine learning techniques. For confidentiality reasons, these finance sectors are not able to share their data and store it in the cloud, and thus cannot benefit from centralized machine learning with other organizations.

Data privacy is a fundamental challenge for many machine learning applications depending on data aggregation across different entities, especially in finance sectors. The trade-off between data privacy and learning on aggregated data creates a collaborative circumstance. Decentralized machine learning applies to keeps data safe and ensures privacy under some conditions. A new method called Federated Learning (or Collaborative Machine Learning) [15][19], proposed by Google, offers a way of decentralized and confidential machine learning. By using aggregated updating parameters of the model to train algorithms instead of raw data, federated learning empowers sectors where data cannot be transferred to third parties for confidentiality reasons with data network effects. In fact, federated learning plays a similar role in data parallelism based distributed machine learning. In other words, federated learning is a kind of distributed version of deep neural networks that the data can be partitioned and stored in multiple machines. However, federated learning is only able to transform (or online) deep learning into horizontal parallelism, which splits the data based on the quantity of the data, i.e., the different amount of data subset goes into the parallel computation. Thus, the learning scheme of federated learning cannot handle the situation of vertical parallelism. Additionally, recent

researches [21] have shown that it is possible to obtain the private training data from the publicly shared gradients.

In this paper, we investigate a learning technique that allows two parties to collaboratively train a model while one party (the active party) holds data and another party (the passive party) holds the corresponding labels. We term this **Asymmetrically Collaborative Machine Learning** since the learning task is based on the model that parties actively interact by sharing information and take on asymmetric roles. Compared with federated learning and collaborative machine learning, asymmetrically collaborative machine learning is to transform machine learning algorithms into Vertical parallelism, which splits the data based on one or more specific internal characteristics of the data.

Technically, for this scheme, the straightforward solution is learning on encrypted data. There are two different ways to learn a model on encrypted data: differential privacy [6, 1] and homomorphic encryption [2]. Differential privacy injects noise into query results to avoid inferring information about any specific record. However, it needs careful calibration to balance privacy and model usability. Further, private attributes still remain in plaintext, which are unacceptable for finance sectors, so users may still have security concerns. A more promising solution comes from the recent advance in homomorphic encryption. It allows users to encrypt data with the public key and offload computation to the cloud (or other parties). The cloud computes on the encrypted data and generates encrypted results. Without the secret key, the cloud simply serves as a computation platform but cannot access any user information. But it is extremely costly in computation, thus unsuitable for high dimension data and costly machine learning methods (e.g., deep neural networks).

In this paper, we propose a novel privacy-preserving architecture to solve the problem of how the two parties can collaboratively train a model while one party holds data, and another party holds the label by neural networks. Intuitively, we avoid learning on encrypted data directly. Thus we decompose a Deep Neural Network (DNN) into two components: the 'Feature Extraction' part and the 'Classifier' part. In 'Feature Extraction' a locally unencrypted deep neural network is used to extract more compact features from unencrypted data. In the 'Classifier,' a shallow neural network is used to learn a classifier on encrypted features came from the component of feature extraction. However, such a locally unencrypted and locally encrypted deep neural network results in a new challenge of preserving-privacy. Compared with learning on encrypted data, the 'classifier' needs to calculate the gradient of inputs and passes it back to the 'feature extraction' part. Thus we also need to **avoid information leakage in the gradient**, which has been proved in [21]. Furthermore, we take a two-layer neural network as an example to decompose the forward and backward propagation into four different steps and propose a protocol to avoid information leakage in them. Our contribution includes:

- We define a new scheme of collaborative machine learning, called asymmetrically collaborative machine learning which is promising in many real-world applications.
- We propose a novel privacy-preserving, computationally efficient, homomorphic encryption-based backpropagation algorithm for asymmetrically collaborative machine learning.
- An extensive empirical evaluation of the proposed approach is demonstrated to show the proposed method achieves 100 times speed-up compared with the methods based on learning on encrypted data.

2 Related Work

Traditional encryption methods, such as AES (Advanced Encryption Standard) [3], are extremely fast, and allow data to be stored conveniently in encrypted form. However, it is costly and quite a challenge to perform even simple analytics on the encrypted data (i.e. ciphertexts). For example, the cloud server needs access to the secret key, and the owner of the data needs to download, decrypt as well as operate on the data locally. These commonly lead to security concerns. Homomorphic Encryption (HE) is able to encrypt data before sending to a cloud computing platform while still allowing the operations of search, sort, and edit on the ciphertexts. This property avoids needing to ship data back and forth to be decrypted from the cloud computing platform. HE which supports any function on ciphertexts is known as Fully Homomorphic Encryption (FHE) [7], while Partially Homomorphic Encryption (PHE) [4, 11] includes encryption schemes that have homomorphic properties, with respect to one operation (e.g., only addition or only multiplication, but not both). However, FHE

faces a fundamental problem which extremely costly in computation. Thus it is unpractical for some machine learning methods (e.g. high dimension linear model and neural network). Paillier [16], as well known one method of PHE, supports unlimited numbers of additions between ciphertext, and multiplication between a ciphertext and a scalar constant. In other words, given $Enc(m_1)$ and $Enc(m_2)$, you can not get $Enc(m_1) \otimes Enc(m_2)$. You can only get $Enc(m_1) \oplus Enc(m_2)$ which equals $Enc(m_1 + m_2)$. Given $Enc(m_1)$ and m_2 , you can get $Enc(m_1) \otimes m_2$ which equals $Enc(m_1 \cdot m_2)$. But notice that m_2 , in this case, was not encrypted. \oplus is the homomorphic addition with ciphertext and \otimes is the homomorphic multiplication between ciphertext and a scalar constant. $Enc(x)$ is the ciphertext of plaintext x .

GELU-Net [20] proposes a novel privacy-preserving architecture based on paillier. The main difference between the proposed method and GELU is that GELU works under the situation that one party In this paper, we focus on solving the privacy issue that data and labels are distributed on different parties.

3 Methodology

3.1 Applying Neural Networks to Collaborative Machine Learning

To solve this problem, our main strategy is making a deep neural network partially learn on unencrypted data and partially learn on encrypted features to reduce the computation cost in the stage of learning on encrypted data. More specifically, a deep neural network is carefully partitioned into two parts: the 'feature extraction' and the 'classifier' (or 'regression'). The 'feature extraction' plays a role of dimension reduction in the plaintext and produces compact features to the 'classifier'. And then the implementation of 'the classifier' is learning a simplified model (e.g. logistic regression) on encrypted features generated from the 'feature extraction' part. It is easy to observe that this setting is insensitive to the dimension of inputs and network architectures not only because the 'feature extraction' part contains the majority of neural network and it does not use arithmetic operations of homomorphic encryption, but also because the computational complexity of 'classifier' part is related to the dimension of features generated from the 'feature extraction' part rather than the dimension of raw inputs and the former is far more compact. Take a two-layer neural network as an example, one for 'feature extraction' and another one for 'classifier'. The corresponding training objective is shown in Eq. 1, for simplicity the bias items are omitted:

$$\min_{\mathbf{W}_1, \mathbf{W}_2} \frac{1}{|D|} \sum_{\mathbf{x}_i} \mathcal{L}_i(\mathbf{t}_i, \mathcal{F}_{\{\mathbf{W}_1, \mathbf{W}_2\}}(\mathbf{x}_i)) = \sum_{\mathbf{x}_i} \mathcal{L}_i(\mathbf{t}_i, \text{Softmax}(\mathbf{W}_2 \sigma(\mathbf{W}_1 \mathbf{x}_i))), \mathbf{x}_i \in D \quad (1)$$

where D is the dataset. \mathbf{x}_i and \mathbf{t}_i represent the input data sample and its related target (label). $\sigma(\cdot)$ is ReLU function [9] $\mathbf{W}_1 \in R^{d_h \times d_i}$ and $\mathbf{W}_2 \in R^{c \times d_h}$ are parameters of two layers respectively. d_i is the dimension of input sample. d_h is the dimension of hidden layer. c is the output dimension as the same as the number of categories. Assuming \mathcal{L}_i is CrossEntropy [14], η is learning rate, We can further decompose forward and backward propagation into two different parts respectively, and then there are four steps as following:

- **Step 1** The forward propagation on the active party: the active party feeds the data into the neural net (feature extraction) on the active party. The output activations $\mathbf{a}_i = \sigma(\mathbf{W}_1 \mathbf{x}_i) \in R_h^d$ is then send to the passive party.
- **Step 2** The forward propagation on the passive party: the passive party propagates the received activation \mathbf{a}_i through its neural nets $\mathbf{p}_i = \text{softmax}(\mathbf{z}_i)$, $\mathbf{z}_i = \mathbf{W}_2 \mathbf{a}_i$ and compute the CrossEntropy loss $\mathcal{L}_i(\mathbf{t}_i, \mathbf{p}_i) = \mathbf{t}_i \log(\mathbf{p}_i)$.
- **Step 3** The back propagation on the passive party: the passive party compute the required gradients: $\frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} = \mathbf{t}_i - \mathbf{p}_i$, $\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \frac{\partial \mathbf{p}_i}{\partial \mathbf{W}_2} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \mathbf{a}_i$, $\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \frac{\partial \mathbf{p}_i}{\partial \mathbf{a}_i} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \mathbf{W}_2$ and update parameter via $\mathbf{W}_2 = \mathbf{W}_2 - \eta \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}$ and send $\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}$ back to the active party.
- **Step 4** The back propagation on the active party: the active party receives the gradient $\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}$ from passives party, computes the gradient $\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_1} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i} \frac{\partial \mathbf{a}_i}{\partial \mathbf{W}_1} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i} \mathbf{x}_i$ and updates the parameters $\mathbf{W}_1 = \mathbf{W}_1 - \eta \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_1}$.

To fulfil the requirement that both data and label cannot get or infer from the other side, we encrypt the intermediate results exchanged in both parties, and carefully design a Privacy-Preserving Back-Propagation that is compatible with the PHE in the setting of Asymmetrically Collaborative Machine Learning. We detail the privacy issue and the algorithm in the following section.

3.2 Secure Forward Propagation on the active party

The secure forward propagation on the active party is similar to the normal forward propagation used in training neural nets. The only difference is that the last layer activations (outputs) \mathbf{a}_i in the secure forward propagation needs to be encrypted with PHE. We note the additive homomorphic encryption as $[\cdot]_c$. Since these activations will be transmitted to the passive party, leaving them in the plaintext will lead to the issue of information leakage. The passive party or attacker can collect these activations as meaningful features for later use. Potentially, the passive party or attacker may infer the personal information from these activations. Thus, the active party will encrypt the activations to $[\mathbf{a}_i]_c$ and then send to the passive party.

Algorithm 1: Privacy-preserved Forward Propagation

Initialization: $\epsilon_{acc}, \widetilde{\mathbf{W}}_2, \mathbf{W}_1$
Input: learning rate η , data sample \mathbf{x}
Active Party:
 $\mathbf{a}_i \leftarrow \sigma(\mathbf{W}_2 \mathbf{x}), [\mathbf{a}_i]_c \leftarrow Enc(\mathbf{a}_i)$
 Send $[\mathbf{a}_i]_c$ to passive party
Passive Party:
 Compute the weighted sum $[\tilde{\mathbf{z}}_i]_c \leftarrow \widetilde{\mathbf{W}}_2 \otimes [\mathbf{a}_i]_c$ and add random noise $[\tilde{\mathbf{z}}_i + \epsilon_s]_c \leftarrow \epsilon_s \oplus [\tilde{\mathbf{z}}_i]_c$
 Sent $[\tilde{\mathbf{z}}_i + \epsilon_s]_c$ to active party
Active Party:
 $\tilde{\mathbf{z}}_i + \epsilon_s \leftarrow Dec([\tilde{\mathbf{z}}_i + \epsilon_s]_c)$
 Remove noise: $\mathbf{z}_i + \epsilon_s \leftarrow \tilde{\mathbf{z}}_i - \epsilon_{acc} \mathbf{a}_i + \epsilon_s$;
 Send $\mathbf{z}_i + \epsilon_s$ to the passive party
Passive Party:
 Remove noise: $\mathbf{z}_i \leftarrow \mathbf{z}_i + \epsilon_s$
 Compute softmax result $\mathbf{p}_i = Softmax(\mathbf{z}_i)$
Return \mathbf{p}_i

3.3 Secure Forward Propagation on the passive party

After receiving the encrypted activation $[\mathbf{a}_i]_c$, the passive party keeps going forward propagation, as shown in the step 1 of Sec 3.1. It calculates the weighted sum ($[\mathbf{z}_i]_c = \mathbf{W}_2 \otimes [\mathbf{a}_i]_c$) and applies softmax. However, the non-linearity $e^{[\mathbf{z}_i]_c}$ cannot be computed in the ciphertext. The solution to this problem is transmitting the weighted sum $[\mathbf{z}_i]_c$ back to the active party for decryption and get the plaintext \mathbf{z}_i to calculate the softmax results [20]. But directly sending the weighted sum $[\mathbf{z}_i]_c$ without any protection will leak the prediction to the active party. The active party can use the activation prediction pairs $(\mathbf{a}_i, \mathbf{z}_i)$ to learn the classifier part in the passive party. In this way, the active party can learn the weights of the model on the passive party and further approximate the label. To end this, instead of transmitting the weighted sum $[\mathbf{z}_i]_c$ directly back to the active party, the passive party will inject random noise to it $[\mathbf{z}_i]_c \oplus \epsilon_s$. The noise ϵ_s hides the real weighted sum, which prevents the active party from accumulating activation prediction pairs to infer the weights of the neural network on the passive party. Finally, the active party decrypts the noisy weighted sums $[\mathbf{z}_i + \epsilon_s]_c$ and sends the decrypted $\mathbf{z}_i + \epsilon_s$ to the passive party. And then the passive party removes the noise injected before and computes the prediction (softmax result).

Another problem here is that the passive party get both \mathbf{W}_2 and \mathbf{z}_i and can easily get \mathbf{a}_i via linear regression. To end this, the passive party should use noisy weight $\widetilde{\mathbf{W}}_2$ to calculate the weighted sum ($[\tilde{\mathbf{z}}_i]_c = \widetilde{\mathbf{W}}_2 \otimes [\mathbf{a}_i]_c$) where $\widetilde{\mathbf{W}}_2 = \mathbf{W}_2 + \epsilon_{acc}$. Note that ϵ_{acc} is generated by the active party, we will discuss how to inject ϵ_{acc} to \mathbf{W}_2 in the Sec 3.4. With same procedure, the passive party still need to add additional noise to $[\tilde{\mathbf{z}}_i]_c$ and send $[\tilde{\mathbf{z}}_i + \epsilon_s]_c$ back the active party to avoid computing

Algorithm 2: Privacy-preserved Backward Propagation

Input: Prediction: \mathbf{p}_i on passive party; Target \mathbf{t}_i ; The encrypted activation $[\mathbf{a}_i]_c$;

Passive Party ;

Compute the following gradients;

$$\frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \leftarrow \mathbf{t}_i - \mathbf{p}_i, [\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c \leftarrow \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \otimes [\mathbf{a}_i]_c, \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}} \leftarrow \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \widetilde{\mathbf{W}_2};$$

Add noise $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s]_c \leftarrow [\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c \oplus \epsilon_s$;

Send $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s]_c$ to the active party ;

Active Party ;

$$\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s \leftarrow \text{Dec}([\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s]_c);$$

Add noise: $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} + \epsilon_s \leftarrow \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s - \frac{\epsilon_w}{\eta}$;

Encrypt noise: $[\epsilon_{acc}]_c \leftarrow \text{Enc}(\epsilon_{acc})$;

Accumulate noise: $\epsilon_{acc} \leftarrow \epsilon_{acc} + \epsilon_w$;

Send $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} + \epsilon_s$ and $[\epsilon_{acc}]_c$ to passive party;

Passive Party ;

$$\text{Remove noise: } \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} \leftarrow \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} + \epsilon_s;$$

$$\text{Update weights } \widetilde{\mathbf{W}_2} \leftarrow \widetilde{\mathbf{W}_2} - \eta \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}};$$

$$\text{Remove noise from gradients: } [\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}]_c \leftarrow \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}} - [\epsilon_{acc}]_c \otimes \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i};$$

Send $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}]_c$ to the active party;

Active Party

$$\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i} \leftarrow \text{Dec}([\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}]_c);$$

Do the normal backpropagation with $\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}$;

non-linearity homomorphically. To perform the correct forward propagation the active party will cancel the noise in $[\widetilde{\mathbf{z}}_i]_c$ via $[\mathbf{z}_i]_c = [\widetilde{\mathbf{z}}_i]_c - \epsilon_{acc} \mathbf{a}_i$ and send $[\mathbf{z}_i]_c$ to the passive party for computing the true softmax output \mathbf{p}_i with respect to \mathbf{W}_2 . Since the passive party can only observe the noisy $\widetilde{\mathbf{W}_2}$ and $[\mathbf{z}]_c$ with respect to \mathbf{W}_2 . The passive party cannot infer the activation \mathbf{a}_i . The whole forward propagation performs in a privacy-preserved manner.

3.4 Secure Backward Propagation on the passive party

During the backpropagation we need to estimate two gradient: the gradient $\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}$ and the gradient $\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}$. Note that these two gradients are the linear transformation of either \mathbf{a}_i or \mathbf{W}_2 , both the active party and the passive party can derive what they want via regression. Not carefully dealing with gradient updating may cause a significant information leak. In backpropagation, the passive party will compute the following gradients: $\frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} = \mathbf{t}_i - \mathbf{p}_i$, $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c = \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \otimes [\mathbf{a}_i]_c$ and $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i} \widetilde{\mathbf{W}_2}$. Note that the gradient of weights $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c$ is in the encrypted form. After weights updating $[\mathbf{W}_2]_c = \mathbf{W}_2 - \eta [\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c$, the weights $[\mathbf{W}_2]_c$ will result in the encrypted form. This causes the issue that in the forward propagation of the next iteration, there will be two encrypted quantities in calculating weighted sum $\mathbf{z}_i = [\mathbf{W}_2]_c [\mathbf{a}_i]_c$, which is incompatible with PHE. To avoid this situation, the passive party need to send the gradients of weight $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c$ to the active party and get the decrypted gradients $\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}$ back. However, this solution is dangerous. Since the passive party holds $\frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i}$ and the active party holds the \mathbf{a}_i , knowing the gradient $\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}$ make both parties leak information at the same time. Thus, both two parties need to add random noise to the gradients of weights before sending it to the other side. Specifically, they do

- The passive party add noise ϵ_s to $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}]_c$ and send $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s]_c$ to the passive party.
- the active party decrypt $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s]_c$

- The active party add random noise $\frac{\epsilon_w}{\eta}$: $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} + \epsilon_s \leftarrow \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_s - \frac{\epsilon_w}{\eta}$
- The active party send $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} + \epsilon_s$ to the passive party
- The passive party remove noise ϵ_s : $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} \leftarrow \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} + \epsilon_s$

Note that noise generated by the passive party can be removed immediately while the gradients of weight $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}}$ still contain noise where $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} - \frac{\epsilon_w}{\eta}$. With $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2}}$ the passive party blindly update the parameters as:

$$\widetilde{\mathbf{W}_2}^{t+1} = \mathbf{W}_2^t - (\eta \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} - \frac{\epsilon_w}{\eta}) \Rightarrow \widetilde{\mathbf{W}_2}^{t+1} = \mathbf{W}_2^t - \eta \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_2} + \epsilon_w \Rightarrow \widetilde{\mathbf{W}_2}^{t+1} = \mathbf{W}_2^{t+1} + \epsilon_w$$

We can see that the noise ϵ_w will accumulate in weight \mathbf{W}_2 in each iteration. If we note the accumulated noise as $\epsilon_{acc} = \epsilon_w^1 + \epsilon_w^2 + \dots + \epsilon_w^t$, the true weights that supposed to be used in the forward and backward propagation should be $\mathbf{W}_2^{t+1} = \widetilde{\mathbf{W}_2}^{t+1} - \epsilon_{acc}$. To perform the right forward propagation, the active party needs to cancel the noise by subtracting $\mathbf{a}_i \epsilon_{acc}$ from the noisy weighted sums $\tilde{\mathbf{z}}_i$ as described in Sec 3.3. Similar to the forward propagation, in the back propagation, the extra noisy gradients is also added to $\widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}}$ and need to be removed before backpropagating to the active party. To achieve this, the active party needs to send the encrypted $[\epsilon_{acc}]_c$ to the passive party. the passive party calculate the true gradient $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}]_c = \widetilde{\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}} - [\epsilon_{acc}]_c \otimes \frac{\partial \mathcal{L}_i}{\partial \mathbf{p}_i}$ and send the encrypted gradient $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}]_c$ to the active party.

3.5 Secure Backward propagation on the active party

The active party decrypt the gradient $[\frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i}]_c$ received from the passive party, compute the gradient $\frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_1} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i} \frac{\partial \mathbf{a}_i}{\partial \mathbf{W}_1} = \frac{\partial \mathcal{L}_i}{\partial \mathbf{a}_i} \mathbf{x}_i$ and update the parameters $\mathbf{W}_1 = \mathbf{W}_1 - \eta \frac{\partial \mathcal{L}_i}{\partial \mathbf{W}_1}$. The whole privacy preserved backpropagation is detailed in Algorithm 1 and Algorithm 2.

4 Experiment

To evaluate the proposed method, specifically, we determine if our model (i) achieves lossless performance in classification tasks and (ii) if it brings advantages over other solution based on learning on encrypted data. Please note we don't want to highlight the performance of neural networks but we can achieve a lossless performance. we implement the passive party and the active party both on two PCs with CPU Core i7-6850k and 64GB RAM connected by 1Gbps LAN. The neural network of the active party is built using pytorch [17] and the neural net of the passive party is implemented by pure python integrated with *numpy*. We compare the proposed method with two previous studies that have considered privacy-preserved training with homomorphic encryption for deep neural networks. GELU [20] using PHE [16] and CryptoNets [8].

4.1 Setting

In order to make comparison with previous work: GELU and CryptoNets [8]. We implement the following architecture of the proposed method:

- **Multinomial Logistic Regression(MLR:** Data-Dense(10)-Softmax
- **Conv-1:** Data-Conv(5×5, stride 2, 5 filter) -ReLU-MeanPooling-ReLu-Dense(84))-Dense(10)-Softmax
- **LeNet-5:** Data-Conv(5×5, stride 1, 6 filter)-MeanPooling-ReLu-Conv(5×5, stride 1, 16 filter)-MeanPooling-ReLu-Dense(120)-Dense(84)-Dense(10)-Softmax

For the proposed method, the final layer, Dense(10)-Softmax, is on the passive party side, the rest of layers are on the active party side.

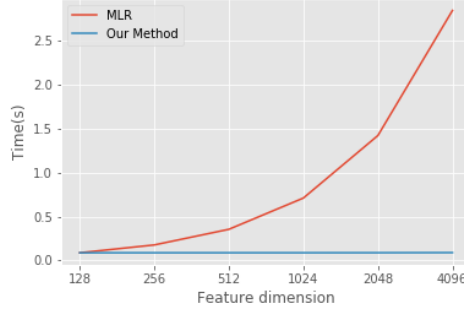


Figure 1: The computation speed for one inference with different input feature dimension

4.2 Training Accuracy

In this section, we show the proposed method is a lossless solution. The neural network architecture we use is Conv-1. Due to arithmetic operations of homomorphic encryption only support multiplication and addition, CryptoNets uses the square function to avoid computing the non-linear activation. However, this makes the training unstable and damage to the accuracy [8]. From the Table. 1, we can see that CryptoNets suffers an accuracy loss ranging from 2% to 5% compared with the proposed method. We also note that GELU is also a lossless solution. This is because GELU adopts the similar round trip strategy that sending activation back and forth between the passive party and the active party for handling non-linear operation as we do.

Table 1: Test accuracy of different Architecture

Architecture	GELU	CryptoNets	Ours
Iris	0.982	0.966	0.980
Diabetes	0.758	0.741	0.760
kr-vs-kp	0.967	0.948	0.965
MNIST	0.969	0.919	0.970

4.3 Computation Speed

As above mentioned, the dimension of inputs and the neural network architecture are key factors to other methods. In this section we will demonstrate that the proposed method is insensitive to these two factors.

Sensitivity of Input Dimension One problem of learning on the encrypted data is the computation speed depend on the input dimension. It is because the dimension of the encrypted data directly increases the number of homomorphic encryption operations. We compare our model with multinomial logistic regression that learned on encrypted data. We experiment with simulated data with various feature lengths. As shown in Fig. 1, our proposed method is insensitive to the dimensions of input data compared with multinomial logistic regression (i.e., shallow network with softmax activation). We do the experiment on the real word data using MNIST [13] and CIFAR-10 [12]. We can observe from the table. 2 the result of CIFAR-10 [12] (dimensions is $3 \times 32 \times 32$) is very similar to the result on MNIST [13] (dimensions is $1 \times 28 \times 28$). This benefits from we employ learning on encrypted features generated from the 'feature extraction' of the deep neural network, which can significantly reduce raw data dimensions. Compared with learning on encrypted data, feature extraction is very efficient. So that is why the proposed method consumes similar time in the different datasets.

Sensitivity of Neural Network Architectures Note that the proposed method is designed to work on any architecture without much computation speed degrade. In comparison, the other baselines

Table 2: Time for different architectures on MNIST and CIFAR-10 dataset

Architecture	Time(s)
Multinomial Logistic Regression (MNIST)	0.5887
Multinomial Logistic Regression (CIFAR-10)	2.7027
LeNet-5 (MNIST)	0.0583
LeNet-5 (CIFAR-10)	0.0592

models like GELU and CryptoNet are sensitive to either the neural networks architecture or input data dimension. Thus, using complex neural net such as VGG [18], ResNet [10] with high dimension input such as ImageNet [5] is infeasible to the methods of learning on encrypted data, and it will take an extremely long time. Moreover, since the arithmetic operations in PHE is much faster than arithmetic operations in FHE. We mainly focus on comparing the proposed method with GELU. Thus, to make a fair comparison, we train the proposed method and GELU on different architecture described in Sec. 4.1. We report the computation time (for one inference). Table.3 shows the computation time

Table 3: Test accuracy of different Architectures

Architecture	Time(s)	Accuracy
GELU-Net(LeNet-5)	7.855	0.989
Multinomial Logistic Regression	0.588	0.93
Our Method(LeNet-5)	0.0583	0.99

Table 4: Time for the proposed method and GELU-Net on MNIST

Architecture	Time(s)
GELU-Net(Conv-1)	3.8437
Our Method (Conv-1)	0.0582
Our Method(LeNet-5)	0.0583

(for one inference) and the accuracy on MNIST [13]. We observe that the proposed method achieves more than 100x speed-up over GELU-Net with no accuracy loss. Even compared with simpler architecture multinomial logistic regression (MLR), our method is much faster. Therefore our method works much faster than GELU and performs much better than the linear model with encrypted data due to the deep neural network can learning more semantic representation for targets. Table. 4 shows the computation speed of the proposed method in both deep (LeNet-5) and shallow neural net (Conv-1). Result reveals that the time for one inference is almost invariant to the architectures as long as the output dimension is the same (both Conv-1 and LeNet-5 are 84). That means the mainly computational bottleneck is on the 'classifier' which learns the part model on encrypted data. It also shows that our deep model is highly potential to apply to more complicated data which need the deeper neural network.

5 Conclusion

In this paper, we have proposed a scheme, called asymmetrically collaborative machine learning where one party has data, but the other party has labels only. A deep neural network with a partly unencrypted and partly encrypted strategy is proposed to avoid learning on encrypted data directly for this scheme. Beyond that, we offer a series of solutions to preserve privacy from both parties involved. The design has ensured the efficiency and effectiveness of the proposed method. We have carried out extensive experiments that demonstrate more than 100× times speedup compared with the state-of-the-art solutions.

References

- [1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 308–318. ACM, 2016.
- [2] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: theory and implementation. *ACM Computing Surveys (CSUR)*, 51(4):79, 2018.
- [3] Joan Daemen and Vincent Rijmen. Aes proposal: Rijndael. 1999.
- [4] Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Annual Cryptology Conference*, pages 643–662. Springer, 2012.
- [5] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition*, pages 248–255. Ieee, 2009.
- [6] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.
- [7] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.
- [8] Ran Gilad-Bachrach, Nathan Dowlin, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In *International Conference on Machine Learning*, pages 201–210, 2016.
- [9] Xavier Glorot, Antoine Bordes, and Yoshua Bengio. Deep sparse rectifier neural networks. In *Proceedings of the fourteenth international conference on artificial intelligence and statistics*, pages 315–323, 2011.
- [10] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.
- [11] Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha Chandrakasan. {GAZELLE}: A low latency framework for secure neural network inference. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 1651–1669, 2018.
- [12] Alex Krizhevsky and Geoffrey Hinton. Learning multiple layers of features from tiny images. Technical report, Citeseer, 2009.
- [13] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.
- [14] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. Deep learning. *nature*, 521(7553):436, 2015.
- [15] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, pages 1273–1282, 2017.
- [16] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 223–238. Springer, 1999.
- [17] Adam Paszke, Sam Gross, Soumith Chintala, Gregory Chanan, Edward Yang, Zachary DeVito, Zeming Lin, Alban Desmaison, Luca Antiga, and Adam Lerer. Automatic differentiation in pytorch. In *NIPS-W*, 2017.
- [18] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.

- [19] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):1–19, 2019.
- [20] Qiao Zhang, Cong Wang, Hongyi Wu, Chunsheng Xin, and Tran V. Phuong. Gelu-net: A globally encrypted, locally unencrypted deep neural network for privacy-preserved learning. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18*, pages 3933–3939, 7 2018.
- [21] Ligeng Zhu, Zhijian Liu, and Song Han. Deep leakage from gradients. In *Advances in Neural Information Processing Systems*, pages 14747–14756, 2019.