算法1

一．代码介绍

本代码是论文<HD-FL: A Federated Learning Privacy Preservation Model Based on Homomorphic Encryption >的源码实现。

本代码将联邦学习中的梯度参数添加拉普拉斯噪声后同态加密，在服务器端平均聚合更新全局梯度。（联邦学习源代码来源于2019 Federated-Learning-with-Differential-Privacy算法）

二．运行环境及主要依赖包

运行环境： Python with Intel Core i5 CPU 1.8 GHz and 8 GB RAM, running Windows10。

包 版本

numpy 1.16.2

tensorflow-privacy 0.5.1

pytorch 1.4.0

torch 1.7.1

syft 0.2.9

scipy 1.4.1

phe 1.4.0

FLClient函数是客户端函数，客户端本地训练模型

encrypt\_vector函数是加密函数

decrypt\_vector函数是解密函数

sum\_encrypted\_vectors是加密计算

update函数用于更新模型参数

update\_grad 更新梯度参数

test\_acc 准确率

FLServer函数是服务器端函数，服务器端更新全局模型

aggregated fedavg更新，权重平均

global\_update 全局更新

aggregated\_grad 梯度fedavg

global\_update\_grad fedavg梯度更新，梯度平均

三．程序运行结果：

