HOMOMORPHIC ENCRYPTION ON MACHINE LEARNING

隊名:密碼不太隊

隊長: 111550105 郭宗信
隊員: 111550061 邱冠崴
111550148 陳冠達
109550060 陳星宇
111550129 林彥亨

ABSTRACT

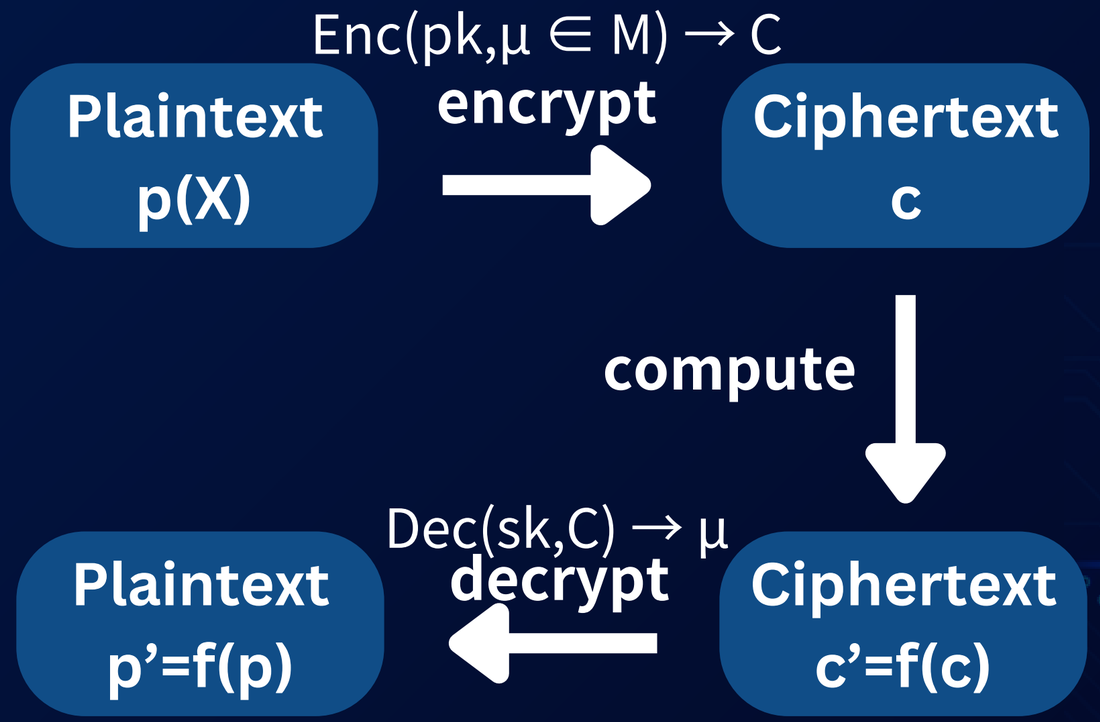
- Introduction
- Experiment
- Contribution
- Reference

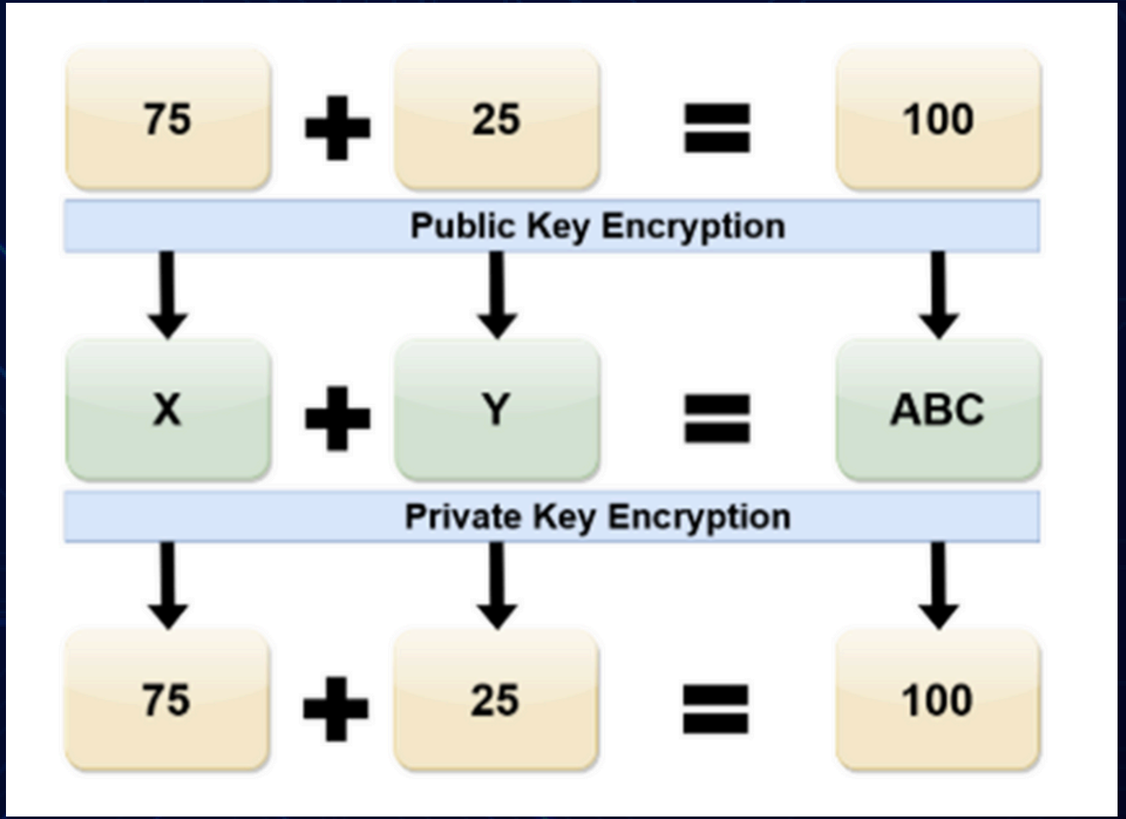
INTRODUCTION

With the development of artificial intelligent, machine learning plays a crucial role in AI, which enables systems to learn and improve from experiment.

Also, machine learning relies on vast datasets to train models. In order to protect personal data in machine learning, using homomorphic encryption on the training data is a solution.

ABOUT HOMOMORPHIC ENCRYPTION





EXPERIMENT

Prediction of Tumor Benignity and Malignancy

Logistic regression training
on plain dataset

Encryption Logistic regression training
on encrypted dataset

EXPERIMENT

Logistic regression training on plain dataset

sigmoid function

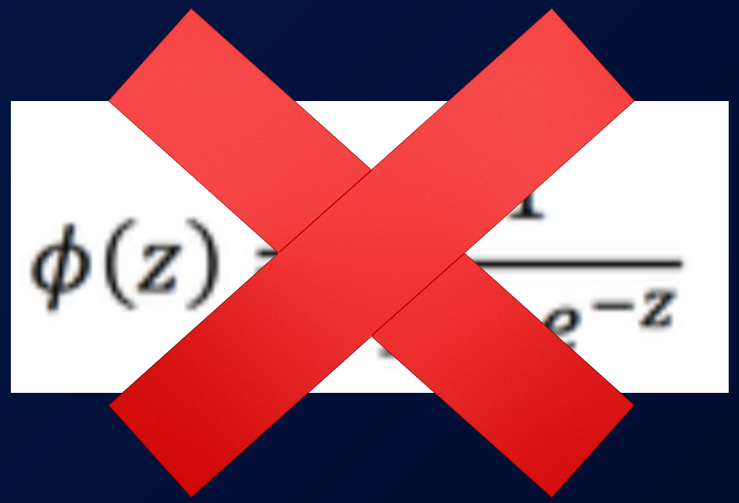
criterion:
Binary Cross Entropy Loss

optimizer: SGK

EXPERIMENT

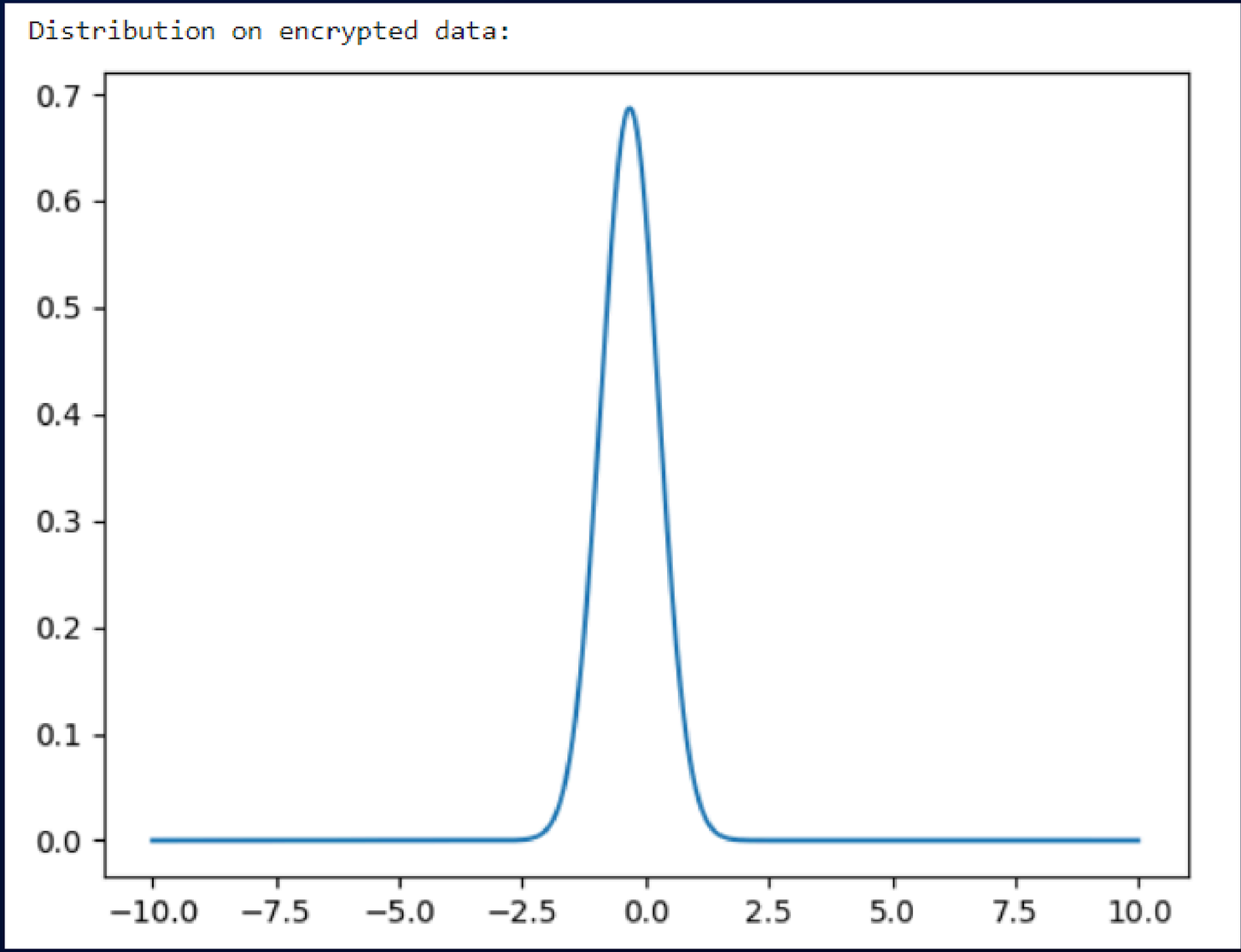
Encryption Logistic regression training on encrypted dataset

problem 1: sigmoid function



$$\sigma_3(x) = -0.004x^3 + 0.197x + 0.5$$

EXPERIMENT


Distribution on encrypted data:
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0

EXPERIMENT

Encryption Logistic regression training on encrypted dataset

problem 2: SGK

$$\theta_j = \theta_j - \alpha \left[\frac{1}{m} \sum_{i=1}^{m} (\hat{y}^{(i)} - y^{(i)}) x^{(i)} + \frac{\lambda}{m} \theta_j\right]$$

EXPERIMENT

analysis

	original	encrypted
accuracy	0.9473684430	0.710526287
average_time	0.033954322 seconds	39.074773848 seconds
memory	0.0MB	0.75 MB

SYSTEM ARCHITECTURE

encrypted dataset & parameters

trained model

Client

Server

EXPERIMENT

Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data without decrypting it.

The client can send encrypted dataset to the server for processing, then the server returns the trained model back to the client.

CONTRIBUTION

Traditionally, data required for model operations needs to be decrypted during processing due to operational needs. However, today we can directly operate on encrypted data, including model training, loading, and prediction.

CONTRIBUTION

Data Privacy Protection

Direct Operations on Encrypted Data
No Decryption Needed
Data Security

Enhancing Security of Operating Environment

Secure Interaction with Unsecured Server
Secure Operations
Accelerated Deployment

Model Security and Privacy

Protecting Models and Data
Training Protection
Collaborative Training

Practical Application Scenarios

Medical Data Analysis
Financial Data Processing
Government and Public Data

FUTURE WORK

01

- Algorithm Optimization
- Parallel Processing
- Device Integration
- Synchronization
- Web-based Interface
- Cloud Integration

02

- Model Diversity
- Custom Model Support
- Real-time Analysis
- Latency Reduction
- GPU Utilization
- Specialized Hardware

REFERENCE

Building a Fully Homomorphic Encryption Scheme in Python

- https://courses.csail.mit.edu/6.857/2019/project/15-Hedglin-Phillips-Reilley.pdf

GSW13 Fully Homomorphic Encryption

- http://www.cse.iitm.ac.in/~shwetaag/6115/Lec7.pdf

Homomorphic Encryption for Arithmetic of Approximate Numbers

- https://eprint.iacr.org/2016/421.pdf

Logistic regression over encrypted data from fully homomorphic encryption

- https://eprint.iacr.org/2018/462.pdf

THANK YOU