Secure Activation function using Functional Encryption

Prajwal Panzade

Team: Prajwal

Georgia State University

Ouline

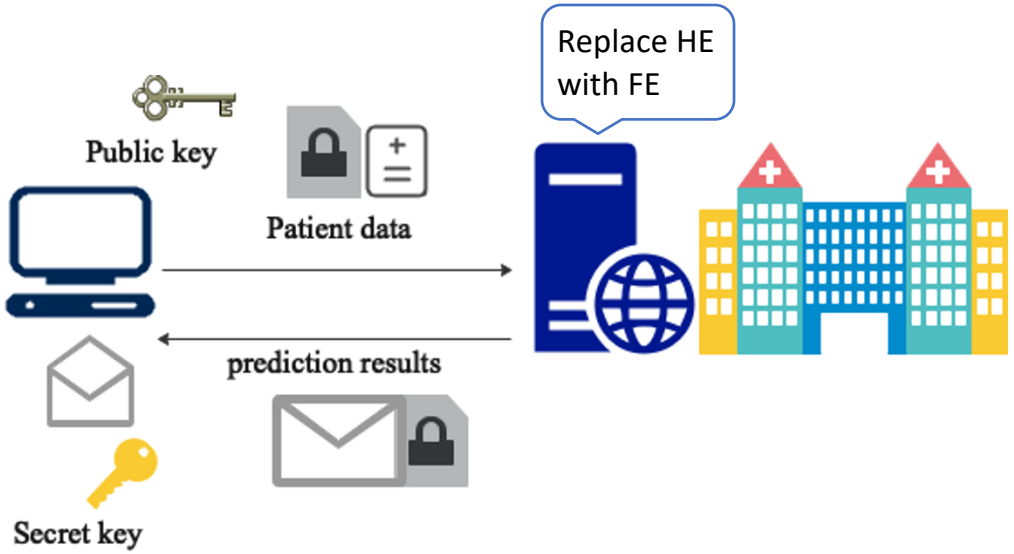
- Introduction
- Motivation
- Framework
- SecureRelu
- Implementaion and Results

Introduction

- Many AI applications in the fields like computer vision and NLP
- Google cloud AI, Microsoft azure learning (MLaaS)
- Cloud server is responsible for training a ML model for classification, regression, etc
- Trained on the data collected from the customers
- Privacy ?

Introduction

- E.g. Privacy-preserving cardiovascular disease prediction service using homomorphic encryption



Motivation

- Homomorphic Encryption and Secure Multiparty computation are already doing a great job in PPML then why use Functional Encryption?

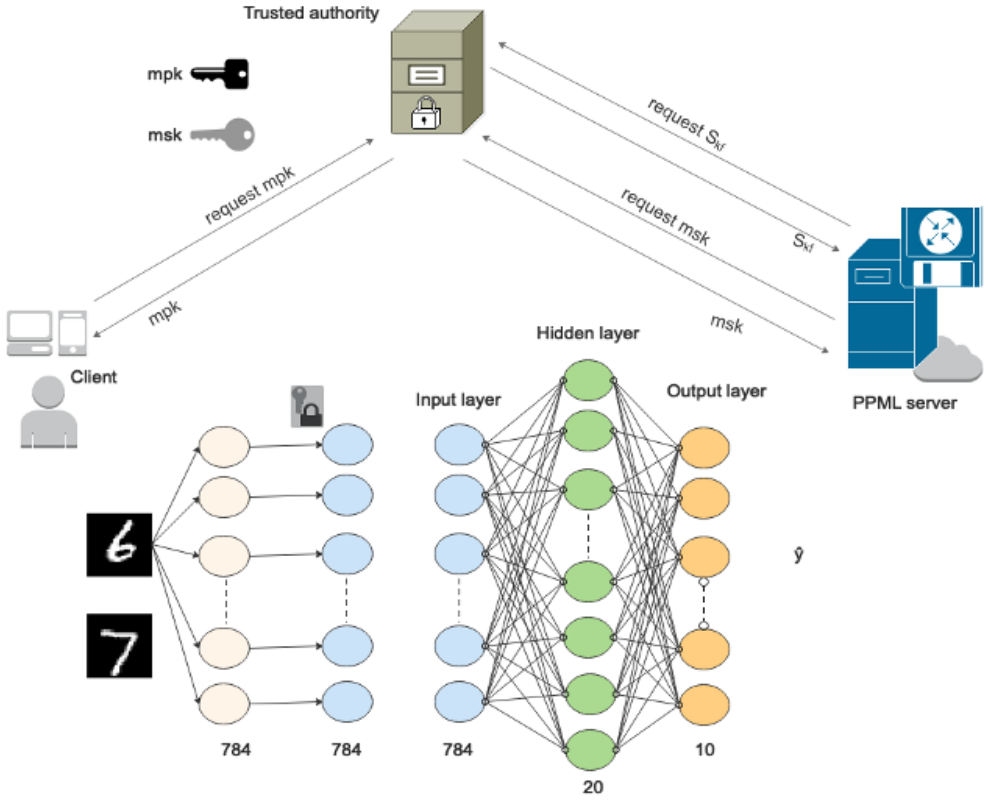
  Encrypted results, training on encrypted data is not allowed

- Can the server train the model without seeing the data but reveals the result in plain?

  Functional Encryption is here to help

How to do machine learning out of it ?

Framework



Live demo

SecureReLU

Algorithm 1: SecureRelu

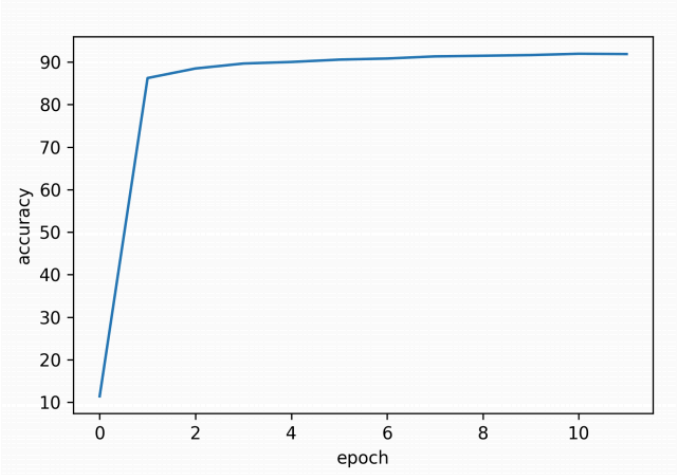
Input: Encrypted X, W, b
Output: Relu(W.X+b)
for $i \leftarrow 0$ **to** $W.size$ **do**
    $prod_i \leftarrow Decrypt(Ct_i, sk_{fe}, W_i)$
    $result_i \leftarrow Relu(prod_i + b)$
return result

Implementation

- 2-layer Neural Network, SGD, categorical cross entropy
- MNIST with 20-30% samples
- Numpy (we can’t directly use sklearn and keras)
- Developed python functions to use CiFEr [7] library functions
- All computations are done on CPU

Results

MNIST	Epoch	Training time	Accuracy
20 % samples	10	> 2 hrs	85 %



Function	Time
Master keys generation	1.8032 s
FE key generation	0.00196 s
Encryption	0.0109 s
Decryption	0.021168 s

Challenges

- FE has been growing richer and richer in theoretical aspects, but Library support is still limited
- ML computations usually involve large no. of inner products; so computing and managing those many ciphertexts and keys is an overhead
- no GPU support is available for the libraries; so model takes forever to run

References

1. https://en.wikipedia.org/wiki/Functional_encryption
2. https://www.cs.virginia.edu/dwu4/fe-project.html
3. Boneh D, Sahai A, Waters B. Functional encryption: Definitions and challenges. InTheory of Cryptography Conference 2011 Mar 28 (pp. 253-273). Springer, Berlin, Heidelberg.
4. Abdalla M, Bourse F, De Caro A, Pointcheval D. Simple functional encryption schemes for inner products. InIACR International Workshop on Public Key Cryptography 2015 Mar 30 (pp. 733-751). Springer, Berlin, Heidelberg.
5. Xu R, Joshi JB, Li C. CryptoNN: Training Neural Networks over Encrypted Data. In2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS) 2019 Jul 7 (pp. 1199-1209). IEEE.
6. Sans ED, Gay R, Pointcheval D. Reading in the Dark: Classifying Encrypted Digits with Functional Encryption. IACR Cryptology ePrint Archive. 2018;2018:206.
7. http://fentec.eu/content/functional-encryption-library

Thank you!
Questions?