Secure Collaborative Design of Experiments with Homomorphic Encryption

Jin Chao, Khin Mi Mi Aung, Zhang Xin

Institute for Infocomm Research, A*STAR

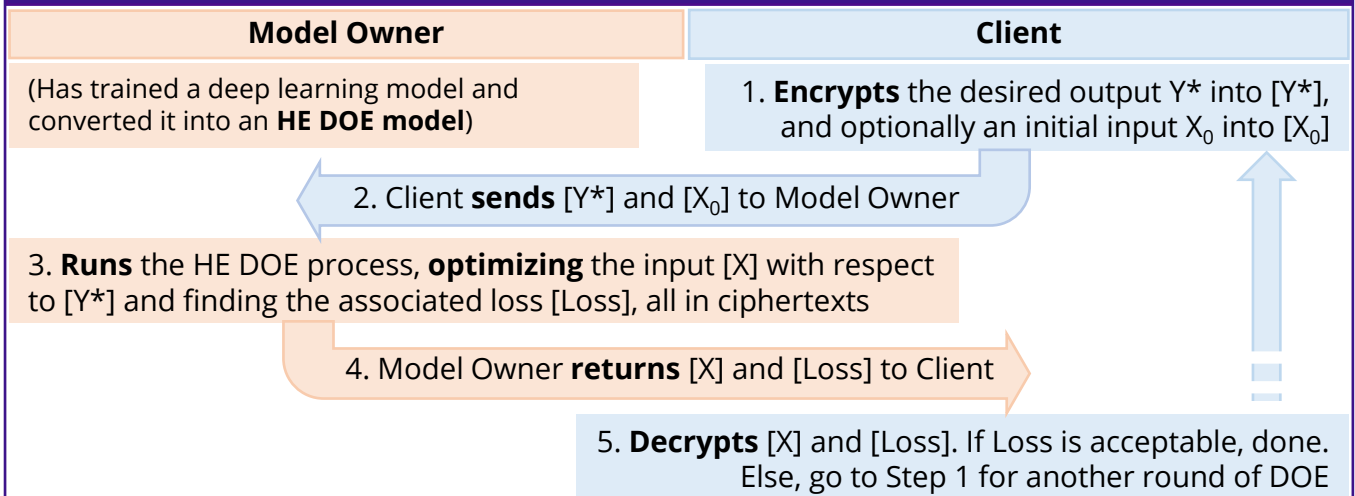Enables the client to outsource the DOE process to the model owner while keeping the target output confidential

Design of Experiments (DOE)

Given a **model f** and a **target output Y***, DOE is the **inverse** process of finding an input X such that Y = f(X) is close to Y*, and the **loss** measures the distance between Y and Y*.
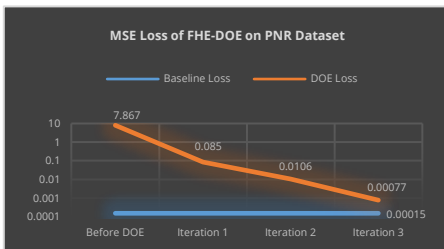

Forward Process

DOE (Inverse Process)
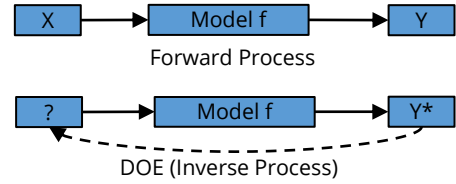
We focus on **deep learning** models, whose DOE process can be implemented by the **backpropagation** algorithm optimizing the inputs with respect to the output loss.
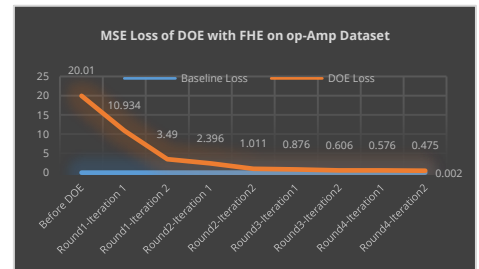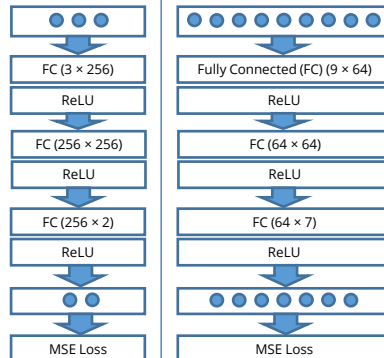
Homomorphic Encryption (HE) DOE Protocol

Model Owner	Client
(Has trained a deep learning model and converted it into an **HE DOE model**)	1. **Encrypts** the desired output Y* into [Y*], and optionally an initial input X_0 into $[X_0]$

2. Client **sends** [Y*] and $[X_0]$ to Model Owner

3. **Runs** the HE DOE process, **optimizing** the input [X] with respect to [Y*] and finding the associated loss [Loss], all in ciphertexts

4. Model Owner **returns** [X] and [Loss] to Client

5. **Decrypts** [X] and [Loss]. If Loss is acceptable, done. Else, go to Step 1 for another round of DOE

Test Outcomes

➢ We use the CKKS scheme for HE, which works with **polynomial** computations. Hence, we **approximate** activation functions using polynomials in the HE DOE process.

➢ The approximations and the noise in fixed-point arithmetic introduce errors, but the convergence trends in the following graphs show **the errors are small**. The loss in the HE DOE process is close to the loss in the DOE process on plaintext data after the same number of iterations.

MSE Loss of FHE-DOE on PNR Dataset

Baseline Loss — DOE Loss

7.867, 0.085, 0.0106, 0.00077, 0.00015

Before DOE, Iteration 1, Iteration 2, Iteration 3

PNR: a simulation dataset generated by pre-defined functions
MSE Loss of the plaintext model (after 500 epochs): 0.00015

For one-core CPU, one iteration on encrypted data under 128-bit security parameters takes 245 seconds, while one iteration on plaintext takes 0.523 seconds.

FC (3 × 256)
ReLU
FC (256 × 256)
ReLU
FC (256 × 2)
ReLU
MSE Loss

Fully Connected (FC) (9 × 64)
ReLU
FC (64 × 64)
ReLU
FC (64 × 7)
ReLU
MSE Loss

MSE Loss of DOE with FHE on op-Amp Dataset

Baseline Loss — DOE Loss

20.01, 10.934, 3.49, 2.396, 1.011, 0.876, 0.606, 0.576, 0.475, 0.002

Before DOE, Round1-Iteration 1, Round1-Iteration 2, Round2-Iteration2, Round2-Iteration2, Round3-Iteration1, Round3-Iteration2, Round4-Iteration1, Round4-Iteration2

Op-Amp: a simulation dataset for manufacturing conditions (e.g., temperature, pressure) and the corresponding outputs

MSE loss of the plaintext model (after 6000 epochs): 0.002

Institute for Infocomm Research

ARES PUBLIC   Emails: jin_chao@i2r.a-star.edu.sg   mi_mi_aung@i2r.a-star.edu.sg   zhang_xin@i2r.a-star.edu.sg