Secure Collaborative Design of Experiments with Homomorphic Encryption

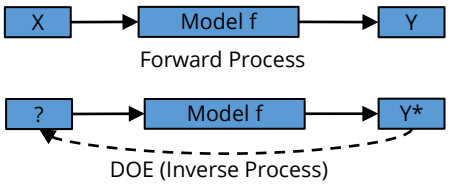
Chao Jin, Khin Mi Mi Aung, Xin Zhang

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*.



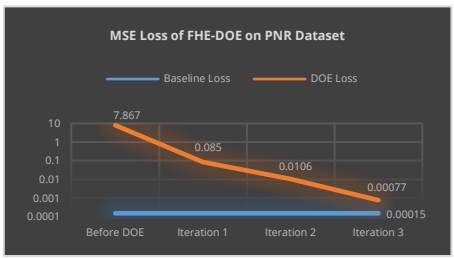
We focus on **deep learning** models, whose DOE process can be implemented by the **backpropagation** algorithm optimizing the inputs with respect to the output loss.

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

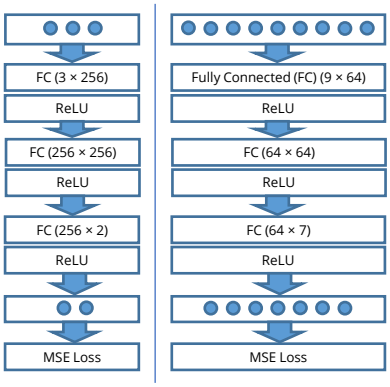
- We use the CKKS scheme for HE, which works with **polynomial** computations. Hence, we **approximate** activation functions using polynomials in the HE DOE process.
- The approximations and the noise in fixed-point arithmetic introduce errors, but the convergence trends in the following graphs show **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.

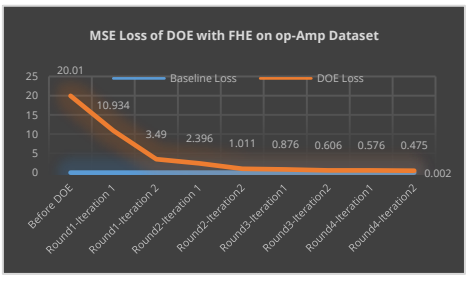


PNR: a simulation dataset generated by pre-defined functions

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.





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

This research is supported by Institute for Infocomm Research, A*STAR Research Entities under its RIE2020 Advanced Manufacturing and Engineering (AME) Programmatic Programme (Award A19E3b0099).

Institute for Infocomm Research

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