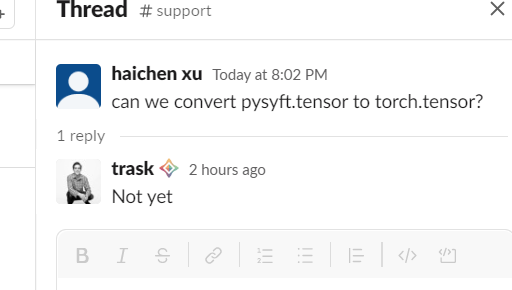


Pysyft does not support sharing float. Our original plan is to share the model parameter to the center with encryption. However, pysyft domain node serve as a database for each data owner with automatic differential privacy. Though the latest version support float , but the core team member said the tutorial for getting the data is still coming.

Pysyft can not convert py.tensor to torch.tensor neither.



Our main idea is not letting the data be shared with anyone even with auto dp. So we might abandon syft or use syft to store the pointer to the model parameter. And I should take a look into homomorphic encryption first : tenseal.

Tenseal only has one key thats not what we want: model owner generate a key and client generate a key. One way I am considering is to store the key on the blockchain and only the smart contract and the owner can use it.

SMPC and SYMPC is not applicable for complicated network.

task this week:

Problem encountered:

Sy.tensor does not support float

Solution:

Change to 0.7version

Consequence:

The Auto dp is not functioning. Publish (sigma) would return a dangling pointer (unsolved)

Problem encounter:

Sy.tensor does not support str

Solution :upload the model structure as the description or metadata.

Consequence: unknown.

Problem encounter:

For homomorphic encryption on convolution , Tenseal runs too long.(unsolved)