1. *Understanding which is the most ZKP time-intensive part when generating proof for LIME.*

Setup : We present experiments with the credit dataset (without loss of generality) since credit dataset has the highest feature dimensionality. We fix the number of hidden units in each layer of MLP to 16 while change the number of layers to 2,10,20,40. The experiments are for the G+E variant (as is the most time intensive variant Fig. 3 main paper) for sampling neighborhood n=300. The results are displayed for one input point picked randomly as the variance in ZKP time is almost zero, as seen from experiments in the main paper (Fig. 3). The same server as the main paper is used.

Evaluation : We provide the 'proof generation' time since proof generation is the most expensive and time-consuming part in a ZKP system. To understand which part of zk_LIME takes the most time, we split zk_LIME in three broad categories — the checks/proof generation needed for (1) inference (step 9 & 31 Alg. 6), (2) lasso (step 33 Alg. 6) and (3) sampling (step 13 & 26 Alg. 6).

Results* :

(1.1) Proof generation time for Sampling and Lasso is almost same across different model sizes and is therefore independent of model size.

(1.2) Proof generation for Inference is the most time-intensive part of the entire proof generation and dominates the total proof generation time. This time grows with increase in model size.

Conclusion : Reducing the time needed for inference proofs is one of the most active research areas in Zk x ML field. Current research generates proofs for 13 billion parameters in under 15 minutes [1]. **The improvements in inference proof times directly translate to us, as ExpProof just uses inference proof engines as a plug-and-play module** and is agnostic to the actual library in theory, so when a new faster library for inference proofs comes out, it can just be used in ExpProof.

#hiddenlayers	Inferences-Only Proof Generation Time (secs)	Lasso-Only Proof Generation Time (secs)	Sampling-Only Proof Generation Time (secs)
2	42.15	59.62	23.54
10	108.23	60.34	24.11
20	179.00	60.70	24.50
40	319.48	62.30	25.59

Table 1. Proof generation time split.

[1] zkLLM: Zero Knowledge Proofs for Large Language Models 2024 Sun et.al.

*The time split is approximate due to stuff related to ZKP but close to exact and shows the expected trend correctly. More specifically, the sum of the proving times for the parts does not equal the proving time of the whole computation - but it shows how expensive each part is (in ZKP terms, it shows which parts have the most constraints).

2. Understanding how the current implementation of ZKPs for LIME scales with model size.

Setup : Same as above except the number of units in each hidden layer is one of {16,32,64} and the number of hidden layers is {2,5,10,20}.

Results :

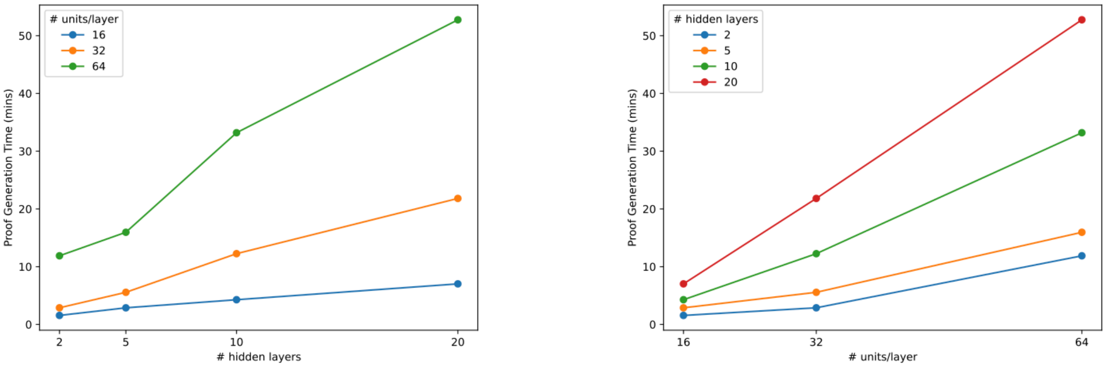

Fig. 1. Proof generation time (in mins) across different #hiddenlayers and #units in each hidden layer.

(2.1) Proof generation time increases both as the number of hidden layers or the units in each hidden layer increase.

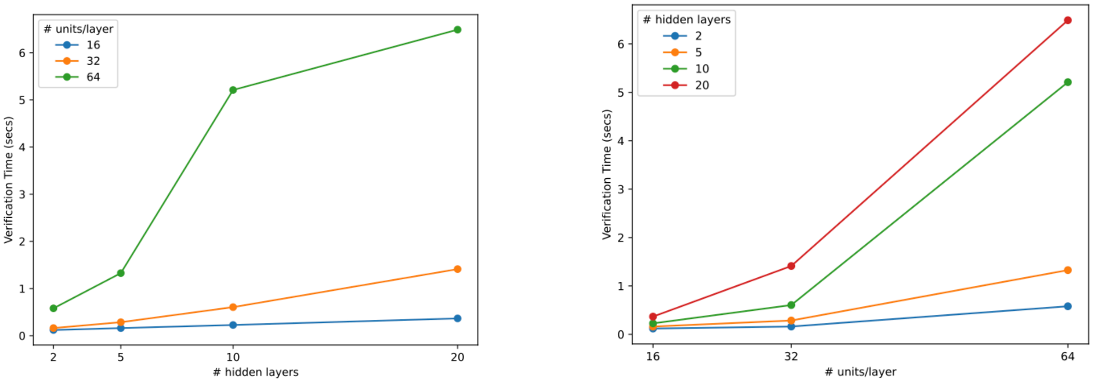

Fig. 2. Verification time (in secs) across different #hiddenlayers and #units in each hidden layer.

(2.2) Verification time increases exponentially both as the number of hidden layers or the units in each hidden layer increase.

Conclusion : **As the most time of the ZKP system can be attributed to that related to inference proofs/verification (from exp 1), the proof generation and verification time will**

reduce with research advancements in this area. As mentioned before, inference proofs are a very active research area and ExpProof treats inference proof module as a black-box and can work with any advanced inference proof library.