



The Implementation of Model Pruning to Optimize zk-SNARKs in Machine Learning

By: Abigail Thomas

Mentor: Yu Xia

Introduction

- ◎ Cloud Computing
- ◎ How is it Secure?



Introduction

- ◎ Cloud Computing
- ◎ How is it Secure?

- ◎ (zero-knowledge)
Succinct Non-Interactive
Argument of Knowledge
(zk-SNARK)



Our Goal

- ◎ Proof must be less computationally expensive than outsourced program
- ◎ Proposed Optimization:
 - Model Pruning

A decorative network diagram in the top-left corner, consisting of various sized nodes (some solid, some hollow) connected by thin lines, forming a complex web-like structure.

1.

zk-SNARKs

(zero-knowledge) Succinct Non-Interactive Argument
of Knowledge

3 Properties

- ◎ Completeness
- ◎ Soundness
- ◎ Zero-Knowledge

Constructing a zk-SNARK

◎ R1CS

Example: $x^3 + x + 5 == 35$

```
sym 1 = x * x
y = sym 1 * x
sym 2 = y + x
~out = sym_2 + 5
```

Constructing a zk-SNARK

- ◎ R1CS
- ◎ zk-SNARK

Example: $x^3 + x + 5 == 35$

```
sym 1 = x * x
y = sym 1 * x
sym 2 = y + x
~out = sym_2 + 5
```

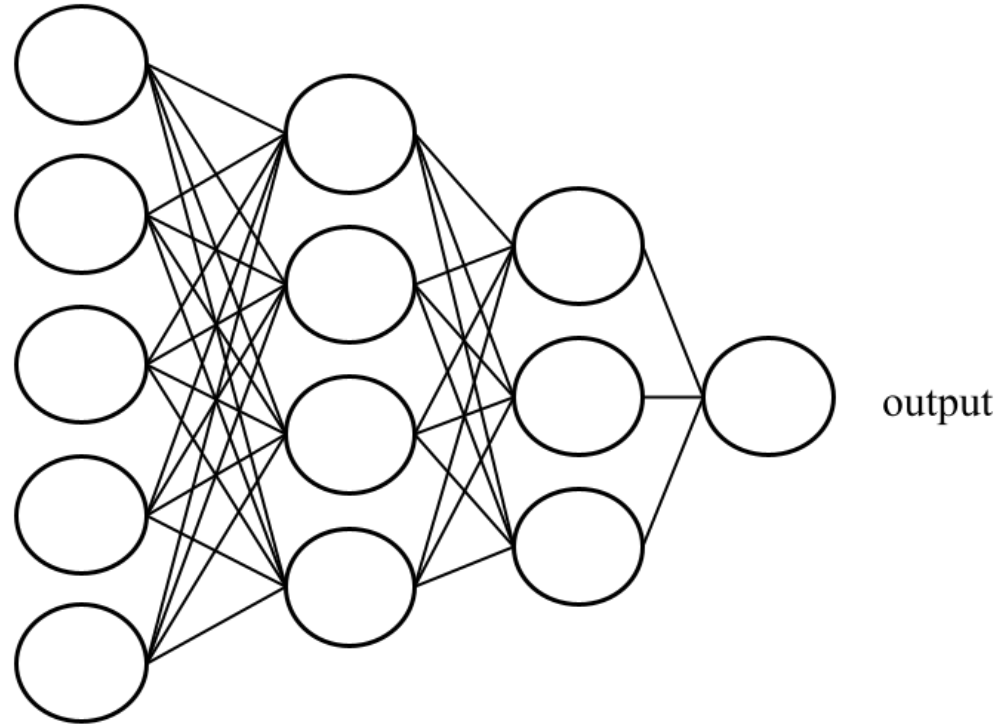



2.

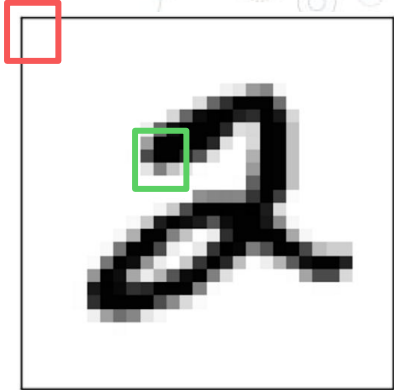
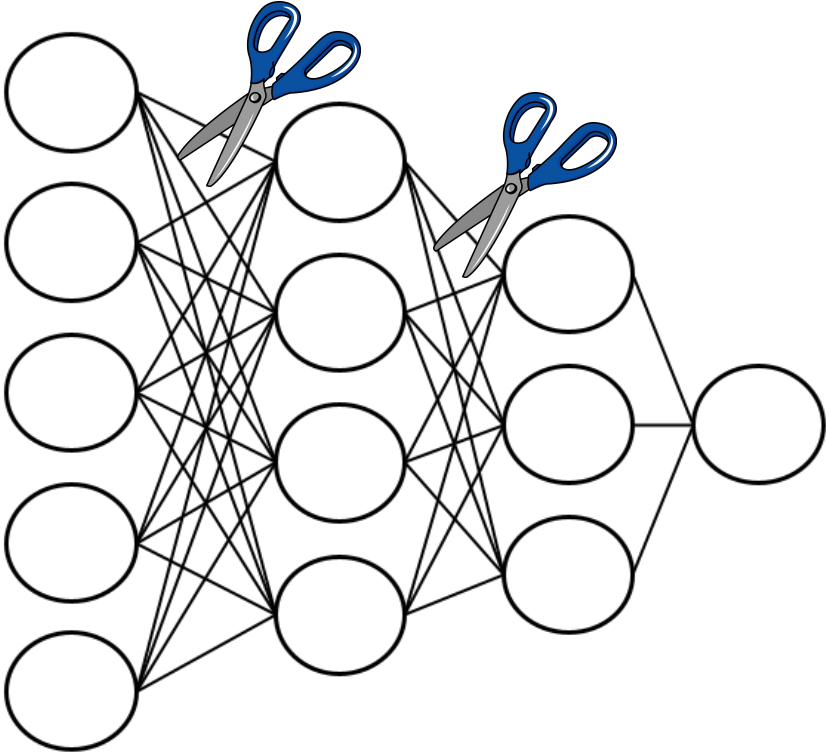
Model Pruning



Network Pruning

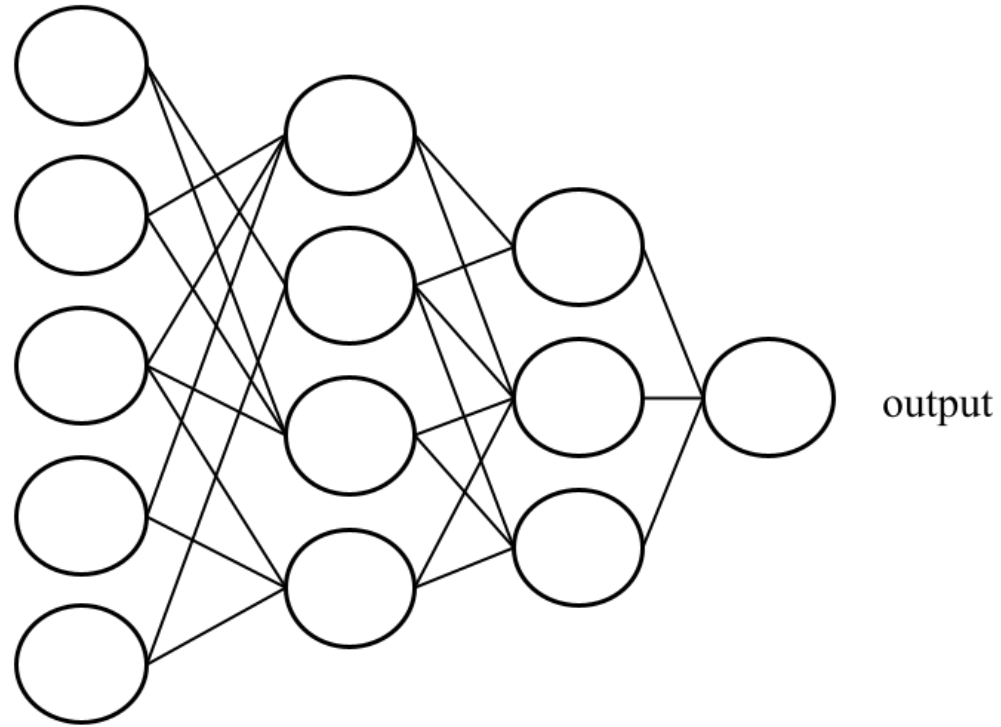


Network Pruning

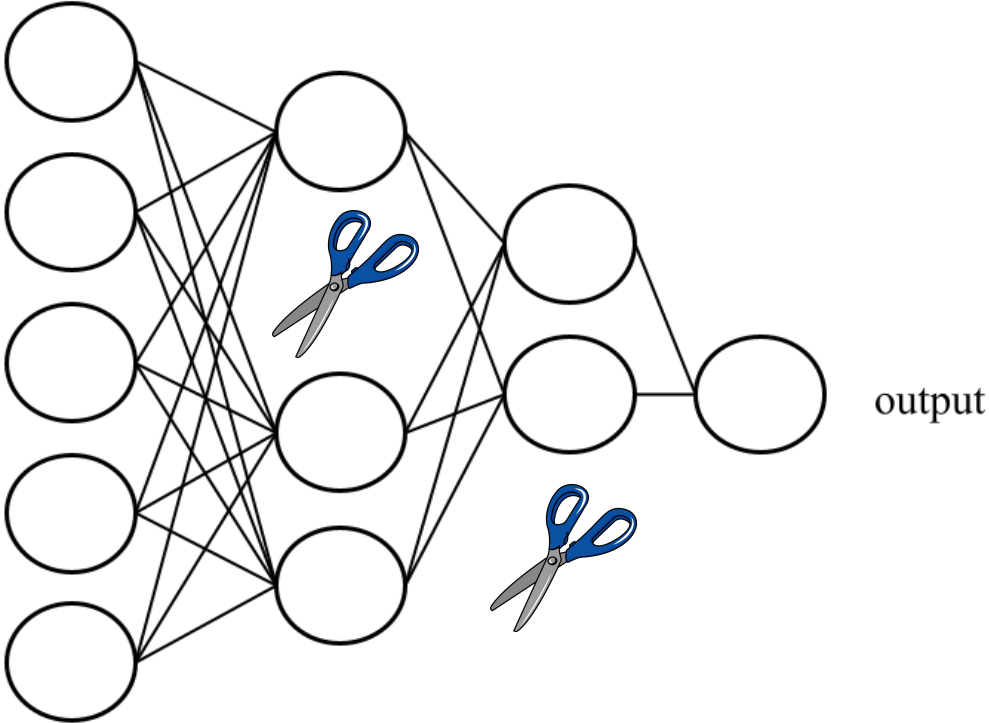


output

Network Pruning



Network Pruning

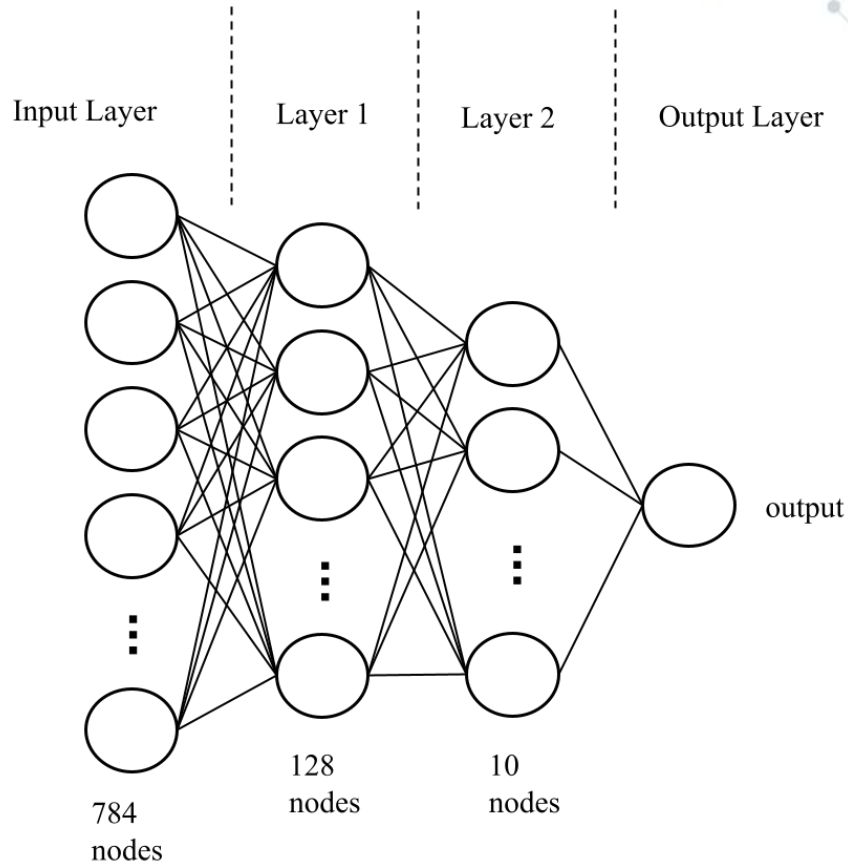


A decorative network diagram in the top-left corner, consisting of various sized nodes (some solid grey, some hollow white) connected by thin grey lines, forming a complex web structure.

3. Methods

Neural Network

- ◎ MNIST-dataset
- ◎ Shallow-Net Architecture



ZEN (Zero-Knowledge Proof for Neural Networks)

- ◎ ZEN reduces R1CS constraints → less complex proof
- ◎ Other Characteristics:
 - ZEN_{infer} and ZEN_{acc}
 - zk-SNARKs only support integers

Experiment

- ① Calculate constraints for neural network without pruning (0, 0.50, 1.0)
- ① Find accuracy of model

A decorative network diagram in the top-left corner, consisting of various sized nodes (some solid grey, some hollow white) connected by thin grey lines, forming a complex web-like structure.

4. Results

Amount Pruned	Accuracy	# of Constraints
0%	0.9516	363736
50%	0.9505	363719
100%	0.0980	363644





5. Conclusion

Applications of this Research

- ◎ Contributions to Cloud Computing
 - outsource more powerful computations
- ◎ Decrease complexity of authentication proofs

Further Research

- ◎ Further decrease number of constraints
- ◎ Experiment with:
 - pruning methods (movement pruning)
 - neural network structures
 - datasets

Acknowledgements

Special Thanks to:

- ◎ My mentor, Yu Xia
- ◎ PRIMES
- ◎ My family