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

Twelfth Annual Spring Term PRIMES Conference, May 21-22, 2022

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
1. zk-SNARKs

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

◎ Completeness: prover can convince the verifier through a proof given a statement and a witness
◎ Soundness: in the case the prover is a malicious party, the verifier cannot be convinced of a false statement
◎ Zero-Knowledge: the prover will not reveal its witness.
Constructing a zk-SNARK

R1CS: rank 1 constraint system

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: rank 1 constraint system
- zk-SNARK

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

```python
sym_1 = x * x
y = sym_1 * x
sym_2 = y + x
~out = sym_2 + 5
```
2. Model Pruning
Network Pruning
Network Pruning
Network Pruning
Network Pruning
3. Methods
Neural Network

MNIST-dataset
Shallow-Net
Architecture

- Input Layer
- Layer 1: 128 nodes
- Layer 2: 10 nodes
- Output Layer
ZEN (Zero-Knowledge Proof for Neural Networks)

- ZEN reduces R1CS constraints → less complex proof
- Other Characteristics:
  - \( ZEN_{\text{infer}} \) and \( ZEN_{\text{acc}} \)
  - zk-SNARKs only support integers
Experiment

- Calculate constraints for neural network without pruning (0, 0.50, 1.0)
- Find accuracy of model
4. Results
<table>
<thead>
<tr>
<th>Amount Pruned</th>
<th>Accuracy</th>
<th># of Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0.9516</td>
<td>363736</td>
</tr>
<tr>
<td>50%</td>
<td>0.9505</td>
<td>363719</td>
</tr>
<tr>
<td>100%</td>
<td>0.0980</td>
<td>363644</td>
</tr>
</tbody>
</table>
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
- MIT PRIMES
- My family