On Polynomial Approximations for Privacy-Preserving and Verifiable ReLU Networks

Ramy E. Ali Jinhyun So A. Salman Avestimehr

Ming Hsieh Department of Electrical and Computer Engineering

E-mails: reali@usc.edu, jinhyuns@usc.edu, avestimehr@ee.usc.edu

USC University of Southern California

Overview

- Outsourcing neural network inference tasks to an untrusted cloud raises data privacy and integrity concerns.
- To address these challenges, several privacy-preserving and verifiable inference techniques replace activation functions such as the ReLU function with polynomials.
- Such techniques may require the coefficients to be in a finite field.
- Previous works proposed replacing the ReLU activation function with

$$\sigma_{\text{square}}(x) = x^2.$$

- We empirically show that the square function is not the best second-degree polynomial that can replace the ReLU function. We instead propose

$$\sigma_{\text{poly}}(x) = x^2 + x.$$

- Our experiments on the CIFAR-10 dataset show that our proposed activation function significantly outperforms the square activation function.

Closely-Related Works

- CryptoNets [3] proposed a privacy-preserving inference technique based on leveled homomorphic encryption [1], replacing the ReLU with the square function and replacing the max-pooling layers with sum-pooling layers.
- SafetyNets [2] proposed a verifiable inference approach based on the sum-check protocol [7, 8, 4], replacing the ReLU function with the square function and replacing the max-pooling layers with sum-pooling layers. The square function was shown to work well in a few experiments with 3-layer and 4-layer networks on the MNIST and the TIMIT datasets.

Polynomial Approximations of the ReLU

1. Fourier Series Based Approximation

$$p_2(x) = \frac{4}{3\pi}x^2 + \frac{1}{2}x + \frac{1}{3\pi}. \quad (1)$$

2. Least-Squares Approximation

$$p_2(x) = \frac{15}{32}x^2 + \frac{1}{2}x + \frac{3}{32}. \quad (2)$$

3. Minimax Approximation

$$p_2(x) = \frac{1}{2}x^2 + \frac{1}{2}x + \frac{1}{16}. \quad (3)$$

This motivates us to propose the activation function

$$\sigma_{\text{poly}}(x) = x^2 + x. \quad (4)$$

Evaluation

We consider an image classification problem on CIFAR-10.

1. We first consider the network architecture of [6]. This network has 7 convolutional layers, 7 ReLU (or polynomial) activation layers, 2 max-pooling (or sum-pooling) layers, a fully connected layer and a Softmax activation layer.

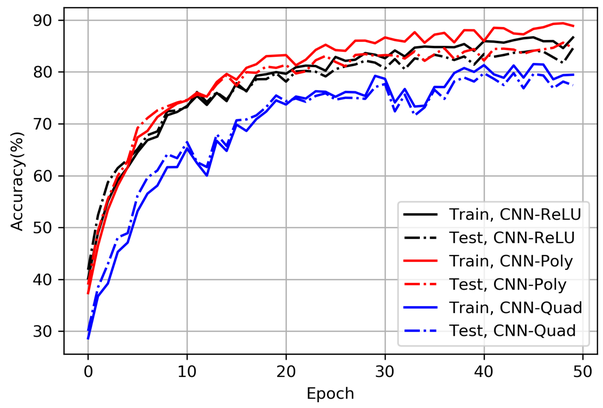

Fig. 1: Accuracy of the CNN architecture in [6].

2. We also consider the "Network In Network (NIN)" architecture of [5].

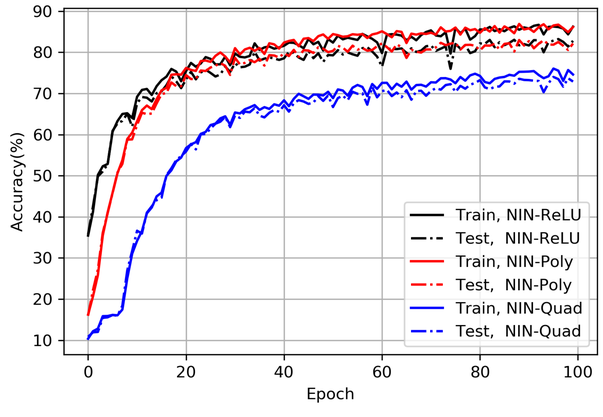

Fig. 2: Accuracy of the Network In Network architecture in [5].

Concluding Remarks

- In this work, we have empirically shown that a second-degree polynomial that has a first order term can significantly outperform the square function.
- Our future work aims to test our activation function on deeper networks and other datasets and to investigate its optimality.

Acknowledgements

This material is based upon work supported by ARO award W911NF1810400, NSF grants CCF-1703575 and CCF-1763673, and ONR Award No. N00014-16-1-2189.

References

[1] Joppe W Bos et al. "Improved security for a ring-based fully homomorphic encryption scheme". In: *IMA International Conference on Cryptography and Coding*. Springer. 2013, pp. 45–64.

[2] Zahra Ghodsi, Tianyu Gu, and Siddharth Garg. "Safetynets: Verifiable execution of deep neural networks on an untrusted cloud". In: *Advances in Neural Information Processing Systems*. 2017, pp. 4672–4681.

[3] Ran Gilad-Bachrach et al. "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy". In: *International Conference on Machine Learning*. 2016, pp. 201–210.

[4] Shafi Goldwasser, Yael Tauman Kalai, and Guy N Rothblum. "Delegating computation: interactive proofs for muggles". In: *Journal of the ACM (JACM)* 62.4 (2015), pp. 1–64.

[5] Min Lin, Qiang Chen, and Shuicheng Yan. "Network in network". In: *ICLR* (2014).

[6] Jian Liu et al. "Oblivious neural network predictions via minionn transformations". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 619–631.

[7] Carsten Lund et al. "Algebraic methods for interactive proof systems". In: *Journal of the ACM (JACM)* 39.4 (1992), pp. 859–868.

[8] Justin Thaler. "Time-optimal interactive proofs for circuit evaluation". In: *Annual Cryptology Conference*. Springer. 2013, pp. 71–89.