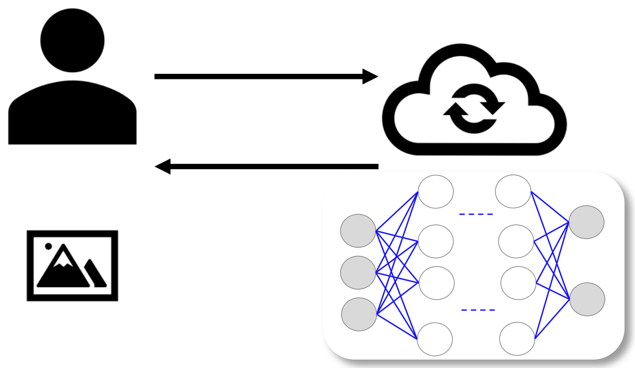
On Polynomial Approximations for Privacy-Preserving and Verifiable ReLU Networks

Ramy E. Ali, Jinhyun So and Salman Avestimehr

USC University of Southern California

Introduction

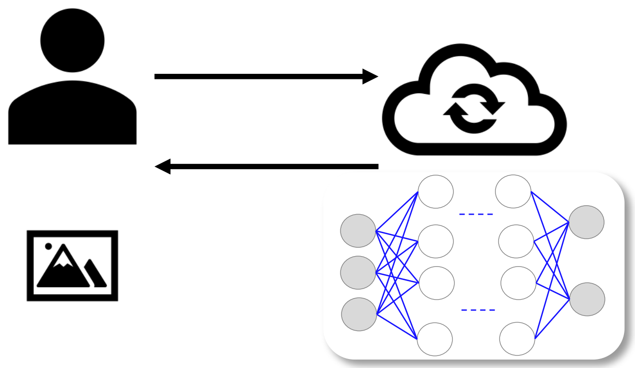
- Outsourcing inference tasks raises several privacy and integrity concerns.
  - The users must verify the correctness of the computations.
  - The users may want to keep their data private.
  - The cloud also may want to keep its model private.



Introduction

- Outsourcing inference tasks raises several privacy and integrity concerns.

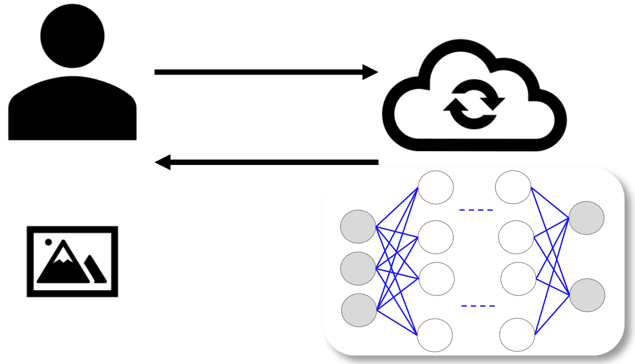
  - The users must verify the correctness of the computations.
  - The users may want to keep their data private.
  - The cloud also may want to keep its model private.



- While there are many efficient privacy-preserving and verifiable techniques for polynomial-based computations [1-4], neural networks involve non-polynomial computations.

Introduction

- Outsourcing inference tasks raises several privacy and integrity concerns.
  - The users must verify the correctness of the computations.
  - The users may want to keep their data private.
  - The cloud also may want to keep its model private.



- While there are many efficient privacy-preserving and verifiable techniques for polynomial-based computations [1-4], neural networks involve non-polynomial computations.

- Hence, several frameworks as CryptoNets [5] and SafetyNets [6] replace the non-polynomial functions with polynomial functions.

Previous Work

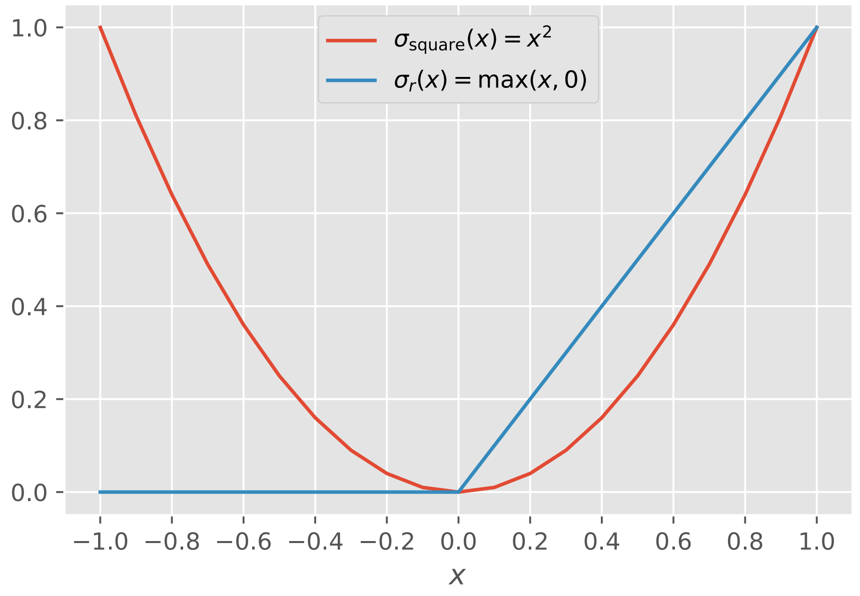
- Much previous works as [5, 6] replace the ReLU function

$$\sigma_{\mathrm{r}}(x) = \max(x, 0)$$

with the square function

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

- Rationale [5]: "the lowest-degree non-linear polynomial function"



Previous Work

- Much previous works as [5, 6] replace the ReLU function
$$\sigma_{\mathrm{r}}(x) = \max(x, 0)$$
with the square function
$$\sigma_{\mathrm{square}}(x) = x^2.$$
- Rationale [5]: "the lowest-degree non-linear polynomial function"

- Max-pooling layers also are replaced with sum-pooling layers.

- This was shown empirically to work well for networks with small number of activation layers (3 or 4 layers).

This Work

- We empirically show that $\sigma_{\mathbf{square}}(x) = x^2$ does not work well for deeper networks.

- We instead propose
$$\sigma_{\mathbf{poly}}(x) = x^2 + x.$$

- $\sigma_{\mathbf{poly}}$ improves the test accuracy by up to $\mathbf{9.4\ \%}$ compared to $\sigma_{\mathbf{square}}$.

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

1. What can be approximated with polynomials with integer coefficients? [9]

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

1. What can be approximated with polynomials with integer coefficients? [9]
   - Only those polynomials themselves over intervals of length 4 or more!

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

1. What can be approximated with polynomials with integer coefficients? [9]
    - Only those polynomials themselves over intervals of length 4 or more!

2. Can we uniformly approximate the ReLU even over $\mathbf{I} = [-1, 1]$?

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

1. What can be approximated with polynomials with integer coefficients? [9]
   - Only those polynomials themselves over intervals of length 4 or more!

2. Can we uniformly approximate the ReLU even over $\mathbf{I} = [-1, 1]$?
   - No

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

1. What can be approximated with polynomials with integer coefficients? [9]
   - Only those polynomials themselves over intervals of length 4 or more!

2. Can we uniformly approximate the ReLU even over $\mathbf{I} = [-1, 1]$?
   - No

3. What can be done?

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

1. What can be approximated with polynomials with integer coefficients? [9]
    - Only those polynomials themselves over intervals of length 4 or more!

2. Can we uniformly approximate the ReLU even over $\mathrm{I} = [-1, 1]$?
    - No

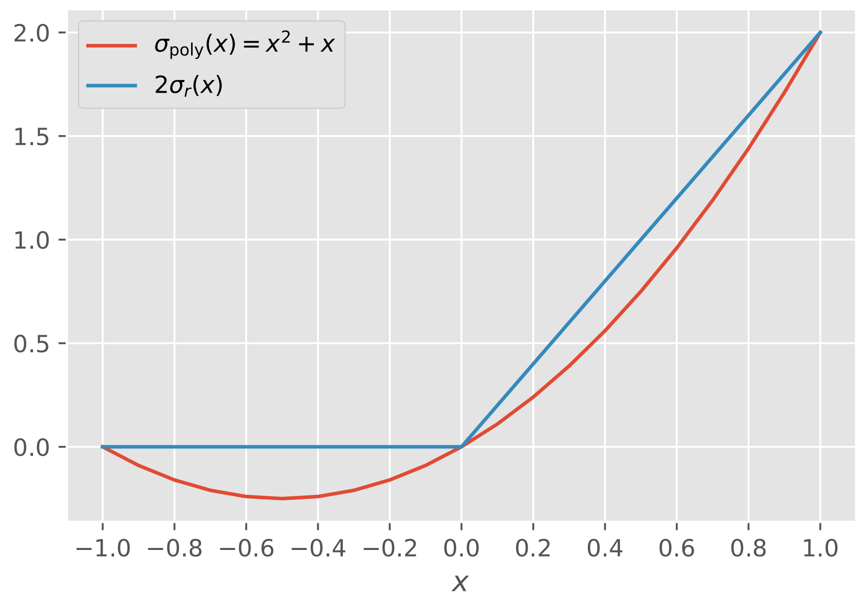
3. What can be done?
    - Uniform approximation of $\sigma_{\mathrm{sr}}(x; \mathrm{c}) = c \max(x, 0)$ with polynomial with integer coefficients over $\mathrm{I} = [-1, 1]$, where c is even.

Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

3. What can be done?
   - Uniform approximation of $\boldsymbol{\sigma_{\mathrm{sr}}(x;\mathrm{c}) = c\max(x,0)}$ with polynomial with integer coefficients over $\mathbf{I} = [-1,1]$, where $\boldsymbol{c}$ is even (e.g., $\boldsymbol{c} = 2$).
   - The "best" degree-$\mathbf{2}$ polynomial is given by

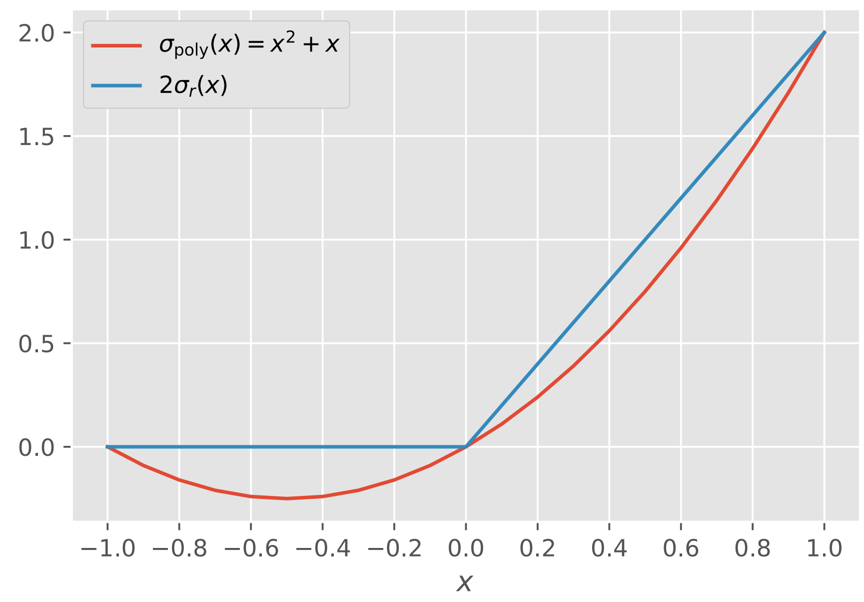
$$\sigma_{\mathrm{poly}}(x) = x^2 + x.$$



Theoretical Insights

Goal: Uniform approximation of ReLU with a polynomial with integer coefficients.

3. What can be done?
   - Uniform approximation of $\sigma_{\mathrm{sr}}(x;\mathrm{c}) = c\max(x,0)$ with polynomial with integer coefficients over $\mathrm{I} = [-1,1]$, where c is even (e.g., $c = 2$).
   - The "best" degree-2 polynomial is given by
   $$\sigma_{\mathrm{poly}}(x) = x^2 + x.$$



4. What about large intervals $I = [-a,a]$?
   - Use Minimax approximation and round the coefficients.
   - This polynomial is given by
   $$\sigma_{\mathrm{poly}}(x) = x^2 + \mathrm{a}x.$$

Evaluation

1. We consider the convolutional network of [7].

The network has

- 7 convolutional layers
- 7 ReLU activation layers
- 2 max-pooling layers
- a fully connected layer and
- a Softmax activation layer.

Test Accuracy

Activation	CIFAR-10	CIFAR-100
CNN-ReLU	84.6%	54.7%
CNN-Poly	83.0%	55.3%
CNN-Quad	77.4%	51.3%

Evaluation

2. We consider the "Network In Network" architecture of [8].

The network has

- 9 convolutional layers
- 9 ReLU activation layers
- 2 max-pooling layers, Global pooling layer and
- a Softmax activation layer.

Test Accuracy

Activation	CIFAR-10	CIFAR-100
NIN-ReLU	88.5%	64.2%
NIN-Poly	88.7%	55.4%
NIN-Quad	81.0%	46.0%

Discussion

- We have that empirically shown that $\sigma_{\mathbf{poly}}(x) = x^2 + x$ significantly outperforms $\sigma_{\mathbf{square}}(x) = x^2$.
- Our future work aims to test our activation function on deeper networks and other datasets and to investigate its optimality.

Questions?

Thank you

References

[1] Ronald L Rivest, Len Adleman, Michael L Dertouzos, et al. **On data banks and privacy homomorphisms**. Foundations of secure computation, 4(11):169–180, 1978.

[2] Craig Gentry. **Fully homomorphic encryption using ideal lattices**. In Proceedings of the fortyfirst annual ACM symposium on Theory of computing, pages 169–178, 2009.

[3] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. **Algebraic methods for interactive proof systems**. Journal of the ACM (JACM), 39(4):859–868, 1992.

[4] Joppe W Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. **Improved security for a ring-based fully homomorphic encryption scheme**. In IMA International Conference on Cryptography and Coding, pages 45–64. Springer, 2013.

[5] Ran Gilad-Bachrach, Nathan Dowlin, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. **Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy**. In International Conference on Machine Learning, pages 201–210, 2016.

[6] 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, pages 4672–4681, 2017.

[7] Jian Liu, Mika Juuti, Yao Lu, and Nadarajah Asokan. **Oblivious neural network predictions via minionn transformations**. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pages 619–631, 2017.

[8] Min Lin, Qiang Chen, and Shuicheng Yan. **Network in network**. ICLR, 2014.

[9] Le Baron O Ferguson. **What can be approximated by polynomials with integer coefficients**. The American Mathematical Monthly, 113(5):403–414, 2006.