Privacy-Preserving Inference on Neural Networks with FHE/PHE Schemes

Skanda Koppula

6.875 Final Project, Spring 2017

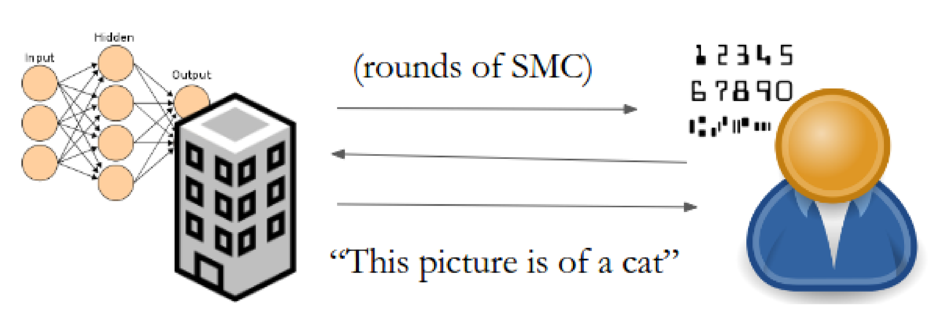
Problem Overview

In the past decade, neural networks have achieved state-of-art results on many inference benchmarks. In practice, many reasons to perform inference on encrypted data using neural networks:

- Hospital sending private patient data to cloud engine to predict a diagnosis
- Prediction over patentable drug candidates, voice biometric classification, etc.

We provide an overview of existing literature on neural network inference over encrypted data using SHE schemes [1, 2, 3]. We implement one such scheme using Simple Encrypted Arithmetic Library, and propose 2PC-based extensions on existing schemes.

The Multi-Party Game



Preliminaries

Neural Networks
State-of-art networks use a few key operations:

- Matrix-multiplication ($Ax + b$) for FCN layers
- Non-linear activations between linear layers:
  - Sigmoid: $\frac{1}{1+e^{-x}}$
  - Max-Pool/Max-Out: $\max(x_1, \ldots, x_n)$
  - ReLU: $\max(0, x)$
  - Softmax: $\frac{e^{z_j}}{\Sigma_{i=1}^{N} e^{z_i}}$

Parameters fixed after training. State-of-art speech networks have known multiplicative depth of 5-8.

R-LWE Assumption

$\nexists$ PPT A that can non-negligibly distinguish independent samples of $(a_i, a_i s + e_i)$ from (a_i, b_i), drawn uniform from $R_q \times R_q$. Generalizes to vectors/polynomials with components a_i.

Preliminaries Cont'd

YASHE
Fan-Ver **Pallier** Damgard-Jurik is a generalization that allows for arbitrary-long plaintexts ($\mod n^s$) used in practice.
The following materials were required to complete the research:

- Curabitur pellentesque dignissim
- Eu facilisis est tempus quis
- Duis porta consequat lorem
- Eu facilisis est tempus quis

The materials were prepared according to the steps outlined below:

1. Curabitur pellentesque dignissim
2. Eu facilisis est tempus quis
3. Duis porta consequat lorem
4. Curabitur pellentesque dignissim

Methods

Lorem ipsum dolor **sit amet**, consectetur adipiscing elit. Sed laoreet accumsan mattis. Integer sapien tellus, auctor ac blandit eget, sollicitudin vitae lorem. Praesent dictum tempor pulvinar. Suspendisse potenti. Sed tincidunt varius ipsum, et porta nulla suscipit et. Etiam congue bibendum felis, ac dictum augue cursus a. **Donec** magna eros, iaculis sit amet placerat quis, laoreet id est. In ut orci purus, interdum ornare nibh. Pellentesque pulvinar, nibh ac malesuada accumsan, urna nunc convallis tortor, ac vehicula nulla tellus eget nulla. Nullam lectus tortor, *consequat tempor hendrerit* quis, vestibulum in diam. Maecenas sed diam augue.

Important Result

Lorem ipsum dolor **sit amet**, consectetur adipiscing elit. Sed commodo molestie porta. Sed ultrices scelerisque sapien ac commodo. Donec ut volutpat elit.

Mathematical Section

Nam quis odio enim, in molestie libero. Vivamus cursus mi at nulla elementum sollicitudin. Nam quis odio enim, in molestie libero. Vivamus cursus mi at nulla elementum sollicitudin.

$$E = mc^2 \tag{1}$$

Nam quis odio enim, in molestie libero. Vivamus cursus mi at nulla elementum sollicitudin. Nam quis odio enim, in molestie libero. Vivamus cursus mi at nulla elementum sollicitudin.

$$\cos^3\theta = \frac{1}{4}\cos\theta + \frac{3}{4}\cos 3\theta \tag{2}$$

Nam quis odio enim, in molestie libero. Vivamus cursus mi at nulla elementum sollicitudin. Nam quis odio enim, in molestie libero. Vivamus cursus mi at nulla elementum sollicitudin.

Results

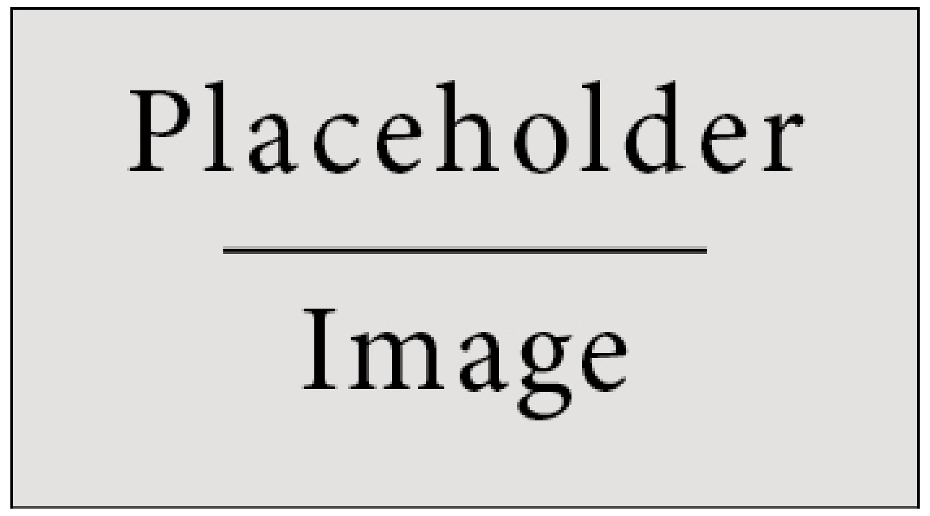


Figure 1: Figure caption

Nunc tempus venenatis facilisis. Curabitur suscipit consequat eros non porttitor. Sed a massa dolor, id ornare enim:

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910

Conclusion

Nunc tempus venenatis facilisis. **Curabitur suscipit** consequat eros non porttitor. Sed a massa dolor, id ornare enim. Fusce quis massa dictum tortor **tincidunt mattis**. Donec quam est, lobortis quis pretium at, laoreet scelerisque lacus. Nam quis odio enim, in molestie libero. Vivamus cursus mi at *nulla elementum sollicitudin*.

Additional Information

Maecenas ultricies feugiat velit non mattis. Fusce tempus arcu id ligula varius dictum.

- Curabitur pellentesque dignissim
- Eu facilisis est tempus quis
- Duis porta consequat lorem

References

[1] 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. 2016.

[2] Pengtao Xie, Misha Bilenko, Tom Finley, Ran Gilad-Bachrach, Kristin Lauter, and Michael Naehrig. Crypto-nets: Neural networks over encrypted data. 2014.

[3] Claudio Orlandi, Alessandro Piva, and Mauro Barni. Oblivious neural network computing via homomorphic encryption. *EURASIP Journal on Information Security*, 2007.

[4] Tancrede Lepoint and Michael Naehrig. A comparison of the homomorphic encryption schemes fv and yashe. Springer, 2014.

[5] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In *USENIX Security Symposium*, 2011.